НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Є.О. ЖИВИЛО, Г.В. ГОЛОВКО, В.С. КУЗЬ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

НАВЧАЛЬНИЙ ПОСІБНИК

Частина 2

ПОЛТАВА – 2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
“ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМ. ЮРІЯ КОНДРАТЮКА”

КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Є.О. ЖИВИЛО, Г.В. ГОЛОВКО, В.С. КУЗЬ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

За редакцією Є.О. ЖИВИЛО

НАВЧАЛЬНИЙ ПОСІБНИК

Частина 2

2023

УДК 004.492.2

ББК 32.971.35-5

Рецензенти:
О.В. Шефер, доктор технічних наук, професор, завідувач кафедри автоматики, електроніки та телекомунікацій Навчально-наукового інституту інформаційних технологій та робототехніки Національного університету “Полтавська політехніка імені Юрія Кондратюка”;
В.В. Васюта, кандидат технічних наук, доцент, доцент кафедри комп’ютерних та інформаційних технологій і систем Навчально-наукового інституту інформаційних технологій та робототехніки Національного університету “Полтавська політехніка ім. Юрія Кондратюка”.

Авторський колектив: доцент кафедри комп’ютерних та інформаційних технологій, кандидат наук з державного управління Є.О. Живило (розділ 1, 4, додаток 1, 2); доцент кафедри комп’ютерних та інформаційних технологій, кандидат технічних наук Г.В. Головко (розділ 3); асистент кафедри комп’ютерних та інформаційних технологій В.С. Кузь (розділ 2).

Системи технічного захисту інформації: навч. посіб. / [Є.О. Живило; Г.В. Головко; В.С. Кузь]; за ред. Є.О. Живило. – П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2023. – 143с.

Навчальний посібник охоплює програмний матеріал підготовки студентів 12 Галузі знань «Інформаційні технології» за спеціальностями 125 - Кібербезпека та захист інформації. Навчальне видання укладено за матеріалами лекцій, групових та практичних занять з дисципліни “Комплексні системи захисту інформації”, а також з дисциплін “Захист програмного забезпечення” та “Захист інформації”, “Ризики інформаційної безпеки”. Посібник призначений для студентів, що навчаються за спеціальностями студентів 12 Галузі знань «Інформаційні технології», а також для самостійного вивчення методів і засобів технічного захисту інформації студентами інших спеціальностей.

У посібнику висвітлено сутність технічного захисту інформації, технічні канали витоку інформації, основні методи і засоби технічного захисту інформації від витоку по технічних каналах. Зазначений навчальний посібник розкриває системний підхід до застосування сучасних методів та засобів інженерно-технічного захисту від витоку інформації з обмеженим доступом.

У першому розділі розглянуті методи та засоби захисту інформації, що обробляються в технічних засобах пересилання, оброблення, зберігання, відображення інформації, а також викладені загальні характеристика каналів витоку інформації, систематизовано основні нормативно-правові документи у галузі технічного захисту інформації.

У другому розділі розглянуто методи та засоби захисту мовної інформації, особливості технічних каналів витоку та захисту мовної інформації, порядок виконання робіт по звукоізоляції приміщень, алгоритм здійснення віброакустичного маскування, а також розкрито: методи й засоби захисту телефонних апаратів та телефонних ліній; системи закриття мовних сигналів.

У третьому розділі розкрито сутність захисту автоматизованих систем і оброблюваної інформації від несанкціонованих дій та несанкціонованого доступу, порядок захисту інформації в автоматизованих системах і засобах обчислювальної техніки від витоку каналами побічного електромагнітного випромінювання і наведення, а також висвітлена методика проведення спеціальних досліджень технічних засобів електронно-обчислювальною технікою.

У четвертому розділі сформовано контроль ефективності інженерно-технічного захисту, означено порядок здійснення державного контролю за станом технічного захисту інформації та інструментального контролю захищеності інформації, яка циркулює на об’єктах “особливої норми”. Визначено класифікацію порушень з технічного захисту інформації.

В основу навчального посібника покладено тенденції розвитку об’єднаних комунікаційних мереж, загальні світові тенденції розвитку інформаційно-комунікаційних систем і технологій, нормативно-правова база держави та нормативні документи системи технічного захисту інформації, наукові розробки авторів та дослідження у вітчизняних і міжнародних виданнях.

Рекомендовано до друку науково-методичною радою Національного університету “Полтавська політехніка імені Юрія Кондратюка”
Протокол № 2 від 28 грудня 2023 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АЕ	–	акустичний екран
АКол	–	акустичні коливання
Амаск	–	акустичне маскування
АП	–	акустичне поле
АС	–	автоматизована система
Асиг	–	акустичний сигнал
Ахв	–	акустична хвиля
ВІ	–	виток інформації
ВЧ	–	висока частота
ДССЗІ	–	Державна служба спеціального зв'язку та захисту інформації
ДТЗС	–	допоміжні технічні засоби і системи
ЕМВ	–	електромагнітні випромінювання
ЕМС	–	електро-магнітна сумісність
ЕМП	–	електромагнітне поле
ЕОТ	–	електронно-обчислювальна техніка
ЕЦП		електронний цифровий підпис
ЕПТ	–	електронно-променева трубка
ЗІ	–	захист інформації
ЗВА	–	зосереджена випадкова антена
ЗОТ	–	засоби обчислювальної техніки
ЗП	–	закладний пристрій
ЗЧР	–	загальний час реагування
ІБ	–	інформаційна безпека
ІзОД	–	інформація з обмеженим доступом
ІТЗ	–	інженерно-технічний захист
ІТС	–	інформаційно-телекомунікаційна система
КЗ	–	канал зв'язку
КонтрЗ		контрольована зона
КСЗІ	–	комплексна система захисту інформації
МІ	–	мовна інформація
НІ	–	носії інформації
НПА		нормативно-правові акти
НСД	–	несанкціонований доступ
НСиг	–	небезпечний сигнал
НЧ	–	низька частота
ОІД	–	об'єкт інформаційної діяльності
ОТЗ	–	основні технічні засоби
ПВП	–	псевдовипадкова послідовність
ПЕМВ	–	побічне електромагнітне випромінювання і наведення
ПЕОМ	–	персональна електронно-обчислювальна машина
СЗ	–	система заземлення
ТЗІ	–	технічний захист інформації
ТЗПІ	–	технічні засоби пересилання, оброблення, зберігання, відображення інформації
ТЗР	–	технічні засоби розвідки
ТКВІ	–	технічні канали витоку інформації
ТЛ	–	телефонна лінія

ВСТУП

Однією з обов'язкових умов інформаційного суверенітету держави є проведення заходів, спрямованих на ЗІ. Актуальність цього завдання обумовлена постійно зростаючим впливом інформаційної компоненти як на подальший науково-технічний так і на безпечний соціально-економічний розвиток суспільства. Інформація стає одним з головних чинників прогресу людської цивілізації і одночасно – суттєвим фактором загрози цьому розвитку, бо зростає небезпека можливого використання інформації з відверто злочинними намірами. Останнє загострює проблему НСД до інформації. Виникає парадокс: глобальна інформатизація суспільства забезпечує його новими прогресивними інформаційними технологіями, засобами автоматизації, телекомунікації, зручною оргтехнікою, і водночас приводить до створення технічних засобів інформаційного впливу на системи управління, до розробки найрізноманітніших засобів і методів ТР та інформаційного шпигунства. Метою НСД до інформації є здебільшого політичний, промисловий та військовий інтерес.

Наслідком неправомірних дій з інформацією є порушення її конфіденційності, спостережливості, цілісності та доступності, що, у свою чергу, призводить до порушення як режиму управління, так і його якості в умовах спотвореної або неповної інформації, виток ІзОД. Ці негативні фактори впливу можна класифікувати, залежно від його джерел, на три групи:

Антропогенні фактори (безпосередньо створюється людиною), які складають:

– ненавмисні або навмисні діяння обслуговуючого і управлінського персоналу, програмістів, користувачів, служби безпеки інформаційної системи;

– дії несанкціонованих користувачів (діяльність іноземних розвідувальних і спеціальних служб, а також протиправна діяльність інших окремих осіб).

Техногенні фактори (випадковий вплив технічних об'єктів):

– внутрішні (неякісні технічні і програмні засоби обробки інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що застосовуються в установі);

– глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо), які призводять до зникнення або коливання електропостачання та інших засобів забезпечення і функціонування, відмов та збоїв апаратно-програмних засобів;

– ЕМВ і наведення, віброакустичні канали витоку.

Природні фактори (вплив негативних природних чинників) – стихійні лиха, магнітні бурі, радіоактивний вплив.

РОЗДІЛ 1. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ОБРОБЛЯЮТЬСЯ В ТЕХНІЧНИХ ЗАСОБАХ ПЕРЕСИЛАННЯ, ОБРОБЛЕННЯ, ЗБЕРІГАННЯ, ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ

Важливим аспектом ІБ є ЗІ, яка передається, зберігається, обробляється та відображається за допомогою ТЗПІ (див. розд. 2, ч. 1). Джерелами НСиг ТЗПІ є, в першу чергу, радіо й електротехнічні елементи будь-яких радіоелектронних і електричних пристроїв та приладів цих засобів, а загрозу розкрадання інформації шляхом її витоку створюють сигнали, що випадково виникають у результаті побічних випромінювань і наведень.

ЗІ в ТЗПІ здійснюється з використанням активних і пасивних методів та засобів, сутність яких була розглянута в розд. 1, ч. 1. Тому в цьому розділі основну увагу буде приділено питанням практичної реалізації ЗІ в ТЗПІ.

Слід відмітити, що організація ЗІ ІзОД у ТЗПІ здійснюється відповідно до вимог і рекомендацій НД [18], а також [7].

Метою ТЗІ в ТЗПІ є запобігання витоку або порушенню цілісності ІзОД.

Мета ТЗІ може бути досягнута побудовою системи ЗІ, що є організованою сукупністю методів і засобів забезпечення ТЗІ. ТЗІ здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи ЗІ;

3 етап – реалізація плану ЗІ;

4 етап – контроль функціювання та керування системою ЗІ.

1.1. Характеристика каналів витоку інформації при експлуатації технічних засобиів пересилання, оброблення, зберігання, відображення інформації

В залежності від фізичної природи виникнення інформаційних сигналів в ТЗПІ, а також середовища їх розповсюдження і способів перехоплення засобами ТР ТКВІ поділяються на електромагнітні, електричні і параметричні.

До електромагнітних каналів ВІ відносяться:

– перехоплення ПЕМВ елементів ТЗПІ;

– перехоплення ПЕМВ на частотах роботи ВЧ генераторів в ТЗПІ і ДТЗС;

– перехоплення ПЕМВ на частотах самозбудження підсилюва-чів НЧ ТЗПІ.

Перехоплення ПЕМВ ТЗПІ здійснюється засобами радіо-технічної розвідки, що розміщені за межами КонтрЗ.

Електричні канали ВІ включають:

– знімання наведень ПЕМВ ТЗПІ зі з’єднувальних ліній ДТЗС і сторонніх провідників;

– знімання інформаційних сигналів з ліній електроживлення ТЗПІ;

– знімання інформаційних сигналів з ланцюгів заземлення ТЗПІ і ДТЗС;

– зніманння інформації шляхом встановлення в ТЗПІ електронних пристроїв перехоплення інформації.

Перехоплення інформаційних сигналів по електричних каналах витоку можливе шляхом безпосереднього підключення до з’єднувальних ліній ДТЗС і сторонніх провідників, що проходять крізь приміщення де встановлені ТЗПІ, а також до систем електроживлення і заземлення ТЗПІ. Для цих цілей застосовуються спеціальні засоби радіотехнічної розвідки, а також спеціальна вимірювальна апаратура.

Параметричний канал ВІ утворюється шляхом ВЧ опромінення ТЗПІ. Для перехоплення інформації по даному каналу необхідні спеціальні ВЧ генератори з антенами, що мають вузькі діаграми направленості, та спеціальні радіоприймальні пристрої. Як слідує з наведеного, найбільш розповсюдженим і небез-печним в ТЗПІ є канал ПЕМВН.

1.2. Захист інформації в технічних засобах пересилання, оброблення, зберігання, відображення інформації від витоку каналами побічного електромагнітного випромінювання і наведення

1.2.1. Аналіз можливого витоку інформації каналами побічного електромагнітного випромінювання і наведення

Під час пересилання ІзОД в елементах схем, конструкцій, підвідних і з’єднувальних проводах технічних засобів протікають струми інформативних (НСиг) сигналів. ЕМП, що виникають при цьому, можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів ВІ.

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.

Специфічний канал ВІ в ТЗПІ створює ПВЧГ – ВЧ паразитні коливання, промодульовані інформативним (НСиг) сигналом за амплітудою, частотою і фазою (активна ПВЧГ) або за амплітудою і частотою (пасивна ПВЧГ). 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 перемикань через виник-нення перехідних процесів.

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

– у результаті проходження інформативного (НСиг) сигналу через технічні засоби на вхідному 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 (НСиг) сигналом, який проходить через підсилювач. Джерелами утворення інформативних (НСиг) 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 виходять за межі контрольованої території, плінти кабельні, що служать для комутації вихідних ліній у кросах, монтажні колодки, роз'єми блоків, контакти перемикачів та реле, які використовуються для комутації вихідних ліній, блоки, що зазнають впливу ЕМП.

Витік інформації колом заземлення може статися з таких причин:

– за наявності контурів у СЗ, 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.

Під час надходження ВЧ сигналів у нелінійні (або параметричні) кола, що несуть ІзОД, відбувається модуляція ВЧ сигналу. Таким чином, ВЧ коливання стають носіями інформативних (НСиг) сигналів і створюють канал ВІ.

Під час виникнення несправностей в апаратурі або несанкціонованих діях обслуговуючого персоналу у схемах керування може виникнути небажана комутація інформативного (НСиг) сигналу, яка призводить до виходу ІзОД у незахищений КЗ.

Таким чином, можливі канали ВІ при експлуатації ТЗПІ утворюються:

– НЧ ЕМП, які виникають під час роботи ТЗПІ та ДТЗС;

– під час впливу на ТЗПІ та ДТЗС електричних, магнітних та АП;

– під час виникнення паразитної ВЧ генерації;

– під час проходження інформативних (НСиг) сигналів у колі електроживлення;

– під час взаємного впливу кіл;

– під час проходження інформативних (НСиг) сигналів у колі заземлення;

– під час паразитної модуляції ВЧ сигналу;

– внаслідок хибних комутацій і несанкціонованих дій.

1.2.2. Рекомендації із технічного захисту інформації при експлуатації технічних засобів перетворення інформації

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

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

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 невиконувані, слід вжити додаткових заходів захисту:

– установити ВЧ ОТЗ в екрановане приміщення (камеру);

– установити в незахищені КЗ, 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 витоку колами заземлення та електроживлення.

1. Рекомендації щодо вибору засобів ТЗІ, ТЗПІ і ДТЗС

1.1. До засобів технічного захисту відносяться:

– фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв’язку, системи директорського та диспетчерського зв’язку;

– пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;

– фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;

– фільтри захисту лінійні (ВЧ) для встановлення в лініях апаратів телеграфного (телекодового) зв’язку;

– генератори лінійного зашумлення;

– генератори просторового зашумлення;

– екрановані камери спеціальної розробки.

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

1.3. 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 АП.

При цьому слід враховувати, що обраний спосіб захисту не повинен порушувати працездатність технічного засобу і погіршувати його технічні параметри.

1.4. ВЧ 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".

1.5. Підключення пристроїв захисту слід проводити без порушення або зміни електричної схеми і ТЗПІ, і ДТЗС.

2. Рекомендації щодо захисту ІзОД від витоку кабелями та проводами.

Захист ІзОД від витоку кабелями та проводами рекомендується здійснювати шляхом:

– застосування екранувальних конструкцій;

– роздільного прокладання кабелів ОТЗ, ТЗПІ та ДТЗС.

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

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

3. Рекомендації щодо електроживлення основних технічних засобів

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 НЧ. 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. Рекомендації щодо заземлення ОТЗ.

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.

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

Утворення петель і контурів у СЗ не допускається.

5. Рекомендації щодо екранування ОТЗ.

Екрани кабельних ліній ТЗПІ, 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 виконуватись умова безпе-рервності екрана від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватись 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, звукопід-силювальних) рекомендується ділити екран на ділянки для одержання малих опорів для ВЧ струмів і кожну ділянку заземляти тільки з одного боку.

Вихідні дані для здійснення ТЗІ наведені у [18].

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

1.3. Екранування технічних засобів

Функціонування будь-якого технічного засобу інформації пов’язане із протіканням по його струмоведучих елементах електричних струмів різних частот та утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні й електричні поля, що називаються побічними ЕМВ.

Вузли й елементи електронної апаратури, у яких мають місце великі напруги й протікають малі струми, створюють у ближній зоні ЕМП з перевагою *електричної* складової.

Вузли й елементи електронної апаратури, у яких протікають великі струми й мають місце малі перепади напруги, створюють у ближній зоні ЕМП з перевагою *магнітної* складової.

Змінні електричне й магнітне поля створюються також у просторі, що оточує з'єднувальні лінії (проводи, кабелі) ОТЗ.

Названі ПЕМВ ОТЗ є причиною виникнення електромагнітних і параметричних каналів ВІ, а також можуть виявитися причиною виникнення наведення інформаційних сигналів у сторонніх струмоведучих лініях і конструкціях.

Для повного усунення наведень (ПЕМВ) від ТЗПІ в приміщеннях, лінії яких виходять за межі КонтрЗ, необхідно не тільки придушити їх у проводах, що відходять від джерела, але й обмежити сферу дії ЕМП, створеного джерелом НСиг.

Ефективним методом зниження рівня ПЕМВН є екранування їхніх джерел.

Розрізняють наступні способи екранування:

– електростатичне (екранування електричного поля);

– магнітостатичне (екранування магнітного поля);

– електромагнітне (екранування ЕМП).

Електростатичне й магнітостатичне екранування засновані на замиканні екраном, що володіє в першому випадку високою електропровідністю, а в іншому – високою магнітопровідністю, відповідно електричного й магнітного полів. На ВЧ застосовується виключно *електромагнітне екранування.*

Ефективність екранування можна оцінити таким параметром, як коефіцієнт екранування $К_е$. Це відношення інтенсивності ЕМП, що виміряна до встановлення екрана, до того же параметра поля після його встановлення та визначене в децибелах.

1.3.1. Електростатичне і магнітостатичне екранування

Електростатичне екранування зводиться до замикання електростатичного поля на поверхню металевого екрана та відводу електричних зарядів на землю (на корпус приладу). Заземлення електростатичного екрана є необхідним елементом при реалізації електростатичного екранування.

Якщо джерело НСиг електростатичної природи оточено металевим екраном, то в наслідок індукції на внутрішній та зовнішній поверхнях екрану здійснеться розподіл електричних зарядів. При цьому в стаціонарному режимі в де-який момент часу зовнішня поверхня екрану буде носієм заряда того ж знаку, що і джерело НСиг.

В випадку, коли екран не заземлений, приймальний пристрій ТЗР буде підданий такому самому впливу, як і при відсутності екрану.

При наявності заземлення заряд, що наводиться на зовнішній поверхні

екрану, відводиться на землю, де його нейтралізує заряд іншого полюсу джерела НСиг.При цьому особливлі вимоги до товщини та проводимості матеріалу металевого екрана не пред'являються.

Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля.

При використанні діелектричного екрана можна послабити поле джерела наведення в ε раз(де ε – відносна діелектрична проникність матеріалу екрана) без заземлення екрана.

Основним завданням екранування електричних полів є зниження ємності зв'язку між елементами конструкції, що екрануються. Отже, ефективність екранування визначається в основному відношенням ємностей зв'язку між джерелом і приймальним пристроїм ТЗР до й після установки заземленого екрана. Тому будь-які дії, що приводять до зниження ємності зв'язку, збільшують ефективність екранування.

Дія металевого листа, що екранує, істотно залежить від якості з'єднання екрана з корпусом приладу й частин екрана один з одним.

Вузькі щілини й отвори в металевому екрані, розміри яких малі в порівнянні з довжиною хвилі, практично не погіршують екранування електричного поля.

Зі збільшенням частоти ефективність електростичного екранування знижується.

Основні вимоги, які пред'являються до електростатичних екранів, можна сформулювати таким чином:

– конструкція екрана повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрана, не виходячи за його межі;

– в області НЧ (при глибині проникнення δ більше товщини d, тобто при $\delta > d$) ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрана з корпусом пристрою або з заземлюючим пристроєм і мало залежить від матеріалу металевого екрана та його товщини;

– в області ВЧ (при $\delta < d$) ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідністю й магнітною проникністю.

Магнітостатичне екранування використовується при необхідності придушити наведення на НЧ від 0 до 10 кГц, тобто в тому числі на частотах мовного сигнала.

При екрануванні магнитних полей застосовуються два основних метода магнитостатичного екранування:

- шунтування магнитного поля НСиг феромагнитними матеріалами;
- витісняння магнитного поля НСиг полем вихрових струмів в екрані.

В ОТЗ найбільш складно забезпечити високу ефективність екранування магнітостатичних і НЧ магнітних полей.

Якщо екран виготовлений з феромагнитного матеріалу, з великим

значенням магнітної проникненості μ, то магнітний потік шунтується (замикається), в основному, на стінки екрана, який має значно менший магнітний опір порівняно з магнітним опіром повітряного простору.

Магнітна проникненість ряда матеріалів наведено в таблиці 1.1.

Таблиця 1.1.

Магнітна проникненість ряда матеріалів

матеріал	магнітна проникненість (Гн/м)
Повітря, вода	$1{,}26 \cdot 10^{-6}$
Ферітна сталь	$2 \cdot 10^{-3}$
Пермалой (сплав 80% нікелю і 20% заліза)	$1 \cdot 10^{-2}$
Залізо (чистота 99,8%)	$2{,}5 \cdot 10^{-1}$
NANOPERM®(магнитом'ягкий нанокристалічний сплав)	$1 \cdot 10^{-1}$

Конструктивно ефективність магнітостатичного екранування, що залежить від значення магнітного опору матеріала екрана, і буде тим вище, чим меньше в ньому буде стиків, швів і розрізів, що ідуть поперек ліній магнітної індукції.

Основні вимоги, які пред'являються до магнітостатичних екранів, діючих за методом шунтування магнітного поля НСиг феромагнітними матеріалами можна звести до наступних:

– магнітна проникність μ матеріалу екрана повинна бути можливо більш високою. Для виготовлення екранів бажано застосовувати магнітом'які матеріали з високою магнітною проникністю (наприклад, пермалой);

– збільшення товщини стінок екрана приводить до підвищення ефективності екранування;

– стики, розрізи й шви в екрані повинні розміщатися паралельно лініям магнітної індукції магнітного поля. Їхнє число повинне бути мінімальним;

– заземлення екрана не впливає на ефективність магнітостатичного екранування.

Ефективність магнітостатичного екранування підвищується при застосуванні багатошарових екранів.

Дія металевого екрана в змінному (ВЧ) магнітному полі засновано на використанні магнітної індукції, що створює в екрані змінні індукційні вихрові струми (струми Фуко). Магнітне поле цих струмів усередині екрана буде спрямовано назустріч збуджуючому полю, а за його межами – в тому ж напрямку, що й збуджуюче поле. Результуюче поле виявляється ослабленим усередині екрана. Вихрові струми в екрані розподіляються нерівномірно по його перетину (товщині). Це викликається явищем

поверхневого ефекту, сутність якого полягає в тому, що змінне магнітне поле слабшає в міру проникнення в глиб металу, тому що внутрішні шари екрануються вихровими струмами, що циркулюють у поверхневих шарах.

Завдяки поверхневому ефекту щільність вихрових струмів і напруженість змінного магнітного поля в міру поглиблення в метал падає за експонентним законом.

Ефективність магнітного екранування, заснованого на використанні магнітної індукції залежить від частоти й електричних властивостей матеріалу екрана. Чим НЧ, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення того високого ефекту екранування. Для ВЧ, починаючи з діапазону середніх хвиль, екран з будь-якого металу товщиною 0,5...1,5 мм діє досить ефективно.

Для частот вище 10 МГц мідна й тим більше срібна плівка товщиною більше 0,1 мм дає значний ефект екранування. Тому на частотах вище 10 МГц цілком припустиме застосування екранів з фольгованого гетинаксу або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям.

Основні вимоги, які пред'являються до магнітостатичних екранів, діючих за методом витіснення магнітного поля НСиг полем вихрових струмів в екрані можна звести до наступних:

– товщина екрана повинна бути значно більше,чим еквівалентна глибина проникнення. Цій умові відповідають як немагнітні, так і магнітні матеріали;

– зниження електричного опору вихрьовим токам в екрані підвищує його ефектівність. Тому, як правило, ВЧ екрани виготовляються з алюмінію, міді та латуні;

– стики, розрізи й шви в екрані повинні розміщатися вздовж напряму вихрьових токів;

– заземлення екрана не впливає на ефективність магнітного екранування, бо не змінює величини збуджених в екрані вихрьових струмів.

1.3.2. Електромагнітне екранування

На ВЧ застосовується винятково електромагнітне екранування. Дія електромагнітного екрана заснована на тім, що ВЧ ЕМП послабляється їм же створеним (завдяки вихровим струмам, що утворюються в товщі екрана) полем зворотнього напрямку. Враховуючи, що ЕМП складається з електричної і магнітної компонент, електромагнітне екранування об'єднує способи ВЧ електричного і магнітного екранування.

Для виготовлення екрана доцільно використати наступні матеріали:

– сталь листова ГОСТ 1386-47 товщиною (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;

– сталь тонколистова оцинкована ГОСТ 7118-54 товщиною (мм) 0,35;

0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;

– сталь тонколистова оцинкована ГОСТ 7118-54 товщиною (мм) 0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;

– сітка сталева ткана ГОСТ 3826-47 номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;

– сітка сталева плетена ГОСТ 5336-50 номер 3; 4; 5; 6;

– сітка з латунного дроту марки Л-80 ГОСТ 6613-53 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Необхідна ефективність екрана залежно від його призначення й величини рівня випромінювання ПЕМВН, звичайно перебуває в межах 60 ... 120 дБ.

Поряд з блоками апаратури екрануванню підлягають і монтажні проводи та сполучні лінії.

Щоб зменшити рівень ПЕМВН, необхідно особливо ретельно виконувати з'єднання оболонки проводу (екрана) з корпусом апаратури. Підключення оболонки повинне здійснюватися шляхом безпосереднього контакту (найкраще шляхом пайки або зварювання) з корпусом.

Разом з тим з'єднання оболонки проводу з корпусом в одній точці не послабляє в навколишньому просторі магнітне поле, створюване струмом, що протікає по проводу. Для екранування магнітного поля необхідно створити поле такої ж величини й зворотнього напрямку. Із цією метою необхідно весь зворотній струм екрануємого ланцюга направити через обплетення проводу, яке екранує. Для повного здійснення цього принципу необхідно, щоб оболонка, яка екранує, була єдиним шляхом для протікання зворотного струму.

Висока ефективність екранування забезпечується при використанні витої пари, захищеною оболонкою, яка екранує.

На НЧ доводиться використовувати більше складні схеми екранування – коаксіальні кабелі з подвійним плетенням (триаксильні кабелі).

На більш ВЧ, коли товщина екрана значно перевищує глибину проникнення поля, необхідність у подвійному екрануванні відпадає. У цьому випадку зовнішня поверхня відіграє роль електричного екрана, а по внутрішній поверхні протікають зворотні струми.

Застосування оболонки, яка екранує, істотно збільшує ємність між проводом та корпусом, що в більшості випадків небажано. Екрановані проводи більш громіздкі й незручні при монтажі, вимагають запобігання від випадкових з'єднань зі сторонніми елементами й конструкціями.

Довжина екранованого монтажного проводу повинна бути менше чверті довжини самої короткої хвилі переданого по проводу спектра сигналу. При використанні більше довгих ділянок екранованих проводів необхідно мати на увазі, що в цьому випадку екранований провід варто розглядати як довгу лінію, що у запобіганні перекручувань форми

переданого сигналу повинна бути навантажена на опір, рівний хвильовому.

Для зменшення взаємного впливу монтажних ланцюгів варто вибирати довжину монтажних ВЧ проводів найменшою, для чого елементи ВЧ схем, зв'язані між собою, варто розташовувати у безпосередній близькості, а неекрановані проводи ВЧ ланцюгів – при перетинанні під прямим кутом. При паралельному розташуванні такі проводи повинні бути максимально віддалені друг від друга або розділені екранами, у якості яких можуть бути використані несучі конструкції електронної апаратури (кожух, панель тощо). Екрановані проводи й кабелі варто застосовувати в основному для з'єднання окремих блоків і вузлів між собою.

Кабельні екрани виконуються у формі циліндра із суцільних оболонок, у вигляді спірально намотаної на кабель плоскої стрічки або у вигляді плетення з тонкого дроту. Екрани при цьому можуть бути одношаровими й багатошаровими комбінованими, виготовленими зі свинцю, міді, сталі, алюмінію і їхніх сполучень (алюміній-свинець, алюміній-сталь, мідь-сталь-мідь та інші).

У кабелях із зовнішніми пластмасовими оболонками застосовують екрани стрічкового типу в основному з алюмінієвих, мідних і сталевих стрічок, що накладають спірально або подовжньо уздовж кабелю.

В області НЧ, корпуса застосовуваних багатоконтактних НЧ з'єднань є екранами й повинні мати надійний електричний контакт із загальною шиною або землею приладу, а зазори між муфтами і корпусом повинні бути закриті електромагнітними ущільнювальними прокладками.

В області ВЧ коаксіальні кабелі повинні бути погоджені по хвильовому опору з використаними ВЧ контактами. При закладанні коаксіального кабелю у ВЧ контакти жила кабелю не повинна мати натягу в місці з'єднання з контактом роз'єму, а сам кабель повинен бути жорстко прикріплений до шасі апаратури поблизу роз'єму.

Для ефективного екранування НЧ полів застосовуються екрани, виготовлені з феромагнітних матеріалів з великою відносною магнітною проникністю. При наявності такого екрана лінії магнітної індукції проходять в основному по його стінках, які мають малий опір у порівнянні з повітряним простором усередині екрана.

Якість екранування таких полів залежить від магнітної проникності екрана й опору магнітопроводу, що буде тим меньше, ніж товще екран і меньше в ньому стиків і швів, що йдуть поперек напрямку ліній магнітної індукції.

1.4. Екранування інформаційних ліній зв'язку

Найбільш економічним способом екранування інформаційних ліній зв'язку між пристроями ТЗПІ вважається групове розміщення їхніх інформаційних кабелів у розподільний короб, який екранує. За відсутності такого короба необхідно екранувати окремо кожну лінію зв'язку [31].

Для захисту ліній зв'язку від наведень необхідно розмістити лінію в оболонку, яка екранує, або фольгу, заземлену в одному місці, щоб уникнути протікання по екрану струмів, викликаних нееквіпотенціальністю точок заземлення. При цьому слід мінімізувати площу контуру, утвореного прямими й зворотними проводами лінії. Якщо лінія являє собою одиночне проведення, а поворотний струм тече по деякій заземлюючій поверхні, то необхідно максимально наблизити проведення до поверхні. Якщо лінія утворена двома проводами, то їх необхідно скрутити, утворивши біфіляр (кручену пару). Лінії, виконані з екранованого проводу або коаксіального кабелю, у яких по обплетенню протікає поворотний струм, також відповідають вимозі мінімізації площі контуру лінії.

Найкращий захист як від електричного, так і від магнітного полів забезпечують інформаційні лінії зв'язку типу екранованого біфіляра, трифіляра (трьох скручених разом проводів, з яких один використовується як електричний екран), триаксіального кабелю (ізольованого коаксіального кабелю, поміщеного в електричний екран), екранованого плоского кабелю (плоского багатопровідного кабелю, покритого з однієї або обох сторін мідною фольгою).

Розглянемо декілька схем, що використовуються на частотах біля 100 кГц (рис. 1.1) [31].

Коло, зображене на рис. 1.1 *а,* має більшу площу петлі, утвореної "прямим" провідником й "землею". Це коло піддається насамперед магнітному впливу (екран заземлений на одному кінці, не захищає від магнітного впливу). Перехідне загасання для цієї схеми приймемо рівним 0 дБ для порівняння із загасанням схем на рис. 1.1 *б – и*.

Схема на рис. 1.1 *б,* практично не зменшує магнітний зв'язок, тому що зворотній провідник заземлений з обох кінців, і в цьому сенсі вона аналогічна схемі на рис. 1.1 *а*. Ступінь покращення порівнянний з погрішністю розрахунку (вимірювання).

Схема на рис. 1.1 *в,* відрізняється від схеми на рис. 1.1 *а,* наявністю зворотнього провідника – коаксіального екрану, але екранування магнітного поля погіршено, тому що ланцюг заземлений на обох кінцях, у результаті чого з "землею" утворюється петля великої площі. Схема на рис. 1.1 *г,* дозволяє істотно підвищити захищеність ланцюга (- 49 дБ) завдяки скрутці проводів. У цьому випадку (у порівнянні зі схемою на рис. 1.1 *б*) петлі нема, оскільки правий кінець кола не заземлений.

Подальше підвищення захищеності кола досягається застосуванням схеми на рис. 1.1 *е*, коаксіальне коло якої забезпечує краще магнітне екранування, ніж скручена пара на рис. 1.1 *г*.

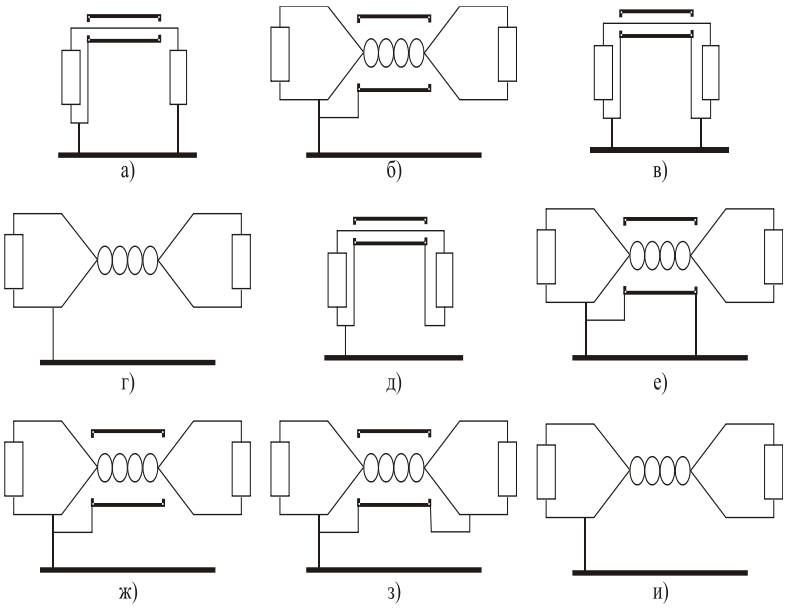


Рис. 1.1. Порівняння захищеності різних ланцюгів від впливу зовнішніх магнітних й електричних полів

а) 0 дБ; *б)* 2 дБ; ***в)*** 5 дБ; *г)* 49 дБ, скручена пара, 18 витків на метр; *д)* 57 дБ;

е) 64 дБ, схема краща на високих частотах; *ж)* 64 дБ; *з)* 71 дБ; *и)* 79 дБ, кручена пара (54 витка на метр)

Площа петлі у схемі на рис. 1.1 *д,* не більше, ніж у схемі на рис. 1.1 *г,* тому що поздовжня вісь екрана коаксіального кабелю збігається з його центральним провідником.

Схема на рис. 1.1 *е,* дозволяє підвищити захищеність кола завдяки тому, що скручена пара заземлена лише на одному кінці. Крім того, у цій схемі використовується незалежний екран.

Схема на рис. 1.1 *ж,* має ту ж захищеність, що й схема на рис. 1.1 *е*: ефект той же, що і при заземленні на обох кінцях, оскільки довжина кола й екрана істотно менше робочої довжини хвилі.

Можливою причиною покращання захищеності схеми на рис. 7.1 *з,* у порівнянні зі схемою рис. 1.1 *ж,* може бути зменшення площі еквівалентної петлі.

Більш щільна скрутка проводів (рис. 1.1 *и*) дозволяє додатково зменшити магнітний зв’язок.

Крім того, при цьому зменшується й електричний зв’язок (в обох провідниках струми наводяться однаково).

Для зменшення магнітного й електричного зв’язку між проводами необхідно зменшити площу петлі, максимально рознести кола й максимально зменшити довжину паралельного пробігу ліній ТЗПІ і сторонніх провідників.

При нульових рівнях сигналів (0 дБ) у з’єднувальних лініях ТЗПІ між

ними і сторонніми провідниками повинно забезпечуватися перехідне загасання не менш 114 дБ.

Таке перехідне загасання забезпечується, як правило, при прокладці кабелів ТЗПІ на відстані не менш 0,1 м від сторонніх провідників.

При цьому допускається прокладка кабелів ТЗПІ впритул зі сторонніми провідниками при сумарній довжині їхнього спільного пробігу не більше 70 м.

1.5. Екранування приміщень

Екрануватися можуть не тільки окремі блоки (вузли) апаратури та їхні з'єднувальні лінії, але й приміщення в цілому.

Теорія й практика показують, що з погляду вартості матеріалу й простоти виготовлення переваги на стороні екранованого приміщення з листової сталі.

Однак, при застосуванні сітчастого екрана можуть значно спроститися питання вентиляції й висвітлення приміщення. У зв'язку із цим сітчасті екрани також знаходять широке застосування.

Металеві листи або полотнища сітки повинні бути між собою електрично з'єднані по всьому периметру.

Для суцільних екранів це може бути здійснено електрозварюванням або пайкою. Шов електрозварювання або пайки повинен бути безперервним для того, щоб одержати суцільнозварну конструкцію екрана.

Для сітчастих екранів придатна будь-яка конструкція шва, що забезпечує гарний електричний контакт між сусідніми полотнищами сітки не рідше чим через 10...15 мм.

Для цієї мети може застосовуватися пайка або точкове зварювання. Екран, виготовлений з лудженої низьковуглеводної сталевої сітки з осередком 2,7 ... 3 мм, дає ослаблення порядку 57 ... 60 дБ, а з такої ж подвійної (з відстанню між зовнішньою й внутрішньою сітками 100 мм) – близько 90 дБ.

Екран, виготовлений з одинарної мідної сітки з осередком 2,5 мм, має ослаблення порядку 67...70 дБ.

У звичайних (неекранованих) приміщеннях основний ефект екрану забезпечують залізобетонні стіни будинків.

Екрануючі властивості дверей і вікон гірше. В табл. 1.2 приведені дані про ступінь екранувальної дії різних типів приміщень в залежності від частоти радіосигналу.

Слід зазначити ефективність екранування віконних отворів в залізобетонних будівлях на частотах 100 – 500 МГц. Це пояснюється тим, що екран з арматури залізобетонних панелей і грати, що закриває віконні прорізи, ефективно послаблює радіовипромінювання. Зменшення екранування на частотах 1 ГГц і вище є наслідком того, що розмір вічка арматури стає порівнянним з ½ довжини хвилі (15 см).

Таблиця 1.2

Екрануючі властивості приміщень (будівель)з віконними прорізами, площа яких становить 30 % площі стіни

Тип будівлі	Ступінь екранування, дБ			Відносна дальність дії
	100 МГц	500 МГц	1000 МГц	
Вікна без грат				
Дерев'яна, з товщиною стін 20 см	5–7	7–9	9–11	2–3
Цегляна, з товщиною стін 1,5 цегли	13–15	15–17	16–19	1
Залізобетонна, з вічком арматури 15 × 15 см і товщиною стін 160 мм	20–25	18–19	15–17	0,4–1,2 (в залежності від частотного диапазону)
Вікна закриті металевими гратами з вічком 5 см				
Деревяна, з товщиною стін 20 см	6–8	10–12	12–24	1,5–2
Цегляна, з товщиною стін 1,5 цеглини	17–19	20–22	22–25	0,5–0,8
Залізобетонна, з вічком арматури 15 × 15 см і товщиною стін 160 мм	28–32	23–27	20–25	0,3–0,8 (в залежності від частотного диапазону)

Існує думка, що металізоване скло ефективно послаблює ЕМВ. Але це твердження позбавлене підстав – металізація алюмінієм товщиною 4 мкм послаблює сигнал на частоті 1 ГГц всього на 5 дБ, а на більш НЧ і того менше. При цьому скло з такою металізацією практично не пропускає денне світло.

Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, у тому числі:

– струмопровідні лакофарбові покриття або струмопровідні шпалери;

– штори з металізованої тканини;

– металізовані вікна (наприклад, із двоокису олова), що встановлюються в металеві або металізовані рами.

У приміщенні екрануються стіни, двері й вікна.

При закритті дверей повинен забезпечуватися надійний електричний контакт зі стінками приміщення (із дверною рамою) по всьому периметру не рідше чим через 10...15 мм. Для цього може бути застосована пружинна гребінка з фосфористої бронзи, що зміцнює, по всьому внутрішньому периметру дверної рами.

Вікна повинні бути затягнуті одним або двома шарами мідної сітки з осередком не більше 2×2 мм, причому відстань між шарами сітки повинна

бути не менш 50 мм. Обидва шари сітки повинні мати гарний електричний контакт зі стінками приміщення (з рамою) по всьому периметру. Сітки зручніше робити зйомними, а металеве обрамлення зйомної частини також повинно мати пружні контакти у вигляді гребінки з фосфористої бронзи.

При проведенні робіт з ретельного екранування подібних приміщень необхідно одночасно забезпечити нормальні умови для працюючого в ньому персоналу, насамперед, вентиляцію повітря й освітлення.

Конструкція екрана для вентиляційних отворів залежить від діапазону частот. Для частот менш 1000 МГц застосовуються стільникові конструкції, що закривають вентиляційний отвір, із прямокутними, круглими, шестигранними вічками. Для досягнення ефективного екранування розміри вічків повинні бути менш однієї десятої від довжини хвилі. При підвищенні частоти необхідні розміри осередків можуть бути настільки малими, що погіршується вентиляція.

Спеціальні екрановані приміщення дозволяють досягти ослаблення сигналу до 80 – 100 дБ. У табл. 1.3 наведені гранично досяжні значення загасання радіохвиль для різних конструкцій екранованих приміщень.

Таблиця 1.3

Ефективність екранування

Тип конструкції для екранованого приміщення	Загасання радіосигналу, дБ
Поодинокий екран із сітки з одними дверима, обладнаними зажимними пристроями	40
Подвійний екран із сітки з подвійними дверима-тамбуром і зажимними пристроями	80
Суцільний сталевий зварний екран з подвійними дверима-тамбуром і зажимними пристроями	100

Розміри екранованого приміщення вибирають виходячи з його призначення й вартості. Звичайно екрановані приміщення будують площею 7 ... 8 м^2 при висоті 2,7... 3 м.

Усередині екранованого приміщення прокладання кабельної мережі виконується в пластикових коробах. Коефіцієнт заповнення перетину короба чи труби не повинен перевищувати 65 %.

Фільтри електроживлення рекомендується встановлювати із зовнішнього боку екранованого приміщення біля місця введення електричних проводів. Проводи між фільтром і екраном прокладають у металевій трубі або в екранувальному обплетенні, які з’єднані як з фільтром, так і з екраном по периметру.

Заземлювач екранованого приміщення потрібно розташовувати не ближче ніж за 10 м до межі території, що охороняється, та інженерних комунікацій, що виходять за неї. Для СЗ не використовуються природні

заземлювачі (трубопроводи, металеві конструкції будівлі тощо).

Екранування електромагнітних хвиль більше 100 дБ можна забезпечити тільки в спеціальних екранованих камерах, у яких електромагнітний екран виконаний у вигляді електрогерметичного сталевого корпуса, а для введення електричних комунікацій використовуються спеціальні фільтри.

Всі вимоги до екранованих приміщень викладені в [25, 31].

1.6. Заземлення ТЗПІ

Необхідно пам'ятати, що екранування ТЗПІ й з'єднувальних ліній ефективно тільки при правильному їхньому заземленні. Тому однією з найважливіших умов по захисту ТЗПІ є правильне заземлення цих пристроїв. Об'єкти, на яких експлуатуються різноманітні ТЗПІ, як правило, мають декілька видів пристроїв заземлення різного призначення. Заземлення технічних засобів забезпечує:

– безпеку обслуговуючого персоналу, цілісність та надійність апаратури;

– екранування для зниження рівня власних випромінювань та екранування від зовнішніх ЕМП.

Для виконання своїх функцій за призначенням заземлення буває відповідно *захисним і технічним*.

Захисне заземлення забезпечує величину "напруги доторкання", що не перевищує допустимо можливої для загрози небезпеці життя обслуговуючого персоналу від ураження електричним струмом. Згідно "Правил експлуатації електропристроїв" допустиме значення величини цієї напруги при будь-якому стані апаратури – справному чи несправному – повинно забезпечувати цілісність та надійність її роботи (наприклад, запобігання пошкодженню ізоляції мережевих провідників і пристроїв для електроживлення апаратури). Значення величини опору такого заземлення не перевищує величину 10 – 20 Ом.

Технічне заземлення ("технологічна земля", "сигнальна земля", "логічний нуль") використовується для заземлення екранів обладнання та забезпечує так звану "безшумну землю", вільну від можливих сторонніх потенціалів, які можуть викликати завади у екранованих схемах. Застосування технологічного заземлення є необхідною умовою при наявності тільки одного захисного заземлення (наприклад, об'єкти ОВ при підвищених вимогах до ЗІ). Як правило, вимоги щодо забезпечення значення величини опору такого заземлення значно жорсткіші, ніж для захисного заземлення (не більше 4 Ом).

Крім провідників, призначених для безпосереднього з'єднання ТЗПІ із заземлювачем, гальванічний (безпосередній) зв'язок із землею можуть мати й різні інші струмопровідні магістралі, що мають вихід за межі КонтрЗ. До них належать:

– нульовий провідник мережі електроживлення;

– металева оболонка кабелів, якими здійснюється зв’язок з іншими системами або об’єктами;

– металеві трубопроводи водо та газопостачання, опалювальної та інших систем забезпечення життєдіяльності об’єкта та його окремих територій, будівель, приміщень тощо;

– металева арматура залізобетонних конструкцій будівель.

Всі ці провідники спільно із заземлювачем створюють розподілену СЗ, через яку можливий витік інформації та її перехоплення за межами КонтрЗ.

У теперішній час існують різні типи заземлень. Найбільш часто використовуються *одноточкові, багатоточкові* та *комбіновані* (*гібридні*) схеми [33].

Одноточкова послідовна схема заземлення (рис. 1.2) найбільш проста схема. Однак їй властивий недолік, пов’язаний із протіканням зворотних струмів різних ланцюгів по загальній ділянці заземлюючого ланцюга. Внаслідок цього можливо поява НСиг в сторонніх колах. *Одноточкова паралельна схема* (рис. 1.3) позбавлена цього недоліку, але вона потребує значної кількості відносно протяжних заземлюючих провідників, що може привести до неможливості забезпечення малого опору заземлення ділянок кола.

Рис. 1.2. Одноточкова послідовна схема заземлення

Крім того, між заземлюючими провідниками можуть виникати небажані зв’язки, які створюють кілька шляхів заземлення для кожного пристрою. У результаті в СЗ можуть виникнути урівнюючі струми й з’явитися різниця потенціалів між різними пристроями.

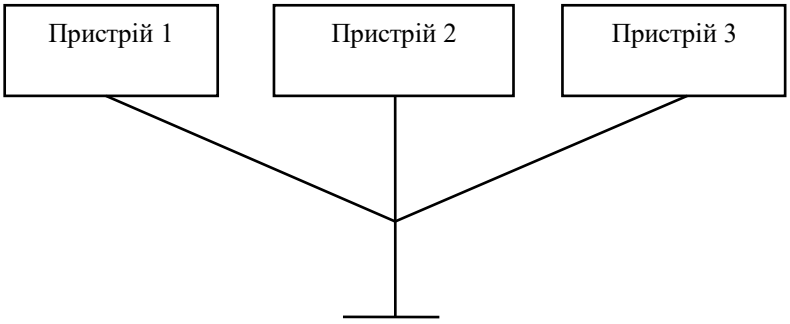


Рис. 1.3. Одноточкова паралельна схема заземлення

Багатоточкова схема заземлення (рис. 1.4) практично позбавлена вищезазначених недоліків. У цьому випадку окремі пристрої й ділянки корпусу індивідуально заземлені. При проектуванні й реалізації багатоточкової СЗ необхідно приймати спеціальні міри для виключення замкнутих контурів.

Як правило, одноточкова схема заземлення застосовується на НЧ при невеликих розмірах пристроїв, що заземлюються, та відстанях між ними менш 0,5 λ.

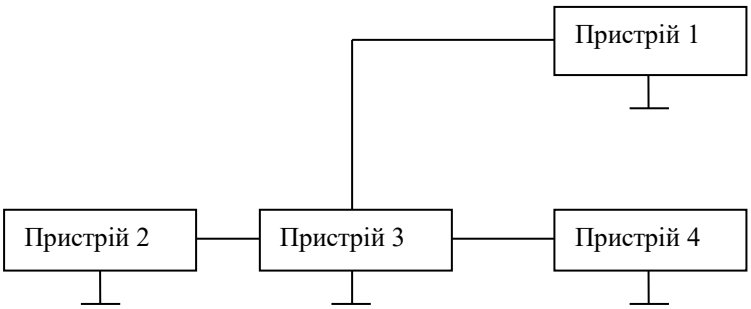


Рис. 1.4. Багатоточкова схема заземлення

На ВЧ при більших розмірах пристроїв, що заземлюють, і значних відстанях між ними використовується багатоточкова СЗ. У проміжних випадках ефективна комбінована (гібридна) СЗ, що представляє собою різні сполучення одноточкової, багаточкової та плаваючої СЗ.

Заземлення ТЗПІ повинне бути виконане відповідно до певних правил (див. п.7.2.4, [18]).

Опір заземлення визначається, головним чином, опором розтікання струму в землі. Величину цього опору можна значно понизити за рахунок зменшення перехідного опору між заземлювачем та ґрунтом шляхом ретельного очищення перед укладанням поверхні заземлювача та утрамбування довкола нього ґрунту, а також підсипанням повареної солі.

Питомий опір різних ґрунтів (тобто електричний опір 1 $см^3$ ґрунту) залежить від вологості ґрунту, її складу, щільності, температури й т. п. і коливається в дуже широких межах (див. табл. 1.4).

Таблиця 1.4.

Значення питомого опору різних ґрунтів

Тип ґрунту	Питомий опір (ρ), $Ом/см^3$		
	середній	мінімальний	максимальний
Золи, шлаки, соляні відходи	2370	500	7000
Глина, суглинок, сланці	4060	340	16300
Те ж саме з домішками піску	15800	1020	135000
Гравій, пісок, камені з невеликою кількістю глини або суглинку	94000	59000	458000

Добре провідні ґрунти втрачають свої властивості при відсутності вологи. Для більшості ґрунтів 30 % вмісту вологи досить для забезпечення малого опору. Наприклад, для суглинків питомий опір при вологості 5 % становить 165 000 Ом/см^3, а при вологості 30 % – 6 400 Ом/см^3.

При промерзанні опір ґрунтів різко зростає. Наприклад, для суглинків питомий опір при вологості 15 % і температурі 20 °С становить 7200 Ом/см^3, при температурі - 5°С – 79 000 Ом/см^3, а при температурі -15°С – 330 000 Ом/см^3.

Змочування ґрунту навколо заземлювачів 2 ... 5 % солевим розчином значно (в 7...10 разів) знижує опір заземлення.

Урахувати всі фактори, що впливають на провідність ґрунта, аналітичним шляхом практично неможливо, тому при обладнанні заземлення величину питомого опору ґрунту в тих місцях, де передбачається розміщення заземлення, визначають дослідним шляхом.

Як правило, вимір опору заземлення проводиться два рази в рік (узимку й улітку).

Якщо заземлювач складається з металевої пластини радіуса r, розташованої безпосередньо біля поверхні землі, то опір заземлення $R_з$ можна розрахувати за формулою:

$$R_з = \frac{\rho}{4r} \text{ Ом.} \qquad (1.1)$$

При збільшенні глибини закапування l пластини опір заземлення зменшується та при $l >> r$ величина $R_з$ зменшується вдвічі.

Досить часто застосовують заземлюючий пристрій у вигляді вертикально вбитої труби. Опір заземлення в цьому випадку визначається формулою:

$$R_з = \frac{\rho}{2\pi l}\left(\ln\frac{4}{r_{тр}} - 1\right), \qquad (1.2)$$

де l – довжина труби, см; $r_{тр}$ – радіус труби, см.

З формули видно, що опір заземлення залежить більшою мірою не від радіуса труби, а від її довжини. Тому при встановлені заземлення доцільніше застосовувати тонкі й довгі труби (стрижні з арматури). У якості одиночних стрижневих заземлювачів доцільно використовувати мідні заземлюючі стрижні.

У табл. 7.4 наведені експериментально отримані значення опору заземлення стрижневого заземлювача (Ø 15,9 мм, l = 1,5м) для різних ґрунтів.

Як видно з табл. 1.5, опір простих одиночних заземлювачів виявляється досить більшим. Тому такі заземлювачі знаходять застосування при невисоких вимогах до заземлюючих пристроїв або при ґрунтах з дуже великою провідністю.

При підвищених вимогах до величини опору заземлення (опір заземлення ТЗПІ не повинний перевищувати 4 Ом) застосовують

багаторазове заземлення, що складається з ряду одиночних симетрично розташованих заземлювачів, з'єднаних між собою.

Таблиця 1.5.

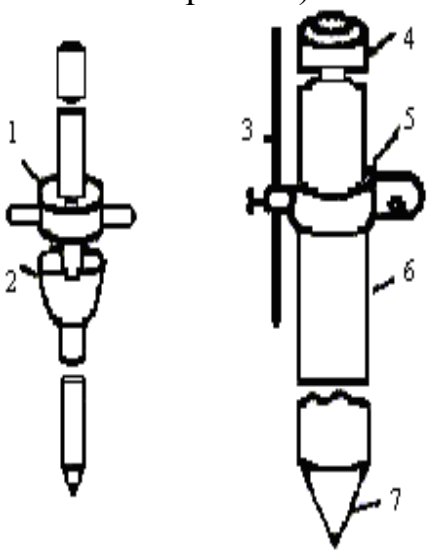
Значення опору заземлювача для різних ґрунтів

Тип ґрунту	Опір заземлення $R_з$, Ом		
	середній	мінімальний	максимальний
Золи, шлаки, соляні відходи	14	3,5	41
Глина, суглинок, сланці	24	2	98
Те ж саме з домішка-ми піску	93	6	800
Гравій, пісок, камені з невеликою кількістю глини або суглинку	554	35	2 700

На практиці найбільше часто в якості заземлювачів застосовують:

– стрижні з металу, що володіють високою електропровідністю, занурені в землю й з'єднані з наземними металоконструкціями засобів ТЗПІ (рис. 1.5);

– сіткові заземлювачі, виготовлені з елементів з високою електропровідністю та занурені в землю (служать як доповнення до заземлюючих стрижнів).



1 – ковзаючий молот

2 – рухомий упор

3 – з`єднувальна мідна шина

4 – головка з фаскою

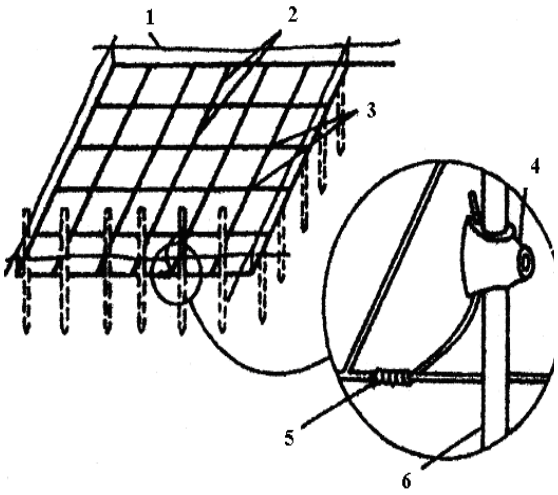
5 – зажим

6 – стрижень

7 – загострений кінець стрижня

Рис. 1.5. Типові стрижні заземлювачів

На рис. 1.6 наведена схема комбінованого заземлення із стрижнів і сітки.



1 – поверхня землі;

2 – сітка;

3 – зварне з’єднання;

4 – зажим;

5 – мідний провідник;

6 – мідний стрижень заземлення.

Рис. 1.6. Схема комбінованого заземлення із стрижнів і сітки

При необхідності встановлення ВЧ заземлення потрібно враховувати не тільки геометричні розміри заземлювачів, їхню конструкцію й властивості ґрунту, але й довжину хвилі ВЧ випромінювання. Сумарний ВЧ опір заземлення Z_C складається з ВЧ опору магістралі заземлення Z_M (проводу, що йде від заземлюючого пристрою до поверхні землі) та з ВЧ опору самого заземлювача $Z_З$ (проводу, металевого стрижня або листа, що перебуває в землі).

Величина заземлення в основному визначається не опором заземлення, а опором заземлюючої магістралі. Для зменшення останнього варто прагнути насамперед до зменшення індуктивності заземлюючої магістралі, що досягається за рахунок зменшення її довжини й виготовлення магістралі у вигляді стрічки, що володіє в порівнянні із проводом круглого перетину меншою індуктивністю. У тих випадках, коли індуктивність заземлюючої магістралі можна зробити досить невеликою або використати її для одержання послідовного резонансу при блокуванні випромінюючих мереж захисними конденсаторами на землю (наприклад, при комплексному придушенні випромінювання в приміщеннях), доцільно значно зменшити величину опору заземлювача $Z_З$. Зменшити величину $Z_З$ можна також багаторазовим заземленням із симетрично розташованих заземлювачів.

При цьому загальний опір заземлення буде тим менше, ніж далі друг від друга розташовані окремі заземлювачі.

При обладнанні заземлення в якості заземлювачів найчастіше застосовуються сталеві труби довжиною 2 ... 3 м та діаметром 37 ... 50 мм, або сталеві смуги перетином 50 ... 100 мм.

Найбільш придатними є труби, що дозволяють досягти глибоких і найбільш вологих шарів землі, що володіють найбільшою провідністю й не піддаються висиханням або промерзанню.

Однак тут необхідно враховувати, що зі зменшенням опору ґрунту зростає корозія металу.

Крім того, використання таких заземлювачів не зв’язане зі значними земляними роботами, що неминуче, наприклад, при виконанні заземлення з металевих листів або металевих стрічок та провідників, що закладаються горизонтально в землю.

Заземлювачі слід з’єднувати між собою шинами за допомогою зварювання. Перетин шин і магістралей заземлення за умов механічної міцності й одержання достатньої провідності рекомендується брати не менш (24 × 4) мм^2.

Провідник, що з’єднує заземлювач із контуром заземлення, повинен бути лудженим для зменшення гальванічної корозії, а з’єднання повинні бути захищені від впливу вологи.

Магістралі заземлення поза будинком необхідно прокладати на глибині близько 1,5 м, а усередині будинку – по стіні або спеціальних каналах таким чином, щоб їх можна було зовні оглядати.

З’єднують магістралі із заземлювачем тільки за допомогою зварювання. До заземлюючого пристрою ТЗПІ магістраль підключають за допомогою болтового з’єднання в одній точці.

Для зменшення опорів контактів найкращим є постійне безпосереднє з’єднання металу з металом, отримане зварюванням або пайкою. При з’єднанні під гвинт необхідно застосовувати шайби (зірчасті або Гровера), що забезпечують сталість щільності з’єднання. При дотику двох металів у присутності вологи виникає гальванічна та (або) електрична корозія. Гальванічна корозія є наслідком утворення гальванічного елемента, у якому волога є електролітом. Ступінь корозії визначається положенням цих металів в електричному ряді. Електрична корозія може виникнути при зіткненні в електроліті двох однакових металів. Вона визначається наявністю локальних електрострумів у металі, наприклад, струмів у заземленнях силових кіл.

Найбільш ефективним методом захисту від корозії є застосування металів з малою електрохімічною активністю, таких, як олово, свинець, мідь. Значно зменшити корозію й забезпечити гарний контакт можна, ретельно ізолюючи з’єднання від проникнення вологи.

На даний час більш перспективним є використання модульно-штирьової СЗ, за допомогою якої можливо створити глибинне заземлення. Наприклад, СЗ фірми “Galmar”, призначена для організації заземлення на телекомунікаційних, енергетичних об’єктах відомчих мереж, операторів мобільного та стаціонарного зв’язку, промислових підприємств. Система забезпечує довгостроковий, надійний контур заземлення зі стабільними електричними параметрами, які не залежать від погодних умов, таких як температура, вологість [33].

1.7. Фільтрація інформаційних сигналів

Одним з методів локалізації НСиг, що циркулюють у технічних засобах і системах обробки інформації, є *фільтрація* [21, 32]. У джерелах ЕМП і наведень фільтрація здійснюється з метою запобігання поширенню небажаних електромагнітних коливань за межі пристрою – джерела НСиг. Для фільтрації сигналів у ланцюгах живлення ТЗПІ використовуються роздільні трансформатори й завадопридушуючі фільтри.

1.7.1. Розділові трансформатори

Розділові трансформатори повинні забезпечувати розв'язання первинного й вторинного ланцюгів по сигналах наведення. Це означає, що у вторинний ланцюг трансформатора не повинні проникати наведення, що з'являються в ланцюзі первинної обмотки. Проникнення наведень у вторинну обмотку пояснюється наявністю небажаних резистивних й ємнісних кіл зв'язку між обмотками.

Для зменшення зв'язку обмоток по сигналах наведень часто застосовується внутрішній екран, виконаний у вигляді заземленої прокладки або фольги, що укладається між первинною й вторинною обмотками. За допомогою цього екрана наведення, що діє в первинній обмотці, замикається на землю. Однак, електростатичне поле навколо екрана також може служити причиною проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються з метою рішення ряду завдань, у тому числі для:

– поділу по ланцюгах живлення джерел і рецепторів наведення, якщо вони підключаються до тих самим шин змінного струму;

– усунення асиметричних наведень;

– ослаблення симетричних наведень у колі вторинної обмотки, обумовлених наявністю асиметричних наведень у колі первинної обмотки.

Засоби розв'язання й екранування, які застосовуються в розділових трансформаторах, забезпечують максимальне значення опору між обмотками й створюють для наведень шлях з малим опором: первинна обмотка – землю. Це досягається забезпеченням високого опору ізоляції відповідних елементів конструкції (~10^4 МОм) і незначної ємності між обмотками. Зазначені особливості трансформаторів для кіл живлення забезпечують більш високий ступінь придушення наведень, чим звичайні трансформатори.

Розділовий трансформатор зі спеціальними засобами екранування й розв'язки забезпечує ослаблення інформаційного сигналу наведення в навантаженні на 126 дБ при ємності між обмотками 0,005 пФ і на 140 дБ при ємності між обмотками 0,001 пФ.

Засоби екранування, які застосовуються в розділових трансформаторах, повинні не тільки усувати вплив асиметричних наведень на пристрій, що захищається, але й не допустити на виході трансформатора

симетричних наведень, обумовлених асиметричними наведеннями на його вході. Застосовуючи в роздільних трансформаторах спеціальні засоби екранування, можна істотно (більш ніж на 40 дБ) зменшити рівень таких наведень.

1.7.2. Завадопридушуючі фільтри

У теперішній час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів у різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові та фільтри, що загороджують, тощо.

Основне призначення фільтрів – пропускати без значного послаблення сигнали із частотами, що лежать у робочій смузі частот, і придушувати (послабляти) сигнали із частотами, що лежать за межами цієї смуги. Для виключення просочування інформаційних сигналів у ланцюзі електроживлення використовуються *фільтри НЧ*. *Фільтр НЧ* (ФНЧ) пропускає сигнали із частотами нижче граничної частоти та придушує сигнали із частотами вище граничної частоти. Послідовна гілка ФНЧ повинна мати малий опір для постійного струму й нижніх частот. Разом з тим для того, щоб вищі частоти затримувалися фільтром, послідовний опір повинен рости із частотою. Цим вимогам задовольняє індуктивність *L*.

Паралельна гілка ФНЧ, навпаки, повинна мати малу провідність для НЧ для того, щоб струми цих частот не шунтувалися паралельним плечем. Для ВЧ паралельна гілка повинна мати більшу провідність, тоді коливання цих частот будуть нею шунтуватися, та їхній струм на виході фільтра буде послаблятися. Таким вимогам відповідає ємність *C*.

Більше складні багатоланкові ФНЧ (Чебишева, Баттерворта, Бесселя та інші) будуються на основі сполучень різних одиничних ланок.

Кількісно величина ослаблення (фільтрації) небажаних (у тому числі й НСиг) сигналів захисним фільтром оцінюється відповідно до вираження:

$$A_{ф} = \frac{U_1}{U_2} = \frac{P_1}{P_2}, \qquad (1.3)$$

де U_1 (P_1) – напруга (потужність) НСиг на вході фільтра;

U_2 (P_2) – напруга (потужність) НСиг на виході фільтра при включеному навантаженні Z_H.

Основні вимоги, що пред’являються до захисних фільтрів, полягають у наступному [21]:

– величини робочої напруги й струму фільтра повинні відповідати напрузі й струму фільтруючого ланцюга;

– величина послаблення небажаних сигналів у діапазоні робочих частот повинна бути не менш необхідної;

– послаблення корисного сигналу в смузі прозорості фільтра повинне бути незначним;

– габарити й маса фільтрів повинні бути мінімальними;

– фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) та механічних навантаженнях (удари, вібрація й т.д.);

– конструкції фільтрів повинні відповідати вимогам техніки безпеки.

До фільтрів ланцюгів живлення поряд із загальними пред'являються наступні додаткові вимоги:

– загасання, внесене такими фільтрами в ланцюги постійного струму або змінного струму основної частоти, повинне бути мінімальним (наприклад 0,2 дБ і менш) та мати велике значення (більше 60 дБ) у смузі придушення, яка залежно від конкретних умов може бути досить широкою (до 10 ГГц);

– мережні фільтри повинні ефективно працювати при сильних проходящих струмах, високих напругах і високих рівнях потужності проходящих та затримуваних електромагнітних коливань;

– обмеження, що накладають на припустимі рівні нелінійних перекручувань форми напруги живлення при максимальному навантаженні, повинні бути досить жорсткими (наприклад, рівні гармонійних складових напруги живлення із частотами вище 10 кГц повинні бути на 80 дБ нижче рівня основної гармоніки).

Розглянемо вплив цих параметрів на роботу фільтра.

Напруга, прикладена до фільтра, повинна бути такою, щоб вона не викликала пробою конденсаторів фільтра при різних стрибках напруги живлення, включаючи стрибки, обумовлені перехідними процесами в ланцюгах живлення. Щоб при заданих масі й об'ємі фільтр забезпечував найкраще придушення наведень у необхідному діапазоні частот, його конденсатори повинні мати максимальну ємність на одиницю об'єму або маси. Крім того, номінальне значення робочої напруги конденсаторів вибирають виходячи з максимальних значень допустимих стрибків напруги ланцюга живлення, але не більше їх.

Струм через фільтр повинен бути таким, щоб не виникало насичення осердь котушок фільтра. Крім того, варто враховувати, що зі збільшенням струму через котушку збільшується реактивне спадання напруги на ній. Це може привести до того, що:

– погіршується еквівалентний коефіцієнт стабілізації напруги в ланцюзі живлення, що містить фільтр;

– виникає взаємозалежність перехідних процесів у різних навантаженнях ланцюга живлення.

Найбільші стрибки напруги при цьому виникають під час відключення навантажень, тому що більшість із них має індуктивний характер.

Характеристики фільтрів залежать від числа використаних реактивних елементів. Так, наприклад, фільтр із одного паралельного конденсатора або однієї послідовної індуктивної котушки може забезпечити загасання лише 20 дБ/декаду поза смугою пропускання, а *LC*-фільтр із десяти або більше елементів – більше 200 дБ/декаду. Через паразитний зв'язок між входом та виходом фільтра на практиці важко одержати загасання більше 100 дБ. Якщо фільтр неекранований і сигнал подається на нього та знімається за допомогою неекранованих з'єднань (проводів), то розв'язка між входом і виходом не перевищує 40 ... 60 дБ. Для забезпечення розв'язки більше 60 дБ необхідно використати екрановані фільтри з роз'ємами й використати для з'єднання екрановані проводи.

Фільтри з гарантованим загасанням 100 дБ виконують у вигляді вузла з електромагнітним екрануванням, що міститься в корпусі, виготовленому з матеріалу з високою магнітною проникністю магнітного екрана. Цим істотно зменшується можливість виникнення усередині корпуса паразитного зв'язку між входом і виходом фільтра через магнітні електричні або ЕМП.

Через вплив паразитних ємностей й індуктивностей фільтр найчастіше не забезпечує необхідного загасання на частотах, що перевищують граничну частоту на дві декади, і повністю може втратити працездатність на частотах, що перевищують граничну частоту на кілька декад.

Конструктивно фільтри підрозділяються на:

– фільтри на елементах із зосередженими параметрами (*LC*-фільтри) – звичайно призначені для роботи на частотах до 300 МГц;

– фільтри з розподіленими параметрами (смугові, коаксіальні або хвильоводні) – застосовуються на частотах понад 1 ГГц;

– комбіновані – застосовуються на частотах 300 МГц ... 1 ГГц. До числа пристроїв, що захищаються мережевими фільтрами, відносять найрізноманітнішу апаратуру: комп'ютери, приймачі діапазону довгих і середніх хвиль, радіотрансляційні приймачі тощо.

Мережний фільтр включають між мережею і пристроєм споживання. На рис. 1.7 представлена принципова схема мережевого фільтра, розрахованого на потужність навантаження в 100 Вт [25]. Він забезпечує живлення одночасно двох споживачів.

У цьому фільтрі використані два способи придушення перешкод: фільтрація розподіленим дроселем Др1, Др2 і екранування мережевої обмотки трансформатора Т1 і вихідної обмотки трансформатора Т2. Електростатичним екраном мережевої обмотки трансформатора Т1 і вихідної обмотки трансформатора Т2 служать магнітопроводи і низьковольтні обмотки трансформаторів, розталовані поверх високовольтних і з'єднані із загальним проводом фільтра і пристроєм споживача.

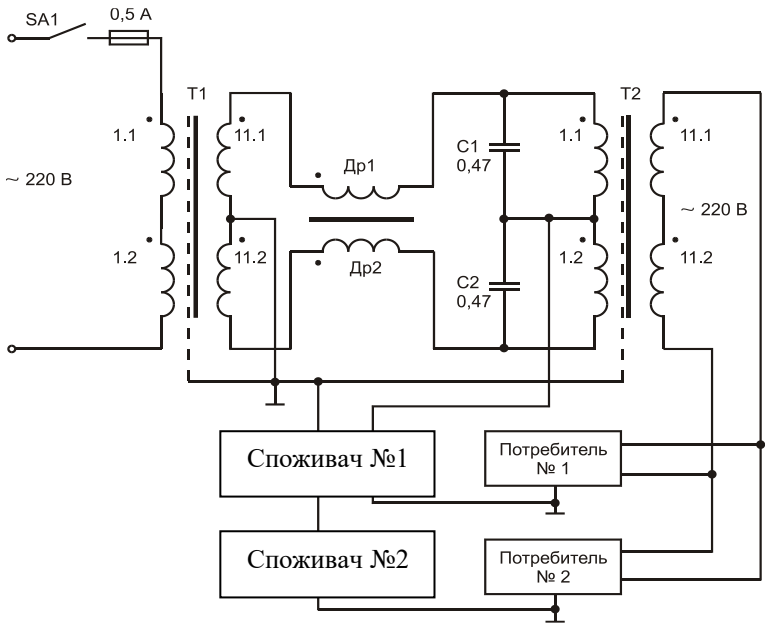


Рис. 1.7. Принципова схема мережевого фільтра

Оскільки напрямки обмотки трансформатора і обмоток індуктивності дроселів Др1 і Др2 однакові, а струми через обмотки Др1 і Др2 противофазні, то сума магнітних полів цих обмоток дорівнює нулю.

Результуючий опір дроселів змінному струму промислової частоти дорівнює активному опору обмоток. Отже, падіння напруги на дроселях Др1 і Др2 практично дорівнює нулю.

У пристрої використано два серійних трансформатора Т1 і Т2 типу ТПП 296-127/220-50. Режекторний дросель Др1 і Др2 виконаний на феритовому кільцевому магнітопроводі марки М4 000 розміром К65 × 32 × 8. Дві обмотки намотуються в два проводи одночасно проводом МГШВ-0,5 і містять по двадцять витків кожна.

Намотування повинно бути в один шар. Марка фериту і розмір сердечника можуть бути іншими, але індуктивність дроселів повинна бути близько 1,5 мГн. Конденсатори С1 і С2 повинні бути розраховані на напругу більше 400 В.

У даний час промисловістю випускаються кілька серій захисних фільтрів (ФЗП, ФМПЗ, ФСП тощо).

Фільтри мережні протизавадні типу ФСП призначені для:

– захисту засобів обробки і реєстрації інформації від витоку по колу електроживлення і колу заземлення;

– захисту засобів обробки і реєстрації інформації від ВЧ мережних завад.

Фільтри сертифіковані і включені до переліку засобів загального призначення, які дозволено застосовувати для технічного ЗІ.

Технічні характеристики:

Номінальна напруга, В 250;

Номінальна частота напруги й струму, Гц 50;

Номінальний струм, А:

ФСП-1 20; ФСП-2 20; ФСП-3 10; ФСП-4 5.

Вносиме затухання несиметричних завад:

– для ФСП-1 на частотах від 0,1 Мгц до 1 000 Мгц, дБ, не менше 60;

– для ФСП-2 на частотах від 0,01 Мгц до 1 Мгц, дБ від 20 до 80; на частотах від 1 Мгц до 1 000 Мгц, дБ, не менше 80;

– для ФСП-3 (рис. 1.8) на частотах від 0,091 Мгц до 1 Мгц, дБ від 20 до 80; на частотах від 1 Мгц до 1 000 Мгц, дБ, не менше 80;

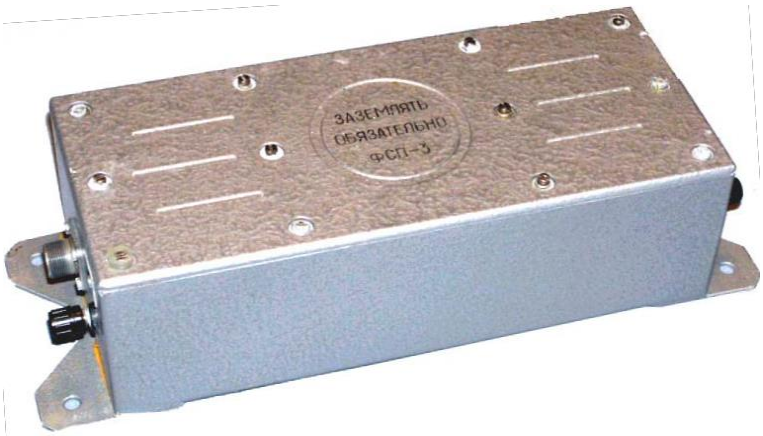


Рис. 1.8. Фільтр мережний противозавадний ФСП-3

– для ФСП-4 на частотах від 0,091 Мгц до 1 Мгц, дБ від 20 до 80; на частотах від 1 Мгц до 1 000 Мгц, дБ, не менше 80.

Розміри корпусів фільтрів, мм:

ФСП-1 430×150×80; ФСП-2 385×125×80; ФСП-3 345×125×80; ФСП-4 325×90×70.

Маса фільтрів, кг, не більше: ФСП-1 5,5; ФСП-2 5; ФСП-3 4; ФСП-4 2,5, ФСП-4 5.

Фільтри мережеві протизавадні типу ФМПЗ забезпечують ЗІ, що обробляється засобами оргтехніки та обчислювальної техніки, від витоку мережами електроживлення.

Фільтри захисні протизавадні типу ФЗП забезпечують ЗІ, що обробляється засобами обчислювальної та іншої оргтехніки, від витоку за рахунок побічних електромагнітних наводів на коло електроживлення, а також зменшення рівня імпульсних завад, які надходять на входи електроживлення апаратури, що підлягає захисту, з мережі електроживлення.

Фільтри мережні протизавадні типу М-9, М-17, М-23 тощо забезпечують подавлення електромагнітних завад та блокування ВІ мережею електроживлення. Для захисту ліній живлення і телефонних або інформаційних ліній широко застосо-вуються також фільтри типу ФСП1, ПЕТЛ, “Рікас-1” або “Рікас-2”, а також “Граніт-8”, що мають такі характеристики:

– діапазон частот – від 0,15 до 1000 МГц;
– максимальний струм 5 А;
– загасання складає 60 дБ;
– максимальна напруга по постійному струму 500 В;
– максимальна напруга по змінному струму 250 В при 50 Гц.

Крім того, при експлуатації сучасних ПЕОМ широко використовуються джерела безперебійного живлення (ДБЖ), які дозволяють забезпечити живлення комп'ютера при відключенні живлення мережі, а також дозволяють забезпечити захист від ВІ по ланцюгах живлення.

1.8. Просторове та лінійне зашумлення

Реалізація пасивних методів захисту, заснованих на застосуванні екранування й фільтрації, приводить до ослаблення рівнів побічних ЕМВ і наведень (НСиг) ТЗПІ і тим самим до зменшення відношення небезпечний сигнал/шум. Однак, у ряді випадків, незважаючи на застосування пасивних методів захисту, на границі КонтрЗ відношення сигнал/шум перевищує припустиме значення. У цьому випадку застосовуються активні міри захисту, засновані на створенні перешкод засобам розвідки, що також приводить до зменшення відношення сигнал/шум. Для виключення перехоплення побічних ЕМВ по електромагнітному каналу використовується *просторове зашумлення*, а для виключення знімання наведень інформаційних сигналів зі сторонніх провідників і з'єднувальних ліній ДТЗС – *лінійне зашумлення*.

До системи просторового зашумлення, яка застосовуєьтся для створення електромагнітних маскуючих перешкод, висуваються наступні вимоги:

– система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних ЕМВ ТЗПІ;
– створювані перешкоди не повинні мати регулярної структури;
– рівень створюваних перешкод (як по електричній, так і по магнітній складовій поля) повинен забезпечити відношення сигнал/шум на границі КонтрЗ менше припустимого значення у всьому діапазоні частот можливих побічних ЕМВ ТЗПІ;
– система повинна створювати перешкоди як з горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);
– на межі КонтрЗ рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати необхідних норм по електромагнітній сумісності (ЕМС).

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечний сигнал/шум на границі КонтрЗ не перевищує деякого припустимого значення, що розраховується по спеціальних

методиках для кожної частоти інформаційного (НСиг) побічного ЕМВ ТЗПІ.

У системах просторового зашумлення в основному використовуються перешкоди типу “білого шуму” або “синфазні перешкоди”. Системи, що реалізують метод “синфазної перешкоди”, в основному, застосовуються для захисту ПЕОМ. В них у якості завадового сигналу використовуються імпульсно-випадкові амплітуди, що збігаються (синхронізовані) за формою й часом існування з імпульсами корисного сигналу. Внаслідок цього по своєму спектральному складу завадовий сигнал аналогічний спектру побічних ЕМВ ПЕОМ. Тобто, система зашумлення генерує “імітаційну перешкоду”, по спектральному складу відповідну приховуваному сигналу. У даний час в основному застосовуються системи просторового зашумлення, що використовують перешкоди типу “білий шум”, тобто випромінюючі широкосмуговий шумовий сигнал (як правило, з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот), істотно перевищуючий рівні побічних ЕМВ. Такі системи застосовуються для захисту широкого класу технічних засобів: ЕОТ; систем звукопідсилення й звукового супроводу; систем внутрішнього телебачення та інших.

Основні характеристики генераторів шуму, що використовуються для просторового зашумлення, представлені в таблиці 1.6 [21, 25, 32].

Генератори шуму виконуються або у вигляді окремого блоку з живленням від мережі 220 В (“Гном”, “Волна”, “ГШ-1000” та ін.), або у вигляді окремої плати, що вбудовується у вільний слот системного блоку ПЕОМ та живиться від загальної шини комп’ютера (“ГШ-К-1000”, “Смог” та ін.). Генератори, виконані у вигляді окремого блоку, мають порівняно невеликі розміри й вагу. Наприклад, генератор шуму “Гном-3” при розмірах 307×95×49 мм важить 1,8 кг.

Діапазон робочих частот генераторів шуму від 0,01... 0,1 до 1000 МГц. При потужності випромінювання близько 20 Вт забезпечується спектральна щільність перешкоди 40 ... 80 дБ. У системах просторового зашумлення в основному використовуються слабо направлені рамкові тверді й гнучкі антени. Рамкові гнучкі антени виконуються зі звичайного проводу та розгортаються у двох-трьох площинах, що забезпечує формування завадового сигналу як з вертикальною, так і з горизонтальною поляризацією у всіх площинах. Останнім часом для створення електромагнітних завад в ефірі широко застосовуються прилади серії “РІАС-1С”, “РІАС-1М”, “РІАС-1К”, “РІАС-1В”.

Так, прилад ВЧ шуму стаціонарний РІАС-1С *призначений для створення електромагнітних перешкод в ефірі в діапазоні частот від 180 Гц до 2 ГГц.* До складу приладу входять генератор ВЧ шуму стаціонарний РІАС-1ГС та антени рамкові м’ягкі РІАС-1АМ. Коефіцієнт якості шуму – не менше 0,8. Коефіцієнт міжспектральних кореляційних

зв’язків – не менше 2,0. Нормований рівень спектральної щільності напруженості електричного і магнітного компонентів нормованого ЕМП шуму – не менше 30 дБ. Максимальне інтегральне значення вихідної потужності – не менше 10 Вт.

Таблиця 1.6.

Основні характеристики генераторів шуму, що використовуються в системах просторового зашумлення

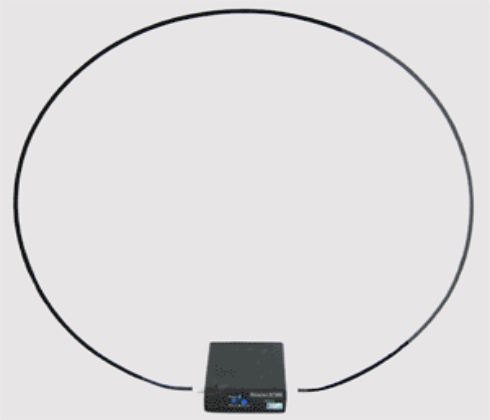
Найменування характеристик	Тип (модель)					
	ГШ-1000	ГШ-К-1000	“Смог”	“Гном-3”	“Гром-ЗИ-4”	“Гном-2С”
Діапазон частот, МГц	0,1-1000	0,1-1000	0,00005-1000	0,01-1000	20-1000	0,01-1000
Спектральна щільність потужності шуму, дБ	45-75	40-75	55….80	45….75	40-90	50-80
Вид антени	рамочна жорстка	рамочна м’яка	підставки під монітор та принтер	рамочна гнучка	телескопічна	рамочна
Конструктивне виконання	переносна	без корпусу вставляється в ПЕОМ	без корпусу вставляється в ПЕОМ	стаціонарна	переносна	стаціонарна

Пристрій “БАЗАЛЬТ - 5ГЕШ” (рис. 1.9) призначений для захисту об’єктів ЕОТ від ВІ по каналах побічних ЕМВ шляхом створення в навколишньому просторі ЕМП шуму в діапазоні частот від 0,1 до 1000 МГц.

У діапазонах частот до 1 МГц і понад 1000 МГц для електричної складової, до 0,1 МГц та понад 30 МГц для магнітної складової рівні ЕМП не нормуються. Пристрій є джерелом шумових електромагнітних сигналів, випромінюваних рамковою антеною. Пристрій призначений для експлуатації у виробничих приміщеннях підприємств і організацій.

У пристрої передбачена можливість автоматичного звукової та візуальної сигналізації у випадку виникнення неполадок у його роботі. Також передбачений режим дистанційного відключення пристрою шляхом подачі зовнішнього напруги (12 ± 1,2) В або замиканням відповідних контактів вихідного з’єднувача. При використанні систем просторового зашумлення необхідно пам’ятати, що поряд з перешкодами засобам розвідки створюються перешкоди й іншим радіоелектронним засоби (наприклад, системам телебачення, радіозв’язку й т. д.). Тому при введенні в експлуатацію системи просторового зашумлення необхідно проводити спеціальні дослідження з вимог забезпечення ЕМС. Крім того, рівні

перешкод, створювані системою зашумлення, повинні відповідати санітарно-гігієнічним нормам.



Технічні характеристики:

1. Діапазон частот 0,1-1000 МГц.

2. Напруга живлення 12 ± 0,6 В.

3. Споживана потужність не біль-ше 6,0 ВА.

4. Габаритні розміри пристрою (з випромінюючою антеною) не більше 750×750×50 мм.

5. Маса пристрою (з випромінюючою антеною) не більше 1,5 кг.

Рис. 1.9. Пристрій "Базальт - 5 ГЕШ"

Однак, норми, на рівні ЕМВ по вимогах ЕМС істотно суворіше санітарно-гігієнічних норм. Отже, основну увагу необхідно приділяти виконанню норм ЕМС.

Просторове зашумлення ефективно не тільки для закриття електромагнітного, але й електричного каналів ВІ, тому що завадовий сигнал при випромінювані наводиться в з'єднувальних лініях ДТЗС та сторонніх провідниках, що виходять за межі КонтрЗ.

Системи лінійного зашумлення застосовуються для маскування наведених НСиг у сторонніх провідниках і з'єднувальних лініях ДТЗС, що виходять за межі КонтрЗ. Вони використовуються в тому випадку, якщо не забезпечується необхідний рознос цих провідників та ОТЗ (тобто не виконується вимога по Зоні 1), однак при цьому забезпечується вимога по Зоні 2 (тобто відстань від ТЗПІ до границі КонтрЗ більше, ніж Зона 2). У найпростішому випадку система лінійного зашумлення являє собою генератор шумового сигналу, що формує маскуючу шумову напругу із заданими спектральними, часовими й енергетичними характеристиками, яка гальванічно підключається в зашумляєму лінію (сторонній провідник). На практиці найбільш часто подібні системи використовуються для зашумлення ліній електроживлення (наприклад, ліній електроживлення освітлювальної та розеточної мереж). Для захисту ІзОД на ОІД від її витоку мережами, лініями, проводами і колами технічних засобів систем пересилання, оброблення, зберігання та відображення інформації застосовується комплекс засобів лінійного ЗІ "РІАС-ЛЗ".

Питання та завдання для самостійної перевірки знань

1. Дайте характеристику основних ТКВІ при експлуатації ТЗПІ? Які напрями охоплюють рекомендації із ТЗІ при експлуатації ТЗПІ ?

2. Назвіть джерела можливого ВІ каналами ПЕМВН?

3. Наведіть призначення і технічні характеристики приладів “РІАС–1С” і “БАЗАЛЬТ - 5ГЕШ”?

4. Порівняйте захищеність різних ланцюгів від впливу зовні-ніх магнітних й електричних полів (рис. 7.1). Які схеми забезпечують захищеність на рівні не менше 50 дБ?

5. Яким повинно бути перехідне загасання у з’єднувальних лініях ТЗПІ і як воно забезпечується ?

6. Охарактеризуйте основні і додаткові способи екранування ОТЗ.

7. Назвіть призначення, види і характеристики засобів технічного заземлення.

8. Які існують засоби фільтрації сигналів у ланцюгах живлення ТЗПІ і які вимоги до них пред’являються ?

9. Яким чином здійснюється виключення перехоплення побічних ЕМВ по електромагнітному каналу?

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

2.1. Особливості технічних каналів витоку та захисту мовної інформації

МІ є однією з найпоширеніших і найбільш сприятливих для витоку, оскільки циркулює скрізь – від квартир окремих громадян чи офісу фірми або підприємства до кабінетів керівних посадових осіб, обробляється технічними засобами та пересилається на великі відстані.

Розвідка МІ може здійснюватись з використанням таких ТКВІ:

– акустичних – у яких Асиг, спричинені мовою, поширюються у повітрі;

– віброакустичних – у яких коливання (вібрації), спричинені АП, поширюються у твердих середовищах (будівельні конструкції, жорсткі комунікації тощо);

–побічних ЕМВ та наведень, що можуть спричинятися технічними засобами обробки МІ чи виникати у колах електро- радіоапаратури під впливом АП внаслідок мікрофонного ефекту.

Перелічені ТКВІ є ненавмисними. Крім того, з метою здобуття інформації ТЗР можуть створюватися навмисні (штучні) ТКВІ: ВЧ “нав’язуванням” та застосуванням ЗП.

Канал ВЧ “нав’язування” створюється шляхом посилання ВЧ сигналу лініями зв’язку, іншими дротовими комунікаціями чи спрямованим променем до технічних засобів із-за меж КонтрЗ та приймання радіовипромінювань, промодульованих мовним сигналом у нелінійних елементах технічних засобів.

Пошук та виявлення ЗП є однією з проблем ТЗІ, однак такий спосіб несанкціонованого здобування інформації має свої особливості, які

розглядалися раніше. Як і для ТЗПІ, існують пасивні і активні методи захисту МІ від несанкціонованого прослуховування.

Пасивні – передбачають ослаблення Асиг, що циркулюють в приміщенні, а також наслідків електроакустичних перетворень в з'єднувальних лініях ДТЗС. Ослаблення Асиг (мовних) здійснюється шляхом звукоізоляції приміщень.

Ослаблення інформаційних електричних сигналів у сполучних лініях ДТЗС і виключення (ослаблення) проходження сигналів ВЧ нав'язування в ДТЗС здійснюється методами фільтрації сигналів.

В основі активних методів захисту акустичної інформації лежить створення маскувальних перешкод за допомогою генераторів перешкод, придушення апаратури звукозапису і підслуховуючих пристроїв, а також знищення останніх.

Організація захисту МІ у ТЗПІ здійснюється відповідно до вимог і рекомендацій нормативних документів НД ТЗІ 2.7-008-08, НД ТЗІ Р-001-2000, НД ТЗІ 2.2-006-08, НД ТЗІ 2.3-017-08, НД ТЗІ 2.7-008-08.

2.2. Звукоізоляція приміщень

Звукоізоляція приміщень спрямована на локалізацію джерел Асиг усередині них і проводиться з метою виключення перехоплення акустичної (мовної) інформації по прямому акустичному (через щілини, вікна, двері, технологічні прорізи, вентиляційні канали й інше) і вібраційному (через конструкції, що обгороджують, труби водо-, тепло- та газопостачання, каналізації й інше) каналах.

Основна вимога до звукоізоляції приміщень полягає в тому, щоб за їх межами відношення акустичний сигнал/шум не перевищувало деякого припустимого значення, що виключає виділення засобом розвідки мовного сигналу на фоні природних шумів. Тому до приміщень, у яких проводяться закриті заходи, пред'являються певні вимоги по звукоізоляції. Звукоізоляція оцінюється величиною ослаблення Асиг.

З огляду на те, що середня гучність звуку мовця в службовому приміщенні становить близько 50 ... 60 дБ, то залежно від категорії приміщення його звукоізоляція повинна бути не менш норм, наведених у табл. 2.1 [21, 25].

Звукоізоляція приміщень забезпечується за допомогою архітектурних та інженерних рішень, а також застосуванням спеціальних будівельних й оздоблювальних матеріалів.

При падінні Ахв на межу поверхонь із різними значеннями питомої щільності більша частина падаючої хвилі відбивається.

Менша частина хвилі проникає в матеріал звукоізолюючої конструкції й поширюється в ньому, гублячи свою енергію залежно від довжини шляху і його акустичних властивостей. Під дією Ахв звукоізолююча поверхня робить складні коливання, які також поглинають енергію

падаючої хвилі. Характер цього поглинання визначається співвідношенням частот падаючої Ахв й спектральних характеристик поверхні засобу звукоізоляції.

Таблиця 2.1.

Вимоги до звукоізоляції приміщень

Частота, Гц	Категорія виділеного приміщення, дБ		
	1	2	3
500	53	48	43
1 000	56	51	46
2 000	56	51	46
4 000	55	50	45

Одним з найбільш слабких звукоізолюючих елементів обгороджуючих конструкцій виділених приміщень є двері й вікна. Двері мають істотно менші в порівнянні зі стінами й міжповерховими перекриттями поверхневі щільності й складно ущільнювальні зазори й щілини.

Стандартні двері не задовольняють вимогам по ЗІ (табл. 2.2) [21, 25].

Збільшення звукоізолюючої здатності дверей досягається щільним пригоном полотна двері до коробки, усуненням щілин між дверима й підлогою, застосуванням ущільнювальних прокладок, оббивкою або облицюванням полотен дверей спеціальними матеріалами й інше. Як видно з табл. 2.2, застосування ущільнювальних прокладок підвищує звукоізоляцію дверей, однак при цьому необхідно враховувати, що в процесі експлуатації в результаті обтиснення, зношування, корозії гумових прокладок звукоізоляція істотно знижується.

Таблиця 2.2

Звукоізоляція звичайних дверей

Конструкція двері	Умови використання	Звукоізоляція (дБ) на частотах, Гц					
		125	250	500	1000	2000	4000
Щитові двері, що облицьовані фанерою з двох сторін	без прокладки	21	23	24	24	24	23
	з прокладкою із пористої резини	27	27	32	35	34	35
Типові двері П-327	без прокладки	13	23	31	33	34	36
	з прокладкою із пористої резини	29	30	31	33	34	41

Для ЗІ в особливо важливих приміщеннях використовуються двері з тамбуром, а також спеціальні двері з підвищеною звукоізоляцією.

Для підвищення звукоізоляції проводиться облицювання внутрішніх поверхонь тамбура звуковбирними покриттями, а двері оббиваються

матеріалами із шарами вати або повсті й використовуються додаткові ущільнювальні прокладки.

Звуковбирна здатність вікон, так само як і дверей, залежить, головним чином, від поверхневої щільності скла й ступеня притиснення притворів. У табл. 2.3 [21, 25] зазначені деякі дані по звукоізоляції найпоширеніших варіантів вікон приміщень.

Таблиця 2.3

Звукоізоляція вікон

Схема вікон	Звукоізоляція (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарне скло:						
товщина 3 мм	17	17	22	28	31	32
товщина 4 мм	18	23	26	31	32	32
товщина 6 мм	22	22	26	30	27	25
Подвійне скло с повітряним проміжком:						
57 мм (товщина 3 мм)	15	20	32	41	49	46
90 мм (товщина 3 мм)	21	29	38	44	50	48
57 мм (товщина 4 мм)	21	31	38	46	49	35
90 мм (товщина 4 мм)	25	33	41	47	48	36

Звукоізоляція вікон з одинарним склом порівнянна зі звукоізоляцією одинарних дверей і є недостатньою для надійного ЗІ в приміщенні. Істотно більшу звукоізоляцію мають вікна зі склом у роздільних плетіннях із шириною повітряного проміжку більше 200 мм або потрійне комбіноване скло.

Звичайні вікна з подвійними плетіннями володіють більше високою (на 4 – 5 дБ) звукоізолюючою здатністю в порівнянні з вікнами зі спареними плетіннями. Застосування пружних прокладок значно поліпшує звукоізоляційні якості вікон. У випадках, коли необхідно забезпечити підвищену звукоізоляцію, застосовують вікна спеціальної конструкції (наприклад, подвійне вікно із заповненням віконного прорізу органічним склом товщиною 20 ... 40 мм і з повітряним зазором не менш 100 мм).

Розроблено конструкції вікон з підвищеним звукопоглинанням на основі склопакетів з герметизацією повітряного проміжку й із заповненням його різними газовими сумішами або створення в ньому вакууму. Підвищення звукоізоляції до 5 дБ спостерігається при облицюванні простору між стеклами по периметру звуковбирним покриттям.

Необхідно відзначити, що збільшення числа стекол не завжди приводить до збільшення звукоізоляції в діапазоні частот мовного сигналу внаслідок резонансних явищ у повітряних проміжках та ефекту хвильового збігу.

Для підвищення звукоізоляції в приміщеннях застосовують АЕ, що встановлюються на шляху поширення звуку на найнебезпечніших (з погляду розвідки) напрямках.

Дія АЕ заснована на відбитті звукових хвиль й утворенні за екраном звукових тіней. З урахуванням дифракції ефективність екрана підвищується зі збільшенням співвідношення розмірів екрана й довжини Ахв. Розміри ефективних екранів перевищують більш ніж в 2−3 рази довжину хвилі. Ефективність АЕ, що досягається реально, становить 8 ... 10 дБ.

Застосування АЕ доцільно при тимчасовому використанні приміщення для захисту акустичної інформації. Найбільш часто застосовуються складні АЕ, які використовуються для додаткової звукоізоляції дверей, вікон, технологічних прорізів, систем кондиціонування, проточної вентиляції й інших елементів конструкцій, що мають звукоізоляцію, яка не задовольняє діючим нормам.

Для підвищення звукоізоляції приміщень також застосовують звуковбирні матеріали. Звукопоглинання забезпечується шляхом перетворення кінетичної енергії Ахв в теплову енергію у звуковбирному матеріалі.

Звуковбирні властивості матеріалів оцінюються коефіцієнтом звукопоглинання, обумовленим відношенням енергії звукових хвиль, поглиненої в матеріалі, до падаючої на поверхню матеріалу й проникаючої (невідбитої) у звуковбирний матеріал.

Застосування звуковбирних матеріалів при захисті акустичної інформації має деякі особливості у порівнянні зі звукоізоляцією. Однієї з особливостей є необхідність створення безпосередньо в приміщенні акустичних умов для забезпечення розбірливості мови в різних його зонах.

Такою умовою є насамперед забезпечення оптимального співвідношення прямого й відбитого від огороджень Асиг.

Надмірне звукопоглинання приводить до погіршення рівня сигналу в різних точках приміщення, а великий час реверберації – до погіршення розбірливості в результаті накладання різних звуків.

Забезпечення раціональних значень розглянутих умов визначається як загальною кількістю звуковбирних матеріалів у приміщенні, так і розподілом звуковбирних матеріалів по конструкціях, що обгороджують, з урахуванням конфігурації й геометричних розмірів приміщень.

Звуковбирні матеріали можуть бути суцільними й пористими. Пористі матеріали використовують у сполученні із суцільними. Один із розповсюджених видів пористих матеріалів – лицювальні звуковбирні матеріали. Їх виготовляють у вигляді плоских плит (плити мінераловатні “Акмигран”, “Акант”, “Силаклор”, “Винипор”, ПА/З, ПА/ПРО, ПП-80, ППМ, ПММ) або рельєфних конструкцій (пірамід, клинів та інше), що

розташовуються або впритул, або на невеликій відстані від суцільної будівельної конструкції (стіни, перегородки, огородження й інше).

Використовуються також звуковбирні облицювання із шару пористо-волокнистого матеріалу (скляного або базальтового волокна, мінеральної вати) у захисній оболонці із тканини або плівки з перфорованим покриттям (металевим, гіпсовим й ін.).

Пористі звуковбирні матеріали малоефективні на НЧ. Окрему групу звуковбирних матеріалів становлять резонансні поглиначі. Вони підрозділяються на *мембранні* й *резонаторні*.

Мембранні поглиначі являють собою натягнуте полотно (тканина), тонкий фанерний (картонний) аркуш, під яким розташовують матеріал, що добре демпфірує (матеріал з великою в'язкістю, наприклад, поролон, губчата гума, будівельну повсть і інше).

У такого роду поглиначах максимум поглинання досягається на резонансних частотах.

Перфоровані резонаторні поглиначі являють собою систему повітряних резонаторів (наприклад, резонаторів Гельмгольця), в усті яких розташований матеріал, що демпфірує.

Середні значення звукоізоляції деяких матеріалів наведені в таблиці 2.4 [21, 25, 31, 32].

Таблиця 2.4

Звуковбирні властивості деяких матеріалів

Матеріал	Коефіцієнт поглинання на частотах, Гц					
	125	250	500	1000	2000	4000
Цегельна стена	0,024	0,025	0,032	0,041	0,049	0,07
Дерев'яна оббивка	0,1	0,11	0,11	0,08	0,082	0,11
Скло одинарне	0,03	*	0,027	*	0,02	*
Штукатурка вапняна	0,025	0,04	0,06	0,085	0,043	0,058
Повсть (товщиною 25 мм)	0,18	0,36	0,71	0,8	0,82	0,85
Ковдра с ворсом	0,09	0,08	0,21	0,27	0,27	0,37
Скляна вата (товщиною 9 мм)	0,32	0,4	0,51	0,6	0,65	0,6
Бавовняна ткань	0,03	0,04	0,11	0,17	0,24	0,35

Підвищення звукоізоляції стін і перегородок приміщень досягається застосуванням одношарових і багатошарових (частіше – подвійних) огороджень.

У багатошарових огородженнях доцільно підбирати матеріали шарів з акустичними опорами, що різко відрізняються (наприклад, бетон – поролон).

Значення ослаблення звуку огородженнями, виконаними з деяких часто застосовуваних будівельних матеріалів, зазначені в таблиці 2.5.

Між приміщеннями будинків і споруджень проходить багато технологічних комунікацій (труби тепло-, газо-, водопостачання та

каналізації, кабельна мережа енергопостачання, вентиляційні короби і т. д.). Для них у стінах і перекриттях споруджень роблять відповідні отвори й прорізи.

Таблиця 2.5

Звуковбирні властивості деяких будівельних конструкцій

Матеріал	Товщина	Звукоізоляція на частотах (Гц), дБ					
		125	250	500	1000	2000	4000
Цегляна стіна	1/2 цегли	39	40	42	48	54	60
Обштукату-рена із двох сторін стіна	1 цегла	36	41	44	51	58	64
	1,5 цегли	41	44	48	55	61	65
	2 цегли	45	45	52	59	65	70
	2,5 цегли	47	55	60	67	70	70
Стіна із залізобетонних блоків	40 мм	32	36	35	38	47	53
	100 мм	40	40	44	50	55	60
	200 мм	42	44	51	59	65	65
	300 мм	45	50	58	65	69	69
	400 мм	48	55	61	68	70	70
	800 мм	55	61	68	70	70	70
Стіна зі шлакоблоків	220 мм	42	42	48	54	60	63
Перегородка із дерево – стружкової плити	20 см	23	26	26	26	26	26

Їх надійна звукоізоляція забезпечується застосуванням спеціальних гільз, коробів, прокладок, глушників, в’язкопружних заповнювачів і т. п. Забезпечення необхідної звукоізоляції у вентиляційних каналах досягається використанням складних акустичних фільтрів та глушників.

Варто мати на увазі, що в загальному випадку звукоізоляція обгороджуючих конструкцій, утримуючих декілька елементів, повинна оцінюватися звукоізоляцією найбільш слабкого з них.

Більш високою акустичною ефективністю (більшим коефіцієнтом ослаблення) володіють кабіни безкаркасного типу. Вони збираються з готових багатошарових щитів, з’єднаних між собою через звукоізолюючі пружні прокладки.

Такі кабіни коштовні у виготовленні, але зниження рівня звуку в них може досягати 50 ... 55 дБ. Для підвищення звукоізоляції кабіни мінімізують можливе число стикувальних з’єднань окремих панелей між собою та каркасом кабіни.

Ретельно герметизують й ущільнюють стикувальні з’єднання, застосовують звуковбирні облицювання стін і стелі. У системах вентиляції й кондиціонування повітря встановлюють спеціальні глушники звуку.

Звукоізолюючі кабіни залежно від вимог до звукоізоляції підрозділяються на 4 класи. У діапазоні 63 – 8 000 Гц кабіни повинні забезпечувати ізоляцію звуку [21, 25]:

1-го класу – на 25 ... 50 дБ;

2-го класу – на 15 ... 49 дБ;

3-го й *4-го класів* – 15 ... 39 й 15 ... 29 дБ відповідно.

Найменші значення відповідають НЧ, найбільші – високим (2 000 – 4 000 Гц).

2.3. Віброакустичне маскування

У випадку, якщо наявні пасивні засоби захисту приміщень не забезпечують необхідних норм по звукоізоляції, необхідно використовувати активні міри захисту.

Активні міри захисту полягають у створенні Амаск перешкод засобам розвідки, тобто використанні віброакустичного маскування інформаційних сигналів. На відміну від звукоізоляції приміщень, що забезпечує необхідне ослаблення інтенсивності звукової хвилі за їхніми межами, використання активного Амаск знижує відношення сигнал/шум на вході ТЗР за рахунок збільшення рівня шуму (перешкоди).

Віброакустичне маскування ефективно використовується для захисту МІ від витоку по прямому акустичному, віброакустичному й оптико-електронному каналам ВІ.

Для формування акустичних перешкод застосовуються спеціальні генератори, до виходів яких підключені гучномовці або вібраційні випромінювачі (вібродатчики).

На практиці найбільш широке застосування знайшли генератори шумових коливань. Саме тому активне Амаск часто називають акустичним зашумленням. Більшу групу генераторів шуму становлять пристрої, принцип дії яких заснований на посиленні коливань первинних джерел шумів. Як джерела шумових коливань використовуються електровакуумні, газорозрядні, напівпровідникові й інші електронні прилади та елементи.

Часовий випадковий процес, близький по своїх властивостях до шумових коливань, може бути отриманий і за допомогою цифрових генераторів шуму, що формують послідовності двійкових символів, що називаються псевдовипадковими.

Поряд із шумовими перешкодами з метою активного Амаск використовують й інші перешкоди, наприклад, “одночасна розмова кількох людей”, хаотичні послідовності імпульсів та інше. Роль кінцевих пристроїв, що здійснюють перетворення електричних коливань в АКол мовного діапазону, звичайно виконують малогабаритні широкосмугові гучномовці, а здійснююче перетворення електричних коливань у вібраційні – вібраційні випромінювачі (вібродатчики).

Гучномовці систем зашумлення встановлюються в приміщенні в місцях найбільш імовірного розміщення засобів акустичної розвідки, а вібродатчики кріпляться на рамах, склі, коробах, трубопроводах, стінах, стелях тощо.

Створювані вібродатчиками шумові коливання в обгород-жуючих конструкціях, трубах, шибках й т. п. приводять до значного підвищення в них рівня вібраційних шумів і тим самим – до істотного погіршення умов прийому й відновлення мовних повідомлень засобами розвідки.

У теперішній час створено велику кількість різних систем активного віброакустичного маскування, успішно використовуваних для придушення засобів перехоплення МІ. До них відносяться: системи “Заслін”, “Кабінет”, “Барон”, “В”, “ОЦЗІ-ВА”, VNG-006 DM, ANG-2000, “МАРС-ТЗО”, “Волна”, “РІАС”, “Базальт” та інші (табл. 2.6).

До складу типової системи віброакустичного маскування входять шумогенератор і від 6 до 12 – 25 вібродатчиків (п’єзокерамічних або електромагнітних). Додатково до складу системи можуть включатися звукові стовпчики (спікери).

Таблиця 2.6.

Основні характеристики систем віброакустичного зашумлення

Найменування характеристик	Модель (тип)		
	VNG – 006 DM	ANG - 2000	“Заслін – 2М”
Смуга частот ефективного захисту на перекритті товщиною 0,25 м, кГц	0,25 … 5,0	0,25 … 5,0	0,1 … 5,0
Максимальна кількість вібродатчиків, шт.	12	18	25
Тип та принцип дії вібродатчиків	КВП-2, КВП-6, КВП -7 (п’єзокерамічні)	TRN-2000 (електромагнітні)	Електромагнітні
Ефективний радіус придушення вібродатчика на перекритті товщиною 0,25 мм	4	5	1,5
Габарити вібродатчиків, мм	Ø 40×30, Ø 50×39, Ø 33×8	Ø 100×338	46×65×53

У комплекс “Барон”, крім звичайного генератора шуму, включені три радіоприймачі, настроєні незалежно на різні радіомовні станції FM (УКВ-2) діапазону. Змішані сигнали цих станцій використовуються в якості перешкодового сигналу, що значно підвищує ефективність перешкоди.

Для повного захисту приміщення по віброакустичному каналу вібродатчики повинні встановлюватися на всіх обгороджуючих конструкціях (стінах, стелі, підлозі), шибках, а також трубах, що проходять через приміщення. Необхідна кількість вібродатчиків для захисту приміщення визначається не тільки його площею, кількістю вікон і труб, що проходять через нього, але й ефективністю датчиків (ефективний

радіус дії вібродатчиків на перекритті товщиною 0,25 м становить від 1,5 до 5 м).

У ряді систем віброакустичного маскування можливе регулювання рівня перешкодового сигналу. Наприклад, у системах “Кабінет” та ANG-2000 здійснюється ручне плавне регулювання рівня перешкодового сигналу, а в системі “Заслін-2М” – автоматичне (залежно від рівня маскуючого мовного сигналу). У комплексі “Барон” можливе незалежне регулювання рівня перешкодового сигналу в трьох частотних діапазонах (центральні частоти: 250, 1 000 й 4 000 Гц).

Для захисту виділених приміщень в основному розгортаються стаціонарні системи віброакустичного маскування, в той же час для захисту приміщень, що тимчасово використовуються для проведення закритих заходів, можуть застосовуватися і мобільні системи. До таких систем відноситься, наприклад, мобільна система віброакустичного зашумлення “В”. До складу системи входять: генератор ANG-2000, вібродатчики TRN-2000 та TRN-2000M й металеві штанги для кріплення датчиків до будівельних конструкцій. Система забезпечує захист приміщення площею до 25 м^2.

Монтаж (демонтаж) системи здійснюється трьома фахівцями протягом 30 хвилин без ушкодження будівельних конструкцій й елементів обробки інтер’єру.

Для створення акустичних перешкод у невеликих приміщеннях або салоні автомобіля можуть використовуватися малогабаритні акустичні генератори, наприклад, WNG-023. Генератор має розміри 111×70×22 мм та створює перешкодовий (типу “білий шум”) Асиг у діапазоні частот від 100 до 12000 Гц потужністю 1 Вт. Живлення генератора здійснюється від елемента типу “Крона” або мережі 220 В.

При організації Амаск необхідно пам’ятати, що акустичний шум може створювати для співробітників додаткові фактори, що заважають, та впливають на нервову систему людини, викликаючи різні функціональні відхилення й приводять до швидкої й підвищеної стомлюваності працюючих у приміщенні. Ступінь впливу перешкод, що заважають, визначається санітарними нормативами на величину акустичного шуму. Відповідно до норм для установ величина шуму, що заважає, не повинна перевищувати сумарний рівень 45 дБ.

2.4. Методи й засоби захисту телефонних апаратів

При захисті ТА і ТЛ необхідно враховувати кілька аспектів:

– *ТА* (навіть при покладеній трубці) можуть бути використані для перехоплення акустичної МІ із приміщень, у яких вони встановлені, тобто для підслуховування розмов у цих приміщеннях;

– *ТЛ,* що проходять через приміщення, можуть використовуватися як джерела живлення акустичних закладок, установлених у цих приміщеннях, а також для передачі перехопленої інформації;

– *можливе перехоплення (підслуховування) телефонних розмов* шляхом гальванічного або через індукційний датчик підключення до ТЛ, закладок (телефонних ретрансляторів), диктофонів й інших засобів несанкціонованого знімання інформації.

ТА має кілька елементів, що мають здатність перетворювати АКол в електричні, тобто, що володіють "мікрофонним ефектом". До них відносять: дзвінковий ланцюг, телефонний й, звичайно, мікрофонний капсулі. За рахунок електроакустичних перетворень у цих елементах виникають інформаційні (НСиг) сигнали.

При покладеній трубці телефонний і мікрофонний капсулі гальванічно відключені від ТЛ, але при підключенні до неї спеціальних високочутливих НЧ підсилювачів можливе перехоплення НСиг, що виникають в елементах тільки дзвінкового ланцюга. Амплітуда цих НСиг, як правило, не перевищує часток мВ.

При використанні для знімання інформації методу "ВЧ нав'язування", незважаючи на гальванічне відключення мікрофона від ТЛ, сигнал нав'язування завдяки ВЧ проходить у мікрофонний ланцюг і модулюється по амплітуді інформаційним сигналом.

Отже, у ТА необхідно захищати як дзвінковий ланцюг, так і ланцюг мікрофона. Для захисту ТА від ВІ (акустичної, мовної) по електроакустичному каналу використовуються як *пасивні*, так й *активні* методи й засоби.

До найбільше широко застосовуваних *пасивних* методів захисту відносяться:

– обмеження НСиг;

– фільтрація НСиг;

– відключення перетворювачів (джерел) НСиг.

Можливість обмеження НСиг ґрунтується на нелінійних властивостях напівпровідникових елементів, головним чином діодів. У схемі обмежувача малих амплітуд використовуються два зустрічно-включених діоди. Такі діоди мають великий опір (сотні кОм) для струмів малої амплітуди й одиниці Ом і менш – для струмів великої амплітуди (корисних сигналів), що виключає проходження НСиг малої амплітуди в ТЛ й практично не впливає на проходження через діоди корисних сигналів. Діодні обмежувачі включаються послідовно в лінію дзвінка або безпосередньо в кожну з ТЛ.

Фільтрація НСиг використовується головним чином для захисту ТА від "ВЧ нав'язування". Найпростішим фільтром є конденсатор, який встановлюється у дзвінковий ланцюг ТА з електромеханічним дзвінком або у мікрофонний ланцюг усіх апаратів. Ємність конденсаторів

вибирається такої величини, щоб зашунтувати зондувальні сигнали ВЧ нав'язування й не робити істотного впливу на корисні сигнали. Звичайно для встановлення у дзвінковий ланцюг використовуються конденсатори ємністю 1 мкФ, а для встановлення у мікрофонний ланцюг – ємністю 0,01 мкФ. Більше складний фільтруючий пристрій являє собою багатоланковий фільтр НЧ на *LC*-елементах.

Для захисту ТА, як правило, використовують пристрої, що об'єднують фільтр й обмежувач. До них відносять: пристрої типу "Екран", "Граніт-8", "Корунд", "Грань-300", "ПЗТА", "РІАС", "Базальт-31" й інші.

Відключення ТА від лінії при веденні в приміщенні конфіденційних розмов є найбільш ефективним методом ЗІ.

Найпростіший спосіб реалізації цього методу захисту полягає в установці в корпусі ТА або ТЛ спеціального вимикача, що вмикається й виключається вручну. Більше зручним в експлуатації є установка в ТЛ спеціального пристрою захисту, що автоматично (без участі оператора) відключає ТА від лінії при покладеній слухавці.

До типових пристроїв, що реалізують даний метод захисту, відноситься виріб "Бар'єр-М1". У його склад входять:

– електронний комутатор;

– схема аналізу стану ТА, наявності викличних сигналів і керування комутатором;

– схема захисту ТА від впливу високовольтних імпульсів.

Пристрій працює в наступних режимах: черговому, передачі сигналів виклику й робочому. *У черговому режимі* (при покладеній слухавці) ТА відключений від лінії, і пристрій перебуває в режимі аналізу підняття слухавки та наявності сигналів виклику.

При цьому опір розв'язки між ТА і лінією АТС становить не менш 20 МОм. Напруга на виході пристрою в черговому прийомі становить 5...7 В. При одержанні сигналів виклику пристрій переходить у *режим передачі сигналів* виклику, при якому через електронний комутатор ТА підключається до лінії. Підключення здійснюється тільки на час дії сигналів виклику.

При піднятті слухавки пристрій переходить у *робочий режим* і ТА підключається до лінії. Перехід пристрою із чергового в робочий режим здійснюється при струмі в ТЛ не менш 5 мА. Виріб встановлюється в розрив ТЛ, як правило, при виході її з виділеного (захищаємого) приміщення або в розподільному щитку (кросі), що перебуває в межах КонтрЗ. Електроживлення пристрою здійснюється від ТЛ при струмі споживання в черговому режимі не більше 0,3 мА. Пристрій "Бар'єр-М1" забезпечує захист ТА не тільки від ВІ по електроакустичному каналу, але також і його захист від впливу високовольтних імпульсів (напругою до 1000 В та тривалістю до 100 мкс).

Активні методи захисту від ВІ по електроакустичному каналу передбачають лінійне зашумлення ТЛ. Шумовий сигнал подається в лінію в режимі, коли ТА не використовується (трубка покладена). При знятті трубки ТА подача в лінію шумового сигналу припиняється.

Для захисту акустичної (мовної) інформації у виділених приміщеннях поряд із захистом ТА необхідно приймати міри й для захисту безпосередньо ТЛ, тому що вони можуть використовуватися як джерела живлення акустичних закладок, установлених у приміщеннях, а також для передачі інформації, одержуваної цими закладками.

2.5. Методи й засоби захисту телефонних ліній

Для захисту безпосередньо ТЛ використовуються як *пасивні*, так й *активні* методи й засоби захисту. *Пасивні методи* захисту засновані на блокуванні акустичних закладок, що живляться від ТЛ в режимі покладеної трубки, а *активні* – на лінійному зашумленні ліній і знищенні (електричному "випалюванні") заставних пристроїв або їхніх блоків живлення шляхом подачі в лінію високовольтних імпульсів.

Захист телефонних розмов від перехоплення здійснюється головним чином *активними* методами.

До основних з них відносять:

– подача під час розмови в ТЛ синфазного НЧ маскуючого сигналу (*метод синфазної НЧ маскуючої перешкоди*);

– подача під час розмови в ТЛ ВЧ маскуючого сигналу звукового діапазону (*метод ВЧ маскуючої перешкоди*);

– подача під час розмови в ТЛ ультразвукового ВЧ маскуючого сигналу (*метод ультразвукової маскуючої перешкоди*);

– підняття напруги в ТЛ під час розмови (*метод підвищення напруги*);

– подача під час розмови у лінію напруги, що компенсує постійну складову телефонного сигналу (*метод* "*обнулення"*);

– подача в лінію при покладеній слухавці НЧ маскуючого сигналу (*метод НЧ маскуючої перешкоди*);

– подача в лінію при прийомі повідомлень маскуючого НЧ сигналу (мовного діапазону) з відомим спектром (*компенсаційний метод*);

– подача в ТЛ високовольтних імпульсів (*метод "випалювання"*).

Суть *методу синфазної маскуючої НЧ перешкоди* полягає в подачі в кожний провід ТЛ з використанням єдиної СЗ апаратури АТС і нульового проводу електромережі (нульовий провід електромережі заземлений) погоджених по амплітуді й фазі маскуючих сигналів мовного діапазону частот (як правило, основна потужність перешкоди зосереджена в діапазоні частот стандартного телефонного каналу: 300 ... 3 400 Гц). У ТА ці завадові сигнали компенсують один одного й не роблять заважаючого впливу на корисний сигнал (телефонна розмова).

Якщо ж інформація знімається з одного проводу ТЛ, то завадовий сигнал не компенсується. Завдяки тому, що його рівень значно перевершує корисний сигнал, перехоплення інформації (виділення корисного сигналу) стає неможливим.

У якості маскуючого завадового сигналу, як правило, використовують дискретні сигнали (ПВП імпульсів).

Метод синфазного НЧ маскуючого сигналу використовується для придушення телефонних радіозакладок (як з параметричною, так і із кварцовою стабілізацією частоти) з послідовним (у розрив одного із проводів) включенням, а також телефонних радіозакладок та диктофонів з підключенням до лінії (до одного із проводів) за допомогою індукційних датчиків різного типу.

Метод ВЧ маскуючої перешкоди полягає в подачі під час розмови в ТЛ широкосмугового маскуючого сигналу у діапазоні ВЧ звукового діапазону.

Даний метод використовується для придушення практично всіх типів пристроїв, що підслуховують, як контактного (паралельного й послідовного) підключення до лінії, так і підключення з використанням індукційних датчиків. Однак ефективність придушення засобів знімання інформації з підключенням до лінії за допомогою індукційних датчиків (особливо тих що не мають попередніх посилювачів) значно нижче, ніж засобів з гальванічним підключенням до лінії.

В якості маскуючого сигналу використовують широкосмугові аналогові сигнали типу “білого шуму” або дискретні сигнали типу ПВП імпульсів. Частоти маскуючих сигналів підбираються таким чином, щоб після проходження селективних ланцюгів модулятора закладки або мікрофонного підсилювача диктофону їхній рівень виявився достатнім для придушення корисного сигналу (мовного сигналу в ТЛ під час розмов абонентів), але в той же час ці сигнали не погіршували якість телефонних розмов.

Чим нижче частота завадового сигналу, тим вище його ефективність і тим більший заважаючий вплив він робить на корисний сигнал. Звичайно, використовуються частоти в діапазоні від 6 ... 8 кГц до 16 ... 20 кГц. Наприклад, у пристрої *“Sel SP-17/T”* перешкода створюється в діапазоні 8 ... 10 кГц.

Такі маскуючі перешкоди викликають значні зменшення відношення сигнал/шум і викривлення корисних сигналів (погіршення розбірливості мови) при перехопленні їх всіма типами підслуховуючих пристроїв. Крім того, у радіозакладок з параметричною стабілізацією частоти (“м’яким” каналом) як послідовного, так і паралельного включення спостерігається “відхід” несучої частоти, що може привести до втрати каналу прийому.

Для виключення маскуючого впливу завадового сигналу на телефонну розмову в пристрій захисту встановлюється спеціальний НЧ фільтр із

граничною частотою 3,4 кГц, що придушує (шунтує) завадові сигнали й не робить істотного впливу на проходження корисних сигналів. Аналогічну роль виконують смугові фільтри, що встановлені на міських АТС, які пропускають сигнали, частоти яких відповідають стандартному телефонному каналу (300 Гц ... 3,4 кГц), і не пропускають завадовий сигнал.

Метод ультразвукової маскуючої перешкоди в основному аналогічний розглянутому вище.

Відмінність полягає в тому, що використовуються завадові сигнали ультразвукового діапазону із частотами від 20 ... 25 кГц до 50 ... 100 кГц.

Метод підвищення напруги полягає у піднятті напруги в ТЛ під час розмови та використовується для погіршення якості функціонування телефонних радіозакладок. Підняття напруги в лінії до 18 ... 24 В викликає в радіозакладці з послідовним підключен-ням і параметричною стабілізацією частоти, "відхід" несучої частоти й погіршення розбірливості мови внаслідок розмиття спектра сигналу.

У радіозакладок з послідовним підключенням і кварцовою стабілізацією частоти спостерігається зменшення відношення сигнал/шум на 3 ... 10 дБ. Телефонні радіозакладки з паралельним під-ключенням при таких напругах у ряді випадків просто відключаються.

Метод "обнуління" передбачає подачу під час розмови в лінію постійної напруги, що відповідає напрузі в лінії при піднятій слухавці, але зворотної полярності.

Цей метод використовується для порушення функціонування підслуховуючих пристроїв з контактним паралельним підключенням до лінії та які використовують її в якості джерела живленням. До таких пристроїв відносять: паралельні ТА; провідні мікрофонні системи з електронними мікрофонами, що використовують ТЛ для передачі інформації; акустичні й телефонні закладки з живленням від ТЛ й інше.

Метод НЧ маскуючої перешкоди полягає в подачі в лінію при покладеній слухавці маскуючого сигналу (найбільш часто, типу "білого шуму") мовного діапазону частот (як правило, основна потужність перешкоди зосереджена в діапазоні частот стандартного телефонного каналу: 300 ... 3400 Гц) і застосовується для придушення провідних мікрофонних систем, що використовують ТЛ для передачі інформації на НЧ, а також для активізації (включення на запис) диктофонів, що підключають до ТЛ за допомогою адаптерів або індукційних датчиків, що приводить до змотування плівки в режимі запису шуму (тобто при відсутності корисного сигналу).

Компенсаційний метод використовується для однобічного маскування (приховання) мовних повідомлень, переданих абонентові по ТЛ. Суть методу полягає в наступному. При передачі прихованого повідомлення на прийомній стороні в ТЛ за допомогою спеціального генератора подається

маскуюча перешкода (цифровий або аналоговий маскуючий сигнал мовного діапазону з відомим спектром). Одночасно цей же маскуючий сигнал (“чистий” шум) подається на один із входів двоканального адаптивного фільтра, на інший вхід якого надходить адитивна суміш прийнятого корисного сигналу − мовного сигналу (переданого повідомлення) і цього ж завадового сигналу. Адитивний фільтр компенсує (придушує) шумову складову й виділяє корисний сигнал, що подається на ТА або пристрій звукозапису. Недоліком даного методу є те, що маскування мовних повідомлень однобічне й не дозволяє вести двосторонні телефонні розмови.

Метод “випалювання” реалізується шляхом подачі в лінію високовольтних (напругою більше 1500 В) імпульсів, що приводять до електричного “випалювання” вхідних каскадів електронних пристроїв перехоплення інформації й блоків їхнього живлення, гальванічно підключених до ТЛ. При використанні даного методу ТА від лінії відключається. Подача імпульсів у лінію здійснюється два рази. *Перший* (для “випалювання” паралельно підключених пристроїв) – при розімкнутій ТЛ, *другий* (для “випалювання” послідовно підключених пристроїв) – при закороченій (як правило, у центральному розподільному щитку будинку) ТЛ. Для захисту ТЛ використовуються як прості пристрої, що реалізують один з методів захисту, так і складні, що забезпечують комплексний захист ліній різними методами, включаючи захист від ВІ по електроакустичному каналу. На вітчизняному ринку є велика розмаїтість засобів захисту. Серед них можна виділити наступні: “SP 17/T”, “SI-2001”, “КТЛ-3”, “КТЛ-400”, “Кому-3”, “Кзот-06”, “Цикада-М”, “Прокруст ПТЗ-003”, “Прокруст-2000”, “Консул”, “Гром-Зи-6”, “Протон”, “Топаз”, “PIAC”, “Базальт-3”, “ПЗАТЛ”, “ПЗЦЛ” й інші. Основні характеристики деяких з них наведені в таблиці 2.7. В активних пристроях захисту ТЛ найбільше часто реалізований метод ВЧ маскуючої перешкоди (“SP 17/T”, “КТЛ-3”, “КТЛ-400”, “Кому-3”, “Прокруст ПТЗ-003”, “Прокруст-2000”, “Гром-Зи-6”, “Протон” й інші) і метод ультразвукової маскуючої перешкоди (“Прокруст” (ПТЗ-003), “Гром-Зи-6”).

Метод синфазної НЧ маскуючої перешкоди використовується в пристрої “Цикада-М”, а метод НЧ перешкоди, що маскує, – у пристроях “Прокруст”, “Протон”, “Кзот-06” й інші. Метод “обнуління” застосовується, наприклад, у пристрої “Цикада-М”, а метод підвищення напруги в лінії – у пристрої “Прокруст”. Компенсаційний метод маскування мовних повідомлень, переданих абонентові по ТЛ, реалізований у виробі “Туман”. Більшість пристроїв захисту роблять автоматичний вимір напруги в лінії й відображають його значення на цифровому індикаторі. Пристрої захисту ТЛ мають порівняно невеликі розміри й вагу. Живлення їх, як правило, здійснюється від мережі змінного струму.

Для виводу з ладу (“випалювання” вхідних каскадів) засобів несанкціонованого знімання інформації з гальванічним підключенням до ТЛ використаються пристрої типу “ПТЛ-1500”, “КС-1300”, “КС-1303”, “Кобра” і інші. Прилади використовують високовольтні імпульси напругою не менш 1500 ... 1600 В. Потужність імпульсів, що “випалюють”, становить 15...50 ВА.

Таблиця 2.7.

Основні характеристики пристроїв активного захисту ТЛ

Найменування характеристик	Тип пристрою					
	“Прокруст”	“Протон”	“Цикада-М”	Sel SP-17/P	“Гром-ЗИ-6”	“Кзот-06”
1	2	3	4	5	6	7
Метод синфазної НЧ маскуючої завади	-	-	так	-	-	-
Метод ВЧ маскуючої завади	так	так	-	так	так	так
Метод ультразвукової маскуючої завади	-	-	так	-	так	-
Метод підвищення напруги	так	-	-	-	-	-
Метод “обнулення”			так	-	-	-
Метод НЧ маскуючої завади	так	так	-	-	-	так
Метод “випалювання”	-	-	-	-	-	-
Індикація	світлова	світлова	світлова	світлова	світлова, звукова	світлова
Габаритні розміри, мм	62×155 ×195	205×60 ×285	68×176 ×170	152×104 ×34	150×200 ×50	210×85 ×32
Вага, кг	1	2,3		0,6	1,5	0.75
Напруга живлення, В	220	220	220	220/12	220	9
Примітки	Цифрова індикація напруги в лінії	Цифрова індикація напруги в лінії		Частотний діапазон завади 8 … 10 кГц. Рівень сигналу завади 70 дБ	Цифрова індикація зменшення напруги в лінії	

2.6. Системи закриття мовних сигналів

Крім вищеназваних методів і засобів захисту мовної інформації особливе місце в рішенні цієї задачі посідають системи закриття мовних сигналів. Безпека зв'язку при передачі мовних повідомлень ґрунтується на використанні різних методів закриття повідомлень, що змінюють характеристики мови таким чином, що вона стає нерозбірливою і невпізнанною для осіб, що підслуховують і перехоплюють мовну інформацію.

У мовних системах зв'язку відомі два основних методи закриття мовних сигналів, що розділяються по способу передачі по КЗ: аналогове скремблювання і дискретизація мови з наступним шифруванням.

Під *скремблюванням* розуміється зміна характеристик мовного сигналу таким чином, щоб отриманий модульований сигнал, володіючи властивостями нерозбірливості і невпізнанності, займав таку ж смугу частот спектра, що і вихідний відкритий.

Значна частина апаратури засекречування мовних сигналів використовує метод аналогового скремблювання, оскільки це дешево; необхідна для цього апаратура застосовується в більшості випадків у стандартних телефонних каналах зі смугою 3,1 кгц; забезпечується достатня якість дешифрованої мови; гарантується досить висока стійкість закриття. Аналогові скремблери перетворюють вихідний мовний сигнал способом зміни його амплітудних, частотних і часових параметрів в різних комбінаціях. Скрембльований сигнал потім може бути переданий по КЗ в тій же смузі частот, що і вихідний, відкритий.

Звичайно використовується один чи кілька способів аналогового скремблювання з числа наступних:

− скремблювання в частотній області − частотна інверсія (перетворення спектра сигналу за допомогою гетеродина і фільтра), частотна інверсія і зсув (частотна інверсія з мінливим стрибко-подібним зсувом несучої частоти), поділ смуги частот мовного сигналу на ряд піддіапазонів з наступною їхньою перестановкою й інверсією (рис. 2.1 і рис. 2.2 відповідно);

− скремблювання в часовій області − розбивка блоків чи частин мови на сегменти з перемішуванням їх у часі з наступним прямим або реверсивним зчитуванням (рис. 2.3);

− комбінація часового і частотного скремблірування (рис. 2.4).

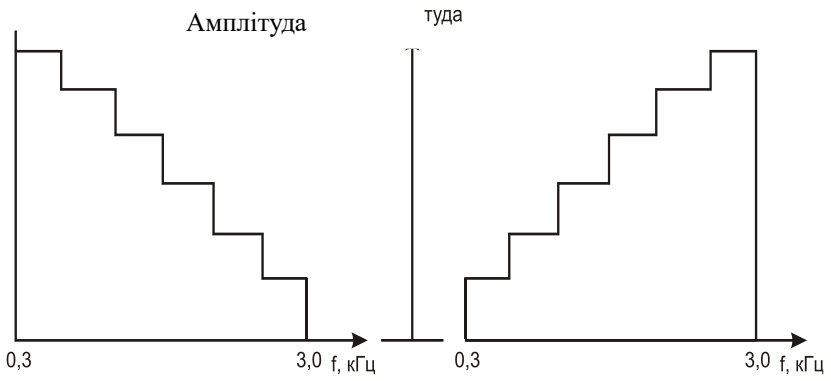


Рис. 2.1. Принцип роботи інвертора мови

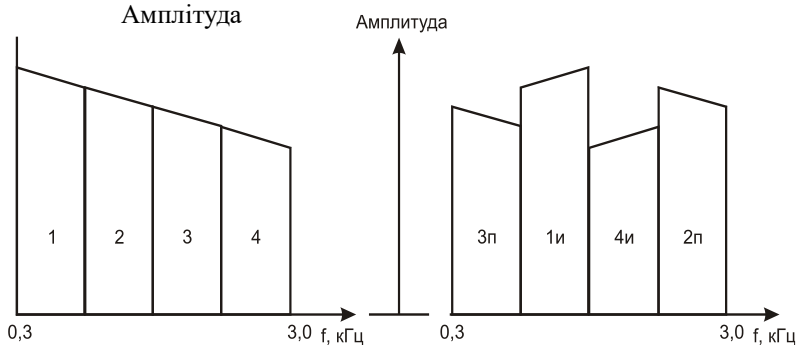


Рис. 2.2. Принцип роботи чотирисмугового інвертора мови

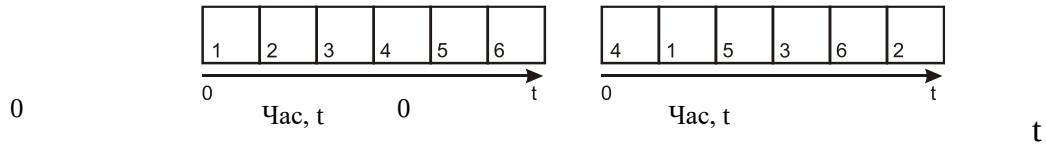


Рис. 2.3. Схема роботи часово́го скремблера з перестановками у фіксованому кадрі

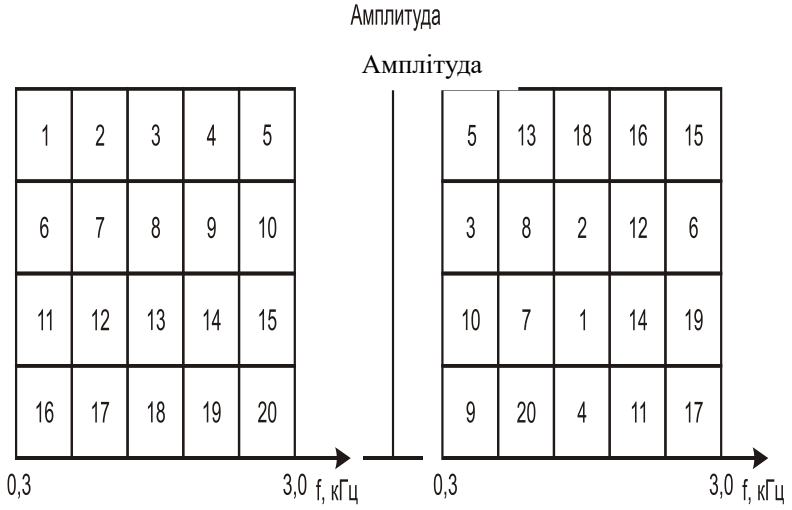


Рис. 2.4. Принцип роботи комбінованого скремблера

Як правило, усі перестановки виділених сегментів чи ділянок мови в часовий і частотній областях здійснюються за законом ПВП, яка

виробляється шифратором по ключу, що міняється від одного сеансу спілкування до іншого.

В якості приклада останньої системи розглянемо скремблер, схема якого представлена на рис. 2.5. У такому скремблері спектр оцифрованного аналого-цифровим перетворювачем АЦП мовного сигналу розбивається за допомогою використання алгоритмів цифрової обробки на частотно-часові елементи, що потім перемішуються на частотно-часовій площині у відповідності з одним із криптографічних алгоритмів і сумуються, не виходячи за межі частотного діапазону вихідного сигналу.

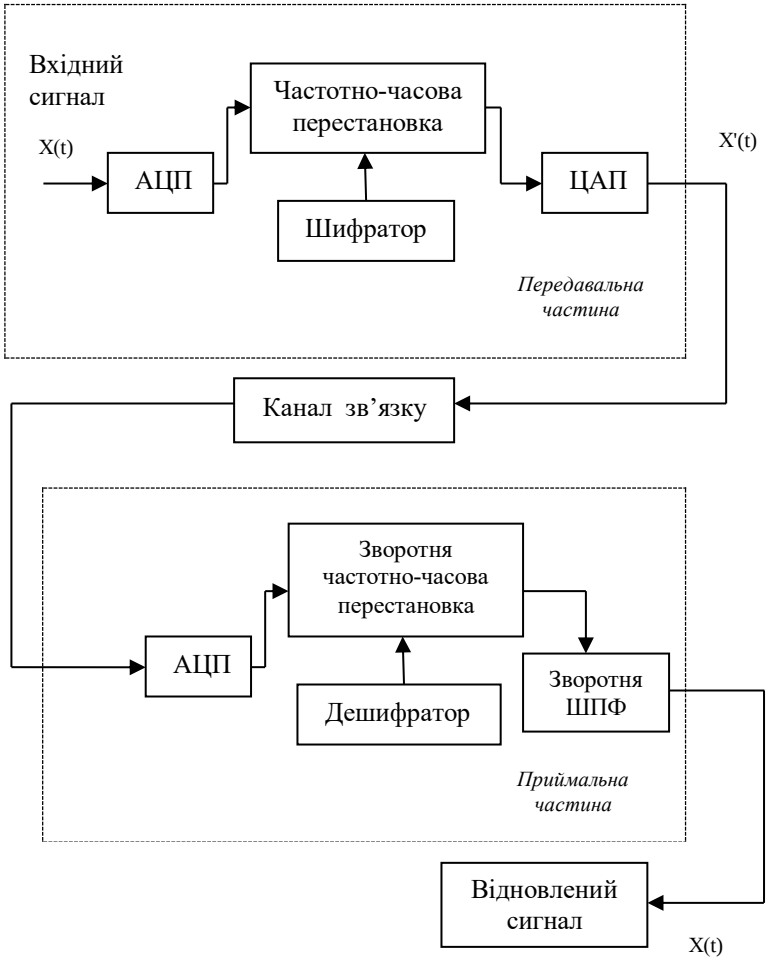


Рис 2.5 Структурна схема комбінованого скремблера

Число частотних смуг спектра, у яких виробляються перестановки з можливою інверсією спектра, дорівнює п'яти. Максимальна затримка частотно-часового елемента в часі дорівнює чотирьом.

Отриманий у такий спосіб закритий сигнал за допомогою ЦАП переводиться в аналогову форму і подається в КЗ. На прийомній стороні виконуються зворотні операції з відновлення отриманого закритого мовного повідомлення.

Стійкість алгоритму порівняння зі стійкістю систем цифрового

закриття мови. Альтернативним аналоговому скремблюванню методом передачі мови в закритому виді є шифрування мовних сигналів, перетворених у цифрову форму, перед їхньою передачею (рис. 2.6). Цей метод забезпечує більш високий рівень закриття в порівнянні з описаними вище аналоговими методами.

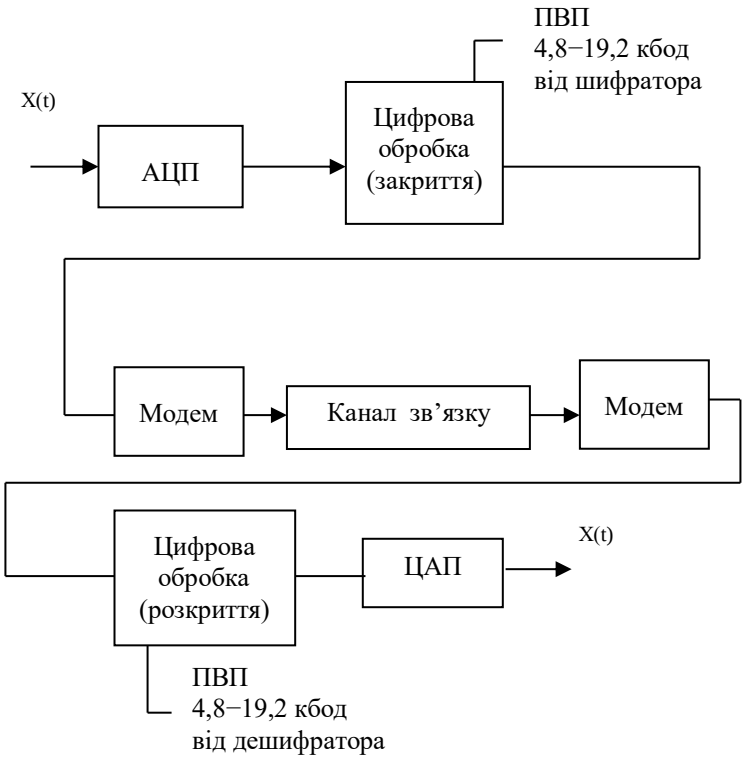


Рис. 2.6. Схема широкосмугової системи закриття мови

В основі пристроїв, що працюють по такому принципу, лежить представлення мовного сигналу у виді цифрової послідовності, що закривається по одному з криптографічних алгоритмів. Передача даних, що представляють дискретизовані відліки мовного сигналу і його параметри, по телефонних мережах, як і у випадку пристроїв шифрування алфавітно-цифрової і графічної інформації, здійснюється через пристрої, що називаються модемами. Основною метою при розробці пристроїв цифрового закриття мови є збереження тих її характеристик, що найбільш важливі для сприйняття слухачем.

В той же час дискретизована мова представлена таким чином, що може передаватися лише по спеціально виділених широкосмугових КЗ із смугою пропускання 4,8−19,2 кГц. Це означає, що вона непридатна для передачі по лініях телефонної мережі загального користування, полоса частот яких 3,1 кГц. У таких випадках використовуються вузькосмугові системи, головною проблемою при реалізації яких є висока складність алгоритмів стиснення мовних сигналів.

Правильне застосування методів цифрової передачі мови з високою інформаційною ефективністю, є вкрай важливим напрямом розробки пристроїв цифрового закриття мовних сигналів.

У таких системах пристрій кодування мови (вокодер), аналізуючи форму мовного сигналу, виробляє оцінку параметрів змінних компонент моделі генерації мови і передає ці параметри в цифровій формі по КЗ на синтезатор, де відповідно до цієї моделі за прийнятими параметрам синтезується мовне повідомлення. На малих інтервалах часу (до 30 мс) параметри сигналу можуть розглядатися, як постійні.

Чим коротший інтервал аналізу, тим точніше можна представити динаміку мовлення, але при цьому повинна бути вище швидкість передачі даних. У більшості випадків на практиці використовують 20-мілісекундні інтервали, а швидкість передачі сягає 2400 біт/с. При цьому за своєю побудовою схема системи закриття мовного сигналу аналогічна приведеній на рис. 8.6, але з меншою швидкістю передачі (1,2−4,8 кБод) і більш складними перетворювачами – АЦП і ЦАП.

Питання та завдання для самостійної перевірки знань

1. Назвіть основні ТКВІ, що характерні при розповсюдженні МІ?
2. Як утворюються навмисні (штучні) ТКВІ при розвідці МІ?
3. Охарактеризуйте пасивні і активні методи захисту МІ від несанкціонованого прослуховування?
4. Назвіть основну вимогу до звукоізоляції приміщень і показник її оцінки?
5. Назвіть основні характеристики звукоізоляції різних елементів визначеного (викладачем) приміщення і способи підвищення її ефективності?
6. Що собою представляють спеціальні звукоізоляційні кабіни?
7. Наведіть призначення і поясніть склад типової системи вібро-акустичного маскування. Назвіть типи існуючих систем?
8. Які аспекти необхідно враховувати при захисті ТА і ТЛ?
9. Охарактеризуйте найбільш відомі пасивні і активні методи захисту ТА?
10. Назвіть і охарактеризуйте пристрої, що застосовуються для захисту ТА?
11. Охарактеризуйте пасивні і активні методи захисту ТЛ?
12. Наведіть приклади і характеристики пристроїв, що застосовуються для захисту ТЛ?
13. В чому сутність закриття мовного сигналу? Які основні методи і технічні рішення їх закриття?
14. Оцініть стійкість криптографічного закриття мовного сигналу для схем, що приведені на рис. 2.4 і рис. 2.5?

15. Визначте засоби захисту ТА і ТЛ від нього для виділеного приміщення?

РОЗДІЛ 3. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ПРИ РОБОТІ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформації, що зберігається і обробляється.

Враховуючи ту роль, яку відіграють ЗОТ та АС у сучасному суспільстві, а також наростаючу тенденцію до використання ПЕОМ для обробки ІзОД, представляється важливим визначення системи заходів, як технічних, так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки.

Слід відмітити, що організація ЗІ ІзОД у ЗОТ, АС і мережах від витоку каналами побічних ЕМВ і наводок (ПЕМВ) здійснюється відповідно до вимог і рекомендацій НД [9, 19], та НД ТЗІ 3.7- 003-05 “Порядок проведення робіт із створення КСЗІ в ІТС”. Прийнято виділяти три основних напрями ТЗІ в АС і ЗОТ [9, 19]:

− захист АС і оброблюваної інформації від несанкціонованих дій та НСД до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування ЗП чи програм, використання комп’ютерних вірусів та ін.;

− ЗІ від витоку технічними каналами, до яких відносяться канали побічних ЕМВ і наведень, акустоелектричні та інші канали;

− ЗІ від спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

3.1. Характеристика каналів витоку інформації при експлуатації автоматизованих систем та засобів ОТ

Носіями інформації**,** яка обробляється, циркулює, відображається в АС і ЗОТ є електричні й ЕМП і сигнали, що утворюються в результаті роботи засобів оброблення ІзОД (ОТЗ) або впливу НСиг на засоби оброблення відкритої інформації, на засоби і системи життєзабезпечення (ДТЗС).

З точки зору ЗІ АС і ЗОТ є наочним прикладом втілення практично всіх каналів ВІ – починаючи з матеріально-речовинних і завершуючи електромагнітним (радіоканалом). Основними об’єктами ВІ в АС і ЗОТ є

ПЕОМ, підсистеми відображення, документування і передачі даних та допоміжне обладнання, в яких існують відповідні джерела ВІ.

З урахуванням того, що АС можуть функціонувати як незалежно одна від одної (АС класу 1), так і у взаємодії з іншими АС у комп'ютерній мережі (АС класу 2, 3), повний перелік тих ланок, де можуть знаходитись відомості, що підлягають захисту, може мати наступний вигляд:

− безпосередньо в оперативній або постійній пам'яті ПЕОМ;

− на знімних магнітних, магнітооптичних, лазерних і інших носіях;

− на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери і т. ін.);

− на екранах пристроїв відображення (дисплеї, монітори тощо);

− в пам'яті пристроїв вводу/виводу (принтери, сканери тощо);

− в пам'яті пристроїв управління і лініях зв'язку, які утворють канали спрягання комп'ютерних мереж.

Канали ВІ утворюються як під час роботи ЕОМ, так і в режимі очікування. Джерелами таких каналів є:

− ЕМП;

− струми і напруги, що наводяться у колах живлення, заземлення, колах з'єднання тощо;

− перевипромінювання інформації, що обробляється, на частотах паразитної генерації елементів і пристроїв технічних засобів ЕОМ;

− перевипромінювання інформації, що обробляється, на частотах контрольно-вимірювальної апаратури.

Окрім цих каналів, обумовлених природою процесів, що протікають в ПЕОМ, та їх технічними особливостями, у ПЕОМ можуть навмисно створюватись додаткові канали ВІ. Для їх створення можуть використовуватись:

− розміщення у ПЕОМ ЗП;

− навмисне застосування таких конструктивно-схемних рішень, які приводять до збільшення ЕМВ у певній частині спектру;

− встановлення ЗП, які забезпечують знищення ПЕОМ за командою зовні (схемні рішення);

− встановлення елементної бази, яка часто виходить з ладу і порушує роботу ПЕОМ.

Крім того, класифікацію можливих каналів ВІ можна також провести на основі принципів, відповідно з якими обробляється інформація, що отримується через можливий канал витоку. При цьому передбачається три типи обробки інформації: людиною, апаратурою, програмою. Відповідно з кожним типом обробки всі можливі канали витоку також розбиваються на три групи.

Стосовно до ПЕОМ першу групу каналів, що визначають обробку інформації людиною, становлять:

− викрадення матеріальних НІ (магнітних дисків, дискет, стрічок і т. ін.);

− зчитування інформації з екрану сторонніми особами;

− зчитування інформації із залишених без догляду паперових розпечаток.

До групи каналів, в яких основним видом обробки є обробка апаратурою, можливо виділити наступні канали витоку:

− підключення до ПЕОМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

− використання спеціальних технічних засобів для перехоплення ЕМВ технічних засобів ПЕОМ.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні канали витоку:

− НСД програм до інформації;

− розшифровування програмою зашифрованої інформації;

− копіювання програмою інформації з носіїв;

− блокування або відключення програмних засобів захисту.

При перехопленні інформації з ПЕОМ застосовуються схема, представлена на рис. 3.1.

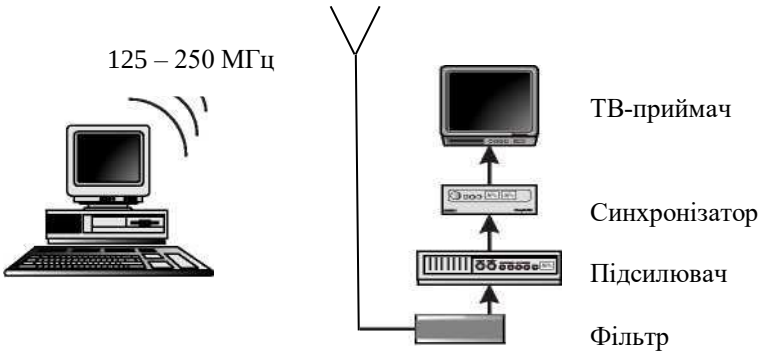


Рис. 3.1. Схема перехоплення інформації з ПЕОМ

При цьому технічному контролю повинні підлягати наступні потенційні канали ВІ:

− ПЕМВ в діапазоні частот від 10 Гц до 100 МГц;

− наведення сигналів в колах електроживлення, заземлення і в лініях зв’язку;

− НСиг, що утворюються за рахунок акусто-електричних перетворень у спеціальній апаратурі контролю інформації. Ці сигнали контролюються в діапазоні частот 300 – 3400 Гц;

− канали ВІ, що утворюються в результаті впливу ВЧ ЕМП на різні сторонні провідники, які знаходяться у приміщенні. В цьому випадку перевірка здійснюється в діапазоні частот від 20 кГц до 100 МГц.

Найбільш небезпечним каналом витоку є дисплей на основі ЕПТ, оскільки з точки зору ЗІ він є самою слабкою ланкою у обчислювальній системі. Так, для стандартного комп'ютерного монітора перехоплення інформації можливе майже до 50-ї гармоніки тактової частоти, а рівень випромінювання до десятків дБ дозволяє приймати сигнали на відстані сотні метрів [18].

Для відображення цифро-літерної інформації на екрані ЕПТ до складу дисплею входить відеоадаптер. У свою чергу, у складі відеоадаптера є спеціалізовані схеми для генерування електричних сигналів управління обладнанням, яке забезпечує генерацію зображення.

Схеми адаптера формують сигнали, які визначають інформацію, що відображається на екрані. Для цього у всіх відео системах є відеобуфер, який являє собою область оперативної пам'яті, що призначена тільки для зберігання тексту або графічної інформації, що виводиться на екран.

Основна функція відеосистеми полягає у перетворенні даних з відеобуфера у сигнали управління дисплея, за допомогою яких на його екрані формується зображення. Ці сигнали зловмисник (порушник) і намагається перехопити.

Підсумовуючи вищесказане перерахуємо характерні ТКВІ при експлуатації АС і ЗОТ:

1. Електромагнітний канал:

− радіоканал (ВЧ випромінювання);

− НЧ канал;

− мережевий канал (наводки в мережі живлення);

− канал заземлення (наводки на провідники заземлення);

− лінійний канал (наводки на лінії зв'язку між ЕОМ та її складовими елементами).

2. Акустичний канал.

3. Канал несанкціонованого копіювання.

4. Канал НСД.

5. Безпосереднє викрадення (втрата) магнітних НІ і документів, що утворюються при обробці даних на ПЕОМ.

3.2. Захист АС і оброблюваної інформації від несанкціонованих дій та несанкціонованого доступу

ЗІ в АС – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією [3]. Однією з небезпечних загроз інформації, що обробляється в АС, є НСД – доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу.

3.2.1. Методи захисту від НСД

Захист від НСД досягається проведенням організаційних заходів та застосуванням апаратних, програмних і криптографічних методів.

Організаційні заходи полягають: у чіткому встановленні обов'язків посадових осіб і обслуговуючого персоналу по ЗІ; організації пропускного режиму; встановлені грифів секретності циркулюючої інформації; здійснені постійного контролю за ефективністю діючої системи захисту і її вдосконаленні.

Апаратні способи, які є важливою складовою частиною загальної системи захисту секретної інформації від, НСД, поділяються на загальні та спеціальні. Загальні апаратні методи реалізуються шляхом використання замків, ключів, комплексу електромеханічних блокувань і сигналізації розтину стійок, шаф, пультів і т. д.

Спеціальні методи захисту передбачають використання різних структурних схем захисту в центральному процесорі, процесорі управління введенням-виводом даних, оперативному запам'ятовуючому пристрої (ОЗУ), пристрої управління зовнішніх запам'ятовуючих пристроїв (ЗЗП), терміналах користувачів. Застосовувані в різних вузлах і блоках ЕОМ структурні схеми захисту забезпечують контроль доступу до інформації з боку користувачів та виявлення помилок в програмах роботи ЕОМ.

Програмні методи ЗІ включають в себе функціональні програми ідентифікації користувачів і визначення їх прав, впізнання терміналів користувачів, захисту масивів інформації (файлів).

Програми ідентифікації користувачів і визначення їх прав виконують дві основні функції: встановлюють законність самого факту звернення користувача до ЕОМ, а також визначають права даного користувача щодо обсягу доступу до інформації.

Ідентифікація користувачів в сучасних ЕОМ проводиться за допомогою спеціальних паролів, які представляють совою кодові набори букво-цифрових знаків.

У ряді випадків в АС застосовують *криптографічні або стеганографічні способи ЗІ*. Необхідність засекречування (шифрування) інформації пов'язана з можливістю розкрадання НІ (магнітних стрічок, дисків, барабанів, перфокарт) і несанкціонованого знімання інформації, переданої по КЗ.

Для засекречування інформації можуть використовуватися такі методи шифрування, як заміна, перестановка, гамування, алгебра матриць, що реалізовані в сучасних криптографічних алгоритмах.

На відміну від криптографії, де зловмисник точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в об'єкти, що не привертають уваги, так, щоб неможливо було запідозрити існування вбудованого таємного повідомлення.

3.2.2. Програмні засоби захисту від несанкціонованого доступу

Основні функції від чужого вторгнення обов'язково передбачають певні заходи безпеки. Основними функціями, які повинні здійснюватися програмними засобами у цьому випадку є:

− ідентифікація суб'єктів та об'єктів;

− розмежування (іноді й повна ізоляція) доступу до обчислювальних ресурсів та інформації;

− контроль та реєстрація дій з інформацією та програмами.

Процедура ідентифікації та підтвердження автентичності передбачає перевірку, чи є суб'єкт, який здійснює доступ (або об'єкт, до якого здійснюється доступ) тим, за кого себе видає. Подібні перевірки можуть бути одноразовими або періодичними (особливо у випадках тривалих сеансів роботи).

Найбільш розповсюдженими методами ідентифікації є парольна ідентифікація.

Практика показує, що парольний захист даних є слабкою ланкою, так як пароль можна підслухати або підглянути, пароль можна перехопити, а, то і просто розгадати.

Для захисту власне пароля напрацьовані певні рекомендації, як зробити пароль надійним. Необхідно пам'ятати, що набраний на клавіатурі пароль часто зберігається в послідовності команд автоматичного входу в систему.

Для ідентифікації програм і даних часто вдаються до підрахунку контрольних сум, проте, як і у випадку парольної ідентифікації, важливо виключити можливість підробки при збереженні правильної контрольної суми. Це досягається шляхом використання складних методів контрольного підсумовування на основі криптографічних алгоритмів. Забезпечити захист даних від підробки (імітостійкість) можна, якщо застосувати різноманітні методи шифрування та методи цифрового підпису на основі криптографічних систем із відкритим ключем.

Захист на рівні апаратури та ПЗ передбачає керування доступом до обчислювальних ресурсів: окремих пристроїв, оперативної пам'яті, операційної системи, спеціальним службовим та особистим програмам користувача.

ЗІ на рівні даних спрямований:

− на ЗІ при звертанні до неї у процесі роботи на ПЕОМ та виконання тільки дозволених операцій над ними;

− на ЗІ при її передаванні КЗ між різними ЕОМ.

Керування доступом до інформації дозволяє дати відповідь на питання:

− хто може виконувати і які операції;

− над якими даними дозволяється виконувати операції.

Об'єктом, доступ до якого контролюється, може бути файл, запис у файлі, а фактором, що визначає порядок доступу, − певна подія, значення

даних, стан системи, повноваження користувача, передісторія звернення та інші дані.

Доступ, що керується подією, передбачає блокування звернення користувача. Наприклад, у певні інтервали часу або при звертанні з певного термінала. Доступ, що залежить від стану, здійснюється залежно від поточного стану обчислювальної системи, керуючих програм та системи захисту. Що стосується доступу, залежного від повноважень, то він передбачає звернення користувача до програм, даних, обладнання залежно від режиму, що надається. Такими режимами можуть бути "тільки читати", "читати та писати", "тільки виконувати" і т. ін.

В основі більшості засобів контролю доступу лежить те або інше представлення матриці доступу.

Основне призначення програм контролю полягає в контролі стану основних компонентів механізму захисту, дотримані правил використання даних, що захищаються, і дотримані правил використання механізму захисту.

Контроль стану компонентів механізму захисту полягає в перевірці їх справності і здатності виконувати свої функції. У простому випадку програми контролю являють собою звичайні діагностичні програми, за допомогою яких перевіряється працездатність технічних і програмних засобів захисту. У розвинених варіантах для контролю розробляється спеціальний пакет програм.

Під реєстрацією в сучасних системах забезпечення безпеки інформації розуміють сукупність засобів і методів, що використовуються для регулярного збору, фіксації, обробки видачі відомостей при всіх запитах, що містять звернення до даних, що захищаються.

Найбільш поширеною формою реєстрації є програмне ведення спеціальних реєстраційних журналів. У реєстраційному журналі рекомендується фіксувати час надходження запиту, ім'я терміналу, з якого надійшов запит, і т. п. події.

Однак, якщо не вжити спеціальних заходів, то при систематичному зборі залишкової інформації з журналів можна безпосередньо отримати інформацію, що захищається, а прочитавши паролі, можна замаскуватися під зареєстрованного користувача і дістати НСД до даних згідно із його повноваженнями.

Тому надійний ЗІ неможливий без вжиття заходів для своєчасного знищення залишкової інформації. Таке знищення може бути надійно здійснено дво-, триразовим записом у відповідних областях пам'яті довільною комбінацією нулів і одиниць.

Під аварійним знищенням інформації розуміють таке її знищення, котре здійснюється за спеціальними командами у тих випадках, коли виявляється невідворотня небезпека НСД. Здійснюється воно програмними

засобами шляхом посилки у відповідні області пам’яті комбінацій нулів і одиниць.

Програми сигналізації призначені, з одного боку, для попередження користувачів про необхідність дотримуватися обережності при роботі з секретними даними, а, з іншого, − для своєчасного попередження фахівців служби безпеки, адміністрації і користувачів АС про несанкціоновані дії.

Перший вид сигналізації здійснюється шляхом автоматичного формування та присвоєння спеціальної ознаки (грифа секретності) всім документам, що видаються на друк або пристрій відображення документів, і містять захищаєму інформацію.

Другий вид сигналізації здійснюється шляхом формування та видачі (подачі) службі безпеки, адміністрації та користувачам АС спеціальних сигналів виявлення спроб несанкціонованих дій, наслідком яких може бути НСД до інформації, що захищається.

3.3. Захист інформації в автоматизованих системах і засобах обчислювальної техніки від витоку каналами побічного електромагнітного випромінювання і наведення

3.3.1. Аналіз можливого витоку інформації каналами побічного електромагнітного випромінювання і наведення

У процесі функціонування засобів обчислювальної техніки в конструктивних елементах та кабельних з’єднаннях циркулюють електричні струми інформативних сигналів, у результаті чого формуються ЕМП, рівні яких можуть бути достатніми для приймання сигналів і здобування інформації за допомогою спеціальної апаратури.

Канали ВІ можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів у лініях зв’язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території (КТ). Інформативні сигнали можуть поширюватися на великі відстані і реєструватися ТЗР за межами КТ.

Частоти, на яких можуть випромінюватися (наводитись) інформативні сигнали, залежать від типів та видів апаратурних засобів і можуть знаходитись у діапазоні від сотень Гц до кількох десятків ГГц. Рівень наводок визначається відстанню між джерелами випромінювання й апаратурою, що підпадає під вплив цих випромінювань, довжиною паралельного пробігу і величиною перехідного затухання ліній, напругою інформативного сигналу в лінії та рівнем шумів (завад). ВІ колами заземлення може виникнути за наявності рознесених точок заземлення інформативних кіл у випадку створення в різних точках СЗ різниці потенціалів і виникнення за рахунок цього струмів у колах заземлення, при великому значенні опору кола заземлення, а також внаслідок

недосконалості екранів, яка призводить до асиметрії ліній відносно екрана і до виникнення у колі між корпусом екрана та землею інформативних струмів.

Максимально допустиме відношення пікової напруги сигналу до середньоквадратичної напруги шуму визначається відповідно до чинних Норм ефективності ЗІ в АС і ЗОТ.

3.3.2. Організація захисту інформації в автоматизованих системах і засобах обчислювальної техніки від витоку каналами побічного електромагнітного випромінювання і наведення

Роботи з ТЗІ в АС і ЗОТ передбачають:

− категоріювання об'єктів ЕОТ;

− включення до технічних завдань на монтаж АС і ЗОТ розділу з ТЗІ;

− монтаж АС і ЗОТ відповідно до рекомендацій [19];

− обстеження (в тому числі технічний контроль) об'єктів ЕОТ;

− установлення (при необхідності) атестованих засобів захисту;

− технічний контроль за ефективністю вжитих заходів.

Для об'єктів ЕОТ, що обробляють ІзОД, проводиться обов'язкове категоріювання згідно з чинним Положенням про категоріювання. Обсяг і зміст робіт із захисту цієї інформації визначаються присвоєною категорією.

Обстеження АС і ЗОТ відповідно до рекомендацій [19] проводиться структурними підрозділами ТЗІ, у віданні яких знаходиться об'єкт, або підприємствами, установами, організаціями і громадянами, що одержали в установленому порядку відповідні ліцензії Державної служби України з питань ТЗІ.

Рекомендований алгоритм обстеження містить такі процедури:

− аналіз у технічних засобах (ТЗ) ЕОТ потоків ІзОД;

− визначення складу ОТЗ і ДТЗС на об'єкті ЕОТ;

− визначення складу кабельних ліній, що виходять за межі КТ і мають паралельний пробіг з кабелями АС і ЗОТ;

− виявлення комунікацій, що проходять через територію об'єкта ЕОТ і мають вихід за межі КТ;

− інструментальне вимірювання інформативних побічних електромагнітних випромінювань та наводок;

− оцінку відповідності рівнів сигналів і параметрів полів, які є носіями ІзОД, нормам ефективності захисту.

За результатами обстеження складається акт, в якому відбиваються:

− категорія об'єкта ЕОТ;

− перелік ОТЗ (найменування, тип, заводський номер);

− перелік ДТЗС і комунікацій, що знаходяться на об'єкті ЕОТ;

− оцінка відповідності монтажу цим рекомендаціям;

− пропозиції щодо застосування додаткових заходів захисту (при необхідності).

До акта додаються:

− схема розміщення ТЗ об’єкта ЕОТ і проходження комунікацій на ньому;

− протоколи вимірювань.

3.3.3. Рекомендації з технічного захисту інформації в автоматизованих системах і засобах обчислювальної техніки від витоку каналами побічного електромагнітного випромінювання і наведення

ЗІ в АС і ЗОТ від витоку каналами ПЕМВН включає наступні складові [18, 19]:

1. ЗІ від перехоплення випромінювань технічних засобів об’єкта ЕОТ.
2. ЗІ від перехоплення наводок на незахищені технічні засоби та ДТЗС, що мають вихід за межі КТ.
3. ЗІ від витоку колами заземлення.
4. ЗІ від витоку колами електроживлення.
5. Застосування системи просторового зашумлення об’єктів ЕОТ.
6. Обладнання та застосування екранувальних конструкцій.

Для забезпення ЗІ від перехоплення випромінювань технічних засобів об’єкта ЕОТ рекомендується виконати наступні дії:

1.1. Навколо ОТЗ повинна забезпечуватися контрольована територія, за межами якої відношення “інформативний сигнал/шум” не перевищує Норм. З цією метою ОТЗ рекомендується розташовувати у внутрішніх приміщеннях об’єкта, бажано, на нижніх поверхах.

1.2. У випадку неможливості забезпечення цієї умови необхідно:

− замінити ОТЗ на захищені;

− провести часткове або повне екранування приміщень чи ОТЗ;

− установити системи просторового зашумлення;

− замінити незахищені ТЗ на захищені;

− застосувати завадозаглушувальні фільтри.

1.3. В екранованих приміщеннях (капсулах) рекомендується розміщувати ВЧ ОТЗ. Як правило, до них відносяться процесори, запам’ятовуючі пристрої, дисплеї тощо.

Для забезпення ЗІ від перехоплення наводок на незахищені технічні засоби та ДТЗС, що мають вихід за межі КТ, рекомендується дотримуватись наступних вимог:

2.1. У незахищених КЗ, лініях, проводах та кабелях ОТЗ і ДТЗС, що мають вихід за межі КТ, установлюються завадозаглушувальні фільтри.

2.2. Проводи і кабелі прокладаються в екранованих конструкціях.

2.3. Монтаж кіл ТЗ, що мають вихід за межі КТ, рекомендується проводити екранованим або прокладеним в екранувальних конструкціях симетричним кабелем.

2.4. Кабелі ОТЗ прокладаються окремим пакетом і не повинні утворювати петлі. Перехрещення кабелів ОТЗ і ДТЗС, що мають вихід за межі КТ, рекомендується проводити під прямим кутом, забезпечуючи відсутність електричного контакту екранувальних оболонок кабелів у місці їх перехрещення.

2.5. Незадіяні проводи і кабелі демонтуються або закорочуються та заземляються.

ЗІ від витоку колами заземлення включає наступні рекомендації:

3.1. СЗ ТЗ ЕОТ не повинна мати вихід за межі КТ і повинна розміщуватися на відстані не менше 10 – 15 м від них.

3.2. Заземлювальні проводи повинні бути виконані з мідного дроту (кабеля) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом.

3.3. Не рекомендується використовувати для СЗ ТЗ ЕОТ природні заземлювачі (металеві трубопроводи, залізобетонні конструкції будинків тощо), які мають вихід за межі КТ.

3.4. Для усунення небезпеки ВІ металевими трубопроводами, що виходять за межі КТ, рекомендується використовувати струмонепровідні вставки (муфти) довжиною не менше 1 м.

3.5. За наявності в ТЗ ЕОТ "схемної землі" окреме заземлення для них створювати не потрібно. Шина "схемна земля" повинна бути ізольованою від захисного заземлення та металоконструкцій і не повинна утворювати замкнену петлю.

3.6. При неможливості провести заземлення ТЗ ЕОТ допускається їх "занулення".

Для забезпечення ЗІ від витоку колами електроживлення слід дотримуватися наступних рекомендацій:

4.1. Найбільш ефективно гальванічну та електромагнітну розв'язку кабелів електроживлення ТЗ ЕОТ від промислової мережі забезпечує їх розділова система типу "електродвигун-генератор". Електроживлення допускається також здійснювати через завадозаглушувальні фільтри.

4.2. Електроживлення повинно здійснюватись екранованим (броньованим) кабелем.

4.3. Кола електроживлення ТЗ ЕОТ на ділянці від ОТЗ до розділових систем чи завадозаглушувальних фільтрів рекомендується прокладати у жорстких екранувальних конструкціях.

Не допускається прокладання в одній екранувальній конструкції кабелів електроживлення, розв'язаних від промислової мережі, з будьякими кабелями, що мають вихід за межі КТ.

4.4. Забороняється здійснювати електроживлення технічних засобів, що мають вихід за межі КТ, від захищених джерел електропостачання без установлення завадозаглушувальних фільтрів.

4.5. Для об’єктів 2−4 категорій допускається не проводити роботи із захисту кіл електроживлення, якщо всі пристрої і кабелі електропостачання об’єкта ЕОТ, включаючи трансформаторну підстанцію низької напруги із заземлювальним пристроєм, розміщені у межах КТ.

Рекомендації із застосування системи просторового зашумлення об’єктів ЕОТ включають наступні заходи:

5.1. Пристрої просторового зашумлення застосовуються у випадках, коли пасивні заходи не забезпечують необхідної ефективності захисту об’єкта ЕОТ.

5.2. Установленню підлягають тільки сертифіковані Державною службою України з питань технічного ЗІ (ДСТСЗІ, ДССЗЗІ) засоби просторового зашумлення, до складу яких входять:

− надширокосмугові генератори ЕМП шуму (генератор шуму);

− система рамкових антен;

− пульт сигналізації справності роботи системи.

5.3. Установлення генераторів шуму, монтаж антен, а також їх обслуговування в процесі експлуатації здійснюють підприємства, установи й організації, що мають відповідну ліцензію ДСТЗІ (ДССЗЗІ).

5.4. Живлення генераторів шуму повинно здійснюватися від того ж джерела, що і живлення ТЗ ЕОТ. Антени рекомендується розташовувати поза екранованим приміщенням.

Основні рекомендації з обладнання та застосування екранувальних конструкцій включають наступні заходи:

6.1. Екранувальні кабельні конструкції разом з екранувальними конструкціями ТЗ ЕОТ повинні створювати екранувальний замкнений об’єм.

6.2. Виведення кабелів з екранувальних конструкцій і введення в них необхідно здійснювати через завадозаглушувальні фільтри.

6.3. Екранувальні кабельні конструкції можуть бути жорсткими і гнучкими. Основу жорстких конструкцій становлять труби, короби та коробки; основу гнучких конструкцій − металорукави, взяті в обплетення, і сітчасті рукави.

6.4. Для екранування проводів і кабелів застосовуються водогазопровідні труби. Рекомендується застосовувати сталеві тонкостінні оцинковані труби або сталеві електрозварені.

6.5. З’єднання нероз’ємних труб здійснюється зварюванням, роз’ємних − за допомогою муфти та контргайки.

6.6. Для екранування проводів і кабелів застосовуються короби прямокутного перерізу. Їх переваги у порівнянні з трубами – можливість прокладання кабеля з роздільними роз’ємами.

Короби виготовляються з листової сталі. На кінцях секцій короба повинні бути фланці для з'єднання коробів між собою та з іншими екранувальними конструкціями. Для одержання надійного електричного контакту поверхня фланців повинна мати антикорозійне струмопровідне покриття.

6.7. Гнучкі конструкції служать для з'єднання жорстких екранувальних кабельних конструкцій з екранувальними конструкціями ТЗ ЕОТ та одночасно є компенсаторами температурних та монтажних деформацій. Як екран може бути використаний металорукав типу РЗ за ТУ 22-3688-77, поміщений у сталеве оцинковане обплетення. Для збільшення ефективності екранування рекомендується застосовувати комбіновані екрани, що складаються з мідного і сталевого обплетень.

Остаточний висновок про ефективність проведених заходів щодо ТЗІ дається за результатами інструментального контролю.

3.4. Захист інформації від спеціального впливу

Спеціальний вплив на носії ІзОД і засоби забезпечення ТЗІ здійснюється шляхом формування полів, сигналів і програм, що використовуються в технічних засобах забезпечення інформаційної діяльності, з метою зниження ефективності функціонування системи ЗІ, створення ТКВІ, порушення цілісності інформації (модифікації, руйнування, знищення).

Особливе значення при визначенні засобів захисту від спеціально впливу приділяється програмам захисту від копіювання і руйнування.

3.4.1. Програмні засоби захисту від копіювання

Засоби захисту від копіювання запобігають використання викрадених копій ПЗ і на даний час є єдиним надійним засобом, який захищає авторське право розробників-програмістів та стимулює розвиток ринку ПЗ.

Під засобами захисту від копіювання, звичайно, розуміють засоби, які забезпечують виконання програмою своїх функцій тільки при упізнанні деякого унікального елемента, що не піддається копіюванню. Таким елементом (ключовим елементом) може бути флеш-носій, певна частина комп'ютера або спеціальний пристрій, який приєднується до ПЕОМ. Захист від копіювання реалізується виконанням ряду функцій, які є спільними для всіх систем захисту:

− ідентифікація середовища, із якого буде запускатися програма;
− автентифікація середовища, із якого запущена програма;
− реакція на запуск із несанкціонованого середовища;
− несанкціонованого копіювання;
− протидія вивченню алгоритмів роботи системи.

Під середовищем, із якого буде запускатися програма, розуміють або дискету, або ПЕОМ (якщо установка здійснюється на нагромаджувач на

жорсткому магнітному дискові). Ідентифікація середовища полягає в тому, щоб деяким чином поіменувати середовище з метою подальшої його автентифікації. Ідентифікувати середовище − означає закріпити за ним деякі спеціально створені або виміряні характеристики, які рідко повторюються та важко підроблюються. Такі характеристики називаються ідентифікаторами. Ідентифікація флеш-носіїв може бути проведена двома способами.

Перший заснований на нанесенні пошкоджень на деяку частину флеш-носія, розповсюджений спосіб такої ідентифікації − "лазерна діра", при такому способі дискета пропалюється в деякому місці лазерним променем. Очевидно, що зробити точно таку ж дірку в копії флеш-носія і в тому ж місці, як і на флеш-носії оригіналі, достатньо важко. Інший спосіб ідентифікації заснований на нестандартному форматуванні флеш-носія.

Реакція на запуск із несанкціонованого середовища зводиться до видачі відповідного повідомлення.

3.4.2. Програмні засоби захисту від руйнування

Руйнування може відбутися при підготовці й здісненні різних відновлювальних заходів (резервування, створення та оновлення страхувального фонду, ведення архівів інформації і т. ін.). Так як причини руйнування вельми різноманітні (несанкціоновані дії, помилки програм та обладнання, комп'ютерні віруси і т. ін.), про проведення страхувальних заходів є обов'язковими для всіх, хто користується ПЕОМ.

Необхідно спеціально відзначити небезпеку комп'ютерних вірусів.

Комп'ютерний вірус – це невелика, достатньо складна, ретельно складена та небезпечна програма, яка може самостійно розмножуватися, переносити себе на диски, прикріплюватися до чужих програм та передаватися інформаційними мережами. Вірус, звичайно, створюється для порушення роботи комп'ютера різноманітними способами – від "безвинного" видавання будь-якого повідомлення до стирання, руйнування файлів.

За деструктивним можливостям комп'ютерні віруси можна розділити на наступні 4 групи: нешкідливі; безпечні; небезпечні; дуже небезпечні.

Нешкідливі – ніяк не впливають на роботу комп'ютерної системи, крім зменшення кількості вільної пам'яті в результаті свого поширення.

Безпечні – вплив яких обмежується зменшенням вільної пам'яті, а також графічними, звуковими й іншими ефектами.

Небезпечні – які можуть привести до серйозних збоїв у роботі комп'ютерних систем.

Дуже небезпечні – до алгоритму їх роботи введені процедури, які можуть викликати втрату програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті,

сприяти швидкому зносу рухомих частин механізмів (наприклад, вводити в резонанс і руйнувати голівки деяких типів жорстких дисків) і т. д.

Основну масу вірусів створюють зловмисники або так звані хакери − програмісти-хулігани, щоб утішити свої амбіції або заробити гроші на продажі антивірусних програм (антивірусів).

Антивірус − це програма, яка виявляє або виявляє та видаляє віруси. Такі програми бувають спеціалізованими або універсальними.

Спеціалізовані здатні боротися з вже написаними, працюючими вірусами, а універсальні − із ще ненаписаними. До спеціалізованих відноситься більшість антивірусних програм, кожна з них розпізнає один або декілька конкретних вірусів, ніяк не реагуючи на присутність інших.

Універсальні антивіруси призначені для боротьби з цілими класами вірусів. За призначенням антивіруси універсальної дії бувають різноманітними. Широке застосування знаходять резидентні антивіруси та програми ревізори.

І ці, і інші антивірусні програми мають певні можливості, позитивні й негативні (недоліки) характеристики. Спеціалізовані антивірусні програми при своїй простоті надто вузько спеціалізовані. При значній різноманітності вірусів потрібна така ж різноманітність антивірусів.

Окрім використання антивірусних програм в інтересах захисту від вірусів широке застосування знаходять організаційні заходи безпеки. Для зменшення небезпеки вірусних атак можливим є прийняття певних дій, які для кожного конкретного випадку можуть бути скорочені або розширені:

− інформувати всіх співробітників про небезпеку щодо можливих збитків на випадок вірусних атак;

− заборонити співробітникам приносити програми зі “сторони” для установки їх у системи оброблення інформації − повинні використовуватися тільки програми, які розповсюджуються офіційно;

− заборонити співробітникам використовувати комп’ютерні ігри на ПЕОМ, що обробляють інформацію, яка підлягає захисту;

− для виходу на сторонні інформаційні мережі виділяти окреме спеціальне місце;

− створити архів копій програм і даних;

− періодично проводити перевірку контрольним підсумовуванням або порівнянням з “чистими” програмами;

− установити системи ЗІ на особливо важливих ПЕОМ із застосуванням спеціальних антивірусних засобів.

3.5. Криптографічний і стеганографічний захист інформації

Для ефективного ЗІ необхідно комплексне використання

криптографічних і стеганографічних методів і алгоритмів. Якщо *криптографія (тайнопис, від грецьких слів kryptos – таємний,і grapho – запис)* вивчає методи перетворення інформації, що забезпечують її конфінденційність та автентичність, то *стеганографія (скритний, прихований, від грецького слова steganos)* – вивчає методи забезпечення скритності самого факту передавання однієї інформації (секретної) серед іншої.

При цьому, займаючи свою нішу в забезпеченні безпеки інформації, стеганографія не замінює, а доповнює криптографію.

3.5.1. Криптографічні методи захисту інформації

ЗІ методом криптографічного перетворення заключається в перетворенні її складових частин (слів, букв, цифр) за допомогою спеціальних алгоритмів або апаратних рішень і кодів ключів з метою приведення її до неявного виду. Для ознайомлення (читання) із шифрованою інформацією застосовується зворотній процес – декодування (дешифрування). Використання криптографії є одним з розповсюджених методів, що значно підвищують безпеку передачі даних у мережах ЕОМ; даних, що зберігаються у пристроях памяті; при обміні інформацією між віддаленими об'єктами.

Для перетворення (шифрування) звичайно використовується деякий алгоритм або пристрій, що реалізує заданий алгоритм.

Керування процесом шифрування здійснюється за допомогою періодично міняємого коду ключа, що забезпечує щораз оригінальне представлення інформації при використанні того ж самого алгоритму чи пристрою. Знання ключа дозволяє просто і надійно розшифрувати текст. Однак, без знання ключа ця процедура може бути практично нездійсненна навіть при відомому алгоритмі шифрування. Розглянемо схему проходження потоку інформації в криптографічній системі, що забезпечує секретність інформації (рис. 3.2).

Відправник генерує відкритий текст вихідного повідомлення *M*, що повинне бути передано законному одержувачу по незахищеному каналу. За каналом стежить перехоплювач з метою перехопити і розкрити передане повідомлення.

Для того, щоб перехоплювач не зміг довідатися зміст повідомлення *M*, відправник шифрує його за допомогою оборотного перетворення *Ек* і одержує шифртекст (або криптограму) $C = E_K (M)$, що відправляє одержувачу.

Законний одержувач, прийнявши шифртекст С, розшифровує його за допомогою зворотного перетворення $D = E_K^{-1}$ й одержує вихідне повідомлення у виді відкритого тексту М:

$$D_K (C) = E_K^{-1} (E_K (M)) = M. \qquad (1.4)$$

Перетворення *Ек* вибирається з відповідного сімейства криптографічних перетворень. Параметр, за допомогою якого вибирається окреме перетворення, що використовується, називається криптографічним ключем *К*.

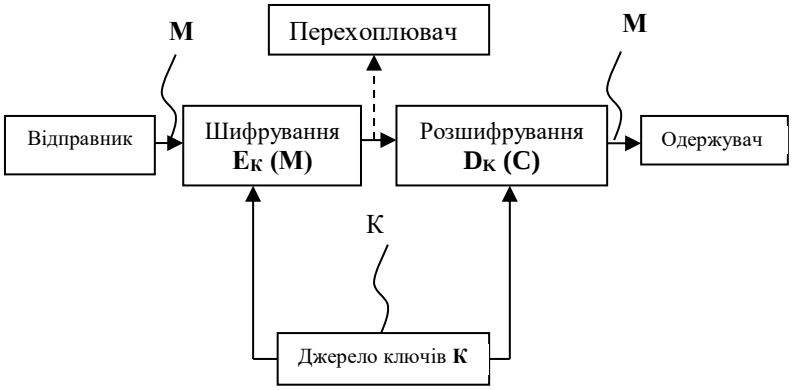


Рис. 3.2. Потік інформації в криптографічній системі, що забезпечує секретність

При цьому (відповідно до принципу Кірхгофа) секретність перетворення забезпечується секретністю ключа, а не секретністю алгоритму шифрування. Хоча, зберігаючи в секреті сутність криптосистеми, можна додатково підвищити стійкість шифру (перетворення). На протязі багатьох сторіч людство використовувало криптографічні методи і засоби для ЗІ при її передачі й зберіганні. В даний час деякі методи шифрування добре пророблені і є класичними. Загальна класифікація криптографічних методів ЗІ приведена на рис. 3.3.

Рис. 3.3. Класифікація криптографічних методів захисту

Методи заміни (підстановки) реалізуються за допомогою шифрів заміни (підстановки). Шифром заміни (підстановки) називається алгоритм шифрування, що робить заміну кожного символу відкритого тексту на відповідний символ зашифрованого тексту. Прикладами шифрів заміни (підстановки) є моноалфавітна заміна (1:1), гомофонічна заміна (1:*m*), поліалфавітна заміна (1:*N*), поліграмна заміна (за спеціальними правилами).

При моноалфавітній заміні кожній букві алфавіту відкритого тексту ставиться у відповідність одна буква шифртексту з того ж алфавіту. Загальна формула моноалфавітної заміни для 30-ти буквенного алфавіту має вид:

$$Ei = K_1 Mi + K_2 \text{ (mod 30)}, \qquad (1.4)$$

де K_1 і K_2 – константи, Mі – символ вихідного тексту, Eі – символ шифртекста.

Шифр, що задається формулою Eі = Mі + Kі (mod 30), називається шифром Віжінера. Тут Kі – i-та буква ключа.

Недоліком розглянутого методу є слабкі статистичні властивості шифртекста, тобто збереження в ньому частот появи букв відкритого тексту.

При гомофонічній заміні кожному символу відкритого тексту ставиться у відповідність m символів (цифр) шифртекста, використовуваних для заміни по черзі. Цей метод застосовується для поліпшення статистичних властивостей шифртекста.

При поліалфавітній заміні використовується (N) алфавітів шифртексту, що використовуються по черзі для заміни символів відкритого тексту.

Поліграмна заміна формується з одного алфавіту за допомогою спеціальних правил, наприклад, матриці шифру Плейфера.

При розгляді шифрів заміни становиться очевидним, що чим більше довжина ключа, тим краще шифр. Істотного поліпшення властивостей шифртексту можна досягти при використанні шифру з автоключем. Шифрування в цьому випадку починається з ключа і продовжується за допомогою відкритого тексту чи криптограми, зміщених на довжину первинного ключа.

Методи перестановки реалізуються за допомогою шифрів перестановки. Шифром перестановки називається алгоритм шифрування, у якому букви (символи) відкритого тексту не заміняються на інші, а міняється сам порядок їхнього проходження у відповідності з ключем.

Прикладами шифрів перестановки є проста перестановка, ускладнена по таблиці, ускладнена по маршрутах (гамільтоновим шляхам).

При простій перестановці послідовність перестановки символів визначається ключем – правилом перестановки. Наприклад, групи з 8 букв із порядковими номерами 1, 2, ..., 8 переставляються у порядок 3, 8, 1, 5, 2, 7, 6, 4.

При ускладненій перестановці по таблиці (матриці) відкритий текст записується в матрицю по визначеному ключу K1, а шифртекст зчитується з цієї матриці по ключу K2.

При ускладненій перестановці по гамільтонових шляхах (маршрутах) відкритий і шифрований текст представляються різними варіантами шляхів (маршрутів) у таблиці (на графі).

Існують і інші способи перестановки, які можна реалізувати програмним і апаратним шляхом. Наприклад, реалізований апаратним шляхом блок перестановки, що для перетворення інформації використовує електричні ланцюги, по яких вона передається рівнобіжним способом. Перетворення тексту полягає в переплутуванні порядку розрядів у цифровій кодограмі шляхом зміни електричного монтажу схеми в блоці. Для дешифрації на приймальному пункті встановлюється інший блок, що відновлює порядок ланцюгів.

Для методів (шифрів) перестановки характерна простота алгоритму, можливість як апаратної, так і програмної реалізації, і низький рівень захисту. З метою удосконалення методу перестановки застосовуються об'ємні (багатомірні) перестановки, наприклад, перестановка за принципом кубика Рубика.

Методи аналітичного перетворення реалізуються за допомогою шифрування за визначеними правилами або залежностям. Прикладом аналітичних перетворень є використання апарата матричної алгебри. Якщо записати вихідний текст у виді матриці ||М||, ключ – у виді матриці ||К||, то шифртекст ||Е|| буде отриманий в результаті множення вихідних матриць

$$||E|| = ||M||x||K||.$$

Відповідно, розшифрований текст отримується за правилом

$$||M||^{-1} = ||E||x||K||.$$

Тут транспонована матриця $||M||^{-1}$ − має розмір 1х*m*, матриця ||К|| − розмір *m*х*n*, матриця ||Е|| − розмір Іх*m*.

Метод гамування полягає в генерації гами *Г*, що представляє собою послідовність випадкових (псевдовипадкових) чисел, і наступному накладанні гами на відкритий текст, за визначеним правилом, наприклад, підсумовуванням за модулем 2:

$$E = Г \oplus M.$$

Для одержання вихідного тексту застосовується зворотне перетворення:

$$M = Г \oplus E.$$

Отриманий цим методом шифртекст достатньо складний для розкриття, оскільки ключ є змінним для кожного блоку, що шифрується. Криптостійкість такого шифру визначається властивостями гама-послідовності.

Комбіновані методи припускають застосування різних методів шифрування в комплексі. Комбіновані методи забезпечують найбільш високу криптостійкість і найчастіше використовуються на практиці.

Новий напрямок застосування засобів криптографічного захисту відкрився із набуттям чинності Закону "Про електронний цифровий підпис". Електронний цифровий підпис − вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним

поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Симетричні криптографічні алгоритми. Схематично зашифрування та розшифрування при використанні симетричних криптографічних алгоритмів зображені на рис. 3.4.

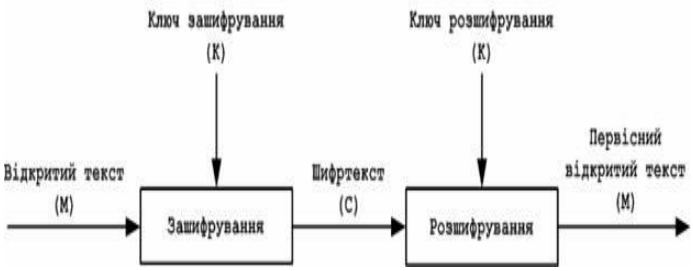


Рис. 3.4. Операції зашифрування та розшифрування у симетричних алгоритмах

Симетричні алгоритми поділяються на дві категорії. Одні алгоритми обробляють відкритий текст побітово (іноді побайтово), вони називаються потоковими алгоритмами або потоковими шифрами. Інші працюють з групами бітів відкритого тексту. Групи бітів називаються блоками, а алгоритми − блоковими алгоритмами або блоковими шифрами.

Прикладами блокових алгоритмів є симетричні алгоритми блочного шифрування – ГОСТ 28147-89 і AES-128.

ГОСТ 28147-89 визначає єдиний алгоритм криптографічного перетворення для систем обробки інформації в мережах електронних обчислювальних машин, окремих обчислювальних комплексах та спец виробах.

Алгоритм криптографічного перетворення призначений для апаратної або програмної реалізації, задовольняє криптографічним вимогам та по своїм можливостям не накладає обмежень на ступінь секретності інформації, що захищається.

Алгоритм обробляє блоки довжиною 64 біта, довжина ключа – 256 біт, кількість раундів перетворення одного блоку – 32.

Стандарт є обов'язковим для організацій, закладів і установ, які використовують криптографічний захист даних, що зберігаються та передаються, в мережах ЕОМ, окремих обчислювальних комплексах та спецвиробах.

Структурна схема алгоритму криптографічного перетворення ГОСТ 28147-89 містить (рис. 3.5):

− ключовий запам'ятовуючий пристрій (КЗП) на 256 біт з восьми 32-розрядних накопичувачів (X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7);

− чотири 32-розрядних накопичувачі (N_1, N_2, N_3, N_4);

− два 32-розрядних накопичувачі (N_5, N_6) із записаними в них постійними заповненнями C_2, C_1;

− два 32-розрядних суматори по модулю 2^{32} ($СМ_1$, $СМ_3$);

− 32-розрядний суматор порозрядного складання по модулю 2 ($СМ_2$);

− 32-розрядний суматор по модулю ($2^{32}-1$) ($СМ_4$);

− суматор по модулю 2($СМ_5$), обмеження на розрядність суматора $СМ_5$ не накладається;

− блок підстановки (K);

− регістр циклічного зрушення на одинадцять кроків убік старшого розряду (R).

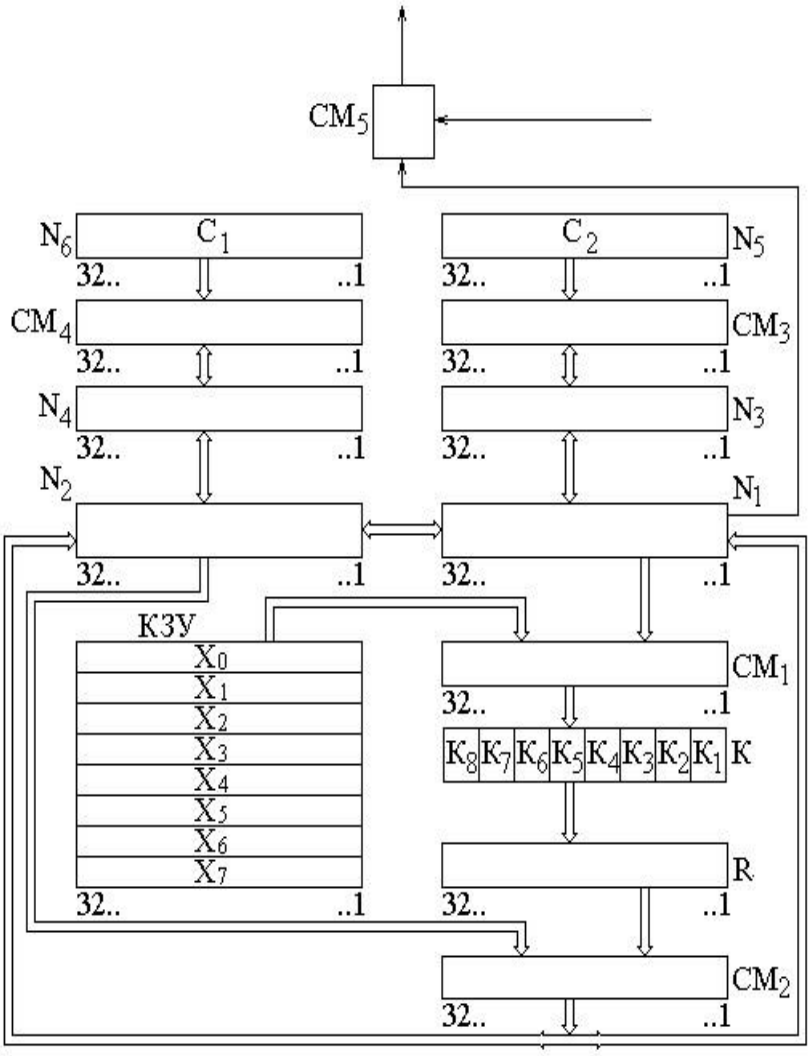


Рис. 3.5. Структурна схема алгоритму криптографічного перетворення ГОСТ 28147-89

Блок підстановки K складається з восьми вузлів заміни K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8 з пам'яттю на 64 біта кожний.

32-розрядний вектор, що надходить на блок підстановки, розбивається на вісім, що послідовно йдуть 4-розрядних вектора, кожний з яких перетвориться в 4-розрядний вектор відповідним вузлом заміни, що

представляє собою таблицю із шістнадцяти рядків, що містять по чотири біта заповнення в рядку. Вхідний вектор визначає адресу рядка в таблиці, заповнення даного рядка є вихідним вектором. Потім 4-розрядні вихідні вектори послідовно об'єднуються в 32-розрядний вектор.

При додаванні і циклічному зрушенні двоїчних векторів старшими розрядами вважаються розряди накопичувачів з більшими номерами.

При записі ключа (W_1, W_2 ..., W_{256}), $W_q \in \{0,1\}$, q=1÷256, у КЗП значення W_1 вводиться в 1-й розряд накопичувача X_0, значення W_2 вводиться в 2-й розряд накопичувача X_0, ... значення W_{32} вводиться в 32-й розряд накопичувача X_0; значення W_{33} вводиться в 1-й розряд накопичувача X_1, значення W_{34} вводиться в 2-й розряд накопичувача X_1, ..., значення W_{64} вводиться в 32-й розряд накопичувача X_1; значення W_{65} вводиться в 1-й розряд накопичувача X_2 і т. д., значення W_{256} вводиться в 32-й розряд накопичувача X_7.

При перезаписі інформації вміст *p*-го розряду одного накопичувача (суматора) переписується в *p*-й розряд іншого накопичувача (суматора).

Ключі, що визначають заповнення КЗП і таблиць блоку підстановки *K*, є секретними елементами і поставляються у встановленому порядку. Заповнення таблиць блоку підстановки *K* є довгостроковим ключовим елементом, загальним для мережі ЕОМ.

Організація різних видів зв'язку досягається побудовою відповідної ключової системи. При цьому може бути використана можливість вироблення ключів (заповнень КЗП) у режимі простої заміни і зашифрування їх у режимі простої заміни з забезпеченням імітозахисту для передачі по КЗ або збереження в пам'яті ЕОМ.

В криптосистемі передбачені чотири види роботи:

− зашифровування (розшифровування) даних в режимі простої заміни;

− зашифровування (розшифровування) даних в режимі гамування;

− зашифровування (розшифровування) даних в режимі гамування з зворотнім зв'язком;

− режим виробки імітовставки.

AES (Advanced Encryption Standard) – новий світовий криптостандарт, оголошений 2 жовтня 2000 року по результатам конкурсу на найкращий стандарт симетричного шифрування. Переможцем конкурсу став бельгійський алгоритм *RIJNDAEL*.

Як блоковий ітеративний шифр, AES зашифровує дані блоками фіксованого (на час виконання) розміру: 128, 192 або 256 бітів.

Можливі довжини ключа рівні відповідно 128, 192 або 256 біт. Для зашифрування даних виробляються циклові підключі за допомогою спеціального алгоритму розгортання – "утворення підключів" (key evolution). При цьому їх кількість на одиницю більша числа виконуваних раундів зашифрування.

Число раундів залежить від розмірів блоку і довжини ключ і дорівнює відповідно 10, 12 або 14.

Схема функції E_k зашифрування криптоалгоритму *RIJNDAEL* при $N_k = N_b = 128$ біт приведена на рис. 3.6.

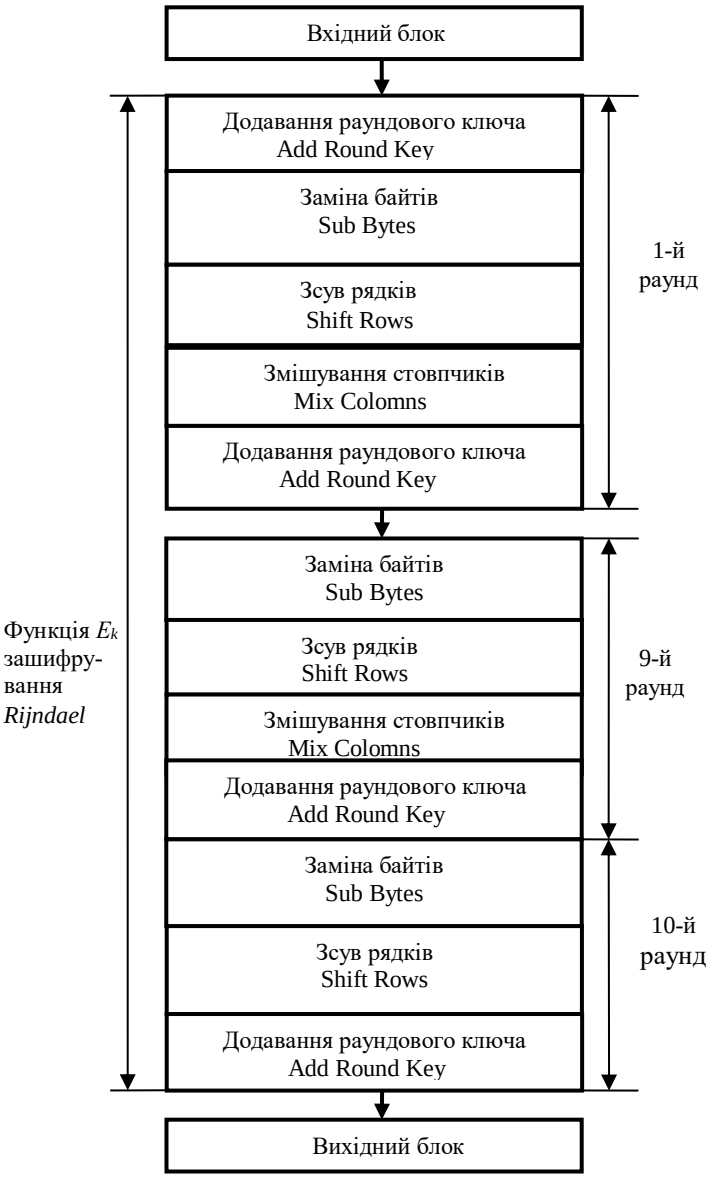


Рис. 3.6. Алгоритм блокового зашифрування *RIJNDAEL*

Шифр *RIJNDAEL* складається:

– з початкового додавання раундового ключа;

– 9-ти раундів;

– заключного десятого раунду, у якому відсутня операція *Mix Columns()*.

Кожен раунд можна описати за допомогою чотирьох основних кроків:

– нелінійна підстановка (заміна байтів);

− зсув рядків;

− змішування стовпчиків;

− додавання раундового ключа (складання з цикловим під-ключем).

Розглянутий стандарт симетричного шифрування AES є останнім стандартом, який прийнятий до виконання більшістю розвинутих держав як міжнародний стандарт.

Однією зі значних переваг цього стандарту в порівнянні з ГОСТ 28147-89 є стандартизовані довжини ключа 128, 192, 256 бітів. Це досить важливий фактор, який дозволяє змінювати рівень криптографічної стійкості системи криптозахисту, якщо це потрібно. Більшість ПЗ сучасних виробників використовує цей стандарт як основний стандарт симетричного шифрування.

Асиметричні криптографічні алгоритми. Алгоритми з відкритим ключем (звані також асиметричними алгоритмами) розроблені таким чином, що ключ, який використовується для зашифрування, відрізняється від ключа розшифрування.

Такі алгоритми називають алгоритмами з відкритим ключем, тому що ключ зашифрування може бути відкритим: хто завгодно може використовувати цей ключ для зашифрування повідомлення, але розшифрувати повідомлення може тільки конкретна людина, яка знає ключ розшифрування.

У таких системах ключ зашифрування часто називають відкритим ключем, а ключ розшифрування – закритим ключем. Закритий ключ іноді називають секретним ключем.

Схематично зашифрування та розшифрування при використанні асиметричних криптографічних алгоритмів зображені на рис. 3.7.

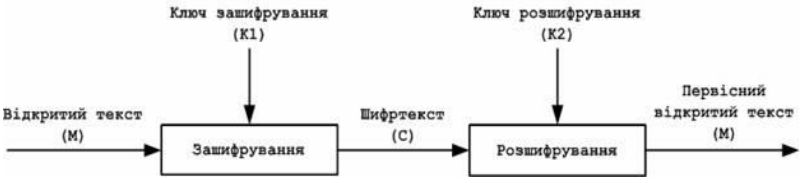


Рис. 3.7. Операції зашифрування та розшифрування в асиметричних алгоритмах

Від часу винайдення криптографії з відкритим ключем було запропоновано безліч асиметричних криптографічних алгоритмів. Найбільшого розповсюдження отримали три алгоритми: RSA, ElGamal (Ель-Гамаля) та Rabin (Рабіна).

Слід відмітити, що вони зашифровують і розшифровують дані набагато повільніше, ніж симетричні алгоритми.

Тому звичайно їх використовують в схемах ЕЦП.

Електронний цифровий підпис. ЕЦП являє собою послідовність символів, вироблену на підставі геш-функції даного документа й особливого коду, що належить власникові підпису. Цей код називається

особистим ключем підпису й повинен бути відомий лише його власникові. У принципі його можна пам'ятати і вводити із клавіатури щораз при виробленні конкретного підпису, але набагато зручніше зберігати цей код в електронному виді – на спеціальному носії, з якого він може бути зчитаний засобами ЕЦП. Вимоги зі зберігання й застосування особистого ключа в цілому аналогічні вимогам для звичайної круглої печатки. Саме ЕЦП виконує функцію посвідчення інформації, оскільки вироблену на його основі послідовність символів завжди можна однозначно співвіднести із власником ключа, хоча конкретний вид послідовності визначається також і геш-функцією.

Звичайно цифровий підпис приєднується до повідомлення й у такому вигляді відправляється адресатові. Модель цифрового підпису з додаванням представлена на рис. 3.8. Схема ЕЦП із додаванням є найпоширенішою схемою в практичних додатках з використанням, як правило, криптографічного алгоритму RSA.

Для верифікації такого ЦП необхідно мати підпис s і відповідне повідомлення m. Нехай необхідно підписати деяке повідомлення довільної довжини $m \in M$, де M – простір повідомлень. Попереднє повідомлення m гешується з використанням однобічної й вільної від колізій геш-функції:

$$h(m) = \tilde{m} \in M_h, \qquad (1.5)$$

де M_h – простір геш-кодів.

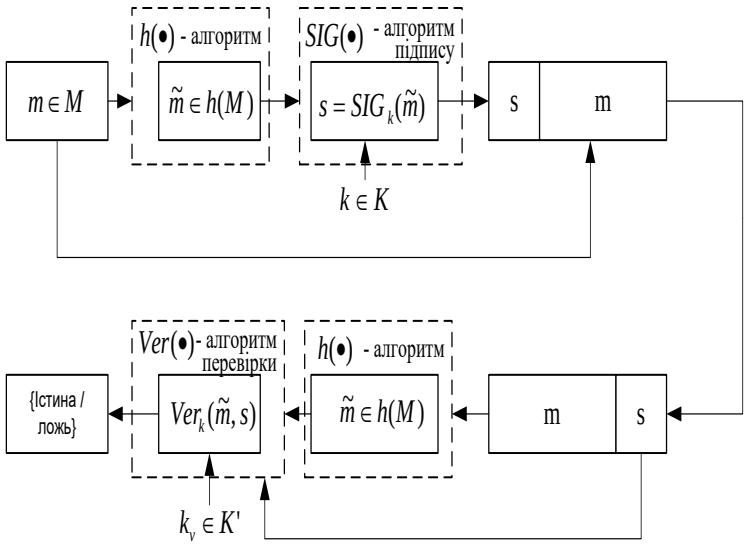


Рис. 3.8. Модель цифрового підпису з додаванням до повідомлення

Використовуючи особистий ключ $k \in K$, де K – простір ключів, обраний алгоритм генерації підпису SIG (•) і геш-код повідомлення $\tilde{m}$, відправник генерує підпис $s \in S$, де S – простір підписів $s = SIG_k(\tilde{m})$.

Повідомлення m і підпис s, що *додається* до нього, відправляється одержувачу. Одержувач робить верифікацію підпису наступним чином.

Він одержує у своє розпорядження автентичну копію ключа верифікації $\in K'$. Потім за отриманим повідомленням m обчислює геш-код = $h(m)$ і, використовуючи алгоритм верифікації $VER(\bullet)$, приймає рішення відносно справжності або хибності підпису:

$$VER_K(m, r, s) \rightarrow \{\text{істина, неправда}\}.$$

Однією з найбільш цікавих альтернатив до класичних криптосистем з відкритим ключем є криптосистема, що заснована на еліптичних кривих, визначених над скінченними полями. Безпека такої криптосистеми залежить від труднощів визначення дискретних логарифмів в групі точок еліптичної кривої.

Криптосистеми з відкритим ключем, засновані на еліптичній кривій, можуть використовувати набагато коротші параметри, ніж *RSA*-системи або системи, що базуються на проблемі класичного дискретного логарифму. Щоб досягти поміркованого захисту (10^{26}) *RSA* повинен мати 1024 бітні ключі, в той час, як криптосистемі на еліптичній кривій достатньо 160-бітного ключа.

3.5.2. Криптографічні засоби захисту інформації

Більшість засобів криптографічного захисту даних реалізовано у вигляді спеціалізованих апаратних пристроїв.

Криптографічні засоби ЗІ апаратної реалізації можна розділити на такі категорії:

− комплекси криптографічного захисту цифрових потоків передачі інформації;

− абонентські засоби криптографічного захисту провідного, радіо й мобільного зв'язку;

− криптографічно сильні генератори випадкових чисел і засоби генерації ключів на їхній основі;

− засоби криптографічного захисту в мережах передачі даних.

До комплексів криптографічного захисту цифрових потоків передачі інформації можна віднести:

“Скрипт-6401” – засіб захисту цифрових потоків El;

Д-300 – засіб криптографічного захисту цифрових потоків El;

Д-300/Ц – центр генерації й запису ключових даних;

МКД – захищений носій ключових даних;

Д-400 – абонентський засіб криптографічного захисту цифрових потоків ISDN;

Д-400/Ц – центр генерації й запису ключових даних.

Абонентські засоби криптографічного захисту дротового, радіо й мобільного зв’язку можна розділити на такі категорії:

“СЕКМОД” – криптографічний ТА;

“Криптон-4М7” – апарат захищеного мовного й факси-мільного зв’язку;

“СЕКТОР” – апарат криптографічного захисту для термінала космічного зв’язку;

“СЕКРЕТ” – апарат криптографічного захисту для термінала мобільного зв’язку;

“ТОПАЗ-8000” – апарат захищеної передачі даних;

“КРИОН” – радіостанція із захищеним цифровим каналом.

До засобів криптографічного захисту в мережах передачі даних відносяться:

“ОНІКС” – пристрій тунельного шифрування інформації у віртуальній приватній мережі;

“КОКОН” – автономний пристрій попереднього шифрування інформації.

До криптографічно сильних генераторів випадкових чисел і засобів генерації ключів на їхній основі відносяться:

МКЕ-5101У, МКЕ-5102 – мікрозборки генераторів випадкових біт;

МКЕ-5121А – гібридна мікрозборка широкополосного генератора шуму;

МКЕ-523О – високошвидкісний модуль генерації випадкових чисел;

TestRNG – апаратно-програмний комплекс тестування генераторів випадкових чисел;

МКЕ-5102STEND – оцінний модуль для генераторів випадкових біт;

Д-300/Ц – центр генерації й запису ключових даних для апаратів Д-300,

Д-400/Ц – центр генерації й записи ключових даних для апаратів Д-400;

“ТОПАЗ-Ц” – центр генерації ключових даних для апаратів “ТОПАЗ”;

Компакт диски з масивами істинно випадкових чисел “CD-TRNG”;

Блок уведення ключових даних “Інжектор”;

Блок запису ключових даних “Ірпінь-2РКД”.

Серед програмних засобів криптографічного ЗІ слід виділити “Грифон-Б” та “Грифон-Л”. Вказані програмні засоби призначені для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах і застосовуються для обміну інформацією усередині корпоративної мережі банку, із клієнтами, що працюють по системі “Клієнт-Банк”, у системах обслуговування пластикових карт й ін.

3.5.3. Стеганографічний захист інформації

На відміну від криптографії, де зловмисник точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні матеріали в звичайні повідомлення так, щоб неможливо було запідозрити сам факт існування таємного послання.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не заміняє, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує імовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифроване, то воно має ще один, додатковий, рівень захисту. Сучасний прогрес в області глобальних комп'ютерних мереж і мультимедійних засобів привів до розробки нових методів в розвитку і вдосконаленні стеганографії – появі комп'ютерної стеганографії. Методи комп'ютерної стеганографії, враховуючи природні неточності пристроїв оцифрування і надмірність аналогового відео або аудіо сигналу, дозволяють приховувати повідомлення в спеціальних комп'ютерних файлах – контейнерах. У сучасній комп'ютерній стеганографії виділяють два основних типи файлів: повідомлення-файл, яке призначене для приховування, та контейнер-файл, який може бути використаний для приховування в ньому повідомлення. При цьому контейнери бувають двох типів. Контейнер-оригінал (або "порожній" контейнер) – це контейнер, який не містить прихованої інформації. Контейнер-результат (або "заповнений" контейнер) – це контейнер, який містить приховану інформацію. Під ключем розуміється секретний елемент, який визначає порядок занесення повідомлення в контейнер. Таким чином, стеганографічна система або стегосистема – сукупність засобів і методів, які використовуються для передачі прихованих повідомлень.

Алгоритм вбудовування повідомлення в найпростішому випадку складається із двох етапів:

1. Вбудовування секретного повідомлення в контейнер-оригінал.
2. Виявлення (виділення) прихованого повідомлення з контейнера-результату.

Виходячи із цього, розглянемо математичну модель стегосистеми. Для тривіального стеганографічного перетворення описується залежність:

$$E: \quad C \times M \rightarrow S \tag{1.6}$$

$$D: \quad C \rightarrow M \tag{1.7}$$

де $S = \{(c_1, m_1,), (c_2, m_2), ..., (c_n, m_n), ..., (c_q, m_q)\} = \{s_1, s_2, ..., s_q\}$ − множина результатів (стеганограм).

Залежність (9.1) описує процес приховування інформації, залежність (9.2) – добування прихованої інформації. При цьому оба адресата (відправник і отримувач) повинні знати алгоритм прямого (E) і зворотного (D) стеганографічного перетворення.

Отже, у загальному випадку стегосистема − це сукупність контейнерів (оригіналів і результатів), повідомлень і перетворень, що пов'язані між собою: $\sum = (C, M, S, E, D)$.

Для більшості стегосистем множини контейнерів C обираються таким чином, щоб у результаті стеганографічного перетворення заповнений контейнер і контейнер-оригінал були подібні, що формально може бути оцінено за допомогою функції подібності. З огляду на все різноманіття стеганографічних систем, звичайно їх зводять до чотирьох наступних типів: безключеві стегосистеми, системи з секретним ключем, системи з відкритим ключем і змішані стегосистеми.

Безпека безключевої стегосистеми заснована на секретності використовуваних стеганографічних перетворень E і D. Якщо припустити, що супротивник знає алгоритми E і D, які використовуються для прихованої передачі інформації, то він здатний витягти будь-яку приховану інформацію з перехоплених стеганограм. Найчастіше для підвищення безпеки безключової системи, перед початком процесу стеганографічного приховування попередньо виконується шифрування інформації, що приховується.

Однак, “сильні” стеганографічні системи, як правило, не потребують попереднього шифрування повідомлень, які приховуються. До таких стегосистем відносяться інші три види стегосистем. Безпека таких стегосистем грунтується на деякій секретній інформації, без знання якої не можна витягнути з контейнера секретну інформацію, що і називається стегоключем. Відправник, вбудовуючи секретне повідомлення в обраний контейнер C, використовує секретний стегоключ k.

Якщо ключ k використовується в стеганографічному перетворенні відомий одержувачу, то він зможе витягти приховане повідомлення з контейнера. Тоді, *стегосистемою з секретним ключем* називається система, для якої $E_K: C \times M \times K \to S^K$ та $D_K: S^K \times K \to M$ – функції прямого і зворотного стеганоперетворення (приховування або вбудовування повідомлення в контейнер і вилучення повідомлення з контейнера), причому $D_K(E_K(c, m, k), k) = m$ для будь-яких $m \in M$, $c \in C$ та $k \in K$.

Стеганографічні системи з відкритим ключем не потребують додаткового каналу ключового обміну. Для їх функціонування необхідно мати два стегоключа: один секретний, який користувач повинен зберігати в таємниці, а другий – відкритий, який зберігається у доступному для всіх місці. При цьому відкритий ключ використовується в процесі приховування інформації, а секретний – для її вилучення. У безключевих стегосистемах часто використовують особливості криптографічних систем з відкритим і (або) секретним ключем. В цьому випадку маємо приклад змішаної стегосистеми. В основі базових підходів до реалізації методів комп’ютерної стеганографії лежить використання того чи іншого інформаційного середовища, виділення малозначущих фрагментів середовища і заміна існуючої в них інформації на інформацію, яку передбачається захистити. Таким чином, незначущі для кадру інформаційного середовища фрагменти відповідно до тих чи інших

алгоритмів або методик замінюються на фрагменти інформації, що приховується. Під кадром інформаційного середовища в даному випадку мається на увазі деяка його частина, виділена за певними ознаками. Наприклад, в якості кадру може бути обраний певний окремий малюнок, звуковий файл, Web-сторінка та ін. За типом інформаційного середовища виділяються стеганографічні методи для текстового середовища, для аудіо середовища, а також для зображень (стоп-кадрів) і відео середовища (рис. 9.9).

Рис. 3. 9. Класифікація методів комп'ютерної стеганографії за типом інформаційного середовища

3.6. Критерії захищеності засобів обчислювальної техніки

Основні канали витоку засобів ЕОТ залежно від середовища поширення інформативних сигналів були розглянуті в п. 3.1 і 3.2.

З точки зору оцінки захищеності кожен канал характеризується розмірами відповідної зони, за межами якої неможливий ефективний прийом або перехоплення, або гранично припустимим значенням відношення потужності інформативного сигналу і нормованої перешкоди.

Так, канал ЕМВ характеризується розміром зони ЕМВ – відстанню між засобом ЕОТ і антеною апаратури перехоплення, за межами якої неможливий ефективний прийом внаслідок природного зниження рівня випромінюваного сигналу.

Канал, що утворюється за рахунок наведених ЕРС в струмопроводящих комунікаціях, гальванічно не пов'язаних з ЕОТ і що мають вихід за межі КонтрЗ, характеризується розмірами їх зони відповідно для ЗВА і РВА.

До ЗВА відносяться будь-які технічні засоби, що мають вихід за межі КонтрЗ. До РВА відносять дроти, кабелі, елементи конструкцій будівлі і т.п. Відстань між ЕОТ і випадковою антеною (ВА), на якій неможливе ефективне перехоплення, визначає розмір КонтрЗ.

З урахуванням викладеного, можна сформулювати критерій захищеності ЗОТ від витоку через ПЕМВН [21].

ЗОТ вважається захищеним, якщо:

− радіус зони ЕМВ не перевищує мінімально допустимої відстані від ЗОТ до межі КЗ;

− відношення потужностей інформативного сигналу і нормованої перешкоди у всіх ВА не перевищує на межі КЗ гранично допустиму величину;

− відношення потужностей інформативного сигналу і нормованої перешкоди в усіх комунікаціях, що відходять, на границі КЗ не перевищує гранично допустиму величину.

Критерієм оцінки захищеності об'єкта обчислювальної техніки є наступна умова – якщо для пристрою ЗОТ відношення сигнал/шум (σ) на виході приймального пристрою перехоплення ІзОД не перевищує гранично допустимого значення δ у всіх можливих каналах витоку, тобто

$$\delta > \sigma = U_{c\ \text{пік}} / U_{ш\ еф}, \qquad (1.8)$$

то пристрій захищений від витоку. Об'єкт вважається захищеним в цілому, якщо захищений кожний пристрій.

Норми на відношення НСиг до шуму (завади) δ відносяться до послідовних та паралельних кодів, а також враховують багаторазове повторення інформації. Випромінювання одного розряду – це таке випромінювання, яке характерно для цього разряду у відсутності випромінювань інщих розрядів машинної комірки та будь-яких інших випромінювань. Якщо виміряне сумарне випромінювання великої кількості розрядів (але не більше 8), то необхідно провести розрахунок енергії на один розряд. Паралельні коди розрядністю більше 8 вважаються безпечними.

Якщо виміряно сумарне випромінювання декількох розрядів (але не більше 8), то необхідно провести нормування цього випромінювання на один розряд шляхом ділення його на експериментально визначений коефіцієнт,еквівалентний умовному числу розрядів у коді, або $n/2$, де n−число разрядів.

При регулярних повтореннях сигналу норма гранично допустимого відношення сигнал /перешкода ($\delta_П$) визначається за формулою:

$$\delta_П = \delta/\sqrt{K_п}\ , \qquad (1.9)$$

де $K_п$ – кількість повторень.

Гранично допустиме відношення сигнал/перешкода ($\delta_П$) визначається за формулою:

$$\delta_П = \delta K_н, \quad (1.10)$$

де $K_н$ – коефіцієнт, що враховує обмеження пропускної здатності даного каналу витоку по відношенню до швидкості роботи $S_{бод}$ джерела НСиг та вимірюється від 1 до 10 при зміні $S_{бод}$ від 50 до 1200. Для швидкості понад 1200 бод вказаний параметр не нормирується.

Слід відмітити, що взагалі рівні ПЕМВ цифрової техніки повинні відповідати вимогам санітарно-гігієнічних норм; норм електромагнітної сумісності (ЕМС); нормам та вимогам по ЗІ від витоку через ПЕМВ.

Як показує аналіз, норми на рівні ЕМВ з точки зору ЕМС суттєво (на декілька порядків) суворіше санітарно-гігієнічних норм. У той же час відповідність ПЕМВ засобів цифрової електронної техніки нормам на ЕМС не може бути гарантією збереження конфіденційності інформації, що обробляється за допомогою цих засобів.

Однак висока ступінь стандартизації методик та аппаратури вимірювання рівня ЕМВ при вирішенні задач оцінки ЕМС робить можливим (з урахуванням деяких особливостей) використання їх при вирішенні завдань ЗІ. При цьому на відміну від завдань ЕМС, де необхідно визначити максимальний рівень випромінення у заданому діапазоні частот, при вирішенні завдань ЗІ необхідно визначити рівень випромінення у заданому діапазоні частот, який відповідає інформативному сигналу. Тому оцінка рівня випромінювань при вирішенні завдань ЗІ повинна починатися з аналізу технічної документації, відбору електричних, ланцюгів, за допомогою яких можливо передавати ІзОД, визначення часових та спектральних характеристик НСиг. Після цього можливо приступати безпосередньо до визначення рівней інформативних ПЕМВ.

3.7. Методика проведення спеціальних досліджень технічних засобів електронно-обчислювальною технікою

При проведенні спеціальних досліджень необхідно вимірювати рівень ПЕМВ та розрахувати радіус зони $R2$, що характеризує мінімальну відстань від технічних засобів, на межі та за межами якого відношення сигнал/шум не перевищує нормованого значення (рис. 3.10).

У загальному випадку ця відстань може знаходитись у ближній, проміжній або дальній (хвильовій) зоні.

Для отримання об’єктивного значення $R2$ необхідно правильно визначати межі кожної зони.

Під ближньою зоною розуміється область навколо випромінювача, для якої $|kr| << 1$, где $k = 2\pi/\lambda$ − хвильове число. Отже, $r << \lambda/(2\pi)$. Під дальньою зоною розуміється область простору навколо випромінювача, для якої $|kr| >> 1$ або $r >> \lambda/(2\pi)$.

Під проміжною зоной розуміється область простору навколо випромінювача, в якому відстань *r* від випромінювача до вимірювальної антени одномірно з довжиною хвилі λ.

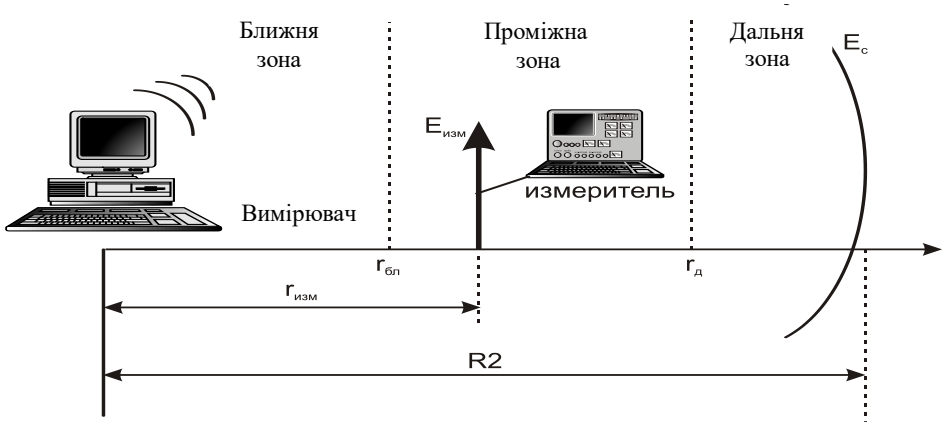


Рис. 3.10. Визначення радіуса зони *R*2

Взаємне порівняння внеску кожної зі складових у амплитуду напруженості електричного поля дозволяє визначити межі зон достатньої для практики точністю. Так, для межі ближньої зони $r_{бл} = \lambda/(2\pi\xi)$**.**

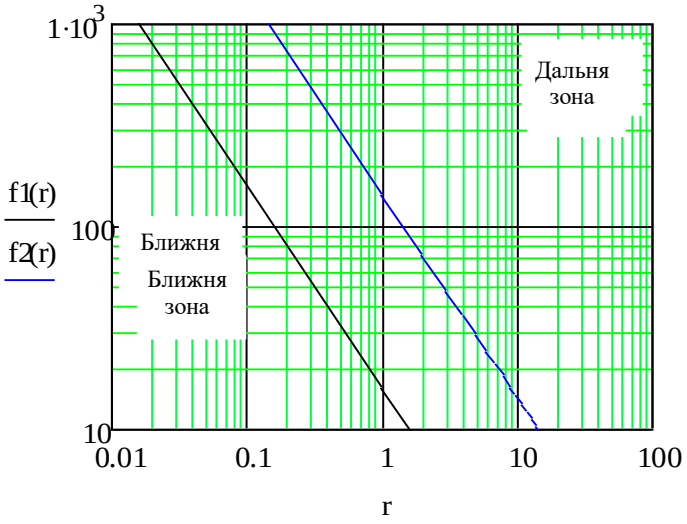
Аналогічно, для межі дальньої зони отримуємо: $r_д = \xi\lambda/2\pi$**.** Тут ξ − величина прийнятого граничного вкладу (перевищення) складових поля у ближній та дальній зонах, яка залежить від необхідної для практичних розрахунків точності та може складати від 3 до 10.

Ширина проміжної зони залежить від довжини хвилі ПЕМВ та обраної точності розрахунків та дорівнює:

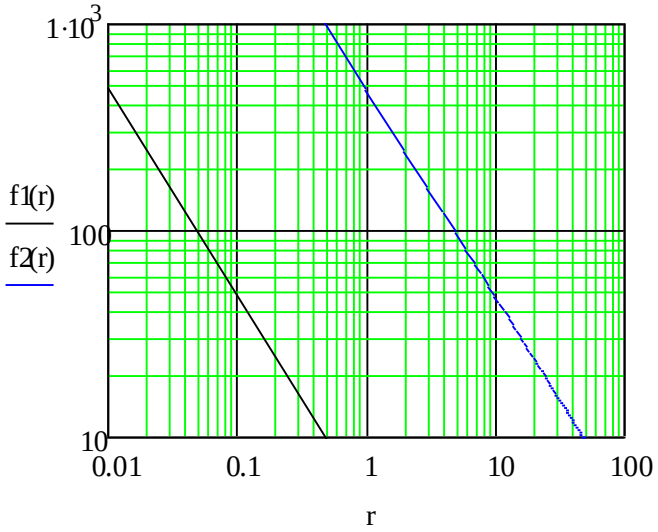
$$D = \lambda\text{Error!}. \qquad (1.11)$$

На рис. 3.11 представлені залежності відстаней до меж ближньої та дальньої зон від частоти ПЕМВ в МГц при ξ = 3 (а) та 10 (б)**.** Для стандартних (ГОСТ 16842-82) відстаней до вимірювача, рівних 1, 3 та 10 м на вимірюваній частоті можна визначити, в якій зоні розташовується вимірювач.

Виявлення НСиг із загальної сукупності сигналів і вимірювання їх рівня здійснюється при спеціально організованих тестових режимах технічних засобів (ТЗ), при яких тривалість та амплітуда інформаційних імпульсів залишаються тими ж, що й в робочому режимі, але використовується періодична імпульсна послідовність у вигляді пачок. Дана вимога пов’язана з тим, що у прийнятій методиці розрахунку результатів СІ значення смуги підсумовування частотних складових та тактова частота інформаційних імпульсів повинні бути константами. В іншому випадку розрахунок результатів стає неможливим.



а)



б)

Рис. 3.11. Залежність відстаней до меж зон від частоти ПЕМВ

Крім того, циклічне повторення одних і тих же “пакетів” інформації дозволяє за рахунок накопичення енергії ПЕМВН у вхідних ланцюгах вузькосмугових засобів вимірювання (приймачі, аналізатори спектра і т. д.) значно простіше виявляти та вимірювати значення НСиг на тлі шумів та завад.

Виявлення сигналу здійснюється з усіх сторін технічного засобу. Вимірювання сигналу здійснюється в піковому (квазіпіковому) режимі з напряму максимального випромінення, де виявлено НСиг.

Для виявлення тест-сигналів і виявлення їх із загальної сукупності прийнятих сигналів використовуються такі ознаки, як збіг частот виявлених гармонік і інтервалів між ними з розрахунковими значеннями, період і тривалість пачок, зміна форми сигналу на виході приймача при зміні параметрів тест-сигналу і т. ін.

Вимірювання рівней ПЕМВН проводиться лише після того, як переконуються, що прийнятий саме тест-сигнал.

Для визначення зони можливого перехоплення інформації необхідно розрахувати нормоване значення сигналу для відповідної частоти, визначити значення часткової зони і з усіх отриманих часткових зон вибрати максимальне, яке відповідає зоні $R2$.

Для забезпечення вимагаємої захищеності ЗОТ необхідно провести відповідні організаційні і технічні заходи.

Організаційні заходи спрямовані на те, щоб, незмінюючи рівня ПЕМВН засобу ЕОТ або рівня електромагнітних шумів, тим чи іншим способом змінити або розташуавння ТЗ, або межі КонтрЗ з тим, щоб зона можливого перехоплення інформації була менше, ніж $R_{кз}$ (КонтрЗ на об'єкті), тобто $R2 < R_{кз}$.

До технічних заходів ЗІ ЗОТ відносяться заходи і засоби, які впливають або на рівень ПЕМВ, або на рівень електромагнітних шумів. Наприклад, електромагнітне екранування – ефективний спосіб ЗІ, але потребує значних економічних витрат та регулярного контролю ефективності екранування. Крім того, повне електромагнітне екранування вносить дискомфорт у роботу обслуговуючого персонала.

Доробка ЗОТ дозволяє суттєво зменшити рівень інформаційних випромінювань, але повністю усунути їх неможливо. У сучасних умовах доробка техніки ЗОТ зводиться до підбору комплектуючих ЗОТ, так як власні разробки засобів ЗОТ у більшості випадків відсутні і збирання ПЕОМ здійснюється із закордонних комплектуючих.

Активне радіомаскування, зашумлення – застосування широкосмугових генераторів шуму. Основне завдання зашумлення ефіру – це підняти рівень електромагнітного шуму і тим самим перешкоджати радіоперехопленню інформаційних сигналів ЗОТ. Техничний ЗОТ буде захищений, якщо зона зашумлення: $R_{ш} > R2$.

3.8. Критерії захищеності автоматизованих систем

АС являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми.

Згідно НД ТЗІ 2.5-005-99, за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас "1" − одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Клас "2" − локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Клас “3” − розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю.

В зв’язку з цим, в кожному класі АС виділяються відповідні підкласи, які характеризуються підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності інформації, що обробляється окремо або у відповідних сполученнях.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС.

Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Нарощення ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проектованої або існуючої АС.

Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте, слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред’являються.

Перелік функціональних послуг безпеки та рівнів гарантій, їх структура і семантичне позначення наведені в НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від НСД”.

Ідентифікатори рівнів функціональних послуг приведені в табл. 3.1.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп’ютерній системі, Критерії містять критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки,

випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

Таблиця 3.1

Ідентифікатори рівнів функціональних послуг

Ідентифікатор послуги	Найменування послуги	Рівні послуги
Критерії конфіденційності		
КД	Довірча конфіденційність	КД-1−КД-4
КА	Адміністративна конфіденційність	КА-1−КА-4
КО	Повторне використання об’єктів	КО-1
КК	Аналіз прихованих каналів	КК-1−КК-3
КВ	Конфіденційність при обміні	КВ-1−КВ-4
Критерії цілісності		
ЦД	Довірча цілісність	ЦД-1−ЦД-4
ЦА	Адміністративна цілісність	ЦА-1−ЦА-4
ЦО	Відкат	ЦО-1−ЦО-2
ЦВ	Цілісність при обміні	ЦВ-1−ЦВ-3
Критерії доступності		
ДР	Використання ресурсів	ДР-1−ДР-3
ДС	Стійкість до відмов	ДС-1−ДС-3
ДЗ	Гаряча заміна	ДЗ-1−ДЗ-3
ДВ	Відновлення після збоїв	ДВ-1−ДВ-3
Критерії спостережності		
НР	Реєстрація	НР-1−НР-5
НИ	Ідентифікація і автентифікація	НИ-1−НИ-3
НО	Розподіл обов’язків	НО-1−НО-3
НВ	Автентифікація при обміні	НВ-1−НВ-3
НП	Автентифікація отримувача	НП-1−НП-2
НК	Достовірний канал	НК-1−НК-2
НЦ	Цілісність комплексу засобів захисту	НЦ-1−НЦ-3
НТ	Самотестування	НТ-1−НТ-3
НА	Автентифікація відправника	НА-1−НА-2

В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп’ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, у свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп’ютерної системи. Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги аналіз прихованих каналів залежність між функціональними послугами і гарантіями відсутня. Рівень послуги цілісність комплексу засобів захисту

НЦ-1 є необхідною умовою абсолютно для всих рівнів та всих послуг. Порядок оцінки АС на предмет відповідності цим критеріям визначається відповідними НД.

Експертна комісія, яка проводить оцінку АС, визначає, які послуги і на якому рівні реалізовані в АС (комп'ютерній системі), і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях.

Для того, щоб до рейтингу АС (комп'ютерної системи) міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Питання та завдання для самостійної перевірки знань

1. Назвіть і охарактеризуйте три основних напрями ТЗІ в АС і ЗОТ.
2. Назвіть і охарактеризуйте джерела каналів ВІ, що утворюються під час роботи ЕОМ. Що собою представляють додаткові канали ВІ.
3. Проведіть класифікацію можливих каналів ВІ, виходячи з принципів, відповідно з якими оброблюється інформація.
4. Поясніть принцип перехоплення інформації з ПЕОМ. Який з елементів ПЕОМ є найнебезпечнішим (рис. 9.1).
5. В чому полягає комплексний захист від НСД?
6. Які основні задачі вирішують програмні засоби захисту від НСД?
7. У яких випадках відбувається аварійне знищення інформації? В чому сутність програм сигналізації?
8. Перерахуйте основні заходи при проведенні робіт з ТЗІ в АС і ЗОТ, що передбачені ТР ЕОМ-95.
9. Назвіть і поясніть основні процедури алгоритму обстеження об'єктів ЕОТ.
10. Які складові включає ЗІ в АС і ЗОТ від витоку каналами ПЕМВН? В чому полягає застосування системи просторового зашумлення об'єктів ЕОТ та обладнання екранувальних конструкцій?
11. Що представляє собою спеціальний вплив на носії ІзОД і засоби забезпечення ТЗІ?
12. Яким чином здійснюється програмний захист від копіювання і руйнування?
13. Приведіть і поясніть класифікацію антивірусних програм. Охарактеризуйте основні групи комп'ютерних вірусів за деструктивними можливостями.
14. Поясніть ідентифікатори рівнів функціональних послуг Критеріїв конфіденційності (табл. 9.1).
15. Які вимоги включають Критерії гарантій? Поясніть основні рівні гарантій?

16. Рівень якої послуги є необхідною умовою абсолютно для всіх рівнів всих інших послуг?

17. Що представляє собою рейтинг АС?

РОЗДІЛ 4. КОНТРОЛЬ ЕФЕКТИВНОСТІ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ

Ефективність функціонування системи ЗІ досягається завдяки впровадженню комплексу взаємно узгоджених та взаємодоповнюючих правових, організаційних, криптографічних та технічних заходів, спрямованих на забезпечення безпеки інформації та захисту національних інформаційних ресурсів. Аналіз ефективності системи ЗІ – оцінювання відповідності фактичного рівня ЗІ від витоку та спеціальних впливів вимогам діючим НД.

4.1. Оцінка ефективності системи захисту інформації

У розділі 3, розглянутий системний підхід до побудови системи ТЗІ. Згідно з ним система задається відповідними цілями і завданнями, входами і виходами, діями та алгоритмами з ЗІ, а також обмеженнями, які необхідно враховувати при побудові (модернізації, оптимізації) системи. Для вибору раціонального варіанта СЗІ використовується критерій у вигляді відношення ефективність/вартість. Під ефективністю розуміють ступінь виконання системою завдань захисту, під вартістю – витрати на захист. В більшості практичних випадків, коли невідомий аналітичний вираз функції ефективності, доцільним є використання лінійної функції:

$$E = \frac{\alpha_1 K_1 + \alpha_2 K_2 + \ldots + \alpha_n K_n}{C_0}, \qquad (1.12)$$

де α_1, α_2 … α_n – вагові коефіцієнти, K_1, K_2, ..., K_n – часткові показники якості, n – кількість показників, $C_0 = C/C_m$ – відносна вартість, C – вартість системи захисту або заходів захисту, C_m – максимально допустиме значення вартості.

В якості міри ефективності $K_{еф}$ застосовуються різні композиції часткових показників, частіше їх “зважена” сума:

$$K_{еф} = \sum_{i=1}^{n} \alpha_i K_i, \qquad (1.13)$$

де α_i – “вага” часткового показника ефективності K_i.

Оцінка ефективності СЗІ можлива на підставі аналізу узагальненої моделі взаємодії системи ЗІ і навколишнього середовища. В даний час широко використовується імовірнісна модель, у відповідності з якою обробка інформації на об’єкті захисту здійснюється в умовах впливу на інформацію множини загроз $\{U_j\}_{j=1,s}$, що характеризуються відповідними значеннями імовірностей P_j і нанесених збитків w_j. Для забезпечення ІБ об’єкта система захисту повинна нейтралізувати вплив дестабілізуючих факторів і загроз, зменшивши імовірність загрози p_j.

Ступінь виконання i-го показника (вимоги) визначається його близькістю до необхідного (оптимального) значення.

У випадку кількісного виміру показника для оцінки ступеню його виконання зручніше за все використовувати нормоване значення:

$$\overline{K_i} = \frac{K_i - K_i^{нк}}{K_i^{нк} - K_i^{нг}}, \text{ якщо } K_i^{нк} \le K_i \qquad (1.14)$$

або

$$\overline{K_i} = \frac{K_i^{нк} - K_i}{K_i^{нк} - K_i^{нг}}, \text{ якщо } K_i \le K_i^{нк}, \qquad (1.15)$$

де K_i – поточне значення *i*-го показника; $K_i^{нк}$ і $K_i^{нг}$ – найкраще і найгірше значення показника; $0 \le \overline{K_i} \le 1$, i = 1, …, *r*.

У випадку якісного виміру показника для оцінки ступеня його виконання доцільно використовувати нечітке значення функції приналежності $K_i^{нч}$, $i = r + 1 \ldots, n$.

Відповідно до постановки задачі (10.1, 10.2) основними етапами її рішення є:

– збір і обробка експертної інформації про характеристики загроз – p_j і w_j;

– збір і обробка експертної інформації для визначення важливості виконання *i*-ї вимоги (показника) α_i для усунення відповідної загрози;

– розробка математичної моделі і алгоритму вибору раціонального варіанта побудови СЗІ відповідно до постановки як задачі нечіткого математичного програмування.

За відсутності інформації про загрози для вирішення задачі (10.1, 10.2) може бути використаний показник виду:

$$E = \frac{\sum_{i=1}^{r} \alpha_i \overline{K_i} + \sum_{i=r+1}^{n} \alpha_i K_i^{нч}}{C_0}. \qquad (1.16)$$

При цьому оцінка вартості системи технічного захисту *C* залежить від ступеня виконання вимог для конкретного варіанта її реалізації.

Оцінка ефективності КСЗІ в АС. КСЗІ представляє собою сукупність організаційних і інженерних заходів, а також програмно-апаратних заходів, які забезпечують ЗІ в АС. Оскільки базовою основою створення і функціонування КСЗІ є НПД в галузі ІБ, то при оцінці ефективності до цього слід додати наявність відповідної нормативно-правовової і наукової бази.

Таким чином, основними показниками ефективності КСЗІ можуть вважатися відповідність діючим вимогам правового, організаційного і інженерно-технічного забезпечення ЗІ в АС на всіх етапах проведення робіт зі створення КСЗІ в АС і в процесі експлуатації [13]. За результатами комплексної оцінки ефективності КСЗІ і оформленого на цій підставі позитивного експертного висновку уповноваженим органом – Адміністрацією ДССЗІ надається Атестат відповідності щодо можливості використання КСЗІ для забезпечення ТЗІ в АС. Повторна експертиза КСЗІ

проводиться після закінчення терміну дії Атестата відповідності – зазвичай, 5 років.

Цілком зрозуміло, що в даному випадку кожний частковий показник має однакову вагу, а значення кожного показника оцінюється експертом по відповідній шкалі (трибальній або двобальній), наприклад, “відповідає або виконано”, “відповідає або виконано не в повному обсязі”, “не відповідає або не виконано”. Тому оціночне значення ефективності визначається відносною вартістю $C_0 = C/C_m$, яка залежить від вартості системи захисту або заходів захисту і максимально допустимого значення вартості – чим менші витрати, тим ефективніше система.

Оцінка ефективності комплексу ТЗІ на ОІД. КТЗІ представляє собою сукупність організаційних, ІТЗ та засобів, призначених для захисту від витоку ІзОД технічними каналами на ОІД.

Оцінка ефективності комплексу ТЗІ на ОІД здійснюється при випробуваннях та атестації комплексу ТЗІ, яким передують виконання передпроектних робіт і розроблення та впровадження заходів із ЗІ [17].

Основними етапами атестації комплексу ТЗІ, що оцінюються, є:

– аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ, результатів випробувань;

– аналіз та оцінка відповідності проектної, конструкторської, експлуатаційної та іншої технічної документації на комплекс ТЗІ вимогам НД з питань ТЗІ;

– перевірка відповідності вихідних даних щодо створення комплексу ТЗІ реальним умовам розміщення ОІД;

– перевірка складу комплексу ТЗІ на відповідність даним, зазначеним у проектній, конструкторській, експлуатаційній та іншій технічній документації;

– перевірка наявності сертифікатів або експертних висновків на засоби забезпечення ТЗІ загального призначення;

– перевірка відповідності монтажу та умов експлуатації засобів забезпечення ТЗІ вимогам експлуатаційної документації;

– перевірка оформлення проекту паспорта на комплекс ТЗІ і паспорта на кожне приміщення;

– розгляд висновків за результатами випробувань.

На підставі позитивних результатів випробувань і атестації уповноваженою установою оформлюється Акт атестації комплексу та паспорт на КТЗІ щодо можливості забезпечення захисту від витоку технічними каналами ІзОД на ОІД, де вона озвучується або обробляється технічним засобами.

Атестація комплексу ТЗІ може бути первинною, черговою та позачерговою.

Термін проведення чергової атестації вказується в акті атестації та паспорті на комплекс ТЗІ (строк дії акта атестації не повинен перевищувати два роки).

Позачергову атестацію, а також необхідні випробування проводять у разі змін умов функціонування ОІД, що приводять до змін загроз для ІзОД, яка озвучуватиметься та/або оброблятиметься технічними засобами тощо, та за висновками органів, які контролюють стан ТЗІ.

Як і у випадку оцінки ефективності КСЗІ кожний частковий показник (етап атестації) має однакову вагу, а значення кожного показника оцінюється експертом по трибальній або двобальній шкалі. Тому оціночне значення ефективності визначається витратами на систему захисту – чим менші витрати, тим ефективніше система.

Модель комплексної оцінки системи ЗІ [23].

Модель комплексної оцінки СЗІ представлена у виді наступних основних блоків показників:

1. Блока показників “ОСНОВИ”.
2. Блока показників “НАПРЯМКИ”.
3. Блока показників “ЕТАПИ”.

Блок показників ОСНОВИ (O_i) включає наступну групу показників:

O_1 – Нормативно-правова і наукова база.

O_2 – Структура і задачі органів.

O_3 – Організаційні міри і методи (політика безпеки).

O_4 – Програмно-технічні способи і засоби.

Блок показників НАПРЯМКИ (H_j) дозволяє виділити наступні основні показники створення й оцінки комплексної СЗІ:

H_1 – Захист об’єктів корпоративних систем.

H_2 – Захист процесів, процедур і програм обробки інформації.

H_3 – Захист КЗ.

H_4 – Придушення ПЕМВ.

H_5 – Керування системою захисту.

Блок показників ЕТАПИ (M_k) розглядає наступні показники:

M_1 – Визначення інформації, що підлягає захисту.

M_2 – Виявлення повного безліч потенційна можливих погроз і каналів ВІ.

M_3 – Проведення оцінки уразливості і ризиків інформації при наявній множині загроз і каналів витоку.

M_4 – Визначення вимог до системи захисту.

M_5 – Здійснення вибору засобів ЗІ і їхніх характеристик.

M_6 – Впровадження й організація використання обраних мір, способів і засобів захисту.

M_7 – Здійснення контролю цілісності і управління системою захисту.

Структура моделі комплексної оцінки СЗІ базується на логічному об’єднанні показників блоків “ОСНОВИ”, “НАПРЯМКИ” і “ЕТАПИ” у

МАТРИЦЮ ОЦІНОК, що складається з K елементів, що визначаються зі співвідношення

(1.17)

На основі проведеного вище аналізу в даному варіанті (за умови, що $O_i = 4$, $H_j = 5$, $M_k = 7$) загальна кількість елементів "матриці" складає

.

Варто звернути увагу на зміст позначення кожного з елементів матриці, що формується із сукупності трьох часткових показників:

– перше знакомісце означає номер показника "ЕТАПИ";

– друге знакомісце – номер показника "НАПРЯМКИ";

– третє знакомісце – номер показника "ОСНОВИ".

На рис. 10.1 представлено приклад елемента матриці 321, що формується з урахуванням наступних показників:

3 – проведення оцінки уразливості і ризиків (показник № 3 блоки "ЕТАПИ");

2 – захист процесів і програм (показник № 2 блока "НАПРЯМКИ");

1 – нормативна база (показник № 1 блока "ОСНОВИ").

У залежності від етапів робіт із створення і оцінки комплексної СЗІ "матриця" має різний зміст.

Іншими словами це декілька однакових за структурою, але різних по змісту "матриць", а саме:

ЕТАПИ	НАПРЯМКИ	010				020			
		Захист об'єктів ІС				Захист процесів та програм			
	ОСНОВИ	Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби
		011	012	013	014	021	022	023	024
010	Визначення ін-формації, що підлягає захисту	111	112	113	114	121	122	123	124
020	Виявлення загроз та каналів ВІ	211	212	213	214	221	222	223	224
030	Проведення оцінки вразливості та ризиків	311	312	313	314	321	322	323	324
040	Визначення вимог до КСЗІ	411	412	413	414	421	422	423	424
050	Здійснення вибору засобів захисту	511	512	513	514	521	522	523	524
060	Втілення та використанняобраних заходів та засобів	611	612	613	614	621	622	623	624
070	Контроль цілісності та управління захистом	711	712	713	714	721	722	723	724

030				040				050			
Захист каналів зв'язку				ПЕМВН				Керування системою захисту			
Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби
031	032	033	034	041	042	043	044	051	052	053	054
131	132	133	134	141	142	143	144	151	152	153	154
231	232	233	234	241	242	243	244	251	252	253	254
331	332	333	334	341	342	343	344	351	352	353	354
431	432	433	434	441	442	443	444	451	452	453	454
531	532	533	534	541	542	543	544	551	552	553	554
631	632	633	634	641	642	643	644	651	652	653	654
731	732	733	734	741	742	743	744	751	752	753	754

Рис. 4.1 Формування елементів матриці знань

1. "Матриці" повноти і якості станів елементів СЗІ.
2. "Матриці" вимог до СЗІ.
3. "Матриці" оцінок ефективності функціонування елементів СЗІ.

Можуть розглядатися й інші функції цієї ж "матриці", головне щоб зміст кожного з елементів "матриці" описував взаємозв'язок складових створюваної СЗІ.

Основним змістом "Матриці повноти і якості" є питання "Які з заходів щодо ЗІ й у якому обсязі уже виконані?"

"Матриця вимог" містить питання: "Якою повинна бути створювана СЗІ? і дозволяє представити вигляд створюваної СЗІ, а також сформулювати вимоги до неї.

"Матриця оцінок" дозволяє визначити ефективність проведених заходів щодо ЗІ, задаючи питання: "Чи правильно будується СЗІ?" При цьому використовуються всі існуючі методики оцінки ефективності функціонування СЗІ.

У загальному випадку для "Матриці експертних оцінок" формуються всі 140 показників (по числу її елементів). Відповіді на ці питання дозволяють скласти повне уявлення про СЗІ й оцінити досягнутий рівень захисту.

Приклад застосування "Матриці експертних оцінок" для оцінки ефективності захищеності КЗ по 28-ми елементах (з 131 по 734) наведений на рис. 4.2 і рис. 4.3.

При цьому кожний показник визначається методом експертних оцінок, використовуючи положення теорії нечіткої логіки і нечітких тверджень.

ЕТАПИ	НАПРЯМКИ	010				020			
		Захист об’єктів ІС				Захист процесів та програм			
	ОСНОВИ	Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби
		011	012	013	014	021	022	023	024
100	Визначення інформації, що підлягає захисту	111	112	113	114	121	122	123	124
200	Виявлення загроз та каналів ВІ	211	212	213	214	221	222	223	224
300	Проведення оцінки вразливості та ризиків	311	312	313	314	321	322	323	324
400	Визначення вимог до КСЗІ	411	412	413	414	421	422	423	424
500	Здійснення вибору засобів захисту	511	512	513	514	521	522	523	524
600	Втілення та використання обраних заходів та засобів	611	612	613	614	621	622	623	624
700	Контроль цілісності та управління захистом	711	712	713	714	721	722	723	724

030				040				050			
Захист каналів зв’язку				ПЕМВН				Керування системою захисту			
Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби	Бази	Структура	Заходи	Засоби
031	032	033	034	041	042	043	044	051	052	053	054
131	132	133	134	141	142	143	144	151	152	153	154
231	232	233	234	241	242	243	244	251	252	253	254
331	332	333	334	341	342	343	344	351	352	353	354
431	432	433	434	441	442	443	444	451	452	453	454
531	532	533	534	541	542	543	544	551	552	553	554
631	632	633	634	641	642	643	644	651	652	653	654
731	732	733	734	741	742	743	744	751	752	753	754

Рис. 4.2. Матриця оцінки ефективності захищеності каналів зв’язку

Величина узагальненого показника рівня захисту визначається на основі часткових показників (рис. 4.3, *а – б*), а також шляхом порівняння заданих профілів безпеки з досягнутими (рис. 4.3, *в*).

Заданий профіль, послуги і механізми безпеки визначаються замовником чи вибираються відповідно до прийнятих “Критеріїв безпеки” у залежності від вимог, що встановлюються до створюваної комплексної СЗІ.

№ етапа	Перелік показників	№ елемента матриці	Коефіцієнт важливості	Профіль безпеки вимагаємий	Профіль безпеки досягнутий	Qд х aj	Порівняння профілів	Ступінь виконання груп вимог	Якісна оцінка	Кількісна оцінка
	m	№	aj	Qтр	Qд	Qдaj	Sпр	Qгруп	Q	S
1	1	131	0,5	0,8	0,7	0,35	0	0,68	0,67	0,39
	2	132	0,2	0,8	0,8	0,16	1			
	3	133	0,15	0,8	0,5	0,075	0			
	4	134	0,15	0,8	0,6	0,09	0			
2	5	231	0,25	0,8	0,5	0,125	0	0,73		
	6	232	0,25	0,8	0,8	0,2	1			
	7	233	0,25	0,8	0,8	0,2	1			
	8	234	0,25	0,8	0,8	0,2	1			
3	9	331	0,25	0,8	0,6	0,15	0	0,60		
	10	332	0,25	0,8	0,6	0,15	0			
	11	333	0,25	0,8	0,6	0,15	0			
	12	334	0,25	0,8	0,6	0,15	0			
4	13	431	0,25	0,8	0,8	0,2	1	0,70		
	14	432	0,25	0,8	0,8	0,2	1			
	15	433	0,25	0,8	0,6	0,15	0			
	16	434	0,25	0,8	0,6	0,15	0			
5	17	531	0,25	0,8	0,6	0,15	0	0,65		
	18	532	0,25	0,8	0,6	0,15	0			
	19	533	0,25	0,8	0,6	0,15	0			
	20	534	0,25	0,8	0,8	0,2	1			
6	21	631	0,25	0,8	0,5	0,125	0	0,65		
	22	632	0,25	0,8	0,5	0,125	0			
	23	633	0,25	0,8	0,8	0,2	1			
	24	634	0,25	0,8	0,8	0,2	1			
7	25	731	0,25	0,8	0,8	0,2	1	0,68		
	26	732	0,25	0,8	0,6	0,15	0			
	27	733	0,25	0,8	0,5	0,125	0			
	28	734	0,25	0,8	0,8	0,2	1			

а)

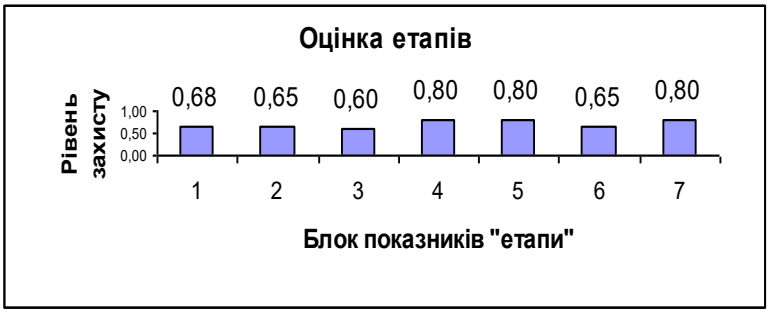
Як слідує з рис. 10.3 рівень захищеності КЗ характеризується значеннями 0,67 (якісна оцінка – по середньому значенню 28-ми експертних оцінок) і 0,39 (кількісна оцінка – по середньому значенню результатів порівняння досягнутих і вимагаємих профілів захисту).

Визначення належності комплексної СЗІ до конкретного класу (рівня захищеності) проводиться на основі функції належності, заданої нечіткими термами класів (табл. 4.1).

Оцінка ефективності СФЗ. СФЗ являє собою сукупність правових норм, організаційних заходів та інженерно-технічних рішень, спрямованих на захист життєво-важливих інтересів і ресурсів підприємства (об’єкта) від

загроз, джерелами яких є зловмисні (несанкціоновані) фізичні впливи фізичних осіб – порушників.

При цьому в єдиному комплексі задіяні люди (служба безпеки, сили охорони) та устаткування (ІТЗ), і від їх чіткої взаємодії залежить ефективність СФЗ. Для аналізу СФЗ і оцінки їх ефективності існує ряд методів та моделей, що дозволяють оцінювати як існуючі, так і проектовані СФЗ.



б)

в)

Рис. 4.3. Оцінка рівня захищеності каналів зв'язку

В більшості з них після вводу вхідних даних виконуються необхідні обчислення і видається відповідний результат. Найвідомішою і достатньо докладною методикою аналізу СФЗ є методика, що розроблена Сандійською національною лабораторією (США) [22]. В ній докладно розглядається програма оцінки імовірності перехоплення порушників, виходячі з аналізу взаємодії процесів виявлення, затримки, реагування і передачі інформації, яка отримала назву – модель EASI (Estimate of Adversary Sequence Interruption). Інші моделі для оцінки ефективності СФЗ, як правило, використовують базові положення, алгоритми або програми EASI.

У моделі EASI як базові параметри використовуються виявлення порушника, його затримка та реагування сил охорони на дії порушника, що відображають основні функції СФЗ.

Функція виявлення подається на вхід моделі у вигляді ймовірності виявлення P_D для кожного датчика, установленого на шляху руху порушника.

Таблиця 4.1.

Таблиця відповідності оцінок

Бальна оцінка (рівень захищеності)	Лінгвістична оцінка (рівень захищеності)	Інтервальна оцінка
5–відмінно	(В) Цілком задовольняє вимогам	0,9–1
4–добре	(ВС) Майже задовольняє	0,7–0,9
3–задовільно	(С) Задовольняє в основному	0,5–0,7
2–незадовільно	(НС) Не задовольняє	0,3–0,5
1–погано	(Н) Цілком не задовільняє	0–0,3

Імовірність P_D представляє собою добуток імовірності виявлення датчиком незаконних або незвичайних дій порушника P_S, імовірності проходження сигналу тривоги до оператора, що робить оцінку тривоги, P_T і ймовірності правильної оцінки цієї тривоги P_A.

У підсумку маємо співвідношення:

$$P_D = P_S P_T P_A. \quad (1.18)$$

На виході моделі EASI виходить оцінка ймовірності того, що сили реагування, у достатній кількості, перехоплять порушників у якійсь точці до того, як вони зроблять акт крадіжки або диверсії. Вихідним результатом є ймовірність переривання P_D. Якщо на шляху порушника перебуває тільки один датчик, то $P_I = P_C P_D$, в інших випадках вираз для обчислення P_I буде складнішим [22].

Передача сигналу тривоги силам реагування подається на вхід EASI у вигляді ймовірності P_C. Оцінка багатьох систем розроблених й впроваджених в лабораторії “Сандія” показала, що їхня більшість працює з імовірністю P_C , рівною – 0,95.

Час затримки – це час, потрібний порушникові для проходження певного шляху до мети. Він складається із часу, що витрачається ним на виконання певних задач або на проходження певних відрізків шляху. Наприклад, порушникові може знадобитися різний час для подолання огородження, зламу дверей або в силу реагування можуть з’явитися труднощі із запуском двигуна автомашини.

Час реагування враховується в моделі EASI як час між моментом спрацювання датчика й моментом появи на шляху порушника сил реагування в кількості, достатній для його перехоплення.

При різних спробах дій порушника параметри затримки й реакції можуть мати розсіювання. Для цього обліку в моделі тривалість кожної із задач порушника вводиться в модель EASI, як середнє значення зі стандартним відхиленням. Всі вхідні параметри відносяться до одного певного шляху порушника.

Розглянемо ситуацію, коли порушники збираються атакувати ціль, що перебуває в життєво важливій зоні (рис. 4.4).

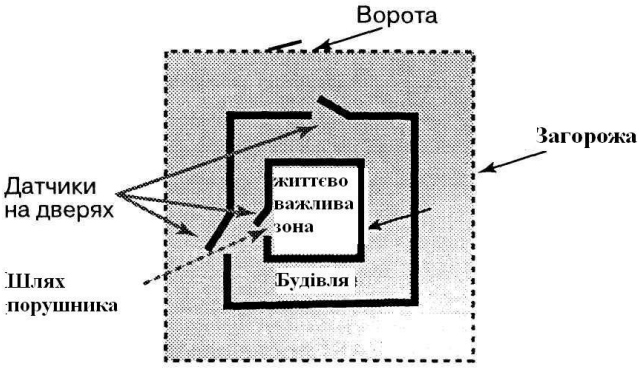
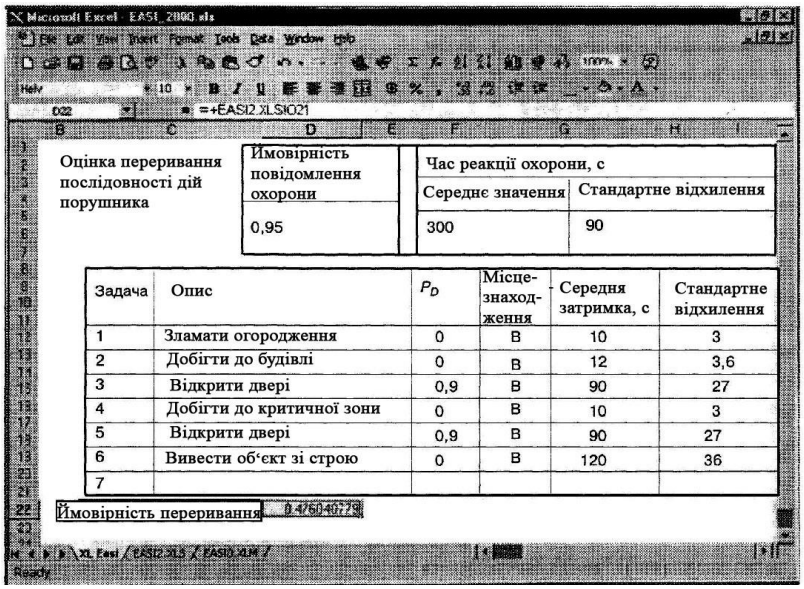


Рис. 4.4. Шлях порушника до критичного предмета

Порушники збираються перебороти загорожу, пройти до будівлі, зламати двері, пройти в критичну зону, зламати ще одні двері, закласти під критичний предмет вибуховий пристрій і підірвати його.

Часи виявлення й затримки наведені на рис. 4.5, а ЗРЧ дорівнює 300 с.



Оцінка переривання послідовності дій порушника	Імовірність повідомлення охорони	Час реакції охорони, с	
		Середнє значення	Стандартне відхилення
	0,95	300	90

Задача	Опис	P_D	Місце-знаход-ження	Середня затримка, с	Стандартне відхилення
1	Зламати огородження	0	В	10	3
2	Добігти до будівлі	0	В	12	3,6
3	Відкрити двері	0,9	В	90	27
4	Добігти до критичної зони	0	В	10	3
5	Відкрити двері	0,9	В	90	27
6	Вивести об'єкт зі строю	0	В	120	36
7					

Імовірність переривання 0,476040779

Рис. 4.5. Результати аналізу шляху порушника за допомогою моделі EASI

Після введення цих даних, модель EASI показала результат: імовірність перехоплення дорівнює 0,48 (рис. 4.5). Аналітик повинен зробити висновок, що P_I занадто мала й необхідно якимось способом її збільшити.

Якщо на зовнішнє огородження встановити датчик з імовірністю виявлення 0,9, то імовірність переривання в збільшиться до 0,58, що можна вважати задовільним, тому установка датчиків на огородженні в цьому випадку оправдана.

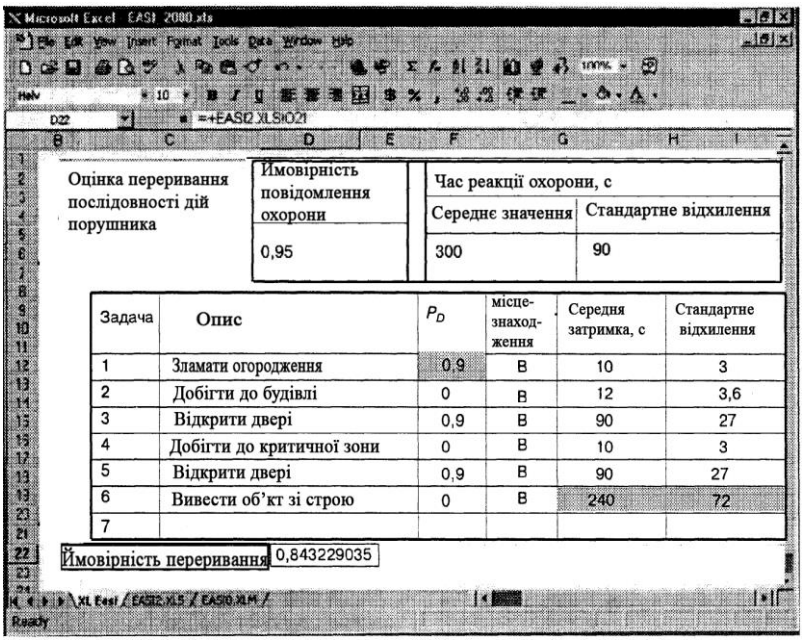


Рис. 4.6. Аналіз системи після збільшення часу затримки біля мети нападу зі збільшенням затримки й установці датчика на огородженні P_I = 0,84

Якщо така величина ймовірності не прийнятна, то можна змоделювати введення додаткового вдосконалення системи. Наприклад, якщо ЗЧР зменшити до 200 с, то нове значення P_I буде дорівнювати 0,83.

Можна вибрати й інший варіант: залишити охорону там же, де вона була (ЗЧР = 300 с), а затримку біля критичного предмета збільшити вдвічі, зміцнивши його захист, наприклад, закривши міцним кожухом. Це дасть величину P_I , рівну 0,84 (рис. 4.6).

4.2. Застосування критерію ризику для оцінки захищеності автоматизованої системи

Для оцінки захищеності АС найбільш розповсюдженим на практиці підходом є застосування критерію ризику:

$$R(Q) = \sum_{i=1}^{w} C_i p_i (1 - q_i) \qquad (1.19)$$

де C_i – цінність ресурсу (наслідки втрати інформації) в разі здій-нення загрози *i*-го виду;

p_i – ймовірність появи *i*-ої загрози;

q_i – ймовірність відбиття *i*-ої загрози;

w – кількість загроз, що діють на систему.

Процес оцінки ризиків складається з декількох етапів:

1) етапу ідентифікації і оцінки ресурсів;

2) етапу ідентифікації і оцінки загроз і уразливостей;

3) етапу оцінки ризиків;

4) етапу мінімізації ризиків.

Класифікація ресурсів визначається, як правило, в документі під назвою “Політика інформаційної безпеки”.

В переліку ресурсів обов’язково вказується тип ресурсу, серійний номер, відповідальний, місцезнаходження, НІ, дата вводу і контрольної перевірки.

Для кожного інформаційного ресурсу встановлюється відповідний рівень конфіденційності, цілісності, доступності і спостережливості по багатобальній шкалі, наприклад, п’ятибальній. Рівень конфіденційності визначається ступінню важливості ресурсу і наслідками розголошення відповідної інформації, рівень цілісності ресурсу – ступінню пошкодження, фінансових втрат і можливістю відновлення, рівень доступності ресурсу – значенням максимального часу, на протязі якого недоступність ресурсу не впливає негативно на діяльність організації, рівень спостережливості – ступінню повноти, якості і контролю використання ресурсу з боку авторизованих користувачів.

Середньоарифметичне значення рівнів конфіденційності, цілісності, доступності і спостережливості кожного ресурсу визначає важливість цього ресурсу.

Результати проведення етапу ідентифікаціїі оцінки ресурсів доцільно представити в табличному вигляді (табл. 4.2).

Таблиця 4.2.

Визначення важливості ресурсу

Назва (номер) ресурсу	Рівень конфіденційності ресурсу	Рівень цілісності ресурсу	Рівень доступності ресурсу	Рівень спостережності ресурсу	Важливість ресурсу
1					
2					
…					
n-1					
n					

Етап ідентифікаціїі оцінки загроз і уразливостей заключається в послідовному виконанні наступних кроків:

1) визначення загроз для ресурсів організації;

2) визначення уразливостей, завдяки яким можуть бути реалізовані дані загрози;

3) визначення існуючих захисних заходів;

4) визначення ймовірності реалізації загроз.

При цьому спочатку необхідно визначити потенційні загрози для кожного ресурсу, враховуючи місцезнаходження джерела загроз, природу його походження та характер прояву загрози.

Далі, для кожного ресурсу слід визначити уразливості, пов'язані з загрозами, і існуючи захисні заходи.

Якщо q_{ik} – ймовірність відбиття i-ої загрози k-м механізмом захисту, то ймовірність відбиття i-ої загрози в цілому буде

$$q_i = \prod_{k=1}^{K} q_{ik}. \qquad (1.20)$$

Відповідно, ймовірність зламу системи захисту становитиме: $\bar{q} = 1 - q$

Насамкінець визначається ймовірність реалізації загрози. В табл. 4.3 приведені 7 рівнів реалізації загрози в залежності від їх можливої частоти (інтенсивності). Подібний підхід можна використати для визначення рівнів уразливості ресурсів, виходячи з їх важливості. В (табл. 4.4) представлені бальні оцінки рівня загроз в залежності від трьох рівнів уразливості – високого (В), середнього (С) і низького (Н).

Таблиця 4.3.

Рівні загрози

Характеристика загрози	Бальна оцінка	Імовірнісна оцінка	Частота загрози
зневажливо мала	1	0–0,05	практично неможлива
дуже низька	2	0,05–0,2	2–3 рази на 5 років
низька	3	0,2–0,4	1 раз на рік
середня	4	0,4–0,6	1 раз напівроку або рідше
висока	5	0,6–0,8	1 раз на місяць або рідше
дуже висока	6	0,8–0,95	декілька разів на місяць
найвища	7	0,95–1	декілька разів на день

Якщо уразливість ресурсу найвища, то рівень реалізації загрози залишається на початковому рівні, тобто бальна оцінка загрози (табл. 2) не зменшується. У випадку використання ефективних захисних механізмів рівень загрози знижується на 2–3 бали.

Таблиця 4.4.

Рівні реалізації загрози

Рівень загрози	Рівень уразливості		
	Н	С	В
1	1	1	1
2	1	1	2
3	1	2	3
4	2	3	4
5	2 - 3	3 - 4	5
6	3 - 4	4 - 5	6
7	4 - 5	5-6	7

Слід відмітити, що при проведенні етапу ідентифікації та оцінки загроз і уразливостей використовують різні методи, в основу яких можуть бути покладені експертні оцінки, статистичні дані і фактори, що впливають на рівні загроз і уразливостей. У випадку застосування ПЗ оцінки ризиків розробник самостійно визначає дані і критерії для таблиць 2 і 3.

Остаточно рівень ризиків визначається як добуток важливості ресурсу і рівня реалізації загрози (табл. 4.5).

Таблиця 4.5.

Рівні ризику

Важливість ресурсу	Рівень реалізації загрози						
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21
4	4	8	12	16	20	24	28
5	5	10	15	20	25	30	35

Можливо використання однієї з різновидностей табличної оцінки ризиків – з трибальною, чотирибальною і восьмибальною шкалою. В таблиці 4 приведені значення рівнів ризику по трибальній шкалі:

1) низький, якщо значення ризику знаходяться в межах 1–5, при цьому припускається, що потенційні втрати мінімальні (до 10 %), вплив на діяльність організації практично відсутній;

2) середній, якщо значення ризику знаходяться в межах 6 –10, при цьому припускається, що потенційні втрати становлять до 20 %, є невеликий негативний вплив на діяльність організації. При необхідності можуть бути початі дії з керування даним ризиком;

3) високий – значення ризику знаходяться в межах 12–35, існують серйозні негативні наслідки для організації, необхідно почати відповідні дії з керування даним ризиком.

В разі отримання високого ризику може бути прийняте рішення щодо нейтралізації загроз або зниження даного ризику до рівня припустимого шляхом застосування захисних заходів.

4.3. Організаційно-технічні заходи захисту інформації

Організаційно-технічні заходи по ЗІ включають два етапи:

– побудова або модернізація системи захисту;

– підтримка ЗІ на необхідному рівні.

Побудова системи ЗІ проводиться в заново створених організаціях, в інших – модернізація існуючої. Організаційні заходи інженерно-технічного ЗІ включають, перш за все, заходи щодо ефективного використання технічних засобів регламентації і управління доступом до інформації, що захищається, а також по порядку і режимах роботи технічних засобів ЗІ. Організаційні заходи інженерно-технічного ЗІ є частиною її організаційного захисту, основу якого складають регламентація і управління доступом.

Технічні заходи передбачають застосування способів і засобів, розглянутих раніше.

Важливою складовою організаційних заходів ІТЗ є обстеження і категорування фізичного середовища і об’єктів установи (ІТС).

Під час *обстеження фізичного середовища* здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

НД, які визначають вимоги та зміст цих заходів є:

1. Порядок проведення робіт зі створення КСЗІ в ІТС (НД ТЗІ 3.7-003-05).

2. НД ТЗІ 1.6-005-2013. Наказ Адміністрації ДССЗІ України від 15.04.2013р. № 215. ЗІ на ОІД. Положення про категоріювання об’єктів, де циркулює ІзОД, що не становить державної таємниці.

3. ДСТУ 3396.1-96 ЗІ. ТЗІ. Порядок проведення робіт.

4. ДСТУ 4163-03 Державна уніфікована система організаційно – розпорядчої документації. Вимоги до оформлювання документів.

Обстеженню та аналізу підлягають такі характеристики фізичного середовища:

– територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

– наявність охорони території та перепускний режим;

– наявність категорованих приміщень, в яких мають розміщуватися компоненти ІТС;

– режим доступу до компонентів фізичного середовища ІТС;

– вплив чинників навколишнього середовища, захищеність від ТЗР;

– наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі КЗ;

– наявність та технічні характеристики СЗ;

– умови зберігання магнітних, оптико-магнітних, паперових та інших НІ;

– наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

Практична робота щодо реалізації цих заходів в установі здійснюється за ініціативою та безпосередньою участю начальника служби безпеки (захисту) інформації (саме він надає пропозиції керівнику установи, ініціює відпрацювання основних організаційно-розпорядчих документів та приймає активну участь у реалізації визначених заходів із створення КСЗІ в ІТС) у такій послідовності:

– наказом керівника установи визначається склад комісії з проведення спеціальних обстежень ОІД та їх категоруванню;

– комісією здійснюються спеціальні обстеження ОІД установи з метою встановлення рівня їх відповідності вимогам НД з питань ТЗІ щодо захищеності ІзОД на цих об'єктах, визначаються: обсяги скритих робіт у приміщеннях, де планується розташування елементів ІТС, спосіб, сили та засоби їх проведення;

– на підставі результатів роботи комісії призначені відповідальні особи, комісія (комісії) виконують скриті роботи у перевірених приміщеннях, складають акти скритих робіт із додатком відповідних схем заземлення, електроживлення, та т. п.;

– після завершення скритих робіт склад комісії здійснює повторне обстеження ОІД на предмет перевірки виконання всього обсягу визначених скритих робіт, придатності приміщень до ведення робіт з ІОД та категорування ОІД;

– результати проведених заходів враховуються на наступних етапах створення КСЗІ в ІТС.

В ході реалізації заходів щодо обстеження фізичного середовища ІТС за безпосередньою участю служби ЗІ установи відпрацьовуються такі основні організаційно-розпорядчі документи:

– проект наказу керівника підприємства про призначення комісії по проведенню спеціальних обстежень ОІД виробничого об'єднання та їх категорування;

– проект акту спеціального обстеження ОІД установи з додатками;

– проект (и) акту (ів) скритих робіт, проведених у приміщенні (ях), призначеного (их) для розміщення елементів ІТС з додатками;

– проект (и) акту (ів) категорування ОІД установи;

– проект наказу керівника підприємства про категорування ОІД з додатком переліку категорованих приміщень установи.

На закінчення слід відмітити, що найважливішим і необхідним напрямом робіт по ЗІ є контроль ефективності захисту. Цей вид діяльності проводиться силами відповідних служб ЗІ, а також керівниками структурних підрозділів. Контроль ІТЗ є складовою частиною контролю ЗІ в організації і полягає у визначенні (вимірюванні) показників ефективності захисту технічними засобами і порівнянні їх з нормативними.

Застосовують наступні види контролю:

– попередній;

– періодичний;

– постійний.

Заходи контролю, також як і захисту, являють сукупність організаційних і технічних заходів, що проводяться з метою перевірки виконання встановлених вимог і норм із ЗІ.

Слід відзначити, що добросовісне і постійне виконання співробітниками організації вимог із ЗІ ґрунтується на раціональному поєднанні способів примусу і спонукання.

4.4. Державний контроль за станом технічного захисту інформації

Державний контроль за станом ТЗІ здійснюється ДССЗІ України відповідно до Законів України “Про Державну службу спеціального зв’язку та захисту інформації України”, “Про захист інформації в інформаційно-телекомунікаційних системах” та Положення про Адміністрацію ДССЗІ, затвердженого Указом Президента України від 30 червня 2011 року № 717/2011.

Державний контроль за станом ТЗІ полягає в перевірці виконання вимог НПА і НД з ТЗІ та здійснюється з метою визначення стану ТЗІ в органах, щодо яких здійснюється ТЗІ, виявлення порушень з ТЗІ та запобігання їм.

Державний контроль за станом ТЗІ здійснюється ДССЗІ шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ стосовно органів, щодо яких здійснюється ТЗІ.

Контрольно-інспекторська робота з питань ТЗІ включає планування, проведення інспекційних перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ (далі – перевірка), аналіз їх результатів та надання рекомендацій щодо вдосконалення стану ТЗІ в зазначених органах.

4.4.1. Організація проведення перевірок стану технічного захисту інформації

Перевірки стану ТЗІ поділяються на комплексні, цільові (тематичні) та контрольні. Зазначені перевірки можуть бути плановими та позаплановими.

При комплексній перевірці визначається відповідність комплексу ТЗІ (КСЗІ) вимогам НПА та НД системи ТЗІ.

При цільовій (тематичній) перевірці перевіряються окремі складові комплексу ТЗІ (КСЗІ) на відповідність упроваджених заходів вимогам НПА та НД системи ТЗІ.

При контрольній перевірці перевіряється повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки. Контрольні перевірки проводяться за потреби, як правило, після отримання повідомлення про усунення недоліків.

Планові перевірки здійснюються згідно з річним планом контрольно-інспекторської роботи з питань ТЗІ, затвердженим Головою ДССЗІ. Витяги з плану контрольно-інспекторської роботи надсилаються до центральних органів виконавчої влади та в разі потреби до підприємств, установ і організацій.

Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог НПА з питань ТЗІ або з метою визначення повноти та достатності заходів з ТЗІ, вжитих органами, щодо яких здійснюється ТЗІ. Зазначені перевірки можуть проводитися з попередженням або без попередження.

Керівництву органів, щодо яких здійснюється ТЗІ, повідомляється про проведення перевірки не менше ніж за десять діб до її початку (за винятком проведення позапланової перевірки).

Перевірки стану ТЗІ здійснюються посадовими особами структурного підрозділу Адміністрації ДССЗІ з питань державного контролю за станом криптографічного та ТЗІ і регіональних органів ДССЗІ. До перевірок можуть залучатися фахівці органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій за погодженням з їх керівниками.

Підставою для допуску посадових осіб ДССЗІ до перевірки стану ТЗІ є наявність припису на право проведення перевірки за підписом керівництва Адміністрації ДССЗІ або начальника регіонального органу ДССЗІ.

4.4.2. Порядок проведення перевірок стану технічного захисту інформації

Для проведення перевірки стану ТЗІ посадові особи ДССЗІ повинні пред’явити керівнику або вповноваженому представнику органу, щодо якого здійснюється ТЗІ, припис на право проведення перевірки та службові посвідчення.

При проведенні перевірки стану ТЗІ контролю підлягають повнота та достатність упроваджених на ОІД заходів з ТЗІ, їх відповідність вимогам НПА, виконання рекомендацій щодо усунення порушень з ТЗІ.

За результатами перевірок посадовими особами ДССЗІ, які їх здійснювали, складаються акти перевірок стану ТЗІ.

Акт комплексної перевірки стану ТЗІ складається за встановленою формою. Акти контрольних та цільових (тематичних) перевірок складаються у довільній формі.

Акт перевірки стану ТЗІ готується в двох примірниках. Перший примірник акта перевірки надсилається до суб'єкта системи ТЗІ, що перевірявся, другий – до структурного підрозділу Адміністрації ДССЗІ з питань державного контролю за станом криптографічного та ТЗІ.

У разі проведення перевірки регіональним органом ДССЗІ готується третій примірник, який надсилається до органу ДССЗІ, посадові особи якого здійснювали перевірку.

Усі примірники акта підписуються посадовими особами ДССЗІ, якими проводилася перевірка, та затверджуються керівником Адміністрації ДССЗІ або начальником регіонального органу ДССЗІ, який підписав припис на проведення перевірки.

Ознайомлення керівника органу, щодо якого здійснюється ТЗІ, з актом здійснюється за його підписом.

У разі відмови керівника органу, щодо якого здійснюється ТЗІ, засвідчити факт ознайомлення з актом перевірки своїм підписом, посадовими особами ДССЗІ, що здійснювали перевірку, робиться в акті відповідний запис.

Керівники органів, щодо яких здійснюється ТЗІ, зобов'язані вжити невідкладних заходів щодо виконання рекомендацій, викладених в актах перевірок, та несуть персональну відповідальність за приведення стану ТЗІ у відповідність до вимог НПА системи ТЗІ. Посадові особи та громадяни, винні в невиконанні норм і вимог технічного захисту секретної інформації, унаслідок чого виникає реальна загроза порушення конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами, цілісності й доступності цієї інформації, несуть відповідальність згідно із законодавством України.

4.4.3. Класифікація порушень з технічного захисту інформації

Порушення в сфері ТЗІ – невиконання вимог НПА та НД системи ТЗІ за категоріями, які визначають можливість реалізації загроз безпеці інформації.

Реальна загроза ВІ (просочення) технічними каналами – наявність технічного каналу поширення інформації за умов підтвердження відповідними інструментально-розрахунковими методами невідповідності впроваджених заходів вимогам та нормам з ТЗІ.

Передумови ВІ (просочення) технічними каналами – наявність технічного каналу поширення інформації за відсутності підтвердженої відповідності впроваджених заходів вимогам та нормам з ТЗІ.

Порушення вимог з ТЗІ поділяються на три категорії, які визначають можливість реалізації загроз безпеці інформації:

перша категорія – невиконання вимог НПА та НД з ТЗІ, унаслідок чого створюється реальна можливість порушення конфіденційності, зокрема за рахунок ВІ (просочення) технічними каналами, цілісності й доступності інформації;

друга категорія – невиконання вимог НПА та НД з ТЗІ, унаслідок чого створюються передумови до порушення конфіденційності, зокрема за рахунок ВІ (просочення) технічними каналами, цілісності й доступності інформації;

третя категорія – невиконання інших вимог з ТЗІ.

Ознаки порушень першої категорії:

– установлення факту циркуляції ІзОД на ОІД, в інформаційних або ІТС за умов підтвердження інструментально-розрахунковими методами наявності технічного каналу поширення ІзОД;

– установлення факту обробки ІзОД в інформаційних або ІТС, які мають вихід незахищеними КЗ за межі КонтрЗ, за умов відсутності атестата відповідності на КСЗІ;

– установлення факту обробки ІзОД в інформаційних або ІТС, які не мають виходу за межі КонтрЗ, за умов доступу до її інформаційних ресурсів користувачів, які мають різні повноваження (права доступу до інформації), та відсутності атестата відповідності на КСЗІ;

– установлення факту НСД користувачів інформаційних, телекомунікаційних або ІТС до ІзОД шляхом порушення встановлених правил розмежування доступу або подолання заходів захисту.

Ознаки порушень другої категорії:

– установлення факту циркуляції ІзОД на ОІД, в інформаційних або ІТС за умов відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;

– установлення факту обробки ІзОД в інформаційних або ІТС, які не мають виходу за межі КонтрЗ, за умов відсутності атестата відповідності на КСЗІ.

Невиконання вимог НПА щодо впровадження організаційних заходів з ТЗІ, а також інших норм та вимог у сфері ЗІ, які не призводять до порушень першої або другої категорії, кваліфікується як *порушення третьої категорії*.

4.4.4. Висновки перевірок стану технічного захисту інформації та рекомендації

Висновок перевірки є результатом адміністративно-правової оцінки стану ТЗІ, повноти та достатності заходів щодо впровадження комплексу ТЗІ (КСЗІ) та їх відповідності вимогам НПА з ТЗІ.

Основним критерієм відповідності стану ТЗІ вимогам НД та НПА є відсутність порушень з ТЗІ.

Висновки перевірок стану ТЗІ та критерії їх складання:

1. Стан ТЗІ відповідає вимогам НПА.

Критерієм висновку є відсутність будь-яких порушень норм та вимог з ТЗІ.

2. Стан ТЗІ відповідає вимогам НПА за винятком виявлених недоліків.

Критерієм висновку є наявність хоча б одного порушення з ТЗІ третьої категорії.

3. Стан ТЗІ не повною мірою відповідає вимогам НПА, що створює передумови для порушення її конфіденційності, цілісності, доступності та (або) витоку технічними каналами.

Критерієм висновку є наявність хоча б одного порушення з ТЗІ другої категорії.

4. Стан ТЗІ не відповідає вимогам НПА, що створює реальну можливість порушення її конфіденційності, цілісності, доступності та (або) витоку технічними каналами.

Критерієм висновку є наявність хоча б одного порушення з ТЗІ першої категорії.

Висновок за результатами контрольної перевірки, крім оцінки стану ТЗІ, повинен відображати повноту виконання рекомендацій (виконано, не виконано, виконано не в повному обсязі) щодо приведення стану ТЗІ у відповідність до вимог НПА та НД з ТЗІ, наданих в акті попередньої перевірки.

Висновок за результатами цільової (тематичної) перевірки повинен визначати оцінку стану ТЗІ в окремих складових комплексу ТЗІ (КСЗІ), що перевірялися.

З метою приведення стану ТЗІ у відповідність до вимог НПА та НД з ТЗІ посадовими особами ДССЗІ, які здійснювали перевірку, в акті перевірки надаються конкретні рекомендації щодо усунення виявлених порушень, виконання яких є обов’язковим для посадових осіб органів, щодо яких здійснюється ТЗІ.

Для з’ясування причин, які призвели до порушень першої категорії, а також притягнення осіб, які їх вчинили, до відповідальності посадовими особами ДССЗІ ініціюється проведення відповідних розслідувань.

У разі виявлення порушень з ТЗІ першої або другої категорії посадовими особами ДССЗІ, що здійснювали перевірку, у встановленому порядку можуть порушуватися питання про припинення інформаційної діяльності на відповідних об’єктах.

Дозвіл на відновлення робіт, під час виконання яких були виявлені порушення норм і вимог з ТЗІ першої або другої категорії, дає керівник органу, щодо якого здійснюється ТЗІ, за погодженням з ДССЗІ після усунення порушень.

З метою приведення стану ТЗІ у відповідність до вимог НПА та НД з ТЗІ, а також виконання рекомендацій, наданих за результатами перевірки, керівниками органів, щодо яких здійснюється ТЗІ, у місячний термін після отримання акта перевірки затверджується план усунення недоліків, один примірник якого надсилається до органу ДССЗІ, посадовими особами якого було здійснено перевірку.

Повідомлення про виконання рекомендацій щодо приведення стану ТЗІ у відповідність до вимог НПА та НД з ТЗІ надсилається керівнику підрозділу ДССЗІ, посадовими особами якого було здійснено перевірку, у терміни, зазначені в акті перевірки та плані усунення недоліків.

Керівники органів, щодо яких здійснюється ТЗІ, мають право оскаржувати результати перевірок у порядку, визначеному законодавством України.

4.4.5. Проведення державного інструментального контролю захищеності інформації, яка циркулює на об'єктах "особливої норми"

Об'єкт "особливої норми" – місце постійного або тимчасового перебування вищої посадової особи держави, призначене для здійснення нею діяльності, пов'язаної з інформацією, необхідність захисту якої визначено законодавством.

Державний інструментальний контроль захищеності інформації, яка циркулює на об'єктах "особливої норми", здійснюється з використанням інструментально-розрахункових методів з метою оцінки повноти та достатності впроваджених на об'єктах організаційних, організаційно-технічних та технічних заходів із ЗІ від поширення (просочення) технічними каналами.

Державний інструментальний контроль захищеності інформації, яка циркулює на об'єктах "особливої норми", здійснюється шляхом проведення:

– спеціальних обстежень об'єктів "особливої норми", у ході яких перевіряються повнота та достатність упроваджених організаційних, організаційно-технічних та технічних заходів із ЗІ від поширення (просочення) технічними каналами, у тому числі каналами, що створюються за рахунок застосування ЗП, відповідність упроваджених заходів вимогам НПА, а також наявність атестаційних документів, які визначають необхідність упровадження заходів ЗІ;

– спеціальних перевірок об'єктів "особливої норми", у ході яких перевіряється наявність технічних каналів поширення інформації, які створюються за рахунок застосування ЗП;

– спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", у ході яких перевіряється відповідність захищеності технічних засобів нормам ефективності ЗІ від поширення (просочення) технічними каналами.

Спеціальні обстеження, спеціальні перевірки об’єктів “особливої норми” та спеціальні дослідження технічних засобів, призначених для встановлення на об’єктах “особливої норми”, можуть бути плановими та позаплановими.

За результатами спеціальних обстежень та спеціальних перевірок об’єктів “особливої норми” посадовими особами ДССЗІ, які їх здійснювали, складаються відповідні акти в довільній формі.

За результатами спеціальних досліджень технічних засобів, призначених для встановлення на об’єктах “особливої норми”, посадовими особами ДССЗІ, які їх здійснювали, оформлюються висновки.

У висновках спеціальних досліджень визначаються можливість, умови та порядок використання технічних засобів на об’єкті.

Питання та завдання для самостійної перевірки знань

1. Який критерій використовується для вибору раціонального варіанта СЗІ, в чому його сутність?
2. В чому полягає оцінка ефективності КСЗІ в АС, які документи визначають позитивні результати комплексної оцінки ефективності КСЗІ, коли проводиться повторна експертиза КСЗІ?
3. В чому полягає оцінка ефективності комплексу ТЗІ на ОІД, які документи визначають позитивні результати цієї перевірки, який термін проведення чергової атестації?
4. Що представляє собою модель комплексної оцінки СЗІ? Поясніть призначення і зміст матриці оцінок на прикладі оцінки ефективності захищеності КЗ.
5. Охарактеризуйте модель EASI: призначення, параметри, критерії оцінки ефективності.
6. Поясніть сутність критерію ризику і основні етапи його формування.
7. Назвіть і поясніть основні етапи організаційно-технічних заходів по ЗІ.
8. Що представляють собою контроль ІТЗ і державний контроль за станом ТЗІ?
9. Які існують види перевірок стану ТЗІ?
10. Назвіть три категорії порушень вимог з ТЗІ і їх ознаки.
11. Що представляє собою висновок за результатами контрольної та цільової (тематичної) перевірки стану ТЗІ?
12. Охарактеризуйте о’бєкт “особливої норми” і особливості державного інструменального контролю захищеності інформації, яка циркулює на ньому.

ЗАКЛЮЧЕННЯ

Інформатизація та комп’ютеризація докорінно змінюють обличчя сучасного суспільства. За таких обставин забезпечення ІБ. Поняття ІБ є комплексним і багатозначним. Саме тому різні органи державної влади мають приділяти особливу увагу гарантуванню цієї безпеки, особливо в контексті неухильного руху суспільства до всеосяжної інформатизації всіх сфер їх життєдіяльності. Особливо це стосується правоохоронних органів та служб безпеки, які мають не лише протидіяти інформаційним атакам всередині держави та на міжнародному рівні, в контексті інформаційної війни, а й бути готовими до боротьби з новою категорією злочинів: кіберзлочинами – правопорушеннями в сфері інформаційних технологій. Не менш відповідальні і складні задачі виникають при безпосередньому виборі раціональних способів і засобів захисту, тобто таких, які забезпечують необхідний рівень захисту при мінімальних витратах, що не перевищують збитку від розкрадання інформації. В знаходженні раціональних варіантів, що задовольняють цим умовам, полягає основна проблема етапу визначення методів, способів і засобів ЗІ. Не дивлячись на різноманіття можливих способів ІТЗ, їх методи можна звести до двох груп: інформаційному та енергетичному приховуванню інформації. Незалежно від вигляду і носія інформації інформаційне приховування зводиться до маскування і дезінформації, а енергетичне – до зменшення енергії носія або підвищення рівня перешкод на вході приймача зловмисника. Такий загальний підхід до ЗІ дозволяє розглядати з єдиних позицій все різноманіття способів і засобів забезпечення безпеки інформації і створює основу для перетворення набору емпіричних рекомендацій з інженерно-технічного ЗІ у відповідну теорію.

СПИСОК ЛІТЕРАТУРИ

1. Закон України “Про інформацію”.
2. Закон України “Про державну таємницю”.
3. Закон України “Про захист інформації в автоматизованих системах”.
4. Концепція технічного захисту інформації в Україні, затверджена постановою КМУ від 08.10.97 р. № 1126.
5. Постанова КМУ від 16 лютого 1998 р. № 180 “Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах”.
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. № 1229.
7. ДСТУ 3396.0-96. Захист інформації, технічний захист інформації. Основні положення.
8. ДСТУ 3396.1-96. Захист інформації, технічний захист інформації. Порядок проведення робіт.
9. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від НСД.
10. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від НСД.
11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в ком’ютерних системах від НСД.
12. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від НСД.
13. НД ТЗІ 2.7-002-99. Методичні вказівки з використання засобів копіювально-розмножувальної техніки.
14. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі.
15. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
16. Наказ Державної служби України з питань технічного захисту інформації від 09 червня 1995 р. № 25 “Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок (ТР ТЗІ – ПЕМВН-95)”.
17. Наказ Державної служби України з питань технічного захисту інформації від 09 червня 1995 р. № 25 (ТР ЕОТ-95).
18. НД ТЗІ 1.6-005-2013. Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 15.04.2013р. № 215. Захист інформації на об’єктах інформаційної діяльності. Положення про

категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

19. Бузов Г.А., Калинин С.В. Защита от утечки по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил.

20. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО “ДС”, 2001. – 688 с.

21. Жельников В. Криптография от папируса до компьютера. – М., ABF, 1996, 336с.

22. Журавський Ю.П., Полторак В.П. Теорія інформації та кодування: Підручник. – К.: Вища школа, 2002. – 235 с.: іл.

23. Конхейм А.Г. “Основы криптографии”. – М., Радио и связь 1987 г.

24. Мельников В. “Защита информации в компьютерных системах”, Москва, 1997 г.

25. Осипов Г.Б. “Криптография в системах связи”, ЗРЭ, № 8 1990г.

26. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, 1999. – 368 с.

27. Торокин А..А. “Основы инженерно-технической защиты информации”.– М.: “Ось-89”, 1998 г. – 336 с.

28. Хорев А.А. "Способы и средства защиты информации".– М.: МО РФ, 2000 г. – 316 с.

29. Хорошко В.А., Чекатков А.А. “Методы и средства защиты информации”.– К.: Юниор, 2003 г. – 504 с.

30. Хоффман Л. “Современные методы защиты информации”. – М., 1980 г.

31. Хорошко В.О., Чирков Д.В., Браіловський М.М. “Методи та засоби захисту інформації: Методичні вказівки та завдання на контрольну роботу та курсовий проект”. – К.: НАУ, 2002. – 20 с.

32. Комплект з 6-ти плакатів з дисципліни “Методи та засоби захисту інформації”, ХНУРЕ, м. Харків.

33. Р45-017-2007 “Рекомендації з монтажу комплектів заземлення за технологією Galmar ”.

ДОДАТОК 1

ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1. Загальні питання організації та функціонування системи технічного захисту інформації

Закони України:

Закон України “Про Державну службу спеціального зв’язку та захисту інформації України”;

Закон України “Про інформацію”;

Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”;

Закон України “Про державну таємницю”;

Закон України “Про основи національної безпеки України”.

Укази, постанови, розпорядження Верховної Ради України, Президента України, Кабінету Міністрів України, накази Адміністрації Держспецзв’язку:

Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229;

Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України. Указ Президента України від 30.06.2011 № 717/2011;

Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126;

Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.

Державні стандарти України:

ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;

ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

2. Вимоги до захисту інформації

Накази Адміністрації Держспецзв’язку, нормативні документи системи ТЗІ:

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95);

Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95);

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1);

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2";

НД ТЗІ 2.7-008-08 Захист інформації на об'єктах інформаційної діяльності. Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки;

НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.

3. Нормування порядку захисту інформації

3.1 Протидія технічним розвідкам

НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення.

3.2 Захист інформації в інформаційно-телекомунікаційних системах

Закони України:

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

Постанови Кабінету Міністрів України:

Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.98 № 121;

Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180;

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.

Накази Адміністрації Держспецзв'язку:

Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ Адміністрації Держспецзв'язку від 04.07.2008 № 112, зареєстрований в Міністерстві юстиції України 25.07.2008 за № 690/15381.

Нормативні документи системи ТЗІ:

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт;

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1);

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

3.3 Захист інформації на об'єктах інформаційної діяльності

Тимчасове положення про категоріювання об'єктів (ТПКО-95). Наказ Державної служби України з питань ТЗІ від 10.07.1995 № 35.

Державні стандарти України, нормативні документи системи технічного захисту інформації:

ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва;

НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення;

НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації;

НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення;

НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки;

НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки;

НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи;

НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;

НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

4. Оцінка якості робіт та послуг у галузі технічного захисту інформації

4.1 Сертифікація

Закони України:

Закон України “Про підтвердження відповідності”;

Закон України “Про акредитацію органів з оцінки відповідності”;

Закон України “Про стандарти, технічні регламенти та процедури оцінки відповідності”.

Державні стандарти України:

ДСТУ 2462-94 Сертифікація. Основні поняття. Терміни та визначення;

ДСТУ 3410-96 Система сертифікації УкрСЕПРО. Основні положення;

ДСТУ 3639-97 Фільтри протизавадні. Загальні технічні умови.

4.2 Державна експертиза у сфері ТЗІ

Закони України:

Закон України “Про наукову і науково-технічну експертизу”.

Накази Адміністрації Держспецзв’язку:

Положення про державну експертизу в сфері технічного захисту інформації. Наказ Адміністрації Держспецзв’язку від16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Нормативні документи системи ТЗІ:

НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах;

НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;

НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

4.3 Державний контроль у сфері ТЗІ

Накази Адміністрації Держспецзв’язку:

Положення про державний контроль за станом технічного захисту інформації. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052.

Інструкція про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення;

Наказ Адміністрації Держспецзв'язку від 29.05.2007 № 100, зареєстрований в Міністерстві юстиції України 12.06.2007 за № 618/13885.

5. Забезпечення діяльності у сфері технічного захисту інформації

5.1 Метрологічне забезпечення захисту інформації

Закони України:

Закон України "Про метрологію та метрологічну діяльність".

5.2 Фінансування захисту інформації

Постанови Кабінету Міністрів України:

Про фінансування заходів щодо криптографічного та технічного захисту інформації, охорона якої забезпечується державою відповідно до законодавства. Розпорядження КМ України від 13.12.2001 № 572-р.

5.3 Підготовка фахівців у сфері захисту інформації

Постанови Кабінету Міністрів України:

Про перелік напрямів, за якими здійснюється підготовка кадрів у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавр;

Постанова КМ України від 13.12.2006 № 1719.

ДОДАТОК 2

Перелік засобів забезпечення технічного захисту інформації загального призначення, на які Держспецзв'язку погоджено технічні умови (вибірковий)

№ з/п	Назва та позначення засобу, призначення засобу (технічні умови)	Розробник (виробник)
1	2	3
1	Електронна обчислювальна машина Мікро-ЕОМ "PLUTON". Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН і НСД до інформації, яка зберігається на ЖМД. (ТУУ 3.88-14312789249-98)	ДНВП "Електронмаш", м. Київ
2	Електронна обчислювальна машина ЕОМ-ПЕОМ-П0 (робоча станція), ЕОМ-П1 (сервер). Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН. (ААБ3.466219.001 ТУ, ААБ3.466219.001 ТУ1, ИЕСН.466219.005ТУ, ИЕСН.466219.005ТУ1)	ЗАТ "Інформаційні Комп'ютерні Системи", м. Київ, НДІ "Вектор", м. Київ
3	Комплекс засобів обчислювальної техніки в захищеному виконанні ЗОТ "Плазма-3В". Робоча станція (персональний комп'ютер), АРМ (пункт електронної пошти), сервер. Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН, у тому числі за рахунок акустоелектричних перетворень, нерівномірності споживання струму в колі електроживлення. (ТУУ 30023446.002 – 99, ТУУ 30023446.002:2006)	ТОВ НВП "Плазмотехніка", м. Київ
4	Персональний комп'ютер із захистом інформації "EXPERT". Робоча станція (персональний комп'ютер), сервер. Оброблення інформації з обмеженим доступом. Захист інформації від витоку каналами ПЕМВН, у тому числі за рахунок акустоелектричних перетворень та спеціального впливу. (ТУУ 30.0-21503308.006-2001)	ТОВ "Епос", м. Київ
5	Місця захищені автоматизовані робочі "ЗАРМ-24-2". Захист інформації, яка обробляється технічними засобами електронно-обчислювальної техніки та системами, від її витоку каналами ПЕМВН. (ТУУ 30.0-34732331-001:2008)	Державний НДІ Спецзв'язку, м. Київ
6	Машини електронно-обчислювальні персональні: "Еверест Т2", "Еверест Т3", "Еверест Т9". Оброблення ІзОД. Захист інформації від витоку каналами ПЕМВН, в тому числі за рахунок акустоелектричних перетворень та спеціального впливу. (ТУУ 30.0-31467680.001-2003)	ДП "Еверест-Консалтинг", м. Київ
7	Пристрій захисту ТЛ ПЗТЛ "Рікас-1", "Рікас-2". Захист інформації від витоку абонентськими ТЛ внаслідок акусто-електричного перетворення в ТА в режимі "очікування виклику". (ТУУ 16400411.001-95, ТУУ 16400411.002-95)	ДНВП "РІКАС", м. Київ

8	Пристрій захисту “Базальт-1”. Захист мовної інформації від витоку двопровідними лініями гучномовного зв’язку внаслідок акустоелектричного перетворення в кінцевих пристроях. (ТУУ3.88-23724999-218-97)	ДП “Укрспецтехніка система”, м. Київ
9	Пристрій захисту “Базальт-3”. Захист мовної інформації від витоку двопро відними лініями телефонного зв’язку внаслідок акустоелектричного перетворення в кінцевих абонентських пристроях, які знаходяться в режимі “очікування виклику”. (ТУУ 3.88-23724999-222-97)	ДП “Укрспецтехніка система”, м. Київ
9	Пристрій захисту ТА (ПЗТА). Захист від НСД до мовної конфіденційної інформації, зокрема: - внаслідок спеціального впливу на телефонний апарат, який знаходиться в режимі “очікування виклику”, з візуальною та звуковою індикацією загрози; - за рахунок підключення ТА до лінії тільки у разі підняття телефонної трубки або при наявності сигналу виклику. Не призначений для захисту секретної інформації. (МИСК. 468266.001 ТУ)	ВАТ “Інститут радіовимірювальної апаратури”, м. Київ
10	Пристрій захисту телефонних та радіотрансляційних ліній (ПЗТРЛ) “Топаз-1”. Захист мовної інформації від витоку лініями телефонного зв’язку і радіотрансляції за рахунок акустоелектричних перетворень та високочастотного зондування у кінцевих пристроях. (ТУУ 24787625.001-2001)	ВАТ Миколаївське підприємство “ЕРА”, м. Миколаїв
11	Фільтр захисний телефонний ФЗТ-2. Захист інформації, що циркулює в інформаційних та телекомунікаційних системах проводового зв’язку, від витоку за рахунок побічних електромагнітних наведень. (ТУУ 31.1-31731859-002:2007)	ТОВ “ЕМСБІ”, м. Київ
12	Фільтр мережевий протизавадний “ФСП-1”. Подавлення радіозавад у колах електроживлення пристроїв. (ТУУ 31.6-14309787.014-2003, ТУУ 31.6-14309787-232:2010)	ДП “СхідГЗК”, НВК “АіМ”, м. Жовті Води
13	Фільтр протизавадний “М-9”. Подавлення електромагнітних завад та блокування витоку інформації лініями пожежної та охоронної сигналізації. (ТУУ 30267382.003-99)	МП Виробничо-комерційна фірма “Мережеві технології”, м. Нетішин
14	Фільтри мережеві протизавадні: “М-11”, “М-13”, “М-15”, “М-17”, “М-23”. Подавлення електромагнітних завад та блокування витоку інформації мережами електроживлення. (ТУУ 30267382.003-99, ТУУ 30267382.001-99)	МП Виробничо-комерційна фірма “Мережеві технології”, м. Нетішин
15	Фільтр мережевий протизавадний “М-17-3”. Подавлення електромагнітних завад та блокування витоку інформації 3-х фазною мережею електроживлення. (ТУУ 30267382.002-99)	МП Виробничо-комерційна фірма” Мережеві технології”, м. Нетішин
16	Аналізатор ТЛ АТЛ “Рікас-4”. Індикація несанкціонованого гальванічного підключення до ТЛ. (ТУУ 16400411. 004-95)	ДНВП “РІКАС”, м. Київ

17	Фільтри мережеві протизавадні “ФМПЗ -1- 1”, “ФМПЗ -1-3”, “ФМПЗ -1- 6”, “ФМПЗ -1-10”. Захист інформації, що обробляється засобами обчислювальної техніки, від витоку мережами електроживлення, зменшення рівня високочастотних кондуктивних завад. (ТУУ 02070921.186-99)	Технопарк “Перспектива”Центр ЕМС НТУУ “КПІ”, м. Київ
18	Фільтри захисні протизавадні “ФЗП1”, “ФЗП 103-1”, “ФЗП 103-2” , “ФЗП 103-3”, “ФЗП 110-1”, “ФЗП 110-2”, “ФЗП 125-1”. Захист інформації, що обробляється засобами обчислювальної та іншої оргтехніки, від витоку за рахунок побічних електромагнітних наведень на коло електроживлення. Зменшення рівня імпульсних завад, які надходять на входи електроживлення апаратури, що захищається, з мережі електроживлення, у тому числі з метою захисту інформації.	ТОВ “ЕМСБІ”, м. Київ
19	Комплекс технічного захисту об’єкта “МАРС-ТЗО”, “МАРС-ТЗО-2”. Захист мовної інформації від витоку акустичними і віброакустичними каналами шляхом створення шумових сигналів. (ТУУ 31.6-14309379.001-2001, ТУУ 31.6-14309379.003-2001)	АТВТ “МАРС”, м. Київ
20	Пристрій захисту “Базальт-2ГС”. Генерація шумових сигналів. Захист мовної інформації від витоку двопровідними лініями електричного живлення внаслідок акустоелектричного перетворення, а також підключення прослуховуючих та передавальних пристроїв.	ДП “Укрспецтехніка система”, м. Київ
21	Комплекс для проведення спеціальних досліджень “Астра-В“. Вимірювання параметрів побічного електромагнітного випромінювання об’єктів. (ТУУ 21474417.001-2000)	ПП фірма “Бумекс”, м. Київ
22	Пристрій захисту “Базальт-4 ГА”. Генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичними і віброакустичними каналами. (ТУУ 3.88-23724999-224-97)	ДП “Укрспецтехніка система”, м. Київ
23	Генератори шумових сигналів: “МАРС-ТЗО-4-1”, “МАРС-ТЗО-4-2”, “МАРС-ТЗО-4М”. Генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичними і віброакустичними каналами. (ТУУ 31.6-14309379-006-2004,	АТВТ “МАРС”, м. Київ
24	Пристрій технічного захисту інформації – колонка акустична захищена “МАРС-АКЗ”. Створення акустичних завад при використанні у складі технічних засобів активного захисту мовної інформації, а також є засобом, захищеним від витоку мовної інформації каналом акустоелектричних перетворень. (ТУУ 31.6-14309379-008:2009)	АТВТ “МАРС”, м. Київ

25	Випромінювач віброакустичний “Базальт-4ДВМ”. Створення віброакустичних завад при використанні у складі технічних засобів активного захисту мовної інформації від витоку віброакустичним каналом. (ТУУ 31.6-30967720-001-2002)	ДП “Укрспецтехніка система”, м. Київ
26	Випромінювач акустичний “Базальт-4ДА”. Створення акустичного сигналу в архітектурно-будівельних конструкціях і елементах інженерно-технічного обладнання споруд при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичними і віброакустичним каналами.	ДП “Укрспецтехніка система”, м. Київ
27	Вібровипромінювачі “ВИ1”, “ВИ2”, “ВИ3”, “ВИ4”. Створення віброакустичних завад при використанні у складі технічних засобів активного захисту мовної інформації від витоку віброакустичним каналом. (ТУУ 31.6-14309379.002-2001)	АТВТ “МАРС”, м. Київ
28	Генератори шуму акустичні “Топаз ГША-4”, “Топаз ГША-4М”. Генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичним і віброакустичним каналами. (ТУУ 33.2-24787625.003-2003)	ВАТ “ЕРА”, м. Миколаїв
29	Віброакустичні випромінювачі ”Топаз - ВВ-1“, ”Топаз ВВ-1М“. Створення віброакустичних завад при використанні у складі тех-нічних засобів активного захисту мовної інформації від витоку віброакустичним каналом. (ТУУ 33.2-24787625.002-2003)	ВАТ “ЕРА”, м. Миколаїв
30	Прилад віброакустичного захисту інфо-рмації “ОЦЗІ-ВА”. Генерація шумових сигналів при використанні у складі технічних засобів активного захисту акустичної (мовної) інформації від витоку акустичним і віброакустичним каналом (ТУУ 73.1-31310763-001-2003)	ТОВ “Об’єднаний центр захисту інформації”, м. Київ
31	Комплекс віброакустичного захисту інформації “СКЕЛЯ-2” у складі: - генератор віброакустичного захисту інформації “СКЕЛЯ-2Г”; - вібровипромінювач електромеханічний “СКЕЛЯ-ЗІ/2ЕМ”. Захист мовної інформації від витоку акустичним і віброакустичним каналами шляхом створення шумових сигналів. (ТУУ 73.1-21474417-003-2003)	ПП фірма “Бумекс”, м. Київ
32	Пристрій захисту “Волна-4”, “Волна-4Р”, “Вектор-4”. Генерація шумових сигналів. Захист інформації, що обробляється засобами обчислювальної техніки, від витоку каналами ПЕМВН. (ТУУ 14309787.034-94, ТУУ 14309787.035-94, ТУУ 33.3-14309787.082-02, ТУУ 31.6-36004020-020:2010)	ДП “НВК АтаМ” м. Жовті Води

33	Пристрій захисту “Базальт-5ГЕШ”. Генерація шумових сигналів. Захист інформації, що обробляється на об’єктах ЕОТ, від витоку каналами ПЕМВН. (ТУУ 32.2-23724999-001-2000)	ВАТ “Укрспецтехніка” м. Київ
34	Комплекс активного захисту інформації “РІАС-АЗ”. Захист інформації з обмеженим доступом на ОІД від її витоку акустичним, віброакустичним каналами та каналами ПЕМВН шляхом генерації шумового сигналу. Прилади “РІАС-1С”, “РІАС-1М”, “РІАС-1К”, “РІАС-1В” – створення електромагнітних завад в ефірі. Прилади “РІАС-2С”, “РІАС-2М” - створення акустичних і віброакустичних завад.	ПП “РІАС”, м. Київ
35	Фільтри захисні протизавадні трифазні “ФЗП 3”, “ФЗП 3-75”, “ ФЗП 3-100”, “ФЗП 3-210”. Захист інформації, що обробляється засобами обчислювальної та іншої оргтехніки, від витоку за рахунок побічних електромагнітних наведень на кола електроживлення. (ТУУ 31.6-31731859-003:2011)	ТОВ “ЕМСБІ”, м. Київ
36	Комплекс лінійного захисту інформації “РІАС-ЛЗ” у складі: - трансформатори розділові з екранованою обмоткою “РІАС-4РТ/1, 2, 5, 8, 10, 15, 20”; - генератори шумоподібного сигналу в мережі електроживлення з вбудованим пристроєм автоматизованого контролю працездатності ”РІАС-4ШМ“, ”РІАС-4НМ“; - прилади захисту інформації в мережі електроживлення з вбудованим пристроєм автоматизованого контролю працездатності “РІАС-4ЗМ/1, 2”; - фільтр загороджувальний верхніх частот в слабкострумових колах “РІАС-4ФС”; - пристрій автоматизованого контролю працездатності засобів просторового та лінійного захисту інформації з виходом на звукову та адресну світлову сигналізацію “РІАС-4КС”; - пристрій автоматизованого контролю працездатності засобів просторового та лінійного захисту “РІАС-4КА”; - комплекс засобів захисту інформації від НСД в автоматизованій системі класу 1 “Рубіж-РСО”. Захист інформації з обмеженим доступом на ОІД від її витоку, середовищем поширення якої є мережі, лінії, проводи і кола технічних засобів систем пересилання, оброблення, зберігання та відображення інформації. (ТУУ 31.6-33694400-002:2009)	ПП “РІАС”, м. Київ
37	Пристрої захисту цифрових ТА “Базальт-31”. Забезпечення захисту мовної інформації з обмеженим доступом від витоку каналами цифрових абонентських ТЛ. (ТУУ 31.6-30967720-004:2008)	ДП “Укрспец - техніка система”, м. Київ

38	Комплекс активного захисту інформації “РІАС-АЗ”. Захист інформації з обмеженим доступом на ОІД від її витоку акустичним, віброакустич-ним каналами та каналами ПЕМВН шляхом генерації шумового сигналу. Прилади “РІАС-1С”, “РІАС-1М”, “РІАС-1К”, “РІАС-1В” – створення електромагнітних завад в ефірі. Прилади “РІАС-2С”, РІАС-2М” – створення акустичних і віброакустичних завад. (ТУУ 33.2-33694400-001:2006)	ПП “РІАС”, м. Київ
39	Аналізатор ТЛ АТЛ “Рікас-4”. Індикація несанкціонованого гальванічного підключення до ТЛ. (ТУУ 16400411.004-95)	ДНВП “РІКАС”, м. Київ
40	Комплекс вимірювально – обчислювальний “Ореол-2”. Вимірювання відношення “сигнал/шум” в звуковому діапазоні і обчислення формантної і складової розбірливості мови. Може застосовуватись для оцінювання ефективності захисту мовної інформації від витоку акустичним і віброакустичним каналами. (ТУУ 33.2-14309379.001-2002)	АТВТ “МАРС”, м. Київ
41	Апаратно-програмний комплекс проведення інженерних досліджень АПК “ТЕМП-1.0“. Автоматизація інженерних досліджень, які проводяться з метою пошуку та ідентифікації електромагнітних випромінювань від технік-них засобів, шляхом візуалізації спектра сигналів, що приймаються в заданому діапазоні частот, і його спеціальної обробки. (ТУУ 33.2-31748176.001-2003)	ТОВ Науково-виробничий центр “ІНФО ЗАХИСТ”, м. Київ
42	Автоматизований комплекс для виявлення електромагнітних випромінювань закладних пристроїв АК ВЗП “ТІКОС-18”. Автоматизація процесу пошуку (виявлення та локалізації) закладних пристроїв шляхом візуалізації спектра радіосигналів, які приймаються в заданому діапазоні частот, та спеціальної обробки цього спектра з метою виділення радіосигналів з певними параметрами із загальної сукупності прийнятих радіосигналів. (ТУУ 33.2-30055792.001-2001)	ТОВ ”Служба технічної безпеки Ратібор“, м. Київ
43	Автоматизовані комплекси виявлення і виміру радіовипромінювань, пошуку закладних пристроїв та виміру ПЕМВН від засобів ЕОТ “АКОР”, “АКОР-1”, “АКОР-2”, “АКОР-3” – перевірка і контроль приміщень, електроме-режі, телефонних та інших провідних ліній на наявність закладних пристроїв, передавальних відеокамер та інфрачервоних передавачів. “АКОР-ПК” – виявлення і вимірювання окремих параметрів сигналів, які створюються засобами ЕОТ. “АКОР-1ПК”, “АКОР-2ПК”, “АКОР-3ПК” – виконання функцій “АКОР-1”, “АКОР-2”, “АКОР-3” і вимірювального “АКОР-ПК” комплексів. Виявлення і вимірювання радіовипромінювань, пошуку закладних пристроїв і перевірки ЕОТ на наявність побічних електро-магнітних випромінювань і наводів. Випускаються в різних модифікаціях, які відрізняються функціональним призначенням.	НТЦ “КВАНТ”, м. Миколаїв

44	Тканина радіо непрозора “РН”. Обладнання екрануючих конструкцій (приміщень, споруд, кабін, кожухів тощо) з метою захисту інформації від витоку каналом ПЕМВ. (ТУУ 20713110.001-99)	НВП “Защита СВМ”, м. Севастополь
45	Засіб технічного захисту інформації від несанкціонованого доступу “ua Token”. Аутентифікація користувачів при доступі до комп’ютерної системи, інформації, а також безпечне зберігання критичної інформації з використанням кодування інформації, переда-ної у засіб через USB порт ПЕОМ. (ТУУ 30.0-32251835-001:2005)	ТОВ “Технотрейд”, м. Київ
46	Кабіни екрановані – ЕК. Захист інформації від витоку за рахунок ПЕМВ. (ТУУ 28.1-22897309.001-2002)	НВПП “Стелс”, м. Київ
47	Камери екрановані “Гарант-ЗРМ”. Захист інформації від витоку за рахунок ПЕМВН. (ТУУ 31.6-24248667-004:2008)	НВ ТОВ “Каліпсо”, м. Київ
48	Комплекси автоматизовані радіомоніторингу і пошуку закладних пристроїв, виявлення та вимірювання ПЕМВН від засобів ЕОТ “АКОР-М” у модифікаціях: “АКОР-2”, “АКОР-3”, “АКОР-ПК/М”, “АКОР-3ПКР”, аудіомоніторинг і пошук закладних пристроїв, виявлення та вимірювання ПЕМВН від засобів ЕОТ. Автоматизований комплекс радіомоніторингу і пошуку закладних пристроїв “АКОР-3“ – перевірка і контроль приміщень, електромережі, телефонних та інших дротових ліній на наявність пристроїв нелегального зняття мовної інформації, відеокамер-передавачів та інфра-червоних передавачів. Автоматизований комплекс виявлення і вимірювання ПЕМВН від засобів ЕОТ “АКОР-ПК/М” – визначення можливості зняття інформації з засобів обчислювальної техніки і оргтехніки. Автоматизований комплекс радіомоніторингу і пошуку закладних пристроїв, виявлення і вимірювання ПЕМВН від засобів ЕОТ “АКОР-3ПК” – виконання функцій пошукового комплексу “АКОР-3” і вимірювального комплексу “АКОР-ПК/М”. (ТУУ 32.3-13847488-002:2010)	НТЦ “КВАНТ”, м. Миколаїв