Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Незгоди Дмитра Михайловича

на здобуття ступеня вищої освіти Бакалавра

Система захисту інформації від витоку акустичними та електромагнітними каналами

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

Шифр КРБКБ.220118.22.01.10 ПЗ

Виконав студент 4 курсу група КБ-22-1 _____ Дмитро НЕЗГОДА

Керівник канд. техн. наук, доцент _____ Віктор ЧЕШУН

Нормоконтролер д-р філософії _____ Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

16 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Бакалавр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
9 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Незгоді Дмитру Михайловичу

1 Тема роботи Система захисту інформації від витоку акустичними та електромагнітними каналами
Керівник роботи канд. техн. наук, доцент, Чешун Віктор Миколайович
Затверджено наказом ректора університету від 8 січня 2026 р. № 7
2 Строк подання студентом кваліфікаційної роботи на кафедру 27 травня 2026р.
3 Вихідні дані до роботи Система захисту інформації від витоку акустичними та електромагнітними каналами для службового приміщення, у якому обробляється конфіденційна інформація, розробляється у вигляді проєкту з урахуванням джерел мовної інформації, технічних засобів обробки даних, кабельних ліній, можливих зон перехоплення та засобів протидії технічним каналам витоку
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз предметної області та понять технічного захисту інформації; аналіз особливостей витоку інформації акустичними, віброакустичними та електромагнітними каналами; огляд існуючих технологій і засобів захисту інформації від витоку технічними каналами; визначення об'єкта захисту та формування моделі загроз для службового приміщення; проєктування підсистем захисту від акустичного, віброакустичного та електромагнітного витоку; розробка загальної структурної схеми системи захисту інформації та обґрунтування вибраних засобів захисту; опис схем блокування каналів витоку інформації; реалізація допоміжного програмного модуля та візуалізація результатів роботи
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема структурна системи. Схема утворення каналів витоку інформації. Схема перекриття каналів витоку інформації

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 12 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент _____ Дмитро НЕЗГОДА

Керівник кваліфікаційної роботи _____ Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система для дослідження технологій і засобів захисту інформації від витоку віброакустичними каналами.

Тема кваліфікаційної роботи: Система захисту інформації від витоку акустичними та електромагнітними каналамии.

Автор роботи: Незгода Дмитро Михайлович.

Керівник роботи: канд. техн. наук, доц. Чешун Віктор Миколайович.

Пояснювальна записка: 81 сторінка, 18 рисунків, 13 таблиць, 1 додаток, 42 посилання.

Графічна частина: 4 плакати.

Ключові слова: захист інформації, акустична інформація, канал витоку, система захисту.

Кваліфікаційна робота присвячена розробці системи для дослідження технологій і засобів захисту інформації від витоку віброакустичними каналами.

В роботі, на підставі аналізу акустичної інформації як об'єкту захисту та каналів її витоку і огляду засобів захисту акустичної інформації від витоку здійснено класифікацію каналів витоку акустичної інформації, запропоновано і надано опис схеми утворення каналів витоку акустичної інформації, розроблено схему системи для дослідження технологій і засобів захисту інформації від витоку віброакустичними каналами, а також схеми блокування акустичних і віброакустичних каналів витоку акустичної інформації.

25.05.2026

ANNOTATION

Theme of qualification work: A system for protecting information against leakage via acoustic and electromagnetic channels.

Author of the work: Nezghoda Dmytro Mykhailovych .

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Explanatory note: 81 pages, 18 figures, 13 tables, 1 appendice, 42 links.

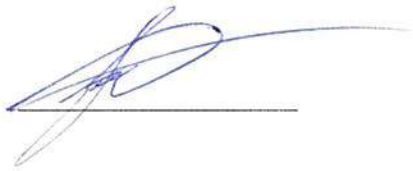
Graphic part: 4 posters.

Keywords: information protection, acoustic information, leakage channel, protection system.

The qualification work is devoted to the development of a system for the study of technologies and means of protecting information from leakage by vibroacoustic channels.

In the work, based on the analysis of acoustic information as an object of protection and its leakage channels and a review of means of protecting acoustic information from leakage, a classification of acoustic information leakage channels is carried out, a description of the scheme for the formation of acoustic information leakage channels is proposed and provided, a system scheme for the study of technologies and means of protecting information from leakage by vibroacoustic channels is developed, as well as schemes for blocking acoustic and vibroacoustic channels of acoustic information leakage.

25.05.2026



ЗМІСТ

ВСТУП

У сучасних умовах розвитку інформаційних технологій питання захисту інформації набуває особливої актуальності. Значна частина службових, персональних, комерційних та технологічних даних обробляється із застосуванням технічних засобів, робота яких супроводжується різними фізичними процесами. До таких процесів належать акустичні коливання, механічні вібрації, електромагнітні випромінювання, електричні наводки та інші побічні явища. За певних умов вони можуть утворювати технічні канали витоку інформації, через які конфіденційні дані можуть бути отримані сторонніми особами без безпосереднього доступу до інформаційної системи .

Особливу небезпеку становлять акустичні та електромагнітні канали витоку інформації. Акустичні канали пов’язані з поширенням мовної інформації у повітряному середовищі, через будівельні конструкції, вікна, двері, вентиляційні канали та інші елементи приміщення. Електромагнітні канали виникають унаслідок побічних електромагнітних випромінювань і наводок, що супроводжують роботу комп’ютерної техніки, засобів зв’язку, кабельних ліній та іншого електронного обладнання. Наявність таких каналів створює ризик несанкціонованого отримання мовної, текстової, графічної або службової інформації.

Актуальність теми кваліфікаційної роботи зумовлена необхідністю розроблення комплексної системи захисту інформації, яка дозволяє зменшити ризик витоку через акустичні та електромагнітні канали. На практиці ефективний захист не може обмежуватися лише одним технічним засобом або окремим програмним рішенням. Він повинен поєднувати інженерно-технічні, організаційні та допоміжні програмні заходи, спрямовані на виявлення потенційних каналів витоку, їх блокування або зниження рівня небезпечних сигналів до прийнятного значення .

Метою кваліфікаційної роботи є розроблення системи захисту інформації від витоку акустичними та електромагнітними каналами, яка включає технічні

засоби протидії, організаційні заходи, структурну схему захищеної зони та допоміжний програмний модуль для оцінювання рівня ризику і формування рекомендацій щодо підвищення захищеності.

Для досягнення поставленої мети необхідно виконати такі завдання:

– проаналізувати основні поняття технічного захисту інформації та класифікацію каналів витоку;

– дослідити особливості формування акустичних, віброакустичних та електромагнітних каналів витоку інформації;

– визначити основні загрози та фактори, що впливають на рівень захищеності інформації;

– розглянути існуючі методи та засоби захисту інформації від витоку технічними каналами;

– сформувати модель загроз для умовного об’єкта захисту;

– обґрунтувати вибір технічних засобів захисту від акустичного, віброакустичного та електромагнітного витоку;

– розробити структурну схему системи захисту інформації;

– спроєктувати допоміжний програмний модуль для оцінювання ризику витоку інформації;

– розробити алгоритм оцінювання ризику та подати його у вигляді послідовності дій і блок-схеми;

– перевірити працездатність запропонованих рішень та оцінити ефективність системи захисту.

Результатом виконання кваліфікаційної роботи є проєкт системи захисту інформації, що включає опис загроз, вибір засобів захисту, схеми перекриття каналів витоку, структурну схему системи та допоміжний програмний інструмент для оцінювання ризику. Такий підхід дозволяє розглядати програмний модуль не як самостійну мету роботи, а як складову частину комплексної системи захисту інформації.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Організація технічного захисту інформації

Технічний захист інформації розглядається як частина загальної системи безпеки, що відповідає за захист від витоку даних через фізичні процеси, які супроводжують роботу технічних засобів. На практиці така проблема виникає не лише під час роботи комп’ютерів або серверів. Джерелом небезпечного сигналу може бути звичайна розмова в приміщенні, робота кабельної лінії, монітора, телефонного апарата, мережевого обладнання або іншого електронного пристрою [1, 2].

На відміну від програмних загроз, технічний витік може відбуватися без прямого доступу до інформаційної системи. Наприклад, для отримання частини мовної інформації не завжди потрібно проникати в приміщення або підключатися до комп’ютера. Іноді достатньо зафіксувати звук, вібрацію конструкції або побічне електромагнітне випромінювання. Саме тому технічні канали витоку становлять окрему проблему, яку потрібно враховувати під час проєктування системи захисту [3–5].

Під технічним каналом витоку інформації розуміють шлях, яким інформація може вийти за межі контрольованої зони у вигляді звукового, електромагнітного, електричного, оптичного або іншого фізичного сигналу. Такий канал зазвичай складається з трьох основних елементів: джерела сигналу, середовища його поширення і засобу можливого перехоплення. Якщо хоча б один із цих елементів усунути або достатньо послабити, ризик витоку суттєво зменшується [6].

Джерелом небезпечного сигналу може бути людина, яка веде переговори, технічний пристрій, що обробляє дані, кабель, лінія живлення або елемент системи зв’язку. Середовищем поширення можуть бути повітря, будівельні конструкції, електричні мережі, кабелі або відкритий простір. Засобами перехоплення виступають мікрофони, вібродатчики, антени, аналізатори спектру, радіоприймальні пристрої, оптичні прилади та інші технічні засоби [7].

Важливим поняттям у технічному захисті є контрольована зона. Це територія або приміщення, у межах яких власник інформації може контролювати доступ людей, розміщення технічних засобів і використання засобів захисту. Межі такої зони визначаються не формально, а з урахуванням реальних умов: товщини стін, типу обладнання, рівня шуму, наявності вікон, кабельних ліній, сусідніх приміщень і можливих точок перехоплення.

У кваліфікаційній роботі як умовний об’єкт захисту розшлянемо службове приміщення, у якому проводяться переговори та використовується комп’ютерна техніка. Саме в такому приміщенні можуть одночасно виникати кілька каналів витоку: акустичний, віброакустичний, електромагнітний і електричний. Це робить задачу захисту комплексною, оскільки один захід не може перекрити всі можливі шляхи витоку.

За фізичною природою сигналу технічні канали витоку поділяють на акустичні, віброакустичні, електромагнітні, електричні та оптичні. Акустичні канали пов’язані з поширенням звуку в повітрі. Найпростішим прикладом є ситуація, коли розмову в приміщенні можна почути через двері, вентиляційний канал або тонку перегородку.

Віброакустичні канали виникають тоді, коли мовна інформація передається не безпосередньо через повітря, а через коливання твердих конструкцій. Звук може викликати мікровібрації скла, стін, труб або перекриттів. Такі коливання можуть бути зчитані спеціальними датчиками або лазерними засобами. Цей тип каналу є небезпечним тому, що джерело перехоплення може знаходитись за межами приміщення.

Електромагнітні канали формуються під час роботи електронної апаратури. Комп’ютери, монітори, сервери, кабельні мережі та засоби зв’язку створюють побічні електромагнітні випромінювання. У звичайному режимі ці сигнали не призначені для передавання інформації, але за певних умов вони можуть містити відомості про оброблювані дані.

Електричні канали пов’язані з поширенням небезпечних сигналів через лінії живлення, заземлення, сигнальні кабелі або мережеву інфраструктуру.

Наприклад, наведення в кабельних лініях можуть створювати умови для поширення фрагментів інформаційного сигналу за межі контрольованої зони. Оптичні канали виникають у випадках, коли інформацію можна отримати через світлові прояви, відбиття від поверхонь або візуальне спостереження.

Узагальнено класифікацію технічних каналів витоку інформації можна подати у вигляді схеми. На рисунку 1.1 наведено класифікацію технічних каналів витоку інформації за фізичною природою сигналу.

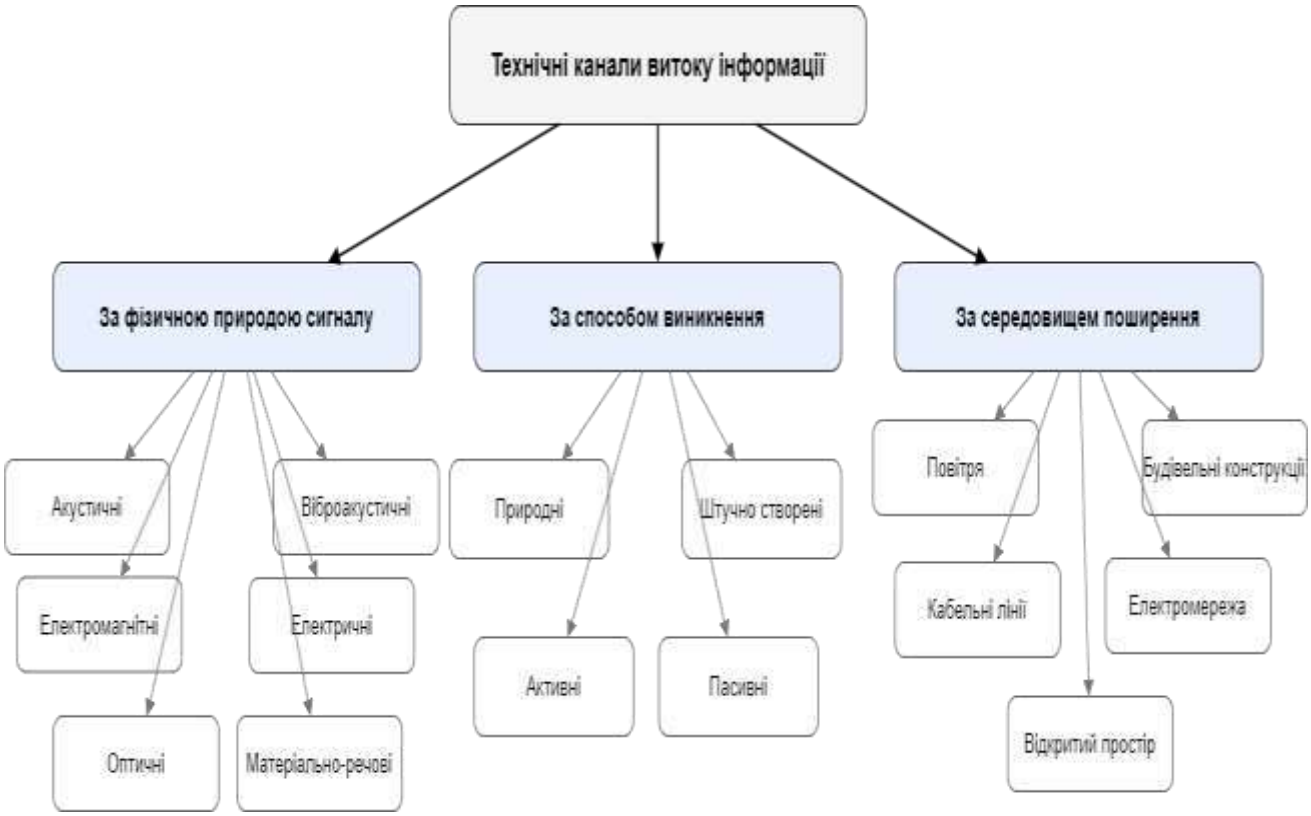


Рисунок 1.1 – Класифікація технічних каналів витоку інформації

Технічні канали також можна поділити за способом виникнення. Природні канали з’являються внаслідок звичайної роботи обладнання або природного поширення фізичних сигналів. Штучні канали створюються навмисно, наприклад шляхом встановлення прихованого мікрофона, радіопередавача, несанкціонованого підключення до кабельної лінії або іншого закладного пристрою. Для зручності основні види технічних каналів витоку подано у таблиці 1.1.

Таблиця 1.1 – Основні технічні канали витоку інформації

Вид каналу витоку	Джерело виникнення	Основний спосіб перехоплення
Акустичний	Мовлення людини, звукові сигнали	Мікрофони, диктофони, спрямовані засоби запису
Віброакустичний	Коливання стін, вікон, труб, перекриттів	Вібродатчики, лазерні мікрофони
Електромагнітний	Побічні випромінювання електронної техніки	Антени, радіоприймальні пристрої, аналізатори спектру
Електричний	Лінії живлення, кабелі, сигнальні мережі	Підключення до кабельних ліній або мереж живлення
Оптичний	Світлові сигнали, відбиття, візуальні прояви	Оптичні прилади, засоби візуального спостереження

Захист від технічних каналів витоку має будуватися не окремими несистемними заходами, а як комплекс рішень. Якщо захищати тільки акустичний канал, але залишити без уваги кабелі живлення або електромагнітні випромінювання, загальний рівень захищеності залишиться недостатнім. Тому для службового приміщення необхідно одночасно враховувати звукоізоляцію, акустичне маскування, демпфування конструкцій, екранування обладнання, правильне заземлення, фільтрацію живлення і контроль доступу [8].

1.2 Аналіз витоку інформації акустичними каналами

Акустичний канал витоку інформації виникає тоді, коли мовна або інша звукова інформація поширюється за межі контрольованої зони і може бути сприйнята або записана сторонніми особами. На практиці такий канал є одним із найочевидніших, але водночас одним із найскладніших для повного усунення. Причина полягає в тому, що звук є природним результатом мовлення людини,

роботи технічних засобів, вентиляційних систем, телефонного обладнання та інших джерел, які можуть бути присутні у службовому приміщенні [13].

Найбільш цінною з погляду захисту є мовна інформація. Під час переговорів, службових нарад або [обговорення робочих питань можуть передаватися відомості з обмеженим доступом. Якщо приміщення не має достатнього рівня акустичного захисту, частина цієї інформації може поширюватися через двері, вікна, вентиляційні канали, стіни або інші конструктивні елементи. У результаті виникає ризик її перехоплення за допомогою мікрофонів, диктофонів, спрямованих акустичних пристроїв або інших технічних засобів [11].

Акустичний витік не завжди потребує складного обладнання. У деяких випадках достатньо погано ізольованих дверей, відкритого вікна або тонкої перегородки між приміщеннями. Водночас сучасні засоби перехоплення дозволяють працювати і в складніших умовах, коли мовний сигнал є слабким, спотвореним або частково замаскованим фоновим шумом.

Акустичні канали витоку можна поділити на кілька основних видів. Першим є повітряний акустичний канал. Він пов’язаний із прямим поширенням звукових хвиль у повітрі. Такий канал виникає під час звичайної розмови, коли звук проходить через відкриті або нещільно закриті двері, вентиляційні отвори, щілини, вікна або тонкі перегородки. Саме повітряний канал найчастіше враховується під час первинного аналізу приміщення.

Другим видом є віброакустичний канал. Він виникає тоді, коли звукові коливання переходять у механічні коливання будівельних конструкцій. Наприклад, мовлення в приміщенні може викликати мікровібрації скла, стін, труб, дверей або перекриттів. Такі коливання можуть поширюватися на певну відстань і бути зчитані за допомогою контактних датчиків або лазерних засобів. Небезпека цього каналу полягає в тому, що перехоплення може виконуватися без прямого доступу до приміщення [12].

Третім видом є електроакустичний канал. Він пов’язаний із перетворенням акустичних сигналів в електричні сигнали в технічних засобах. До таких засобів

належать телефони, мікрофони, гарнітури, системи відеоконференцій, конференц-обладнання та інші пристрої, що мають акустичні перетворювачі. Якщо такі пристрої підключені до мережі або ліній зв'язку без належного контролю, вони можуть створювати додаткові умови для витоку мовної інформації. Окремим різновидом ризику є канали, сформовані високочастотними нав'язуваннями [15]. Для їх виявлення потрібні спеціальні дослідження акустоелектричних каналів витоку [18].

На рівень акустичного витоку впливає багато факторів. Насамперед це гучність мовлення. Чим вищий рівень звукового сигналу, тим більша ймовірність його поширення за межі приміщення. Важливе значення має і відстань до потенційного засобу перехоплення: зі збільшенням відстані сигнал послаблюється, але повністю не зникає. Також потрібно враховувати акустичні властивості приміщення, зокрема наявність відбиття звуку, реверберації, звукопоглинальних матеріалів, меблів та інших елементів інтер'єру [17].

Суттєвий вплив мають конструктивні особливості будівлі. Товщина стін, матеріал перегородок, тип дверей, герметичність вікон, наявність вентиляційних каналів і трубопроводів можуть як зменшувати, так і збільшувати ризик витоку. Наприклад, масивні стіни та якісні ущільнені двері знижують рівень поширення звуку, тоді як легкі перегородки, порожнини в конструкціях і неізольовані вентиляційні канали можуть стати зручними шляхами для поширення мовної інформації.

Окремо слід враховувати рівень фонового шуму. У деяких випадках фоновий шум може частково маскувати мовлення і знижувати розбірливість сигналу. Проте покладатися лише на природний шум недоцільно, оскільки сучасні засоби цифрової обробки можуть частково виділяти мовний сигнал навіть за наявності завад. Тому для захисту використовують спеціальні генератори акустичного або віброакустичного шуму, які створюють контрольовану заваду і ускладнюють відновлення мовної інформації [6]. Узагальнено основні канали витоку інформації подано в таблиці 1.2.

Таблиця 1.2 – Основні види акустичних каналів витоку інформації

Вид каналу витоку	Середовище поширення	Приклад реалізації	Засіб можливого перехоплення
Повітряний акустичний	Повітря	Поширення розмови через двері, вікна, вентиляцію	Мікрофон, диктофон, спрямований мікрофон
Віброакустичний	Стіни, скло, труби, перекриття	Передача мовлення через коливання конструкцій	Вібродатчик, лазерний мікрофон
Електроакустичний	Лінії зв’язку, технічні пристрої	Перетворення звуку в електричний сигнал у мікрофоні або телефоні	Підключення до лінії, закладний пристрій
Канал через вентиляцію	Повітряні канали	Поширення мовлення через вентиляційні шахти	Мікрофон у вентиляційному каналі
Канал через нещільності конструкцій	Щілини, дверні прорізи, віконні рами	Часткове проходження звуку за межі приміщення	Звукозаписувальний пристрій за межами кімнати

Аналіз акустичних каналів показує, що їх не можна розглядати ізольовано від конструкції приміщення та умов його експлуатації. Навіть якщо в приміщенні встановлено сучасне обладнання, слабкі місця можуть залишатися у дверях, вікнах, вентиляційних каналах або будівельних конструкціях. Тому під

час подальшого проєктування системи захисту необхідно враховувати не лише джерела мовної інформації, а й усі можливі середовища її поширення.

Отже, акустичні канали витоку є одним із ключових напрямів, які необхідно враховувати під час побудови системи захисту інформації. Для їх блокування потрібне поєднання звукоізоляції, акустичного маскування, контролю конструктивних елементів приміщення та організаційних обмежень щодо проведення конфіденційних переговорів [14].

1.3 Аналіз витоку інформації електромагнітними каналами

Електромагнітний канал витоку інформації виникає тоді, коли під час роботи електронного або електротехнічного обладнання утворюються побічні електромагнітні випромінювання чи наводки, які можуть містити ознаки оброблюваної інформації. Такий канал є менш очевидним, ніж акустичний, оскільки він не сприймається людиною без спеціальних технічних засобів. Проте саме через це електромагнітний витік є складним для своєчасного виявлення [16].

Під час роботи комп’ютерів, моніторів, серверів, мережевого обладнання, блоків живлення, кабельних ліній та інших пристроїв відбувається проходження електричних струмів, перемикання цифрових схем і формування електромагнітного поля. Частина таких випромінювань є побічною, тобто не призначена для передавання інформації. Однак за певних умов вона може відображати структуру сигналів, що обробляються технічним засобом [7].

Особливість електромагнітних каналів полягає в тому, що перехоплення може здійснюватися без фізичного контакту з обладнанням. Для цього можуть використовуватися антени, радіоприймальні пристрої, аналізатори спектру або спеціалізовані системи цифрової обробки сигналів. У деяких випадках небезпечний сигнал може поширюватися не лише через простір, а й через кабелі живлення, сигнальні лінії або заземлення.

Електромагнітні канали витоку доцільно поділяти на кілька основних груп.

Першу групу становлять побічні електромагнітні випромінювання. Вони виникають під час нормальної роботи електронних пристроїв і можуть бути пов’язані з роботою процесорів, моніторів, відеоінтерфейсів, мережевих адаптерів, периферійного обладнання та кабельних з’єднань. Такі випромінювання можуть містити непрямі ознаки інформаційних процесів, що відбуваються всередині пристрою.

Другу групу становлять електромагнітні наводки. Вони з’являються тоді, коли електромагнітне поле одного технічного засобу впливає на сусідні провідники, кабелі або електронні пристрої. У результаті в цих елементах можуть виникати паразитні сигнали. Якщо такі сигнали поширюються за межі контрольованої зони, вони можуть створювати додатковий канал витоку інформації.

Третю групу становлять паразитні сигнали в лініях живлення і зв’язку. У цьому випадку небезпечний сигнал поширюється не через відкритий простір, а через інфраструктуру об’єкта: електромережу, кабелі передачі даних, лінії зв’язку або заземлення. Такий канал є небезпечним, оскільки лінії живлення та кабельні мережі часто виходять за межі приміщення або мають спільні ділянки з іншими системами.

Основними джерелами електромагнітного витоку є персональні комп’ютери, монітори, сервери, маршрутизатори, комутатори, принтери, блоки живлення, кабельні лінії та інше електронне обладнання. Рівень небезпеки залежить не лише від типу пристрою, а й від режиму його роботи, якості екранування, довжини кабелів, правильності заземлення і відстані до потенційного засобу перехоплення.

На практиці особливу увагу слід приділяти кабельним лініям. Навіть якщо саме обладнання має прийнятний рівень електромагнітної сумісності, неекрановані або неправильно прокладені кабелі можуть стати джерелом випромінювання чи наведень. Також ризик підвищується у випадках, коли силові та інформаційні кабелі прокладені поруч, не мають належного рознесення або проходять через неконтрольовані зони [8].

Для зручності основні види електромагнітних каналів витоку інформації подано в таблиці 1.3.

Таблиця 1.3 – Основні види електромагнітних каналів витоку інформації

Вид каналу витоку	Джерело виникнення	Шлях поширення	Можливий засіб перехоплення
Побічні електромагнітні випромінювання	Комп'ютери, монітори, сервери, периферійні пристрої	Відкритий простір	Антена, радіоприймач, аналізатор спектру
Електромагнітні наводки	Кабелі, блоки живлення, мережеве обладнання	Сусідні провідники та кабельні траси	Підключення до наведеної лінії, вимірювальна апаратура
Витік через лінії живлення	Блоки живлення, електромережа	Кабелі електроживлення	Фільтрувально-вимірювальні або приймальні засоби
Витік через сигнальні кабелі	Мережеві та інтерфейсні кабелі	Кабельні лінії передачі даних	Аналізатор сигналів, підключення до лінії
Випромінювання від засобів зв'язку	Маршрутизатори, телефони, радіообладнання	Радіоканал або навколишній простір	Радіоприймальні пристрої, спеціалізовані антени

Механізм утворення електромагнітного каналу витоку доцільно подати у вигляді схеми. На такій схемі потрібно показати джерело випромінювання, кабельні лінії, напрям поширення побічних сигналів, межу контрольованої зони та можливий засіб перехоплення.

Електромагнітний витік має технічну природу, тому його складно оцінити без спеціальних вимірювань. Проте вже на етапі проєктування системи захисту можна зменшити ризик за рахунок правильного розміщення обладнання, використання екранованих кабелів, рознесення силових та інформаційних ліній, застосування фільтрів живлення, якісного заземлення і контролю сторонніх електронних пристроїв.

1.4 Огляд існуючих технологій і засобів захисту інформації

Захист інформації від витоку технічними каналами не може бути зведений до одного окремого пристрою або одного організаційного правила. На практиці такі канали мають різну фізичну природу, тому для їх перекриття використовують комплекс заходів. Частина з них спрямована на зменшення рівня небезпечного сигналу, інша частина – на створення завад для його перехоплення, а ще одна група заходів пов’язана з організацією контрольованої зони та обмеженням доступу сторонніх осіб.

Для акустичних каналів основним напрямом захисту є зниження розбірливості мовної інформації за межами захищеного приміщення. Якщо мовний сигнал не може бути якісно прийнятий або відновлений, ризик витоку значно зменшується. Для цього застосовують звукоізоляційні матеріали, ущільнення дверей і вікон, акустичні панелі, спеціальні конструктивні рішення, а також генератори акустичного шуму [9].

Звукоізоляція є одним із базових засобів захисту від повітряного акустичного витоку. Вона передбачає зменшення проходження звукових хвиль через стіни, двері, вікна, вентиляційні отвори та інші елементи приміщення. На ефективність звукоізоляції впливають товщина і матеріал перегородок, наявність щілин, якість монтажу дверей, тип склопакетів, а також конструкція вентиляційних каналів. Навіть невеликі нещільності можуть суттєво знизити ефективність акустичного захисту.

Окремим засобом протидії є акустичне маскування. Його сутність полягає у створенні штучного шумового сигналу, який ускладнює сприйняття або технічне відновлення мовлення. На відміну від звукоізоляції, яка зменшує поширення корисного сигналу, акустичне маскування створює додаткову заваду для засобів перехоплення. Такі завади можуть подаватися у приміщення, у суміжні конструкції або в інженерні комунікації залежно від того, який канал необхідно перекрити.

Для захисту від віброакустичного витоку використовують засоби, які зменшують передавання механічних коливань через будівельні конструкції. До них належать демпфувальні матеріали, віброізоляційні прокладки, захист віконних конструкцій, обробка трубопроводів та інших елементів, здатних проводити коливання. У складніших випадках можуть застосовуватися віброакустичні генератори завад, які подають шумовий сигнал на конструкції, що можуть бути використані для зчитування мовної інформації [12].

Важливе значення має захист інженерних комунікацій. Вентиляційні канали, труби, кабельні проходи та технологічні отвори можуть бути зручним шляхом поширення акустичного або віброакустичного сигналу. Тому під час побудови системи захисту необхідно перевіряти не тільки стіни і двері, а й усі елементи, які з’єднують захищене приміщення з іншими зонами будівлі.

Для електромагнітних каналів витоку використовують інші засоби захисту. Їхня основна мета полягає у зменшенні рівня побічних електромагнітних випромінювань, запобіганні поширенню паразитних сигналів через кабелі та зниженні впливу електромагнітних наводок. До основних заходів належать екранування обладнання, використання екранованих кабелів, фільтрація ліній живлення, правильне заземлення, рознесення кабельних трас і контроль розміщення технічних засобів [10].

Екранування є одним із найпоширеніших способів зменшення електромагнітного випромінювання. Воно може виконуватися на рівні окремого пристрою, кабелю, шафи з обладнанням або всього приміщення. Екран перешкоджає поширенню електромагнітного поля за межі захищеної області, а

також зменшує вплив зовнішніх завад на роботу обладнання. При цьому ефективність екранування залежить від матеріалу екрана, якості з’єднань, наявності отворів, способу заземлення та правильності монтажу.

Фільтрація ліній живлення застосовується для запобігання поширенню небезпечних сигналів через електромережу. Технічні засоби під час роботи можуть створювати паразитні сигнали, які потрапляють у мережу живлення і поширюються за межі контрольованої зони. Використання фільтрів дозволяє зменшити рівень таких сигналів і обмежити можливість їх перехоплення.

Заземлення відіграє важливу роль у забезпеченні електромагнітної сумісності та зменшенні рівня наводок. Неправильно виконане або відсутнє заземлення може не тільки знизити ефективність інших засобів захисту, а й саме стати причиною появи небезпечних сигналів. Тому під час проєктування системи захисту необхідно передбачати перевірку якості заземлення та правильність підключення обладнання.

Окремо слід враховувати організаційні заходи. Технічні засоби захисту не будуть достатньо ефективними, якщо не визначено правила доступу до приміщення, не контролюється використання сторонніх пристроїв і не встановлено порядок проведення конфіденційних переговорів. Наприклад, залишений у переговорній кімнаті мобільний телефон або сторонній диктофон може створити ризик витоку навіть за наявності звукоізоляції та екранування.

Організаційні заходи передбачають визначення контрольованої зони, обмеження доступу сторонніх осіб, перевірку приміщення перед проведенням важливих переговорів, контроль використання засобів зв’язку, ведення журналу перевірок і періодичний технічний контроль стану захисту. Такі заходи доповнюють інженерно-технічні рішення і дозволяють зменшити ризик помилок, пов’язаних із людським фактором. У таблиці 1.4 подано узагальнення основних засобів захисту, які можуть застосовуватися для перекриття акустичних, віброакустичних та електромагнітних каналів витоку.

Таблиця 1.4 – Основні технології та засоби захисту інформації від витоку технічними каналами

Канал витоку	Основна загроза	Засоби захисту	Очікуваний результат
Повітряний акустичний	Прослуховування мовлення через повітря	Звукоізоляція, ущільнення дверей, акустичні панелі	Зниження рівня мовного сигналу за межами приміщення
Віброакустичний	Зчитування коливань конструкцій	Демпфування, віброізоляція, віброшумові завади	Зменшення можливості відновлення мовлення через конструкції
Електроакустичний	Витік через мікрофони або лінії зв’язку	Контроль технічних засобів, вимкнення зайвих пристроїв, перевірка ліній	Зменшення ризику несанкціонованого перетворення звуку в електричний сигнал
Електромагнітний	Перехоплення побічних випромінювань	Екранування обладнання, екрановані кабелі	Зниження рівня електромагнітного випромінювання
Електричний	Поширення сигналів через лінії живлення	Фільтри живлення, правильне заземлення	Обмеження поширення паразитних сигналів
Організаційний	Порушення правил роботи з інформацією	Контроль доступу, регламенти, перевірка приміщень	Зниження ризику через людський фактор

Огляд існуючих засобів показує, що найбільш ефективним є не окремий технічний пристрій, а поєднання кількох взаємодоповнювальних заходів. Для захисту службового приміщення необхідно одночасно враховувати мовну інформацію, конструктивні елементи будівлі, технічне обладнання, кабельні лінії, електроживлення і порядок доступу до приміщення. Саме такий підхід буде використано у подальшому під час проєктування системи захисту інформації від витоку акустичними та електромагнітними каналами.

1.5 Постановка задачі

Проведений аналіз показав, що витік інформації через технічні канали є реальною загрозою для службових приміщень, у яких обробляється або обговорюється конфіденційна інформація. Найбільш характерними для такого об’єкта є акустичні, віброакустичні, електромагнітні та електричні канали витоку. Вони мають різну фізичну природу, тому не можуть бути ефективно перекриті одним універсальним засобом.

Для зниження ризику необхідно проєктувати систему захисту, у якій технічні та організаційні заходи доповнюють один одного.

У межах кваліфікаційної роботи як умовний об’єкт захисту розглядається службове приміщення, призначене для проведення переговорів, роботи з документами та використання комп’ютерної техніки.

У такому приміщенні джерелами інформації можуть бути мовлення працівників, комп’ютери, монітори, мережеве обладнання, телефонні засоби зв’язку, кабельні лінії та електроживлення. Кожен із цих елементів може створювати небезпечні сигнали або умови для їх поширення за межі контрольованої зони.

Основна проблема полягає в тому, що наявність стандартного приміщення, звичайних дверей, вікон, вентиляційних каналів, кабельних трас і технічного обладнання не гарантує захищеності інформації.

Мовна інформація може поширюватися через повітря, конструкції будівлі або інженерні комунікації. Електронна техніка може створювати побічні електромагнітні випромінювання, а кабелі живлення і зв’язку можуть бути шляхом поширення паразитних сигналів. Тому задача захисту має вирішуватися не фрагментарно, а на рівні проєктування системи.

Метою подальшої роботи є розроблення системи захисту інформації від витоку акустичними та електромагнітними каналами для службового приміщення. Така система повинна забезпечувати зниження рівня небезпечних сигналів, блокування основних каналів поширення інформації, обмеження можливостей технічного перехоплення та підтримку контролю стану захищеності.

Для досягнення цієї мети у подальших розділах необхідно вирішити кілька практичних завдань. Насамперед потрібно визначити об’єкт захисту та побудувати модель загроз, у якій будуть враховані джерела інформації, можливі канали витоку та потенційні засоби перехоплення. Далі необхідно обґрунтувати вибір засобів захисту для кожного типу каналу: акустичного, віброакустичного, електромагнітного та електричного.

Для акустичних каналів потрібно передбачити заходи, що зменшують поширення мовної інформації за межі приміщення. До таких заходів можуть належати звукоізоляція, ущільнення дверей і вікон, захист вентиляційних каналів, використання акустичного маскування та організаційне обмеження проведення конфіденційних переговорів у незахищених зонах.

Для віброакустичних каналів необхідно передбачити зменшення передавання механічних коливань через конструкції будівлі. У цьому випадку важливими є демпфування вікон, стін, трубопроводів, перекриттів та інших елементів, здатних переносити мовну інформацію у вигляді вібрацій. Також потрібно врахувати можливість застосування віброшумових завад для ускладнення відновлення мовного сигналу.

Для електромагнітних каналів слід передбачити заходи, спрямовані на зниження рівня побічних електромагнітних випромінювань та наводок. До них

належать правильне розміщення технічних засобів, екранування обладнання і кабелів, рознесення силових та інформаційних ліній, використання фільтрів живлення, якісне заземлення та контроль сторонніх електронних пристроїв.

Окремою складовою проєкту має бути допоміжний програмний модуль. Його призначення не полягає у заміні технічної системи захисту, а у підтримці процесу аналізу. Такий модуль повинен дозволяти вводити параметри приміщення і технічного середовища, виконувати попереднє оцінювання ризику, визначати рівень загрози та формувати рекомендації щодо вибору захисних заходів.

Це дасть можливість зробити систему більш зручною для дослідження, порівняння різних сценаріїв та пояснення прийнятих проєктних рішень.

У результаті виконання подальших розділів має бути сформовано проєкт системи захисту інформації, який включає:

– опис об’єкта захисту;
– модель загроз;
– вибір і обґрунтування засобів захисту;
– структурну схему системи;
– схеми перекриття каналів витоку;
– допоміжний програмний модуль для оцінювання ризику.

Така структура дозволяє розглядати роботу як інженерний проєкт системи захисту інформації.

2 ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Визначення об’єкта захисту та моделі загроз

Після аналізу технічних каналів витоку інформації необхідно перейти до проєктування системи захисту. На цьому етапі важливо не просто перелічити можливі засоби захисту, а визначити конкретний об’єкт, для якого буде розроблятися система, встановити потенційні джерела небезпечних сигналів, описати ймовірні канали витоку та сформувати модель загроз.

У межах кваліфікаційної роботи як об’єкт захисту розглядається службове приміщення, у якому проводяться робочі наради, обговорюються службові питання та використовується комп’ютерна техніка для обробки інформації. Таке приміщення може бути розташоване в адміністративній будівлі, навчальному закладі, офісі підприємства або іншій організації, де обробляється інформація з обмеженим доступом. Саме службові приміщення є характерними об’єктами для виникнення акустичних, віброакустичних та електромагнітних каналів витоку.

У приміщенні можуть знаходитися робочі столи, персональні комп’ютери, монітори, мережеве обладнання, телефонні апарати, кабельні лінії живлення та передачі даних. Крім цього, у ньому можуть проводитися переговори між працівниками, під час яких формується мовна інформація. У такій ситуації захисту підлягає не лише інформація, що зберігається або обробляється технічними засобами, а й інформація, яка передається усно.

Основними об’єктами захисту в межах проєктованої системи є мовна інформація, що виникає під час переговорів, дані, які обробляються комп’ютерною технікою, сигнали в кабельних лініях, а також інформація, яка може бути пов’язана з роботою засобів зв’язку. Такий підхід дозволяє розглядати приміщення не як ізольовану кімнату, а як комплексний об’єкт, у якому одночасно присутні різні джерела загроз.

Для побудови системи захисту необхідно визначити межі контрольованої зони. У даному випадку контрольована зона охоплює саме службове приміщення, його огороджувальні конструкції, двері, вікна, вентиляційні канали,

кабельні вводи, електроживлення та суміжні ділянки, через які можуть поширюватися небезпечні сигнали. Якщо частина інженерних комунікацій виходить за межі приміщення, вона також повинна враховуватися під час проєктування системи захисту.

Загрози для такого об’єкта можна поділити на кілька груп. Перша група пов’язана з акустичним витоком інформації. Вона включає можливість прослуховування розмов через двері, вікна, вентиляційні отвори, тонкі перегородки або інші елементи приміщення. Друга група стосується віброакустичного витоку, коли мовна інформація передається через механічні коливання стін, скла, труб або перекриттів. Третя група пов’язана з електромагнітними випромінюваннями від технічних засобів. Четверта група включає витік через лінії живлення, кабелі зв’язку та інші електричні мережі.

При формуванні моделі загроз необхідно враховувати не лише сам факт існування каналу витоку, а й умови, за яких він може бути реалізований. Наприклад, акустичний канал стає небезпечним за наявності недостатньої звукоізоляції, близького розташування сторонніх осіб або відсутності шумового маскування. Електромагнітний канал стає більш імовірним при використанні неекранованих кабелів, відсутності фільтрів живлення, неправильному заземленні або розміщенні обладнання біля меж контрольованої зони [9].

Потенційним порушником у межах цієї роботи вважається особа, яка не має права доступу до конфіденційної інформації, але може перебувати поблизу контрольованої зони або мати можливість використання технічних засобів перехоплення. Це може бути стороння особа в суміжному приміщенні, відвідувач, працівник без відповідних повноважень або особа, яка має доступ до інженерних комунікацій. Така модель є достатньою для навчального проєктування системи захисту, оскільки дозволяє оцінити основні технічні ризики без надмірного ускладнення.

Для подальшого проєктування доцільно систематизувати основні загрози, джерела їх виникнення та можливі наслідки. Така модель наведена у таблиці 2.1.

Таблиця 2.1 – Модель загроз для службового приміщення

Джерело загрози	Канал витоку	Можливий спосіб реалізації	Можливі наслідки
Мовлення працівників	Акустичний	Прослуховування через двері, вікна, вентиляцію	Розголошення змісту переговорів
Вікна, стіни, труби, перекриття	Віброакустичний	Зчитування механічних коливань конструкцій	Відновлення мовної інформації
Комп’ютери, монітори, сервери	Електромагнітний	Перехоплення побічних електромагнітних випромінювань	Отримання даних про роботу технічних засобів
Кабельні лінії	Електричний / електромагнітний	Наведення або поширення паразитних сигналів	Витік інформації через інфраструктуру
Засоби зв’язку	Електроакустичний	Несанкціоноване використання мікрофонів або ліній зв’язку	Перехоплення розмов
Сторонні електронні пристрої	Акустичний / електромагнітний	Прихований запис або передавання сигналів	Неконтрольований витік інформації

На основі наведеної моделі можна визначити основні вимоги до майбутньої системи захисту. Вона повинна зменшувати рівень поширення мовної інформації за межі приміщення, ускладнювати зчитування вібрацій конструкцій, знижувати рівень побічних електромагнітних випромінювань, обмежувати поширення паразитних сигналів через кабелі та забезпечувати

контроль використання сторонніх технічних засобів.

Система захисту не повинна розглядатися лише як набір окремих пристроїв. Вона має бути побудована як сукупність узгоджених заходів. Наприклад, звукоізоляція дверей буде менш ефективною, якщо залишити незахищеними вентиляційні канали. Екранування обладнання не дасть повного результату, якщо сигнали продовжують поширюватися через кабелі живлення. Тому всі елементи системи мають проєктуватися з урахуванням взаємного впливу.

З урахуванням визначених загроз у подальших підрозділах буде розглянуто проєктні рішення щодо захисту від акустичного, віброакустичного та електромагнітного витоку. Окремо буде обґрунтовано вибір засобів захисту та сформовано структурну схему системи. Такий підхід дозволяє перейти від загального аналізу загроз до конкретного інженерного проєктування системи захисту інформації.

2.2 Проєктування захисту від акустичного витоку

Після визначення об’єкта захисту та моделі загроз необхідно спроєктувати заходи, які будуть спрямовані на перекриття основних акустичних каналів витоку інформації. Для службового приміщення, у якому проводяться переговори та обговорюється інформація з обмеженим доступом, акустичний захист є одним із першочергових напрямів. Це пов’язано з тим, що мовна інформація може поширюватися за межі приміщення навіть без використання технічних засобів зв’язку або комп’ютерної мережі.

Основною метою захисту від акустичного витоку є зниження рівня мовного сигналу за межами контрольованої зони до такого стану, за якого його неможливо або суттєво ускладнено сприйняти, записати чи відновити технічними засобами. Для цього система захисту повинна впливати на сам сигнал, середовище його поширення та можливість приймання за межами приміщення.

У межах проєктованої системи доцільно передбачити кілька груп заходів:

звукоізоляційні, маскувальні, конструктивні та організаційні. Звукоізоляційні заходи спрямовані на фізичне зменшення проходження звуку через огороджувальні конструкції. Маскувальні заходи створюють додатковий шумовий фон, який знижує розбірливість мовлення. Конструктивні рішення усувають слабкі місця приміщення, а організаційні заходи визначають правила користування захищеним приміщенням.

Першим елементом акустичного захисту є звукоізоляція стін, дверей і вікон. Стіни та перегородки повинні мати достатню масу і щільність, оскільки легкі конструкції краще передають звукові хвилі. Якщо приміщення має тонкі перегородки або межує з коридором чи іншим робочим приміщенням, необхідно передбачити використання додаткових звукоізоляційних матеріалів. Це можуть бути акустичні панелі, багатошарові конструкції, звукопоглинальні прокладки або інші матеріали, що зменшують проходження мовного сигналу.

Окрему увагу слід приділити дверям. На практиці саме дверні конструкції часто є слабким місцем акустичного захисту. Навіть якщо стіни мають достатній рівень звукоізоляції, щілини між дверима і коробкою можуть забезпечити поширення мовної інформації за межі приміщення. Тому в системі захисту необхідно передбачити ущільнення дверей по периметру, використання дверного порога або автоматичного ущільнювача, а також застосування дверей із підвищеними звукоізоляційними властивостями.

Вікна також можуть бути шляхом акустичного витоку. Крім прямого проходження звуку через нещільності, віконне скло може брати участь у формуванні віброакустичного каналу. Для зменшення акустичного витоку через вікна доцільно використовувати герметичні склопакети, додаткові ущільнювачі, важкі штори або внутрішні акустичні екрани. Якщо вікна виходять у зону, доступну стороннім особам, їх захист має бути посиленим.

Важливою складовою є захист вентиляційних каналів. Вентиляція може передавати мовлення за межі приміщення, особливо якщо повітропроводи з’єднують кілька кімнат або виходять у коридор. Для зменшення такого ризику доцільно використовувати акустичні вставки, шумоглушники, лабіринтні

повітропроводи або інші конструктивні рішення, які перешкоджають прямому поширенню звуку.

Другим напрямом є акустичне маскування. Воно передбачає створення додаткового шумового сигналу, який ускладнює розбір мовлення за межами контрольованої зони. У системі захисту доцільно передбачити використання генератора акустичного шуму. Такий пристрій може створювати широкосмугову заваду, що накладається на мовний сигнал і знижує можливість його технічного відновлення. Генератор шуму доцільно розміщувати таким чином, щоб шумовий сигнал перекривав потенційні шляхи витоку, але не створював надмірного дискомфорту для користувачів приміщення. Наприклад, шумові випромінювачі можуть бути встановлені біля дверей, вікон, вентиляційних каналів або в суміжних зонах. Рівень шуму повинен бути достатнім для маскування мовлення, але не заважати нормальній роботі персоналу.

Третім напрямом є організація простору всередині приміщення. Робочі місця та зона переговорів не повинні розташовуватися безпосередньо біля дверей, вікон або тонких перегородок. Чим далі джерело мовної інформації знаходиться від меж контрольованої зони, тим нижчим є ризик витоку. Тому під час проєктування доцільно розміщувати переговорний стіл ближче до центральної частини приміщення або біля більш масивних конструкцій. У таблиці 2.2 наведено проєктні рішення.

Також необхідно передбачити організаційні обмеження. Конфіденційні переговори повинні проводитися лише після перевірки приміщення, закриття дверей і вікон, вимкнення непотрібних пристроїв запису та контролю наявності сторонніх осіб. Для локального або тимчасового маскування можуть застосовуватися мобільні генератори шуму [28], а для протидії несанкціонованому запису - пригнічувачі диктофонів [29]. Проєктовану систему акустичного захисту доцільно будувати за принципом послідовного перекриття основних шляхів поширення мовної інформації. Спочатку потрібно зменшити рівень вихідного сигналу за рахунок організації простору та регламенту перемовин.

Таблиця 2.2 – Проєктні рішення щодо захисту від акустичного витоку

Елемент приміщення або загроза	Можливий канал витоку	Проєктне рішення	Очікуваний результат
Двері	Поширення звуку через щілини та дверне полотно	Ущільнення дверей, використання порога, двері з підвищеною звукоізоляцією	Зменшення проходження мовного сигналу в коридор
Вікна	Проходження звуку назовні	Герметичні склопакети, ущільнювачі, акустичні штори	Зниження рівня акустичного сигналу за межами приміщення
Стіни та перегородки	Поширення мовлення через конструкції	Додаткові звукоізоляційні матеріали, акустичні панелі	Послаблення звукових хвиль
Вентиляційні канали	Передавання мовлення через повітропроводи	Шумоглушники, акустичні вставки, лабіринтні канали	Блокування прямого поширення звуку
Зона переговорів	Надмірна близькість до меж приміщення	Розміщення джерел мовлення у центральній частині кімнати	Зменшення рівня сигналу біля меж контрольованої зони
Потенційне прослуховування	Запис мовлення за межами приміщення	Генератор акустичного шуму	Зниження розбірливості мовної інформації

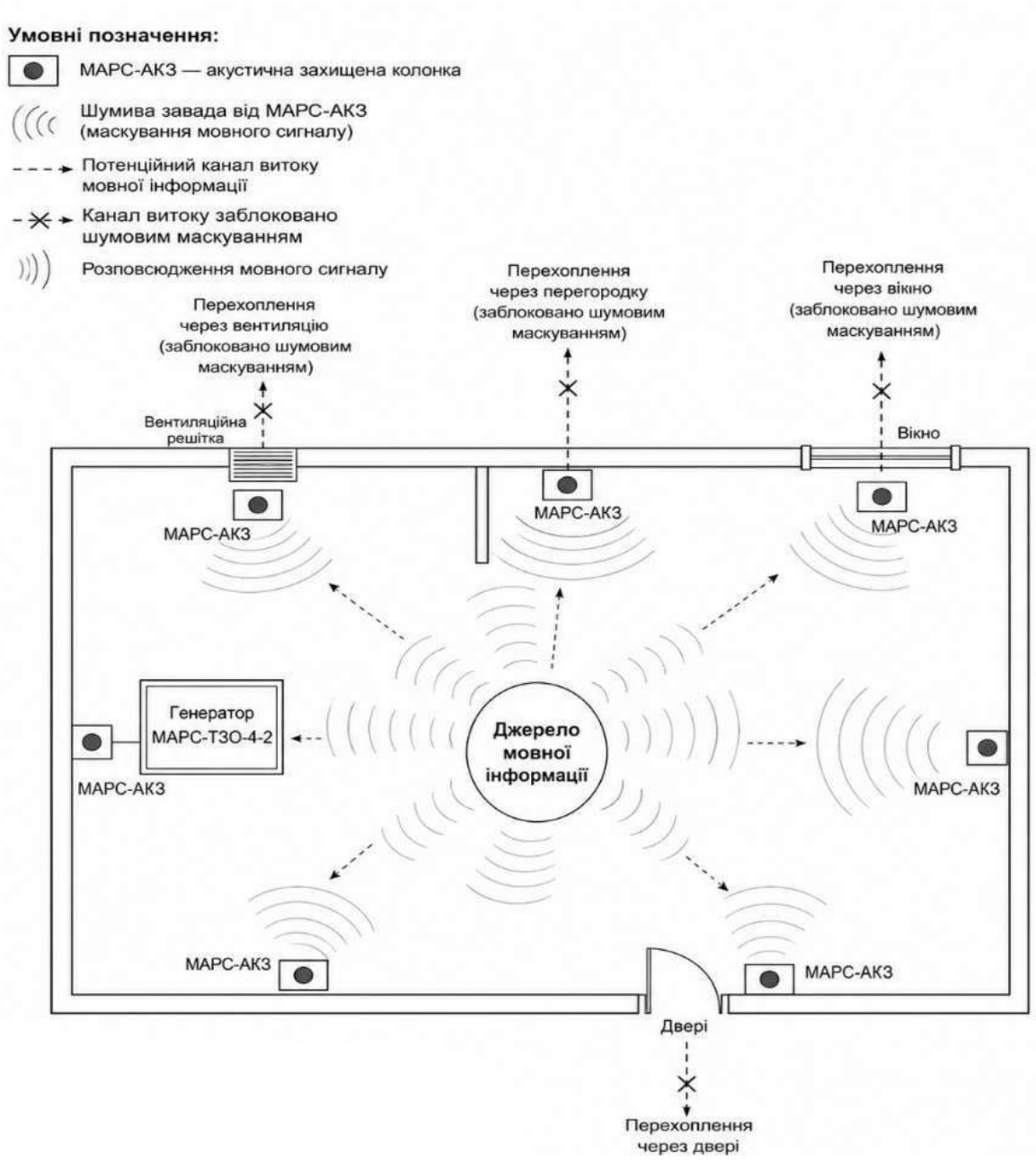


Рисунок 2.1 – Схема перекриття акустичних каналів витоку інформації

У результаті запропоновані рішення дозволяють сформувати базову підсистему акустичного захисту службового приміщення. Вона не обмежується одним засобом, а поєднує звукоізоляцію, акустичне маскування, захист вентиляційних каналів, правильне розміщення джерел мовної інформації та організаційний контроль. Такий підхід зменшує ймовірність витоку мовної інформації та створює основу для подальшого проєктування віброакустичного і електромагнітного захисту.

2.3 Проєктування захисту від віброакустичного витоку

Віброакустичний витік інформації є окремим і досить небезпечним різновидом технічного каналу, оскільки мовна інформація в цьому випадку поширюється не лише через повітря, а й через тверді конструкції приміщення. Під час розмови звукові хвилі впливають на стіни, вікна, двері, труби, перекриття та інші елементи будівлі, спричиняючи їхні мікроколивання. Такі коливання можуть бути зафіксовані спеціальними датчиками або лазерними засобами зчитування, після чого мовний сигнал відновлюється.

На відміну від звичайного повітряного акустичного каналу, віброакустичний канал складніше виявити під час візуального огляду приміщення. Його небезпека полягає в тому, що засіб перехоплення може не перебувати всередині захищеної кімнати. Наприклад, контактний датчик може бути встановлений на трубі або стіні в суміжному приміщенні, а лазерний мікрофон може зчитувати коливання віконного скла ззовні будівлі. Тому система захисту має враховувати не тільки безпосереднє поширення звуку, а й передачу механічних коливань через конструкції.

У межах проєктованої системи основними елементами, через які може формуватися віброакустичний витік, є вікна, стіни, двері, трубопроводи, вентиляційні канали, перекриття та інші інженерні комунікації. Кожен із цих елементів може виконувати роль провідника коливань. Тому захист має бути спрямований на зменшення амплітуди вібрацій, ускладнення їх поширення та створення додаткових завад, які знижують можливість відновлення інформації.

Першим напрямом захисту є демпфування конструкцій. Демпфування передбачає використання матеріалів або конструктивних рішень, які поглинають механічні коливання і зменшують їхню передачу. Для стін, перегородок і дверей можуть застосовуватися багатошарові матеріали, звукопоглинальні та віброізоляційні прокладки. Для труб і металевих елементів доцільно використовувати спеціальні накладки або кріплення, які знижують передачу коливань уздовж конструкції.

Окрему увагу необхідно приділити вікнам. Скло має порівняно малу масу і може реагувати на звуковий тиск усередині приміщення. Через це воно є одним із найбільш небезпечних елементів у контексті віброакустичного витоку. Для зменшення ризику доцільно використовувати багатокамерні склопакети, додаткові ущільнювачі, важкі штори або внутрішні екрани. Якщо приміщення розташоване так, що вікна доступні для зовнішнього спостереження, їх захист має бути посиленим.

Другим напрямом є віброізоляція трубопроводів та інженерних комунікацій. Труби опалення, водопостачання, вентиляційні елементи та металеві конструкції можуть передавати механічні коливання за межі контрольованої зони. У такому випадку засоби перехоплення можуть бути встановлені не в самому приміщенні, а на віддаленій ділянці комунікації. Для зниження такого ризику потрібно передбачити застосування віброізоляційних вставок, гнучких з’єднань, демпфувальних матеріалів і контроль місць проходження комунікацій через огороджувальні конструкції.

Третім напрямом є використання віброакустичного маскування. Якщо конструкція приміщення потенційно може передавати мовні коливання, доцільно створювати додаткові шумові або вібраційні сигнали, які ускладнюють технічне відновлення мовлення (таблиця 2.3). Такий підхід особливо важливий для вікон, труб, стін і дверей, які можуть бути доступні для зчитування ззовні або з суміжних приміщень. Віброшумові перетворювачі можуть встановлюватися на конструктивні елементи і передавати на них шумову заваду.

У проєктованій системі захисту доцільно передбачити використання генератора шумових сигналів або віброакустичних перетворювачів, які можуть створювати маскувальний сигнал на потенційно небезпечних поверхнях. Таке рішення не замінює звукоізоляцію, але доповнює її, оскільки впливає саме на механічний шлях поширення інформації. Поєднання демпфування і шумового маскування дозволяє значно зменшити можливість відновлення мовної інформації з вібрацій конструкцій.

Таблиця 2.3 – Проєктні рішення щодо захисту від віброакустичного витоку

Елемент або загроза	Можливий шлях витоку	Проєктне рішення	Очікуваний результат
Віконне скло	Зчитування коливань скла лазерним мікрофоном	Багатокамерні склопакети, ущільнювачі, штори, віброшумові перетворювачі	Зниження амплітуди коливань і ускладнення відновлення мовлення
Стіни та перегородки	Передавання мовних коливань у суміжні приміщення	Демпфувальні матеріали, багатошарові конструкції, звукопоглинальні панелі	Послаблення механічних коливань
Двері	Коливання дверного полотна і коробки	Ущільнення, масивні двері, демпфувальні вставки	Зменшення передачі вібрацій за межі кімнати
Труби та комунікації	Поширення коливань через металеві елементи	Віброізоляційні вставки, гнучкі з’єднання, демпфування труб	Обмеження поширення сигналу через інженерні мережі
Перекриття	Передавання коливань через підлогу або стелю	Віброізоляційні матеріали, килимове покриття, демпфувальні прошарки	Зменшення передачі механічних коливань
Суміжні технічні зони	Встановлення датчиків за межами приміщення	Контроль доступу, періодична перевірка конструкцій	Зниження ймовірності прихованого перехоплення

Особливе значення має правильне розміщення джерел мовної інформації (рисунок 2.2).

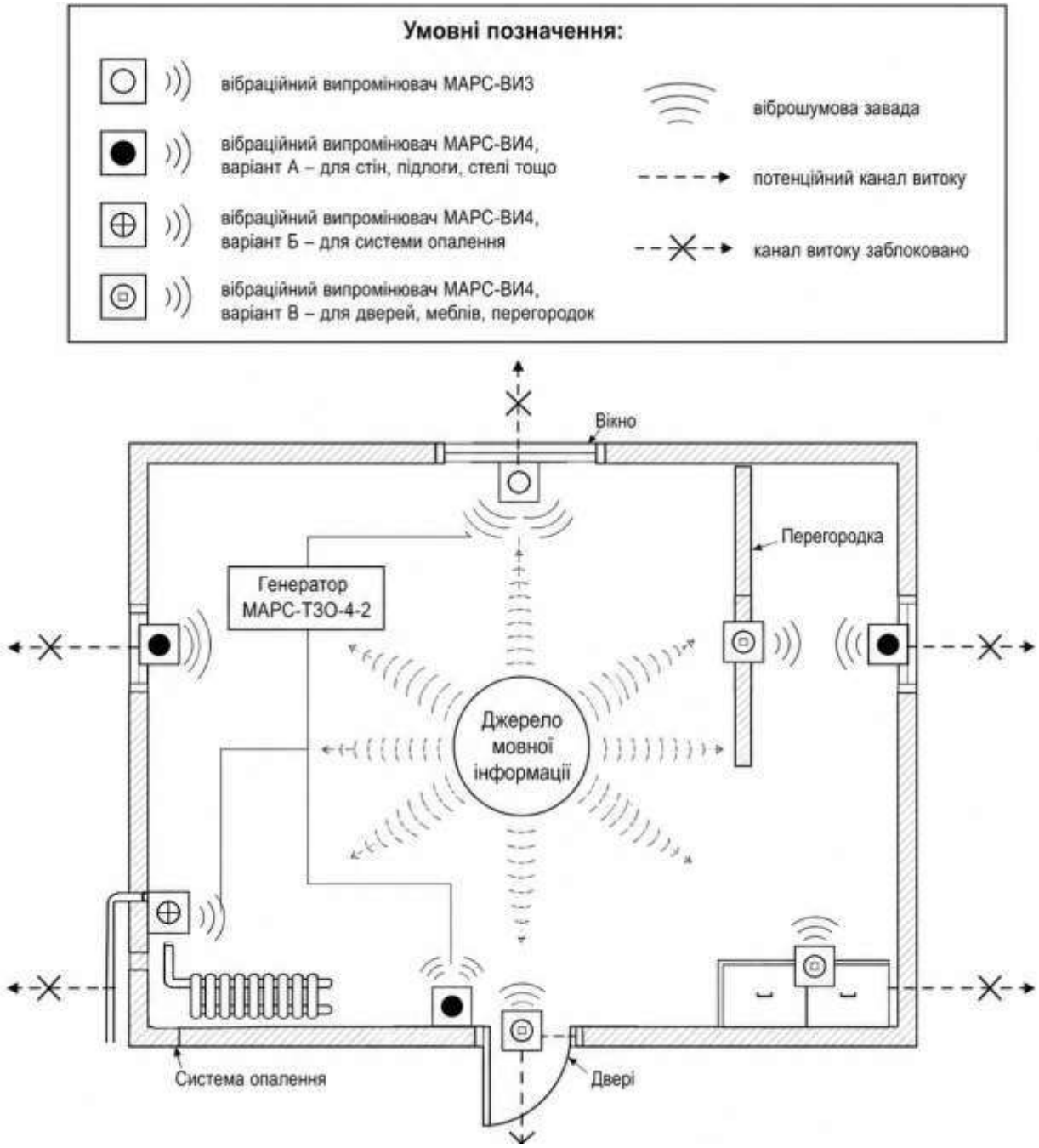


Рисунок 2.2 – Схема перекриття віброакустичних каналів витоку інформації

Якщо переговорний стіл або робоче місце розташовані безпосередньо біля вікна, тонкої перегородки або трубопроводу, ризик утворення віброакустичного каналу зростає. Тому під час проєктування приміщення бажано розміщувати зону переговорів у центральній частині кімнати або на максимальній відстані від

конструкцій, які можуть передавати коливання за межі контрольованої зони.

Для віброакустичного захисту також важливий організаційний контроль. Перед проведенням конфіденційних переговорів необхідно перевіряти відсутність сторонніх предметів на вікнах, трубах, стінах та інших елементах, які можуть бути використані для встановлення датчиків.

Запропоновані рішення дозволяють розглядати віброакустичний захист як окрему підсистему комплексної системи захисту інформації. Її основне завдання полягає не лише у зменшенні рівня звуку в приміщенні, а й у зниженні можливості передавання мовної інформації через тверді конструкції. У поєднанні з акустичним захистом така підсистема дозволяє значно зменшити ризик витоку мовної інформації за межі контрольованої зони.

2.4 Проєктування захисту від електромагнітного витоку

Електромагнітний витік інформації пов’язаний із побічними електромагнітними випромінюваннями та наводками, що виникають під час роботи технічних засобів. Для службового приміщення такими джерелами можуть бути персональні комп’ютери, монітори, серверне або мережеве обладнання, кабелі живлення, сигнальні лінії, периферійні пристрої та засоби зв’язку. На відміну від акустичного витоку, електромагнітний канал не сприймається безпосередньо людиною, тому його наявність складніше виявити без спеціальних вимірювань [20].

Основною метою захисту від електромагнітного витоку є зниження рівня побічних випромінювань і обмеження поширення паразитних сигналів за межі контрольованої зони. У межах проєктованої системи захисту необхідно врахувати як випромінювання від самих технічних засобів, так і можливість поширення небезпечних сигналів через кабельні лінії, електроживлення та заземлення.

Першим напрямом захисту є раціональне розміщення технічного

обладнання. Комп’ютери, монітори, маршрутизатори, комутатори та інші пристрої не слід розташовувати безпосередньо біля зовнішніх стін, вікон або меж контрольованої зони. Чим ближче джерело випромінювання знаходиться до потенційної точки перехоплення, тим вищою є ймовірність фіксації побічного сигналу. Тому обладнання доцільно розміщувати в глибині приміщення або в зоні, максимально віддаленій від неконтрольованого простору.

Другим напрямом є екранування технічних засобів і кабельних ліній. Екранування дозволяє зменшити рівень електромагнітного поля, яке виходить за межі обладнання або кабелю. У проєктованій системі доцільно передбачити використання екранованих кабелів для інформаційних ліній, металевих кабель-каналів, екранованих шаф для мережевого обладнання та корпусів із достатнім рівнем електромагнітного захисту. При цьому важливо, щоб екранування не було формальним: екрани кабелів і корпусів повинні мати правильне електричне з’єднання та відповідне заземлення.

Окрему увагу необхідно приділити кабельній інфраструктурі. Силові кабелі та інформаційні лінії не повинні прокладатися впритул один до одного на значній довжині, оскільки це може сприяти виникненню електромагнітних наводок. У системі захисту доцільно передбачити рознесення кабельних трас, використання окремих каналів для силових та інформаційних кабелів, а також мінімізацію довжини відкритих ділянок кабелів у межах приміщення.

Третім важливим засобом є фільтрація ліній живлення. Під час роботи електронного обладнання паразитні сигнали можуть потрапляти в мережу електроживлення і поширюватися за межі контрольованої зони. Для зменшення цього ризику доцільно використовувати мережеві фільтри, фільтри електроживлення для окремих груп обладнання, а також захисні пристрої на вводі живлення до приміщення. Фільтрація дозволяє обмежити поширення високочастотних складових сигналу через електромережу.

Заземлення є окремою складовою електромагнітного захисту. Неправильно організоване заземлення може знизити ефективність екранування, створити додаткові контури наведення або сприяти поширенню небезпечних сигналів.

Тому в системі захисту необхідно передбачити перевірку цілісності заземлювальних провідників, правильне підключення екранів кабелів і обладнання, а також виключення випадкових або неконтрольованих з’єднань.

Важливим організаційним заходом є контроль сторонніх електронних пристроїв. У службовому приміщенні не повинні безконтрольно використовуватися пристрої, які можуть приймати, записувати або передавати інформацію. До таких пристроїв належать мобільні телефони, диктофони, радіопередавачі, бездротові мікрофони, невідомі USB-пристрої, модеми та інша портативна електроніка. Навіть якщо основне обладнання захищене, сторонній пристрій може створити додатковий канал витоку.

Ще одним напрямом є формування контрольованої зони для технічних засобів. Це означає, що приміщення, кабельні вводи, лінії живлення, мережеві підключення та місця розміщення обладнання повинні бути включені до зони контролю. Особливо важливо враховувати ділянки, де кабелі виходять за межі приміщення або проходять через суміжні простори. Такі ділянки мають бути захищені конструктивно або організаційно.

Для проєктованої системи електромагнітного захисту доцільно прийняти такі основні рішення: розміщення обладнання на відстані від меж контрольованої зони, застосування екранованих кабелів, рознесення силових та інформаційних ліній, встановлення фільтрів живлення, контроль правильності заземлення, обмеження використання сторонніх пристроїв і періодична перевірка технічного стану системи. У таблиці 2.4 наведено проєктні рішення щодо захисту від електромагнітного витоку інформації.

Важливим елементом системи електромагнітного захисту є проведення регулярного технічного контролю та моніторингу рівня побічних електромагнітних випромінювань. Періодичні перевірки дозволяють своєчасно виявляти пошкодження екранів, порушення заземлення, несанкціоновані підключення або зміни параметрів обладнання, які можуть створити нові канали витоку інформації та знизити ефективність усієї системи захисту. Схему перекриття електромагнітних каналів витоку подано на рисунку 2.3.

Таблиця 2.4 – Проєктні рішення захисту від електромагнітного витоку

Елемент або загроза	Можливий канал витоку	Проєктне рішення	Очікуваний результат
Комп'ютери та монітори	Побічні електромагнітні випромінювання	Розміщення в глибині приміщення, використання обладнання з належним рівнем електромагнітної сумісності	Зменшення ймовірності дистанційного перехоплення
Мережеве обладнання	Випромінювання та наведення	Розміщення в екранованій шафі, обмеження доступу	Зниження рівня побічних сигналів і контроль доступу
Інформаційні кабелі	Наведення та випромінювання кабельних ліній	Використання екранованих кабелів, металевих кабель-каналів	Обмеження поширення небезпечних сигналів
Силові та інформаційні лінії	Взаємні електромагнітні наводки	Рознесення кабельних трас, окреме прокладання ліній	Зменшення паразитних наведень
Лінії живлення	Поширення сигналів через електромережу	Встановлення фільтрів живлення	Обмеження виходу паразитних сигналів за межі приміщення
Заземлення	Поширення сигналів через контури заземлення	Перевірка якості заземлення, правильне підключення екранів	Підвищення ефективності екранування
Сторонні електронні пристрої	Неконтрольований прийом або передавання сигналів	Обмеження використання, перевірка приміщення	Зменшення ризику несанкціонованого витоку

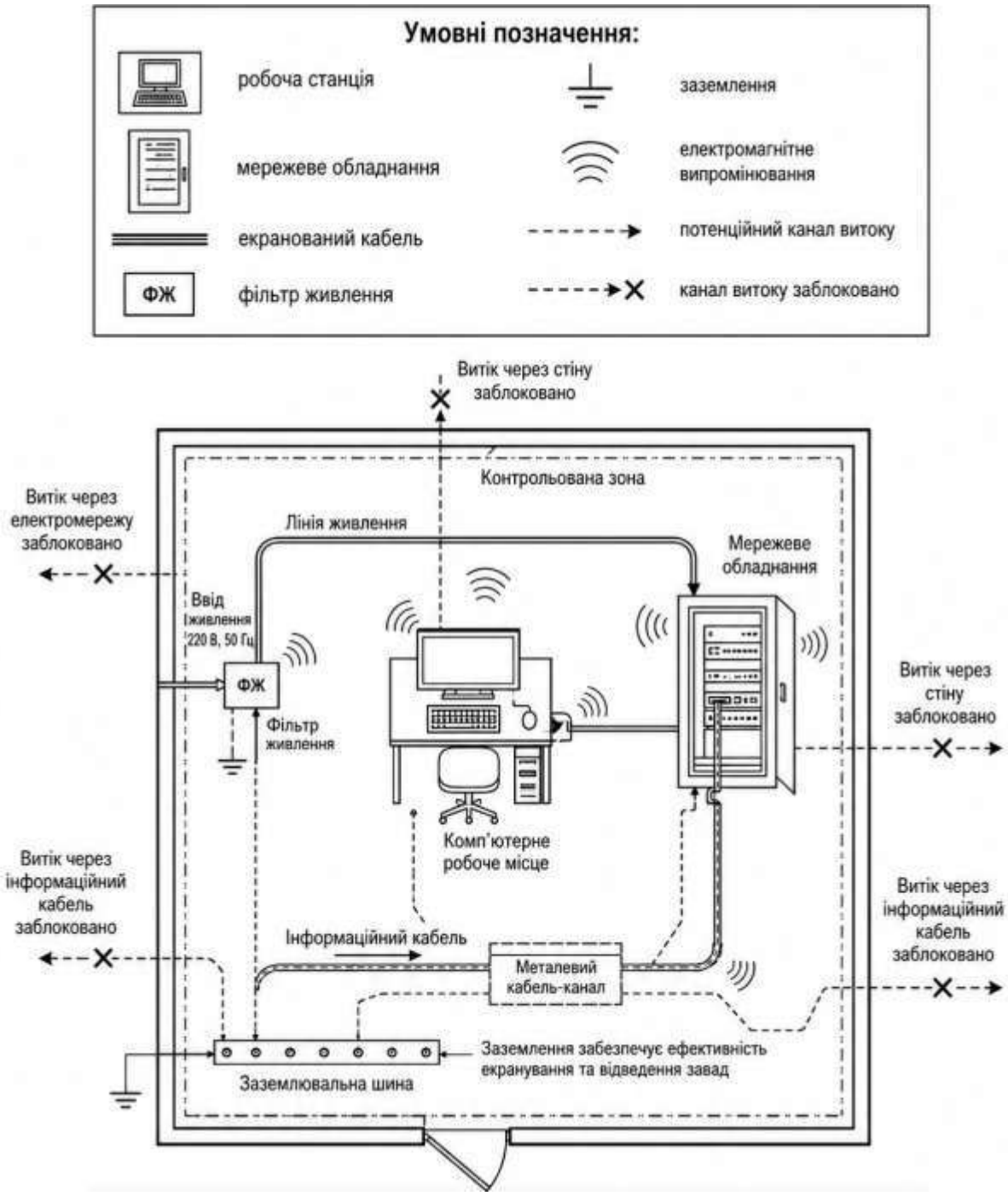


Рисунок 2.3 – Схема перекриття електромагнітних каналів витоку інформації

Запропоновані рішення дозволяють сформувати підсистему електромагнітного захисту, яка доповнює акустичні та віброакустичні заходи. Її ефективність залежить від узгодженого застосування екранування, фільтрації, заземлення, правильного розміщення обладнання та контролю кабельної інфраструктури. У поєднанні з іншими підсистемами це дає змогу створити комплексну систему захисту інформації для службового приміщення.

2.5 Структурна схема системи захисту інформації

Після визначення основних загроз та вибору проєктних рішень для акустичного, віброакустичного й електромагнітного захисту необхідно сформувати загальну структуру системи захисту інформації. Структурна схема повинна показувати не окремий засіб, а взаємодію всіх елементів, які забезпечують зниження ризику витоку інформації через технічні канали.

У межах кваліфікаційної роботи система захисту інформації розглядається як комплекс взаємопов’язаних підсистем. До її складу входять підсистема акустичного захисту, підсистема віброакустичного захисту, підсистема електромагнітного захисту, підсистема організаційного контролю та допоміжний програмний модуль оцінювання ризику. Кожна з цих підсистем виконує окрему функцію, але ефективність досягається саме за рахунок їх спільного застосування.

Підсистема акустичного захисту призначена для зменшення поширення мовної інформації через повітряне середовище. Вона включає звукоізоляцію стін, дверей і вікон, захист вентиляційних каналів, правильне розміщення зони переговорів та застосування акустичного маскування. Її основне завдання полягає у зниженні рівня мовного сигналу за межами контрольованої зони.

Підсистема віброакустичного захисту спрямована на обмеження передавання мовної інформації через механічні коливання конструкцій. До її складу можуть входити демпфувальні матеріали, віброізоляційні вставки, захист віконних конструкцій, демпфування трубопроводів, а також віброшумові перетворювачі. Така підсистема особливо важлива для приміщень, де вікна, стіни або інженерні комунікації можуть бути доступними для зовнішнього зчитування.

Підсистема електромагнітного захисту забезпечує зниження рівня побічних електромагнітних випромінювань і наводок. Вона передбачає використання екранованих кабелів, фільтрів живлення, правильного заземлення, рознесення кабельних трас, розміщення обладнання на безпечній відстані від

меж контрольованої зони та контроль сторонніх електронних пристроїв.

Підсистема організаційного контролю доповнює технічні рішення. Її завдання полягає у встановленні правил доступу до службового приміщення, контролі використання мобільних пристроїв, перевірці приміщення перед проведенням конфіденційних переговорів, веденні журналу перевірок та періодичному контролі стану засобів захисту. Без організаційних заходів навіть технічно правильно побудована система може залишатися вразливою через людський фактор.

Окремою складовою системи є допоміжний програмний модуль. Він не виконує безпосереднього блокування каналів витоку, але підтримує процес аналізу і прийняття рішень. За допомогою такого модуля можна вводити параметри приміщення, оцінювати рівень ризику, порівнювати різні сценарії, отримувати рекомендації щодо вибору захисних заходів і зберігати результати перевірок. У структурі системи цей модуль виконує роль інструмента підтримки проєктування та контролю.

Структурну схему системи захисту інформації доцільно побудувати таким чином, щоб у центрі була контрольована зона або службове приміщення, а навколо нього - підсистеми захисту, які впливають на різні канали витоку. Такий підхід дозволяє наочно показати, що система має комплексний характер і не обмежується лише програмним модулем або одним технічним пристроєм.

Взаємодія елементів системи повинна будуватися за принципом послідовного зниження ризику. Спочатку визначаються джерела інформації та можливі канали витоку. Далі для кожного каналу підбираються відповідні засоби захисту. Після цього виконується оцінювання залишкового ризику і, за потреби, формуються додаткові рекомендації щодо посилення захисту.

Для зручності структуру системи можна подати у вигляді функціональних блоків. Узагальнення цих блоків наведено в таблиці 2.5.

Таблиця 2.5 – Функціональні блоки системи захисту інформації

Функціональний блок	Призначення	Основні елементи
Акустичний захист	Зменшення поширення мовної інформації через повітря	Звукоізоляція, ущільнення дверей, захист вентиляції, генератор шуму
Віброакустичний захист	Обмеження передавання мовлення через конструкції	Демпфери, віброізоляційні матеріали, віброшумові перетворювачі
Електромагнітний захист	Зниження побічних випромінювань і наводок	Екранування, фільтри живлення, заземлення, екрановані кабелі
Організаційний контроль	Регламентація роботи із захищеним приміщенням	Контроль доступу, перевірка приміщення, обмеження сторонніх пристроїв
Програмний модуль	Оцінювання ризику та формування рекомендацій	Введення параметрів, розрахунок ризику, журнал перевірок, статистика

Таким чином, структурна схема системи захисту інформації повинна відображати комплексний підхід до перекриття технічних каналів витоку. У ній поєднуються технічні засоби захисту, організаційні заходи та допоміжний програмний інструмент.

Саме таке поєднання дозволяє перейти від загального аналізу загроз до практичного проєктування системи, яка може бути використана для службового приміщення з обробкою конфіденційної інформації.

2.6 Обґрунтування обраних засобів захисту

Після визначення структури системи захисту інформації необхідно обґрунтувати вибір конкретних засобів і заходів, які доцільно застосувати для службового приміщення. Обґрунтування потрібне для того, щоб показати зв’язок між виявленими каналами витоку, характером загроз і прийнятими проєктними рішеннями. У даному випадку захист не може будуватися випадково або лише за принципом наявності окремих технічних засобів. Кожен елемент системи повинен перекривати конкретний канал або зменшувати вплив певного фактору ризику.

Для проєктованої системи захисту основними є чотири групи каналів витоку: акустичні, віброакустичні, електромагнітні та електричні. Вони мають різну фізичну природу, тому для кожної групи потрібні окремі рішення. При цьому частина заходів може одночасно впливати на декілька каналів. Наприклад, правильне розміщення обладнання зменшує ризик електромагнітного витоку, а організаційний контроль знижує ймовірність як акустичного, так і електромагнітного перехоплення.

Для захисту від повітряного акустичного витоку обрано звукоізоляційні заходи та акустичне маскування. Таке рішення обґрунтоване тим, що мовна інформація поширюється насамперед через повітря, двері, вікна, вентиляційні канали та нещільності в конструкціях. Звукоізоляція дозволяє зменшити рівень мовного сигналу за межами приміщення, а генератор акустичного шуму знижує розбірливість залишкового сигналу. Поєднання цих рішень є доцільним, оскільки тільки звукоізоляція не завжди повністю усуває ризик витоку, особливо в умовах наявності дверних щілин, вентиляції або легких перегородок.

Для дверей і вікон обґрунтованим є використання ущільнювачів, масивніших конструкцій і додаткових ізоляційних елементів. Ці елементи є слабкими місцями службового приміщення, тому їх посилення має першочергове значення. Якщо залишити двері або вікна без додаткового захисту, ефективність інших акустичних заходів буде нижчою, оскільки звук

поширюватиметься саме через ці ділянки.

Для захисту вентиляційних каналів доцільно передбачити акустичні вставки або шумоглушники. Таке рішення пояснюється тим, що вентиляція може створювати прямий повітряний шлях між захищеним приміщенням та іншими зонами будівлі. У цьому випадку навіть якісна звукоізоляція стін і дверей не забезпечить належного результату, якщо мовний сигнал буде поширюватися через повітропровід.

Для віброакустичного каналу обрано демпфування конструкцій, віброізоляцію та застосування віброшумових завад. Ці засоби спрямовані на зменшення механічних коливань, які можуть переносити мовну інформацію через стіни, скло, труби, двері та перекриття. Особливо важливим є захист віконних конструкцій, оскільки скло може реагувати на звуковий тиск і бути використане для дистанційного зчитування коливань.

Захист трубопроводів та інженерних комунікацій також є необхідним. Металеві труби і жорсткі конструктивні елементи можуть передавати коливання на значну відстань. Тому використання гнучких вставок, демпфувальних матеріалів і контролю місць проходження комунікацій через огороджувальні конструкції є обґрунтованим елементом проєктованої системи.

Для електромагнітного захисту обрано екранування технічних засобів і кабельних ліній, фільтрацію живлення, правильне заземлення та рознес98ення кабельних трас. Ці рішення відповідають характеру загроз, оскільки електромагнітний витік може формуватися як через просторове випромінювання, так і через наведення в кабелях або поширення паразитних сигналів у лініях живлення.

Екранування обладнання та кабелів дозволяє знизити рівень побічних електромагнітних випромінювань. Використання екранованих кабелів і металевих кабель-каналів є доцільним для інформаційних ліній, які можуть переносити сигнали з високою частотою або бути джерелом наведень. Водночас саме екранування буде ефективним лише за умови правильного підключення до системи заземлення.

Фільтрація ліній живлення обґрунтована тим, що електронне обладнання може створювати паразитні сигнали, які потрапляють у мережу електроживлення. Якщо така мережа виходить за межі контрольованої зони, вона може стати каналом витоку. Тому встановлення фільтрів живлення дозволяє обмежити поширення небезпечних складових сигналу за межі приміщення.

Правильне заземлення є необхідною умовою роботи екранування і фільтрації. За відсутності якісного заземлення екрани кабелів або корпусів можуть не зменшувати рівень випромінювання, а в окремих випадках навіть створювати додаткові контури наведення. Тому у проєктованій системі заземлення розглядається не як допоміжний елемент, а як обов’язкова складова електромагнітного захисту.

Рознесення силових та інформаційних кабелів обрано для зниження взаємного впливу ліній. Якщо кабелі живлення і передачі даних прокладені поруч, між ними можуть виникати електромагнітні наведення. Через це інформаційні сигнали можуть частково потрапляти в інші лінії або створювати додаткове випромінювання. Роздільне прокладання таких кабелів дозволяє зменшити цей ризик ще на етапі побудови інфраструктури.

Окремо обґрунтовується використання організаційних заходів. Навіть за наявності технічних засобів захисту ризик витоку може залишатися високим, якщо сторонні особи мають доступ до приміщення, якщо не контролюється використання мобільних пристроїв або якщо конфіденційні переговори проводяться без попередньої перевірки умов. Тому регламент доступу, контроль сторонніх технічних засобів, перевірка приміщення та періодичний огляд системи є необхідними елементами захисту.

У таблиці 2.6 наведено узагальнене обґрунтування вибраних засобів захисту.

Таблиця 2.6 – Обґрунтування вибраних засобів захисту

Канал витоку	Основна загроза	Обраний засіб захисту	Обґрунтування вибору
Повітряний акустичний	Прослуховування розмов за межами приміщення	Звукоізоляція, ущільнення дверей і вікон	Зменшують рівень мовного сигналу за межами контрольованої зони
Повітряний акустичний	Відновлення залишкового мовного сигналу	Генератор акустичного шуму	Знижує розбірливість мовлення і ускладнює запис
Вентиляційний акустичний	Поширення звуку через повітропроводи	Акустичні вставки, шумоглушники	Блокують пряме проходження мовного сигналу
Віброакус-тичний	Зчитування коливань скла, стін, труб	Демпфування, віброізоляція	Зменшують амплітуду механічних коливань
Віброакус-тичний	Відновлення мовлення з конструкцій	Віброшумові завади	Маскують корисні коливання шумовим сигналом
Електромаг-нітний	Перехоплення побічних випромінювань	Екранування обладнання і кабелів	Знижує рівень електромагнітного поля за межами обладнання
Електричний	Витік через мережу живлення	Фільтри живлення	Обмежують поширення паразитних сигналів
Електромаг-нітний / електричний	Наведення між кабелями	Рознесення кабельних трас	Зменшує взаємний вплив силових та інформаційних ліній
Організа-ційний	Використання сторонніх пристроїв	Контроль доступу і перевірка приміщення	Знижує ризик прихованого запису або технічного перехоплення
Аналітичний	Складність оцінювання рівня ризику	Допоміжний програмний модуль	Дозволяє оцінювати ризик і формувати рекомендації

Допоміжний програмний модуль також має своє обґрунтування. Він не замінює технічні засоби захисту, однак дозволяє систематизувати процес оцінювання ризику. За допомогою такого модуля можна вводити параметри приміщення, враховувати наявність або відсутність засобів захисту, отримувати попередню оцінку ризику та формувати рекомендації. Це робить систему зручнішою для навчального дослідження і пояснення прийнятих рішень.

Запропонований набір засобів є взаємодоповнювальним. Акустичні заходи знижують поширення мовної інформації через повітря, віброакустичні - обмежують передавання механічних коливань, електромагнітні - зменшують рівень побічних випромінювань і наводок, а організаційні заходи знижують ризики, пов’язані з людським фактором. Саме поєднання цих рішень дозволяє розглядати запропоновану систему як комплексну систему захисту інформації від витоку технічними каналами.

2.7 Висновки

У другому розділі було виконано проєктування системи захисту інформації для службового приміщення, у якому можуть проводитися переговори, оброблятися службові дані та використовуватися комп’ютерна техніка.

Було визначено об’єкт захисту, основні джерела небезпечних сигналів і модель загроз, що враховує акустичні, віброакустичні, електромагнітні та електричні канали витоку.

Для акустичного захисту було запропоновано звукоізоляцію, ущільнення дверей і вікон, захист вентиляційних каналів та використання акустичного маскування. Для віброакустичного захисту передбачено демпфування конструкцій, віброізоляцію інженерних комунікацій і застосування віброшумових завад. Для електромагнітного захисту обґрунтовано використання екранованих кабелів, фільтрів живлення, заземлення, рознесення кабельних трас

і правильне розміщення обладнання.

За результатами виконаних робіт отримано такі результати.

1. Сформовано модель загроз. Як об’єкт захисту визначено службове приміщення (контрольовану зону), в якому обробляється конфіденційна інформація технічними засобами та ведуться усні переговори.

2. Систематизовано основні загрози та шляхи витоку даних, які розподілено на чотири ключові групи: акустичні, віброакустичні, електромагнітні та електричні.

3. Спроєктовано підсистему акустичного та віброакустичного захисту, обґрунтовано інженерні рішення для перекриття повітряних каналів витоку мовної інформації (через ущільнення дверей, вікон, встановлення шумоглушників у вентиляції) та конструкційних шляхів поширення вібрацій (через демпфування стін, перекриттів і трубопроводів). Додатково передбачено використання генераторів акустичного шуму та віброшумових перетворювачів із використанням базового блоку МАРС ТЗО-4-2.

4. Розроблено підсистему електромагнітного захисту, з метою мінімізації ризиків перехоплення побічних електромагнітних випромінювань та наводок (ПЕМВН) запропоновано комплекс заходів, що включає екранування технічних засобів і кабельних ліній, встановлення мережевих фільтрів живлення, рознесення трас силових та інформаційних кабелів, а також організацію надійного заземлення.

5. Обґрунтовано комплексну структуру системи, сформовано загальну структурну схему системи. Доведено, що максимальний рівень безпеки досягається лише за умови узгодженої взаємодії технічних підсистем, суворого організаційного контролю (регламентація доступу, обмеження сторонніх пристроїв) та застосування допоміжного програмного модуля для аналітичного оцінювання залишкових ризиків.

Запропоновані рішення дозволяють перекривати основні канали витоку інформації та створюють основу для подальшої розробки апаратної частини, схем блокування каналів і алгоритму оцінювання рівня захищеності.

3 РОЗРОБКА СИСТЕМИ ДОСЛІДЖЕННЯ ТА ОЦІНЮВАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

3.1 Апаратура та складові проєктованої системи

Для реалізації системи захисту інформації від витоку акустичними, віброакустичними та електромагнітними каналами необхідно визначити склад апаратури, яка безпосередньо впливає на відповідні канали витоку. У цьому розділі апаратна частина розглядається як основна складова захисту, а програмний модуль - як допоміжний інструмент для оцінювання ризику, фіксації результатів і візуалізації стану системи [6; 7].

Апаратна частина системи повинна забезпечувати активне акустичне та віброакустичне маскування мовної інформації, послаблення побічних електромагнітних випромінювань, захист кабельної інфраструктури та обмеження поширення небезпечних сигналів за межі контрольованої зони. Тому склад системи формується не як випадковий набір пристроїв, а як сукупність засобів, кожен з яких пов’язаний із конкретним каналом витоку.

До складу проєктованої системи включено такі елементи: генератор шумових сигналів, акустичні випромінювачі, вібраційні випромінювачі для скла, вібраційні випромінювачі для будівельних конструкцій, засоби екранування, фільтри електроживлення, елементи заземлення, екрановані кабелі та допоміжний комп’ютер із програмним модулем. Такий склад відповідає задачі перекриття акустичних, віброакустичних, електромагнітних та електричних шляхів витоку.

Центральним апаратним елементом акустичної та віброакустичної підсистем є генератор шумових сигналів. Як базовий приклад у роботі розглянуто генератор шумових завадових сигналів типу МАРС-ТЗО-4-2, який використовується для активного захисту мовної інформації від витоку акустичними та віброакустичними каналами [21; 22].

Генератор шумових сигналів формує завадовий сигнал, який подається на акустичні або вібраційні випромінювачі. Його призначення полягає не в

усуненні джерела мовлення, а в маскуванні корисного мовного сигналу. У результаті засоби перехоплення отримують суміш мовлення з шумовою завадою, що ускладнює подальше відновлення змісту розмови. Зовнішній вигляд генератора шумових сигналів МАРС-ТЗО-4-2 наведено на рисунку 3.1.

Рисунок 3.1 – Генератор шумових сигналів МАРС-ТЗО-4-2 [22]

Для блокування повітряних акустичних каналів у системі передбачаються акустичні випромінювачі або захищені акустичні колонки. Їх призначення полягає у створенні шумового поля в мовному частотному діапазоні. Такі випромінювачі доцільно розміщувати не біля джерела мовлення, а біля потенційних напрямів витоку: дверей, вікон, вентиляційних решіток, тонких перегородок або інших слабких місць акустичного захисту [23; 31].

Як приклад апаратної реалізації розглянуто акустичні захищені колонки МАРС-АКЗ. Вони можуть працювати разом із генератором шумових сигналів і призначені для зниження розбірливості мовної інформації за межами контрольованої зони [23]. Приклад акустичної захищеної колонки МАРС-АКЗ показано на рисунку 3.2.

Рисунок 3.2 – Акустична захищена колонка МАРС-АКЗ [23]

Для захисту віконного скла від віброакустичного витоку застосовуються вібраційні випромінювачі спеціального призначення. Віконне скло є небезпечним елементом приміщення, оскільки під дією мовного сигналу воно може працювати як тонка мембрана. Його коливання можуть бути зчитані ззовні, тому на скляні поверхні доцільно встановлювати окремі вібраційні випромінювачі, які передають на скло шумову вібраційну заваду [24; 25].

Прикладом такого пристрою є МАРС-ВИЗ, призначений для встановлення на віконні конструкції. Його використання дозволяє маскувати мікроколивання скла, що виникають під впливом мовлення всередині приміщення. У структурі системи цей пристрій доцільно розміщувати на тих вікнах, які виходять у неконтрольовану або частково контрольовану зону [25]. Зовнішній вигляд вібровипромінювача для захисту віконного скла наведено на рисунку 3.3.

Рисунок 3.3 – Вібраційний випромінювач МАРС-ВИЗ
для захисту віконного скла [25]

Для захисту стін, дверей, підлоги, стелі, труб опалення, меблів та інших твердих конструкцій застосовуються вібраційні випромінювачі універсального типу. Їх призначення полягає у створенні механічних шумових коливань у конструкціях, які потенційно можуть передавати мовну інформацію за межі приміщення. Такі випромінювачі доповнюють звукоізоляцію, оскільки впливають саме на вібраційний шлях поширення інформації [26].

Як приклад може бути використаний вібраційний випромінювач TRN-2000. Його можна встановлювати на стіни, перекриття, труби системи опалення, дверні полотна або інші тверді поверхні. Залежно від місця встановлення можуть застосовуватися різні типи кріплення: настінне, трубне або для легких перегородок і меблів [30]. Приклад універсального вібраційного випромінювача наведено на рисунку 3.4.

Рисунок 3.4 – Вібраційний випромінювач TRN-2000 [30]

Для електромагнітного захисту системи передбачаються засоби екранування. До них належать екрановані корпуси, металеві шафи для мережевого обладнання, екрановані кабель-канали та захисні екрани для ділянок, де розміщене обладнання з підвищеним рівнем електромагнітних випромінювань. Екранування зменшує рівень побічного електромагнітного поля, яке може поширюватися за межі контрольованої зони [16; 20].

У межах проєктованої системи екранування доцільно застосовувати для мережевого обладнання, кабельних трас і технічних засобів обробки інформації. Особливо це стосується ділянок, де інформаційні кабелі проходять поблизу

зовнішніх стін, дверей або інших меж контрольованої зони.

Наступним елементом системи є екрановані кабелі. Їх використання необхідне для зменшення електромагнітного випромінювання кабельних ліній та зниження впливу зовнішніх наводок. Неекрановані кабелі можуть працювати як випромінювачі або приймачі побічних сигналів, тому в захищеному приміщенні доцільно застосовувати екрановані інформаційні лінії [16; 20]. Приклад екранованого кабелю для захисту інформаційних ліній показано на рисунку 3.5.

Рисунок 3.5 – Екранований кабель для захисту інформаційних ліній

Екрановані кабелі повинні використовуватися разом із правильним заземленням. Якщо екран кабелю не має якісного електричного з'єднання із системою заземлення, його ефективність може суттєво знижуватися. Тому кабельна частина системи має проєктуватися разом із підсистемою заземлення.

Для обмеження витоку через мережу електроживлення у системі передбачаються фільтри живлення. Під час роботи електронного обладнання в лініях живлення можуть виникати паразитні сигнали, які здатні поширюватися за межі контрольованої зони. Фільтр живлення використовується для зменшення високочастотних складових таких сигналів та обмеження їх проходження через електромережу [16; 20].

Фільтри доцільно встановлювати на вводі живлення до захищеного

приміщення або перед групою технічних засобів, що обробляють важливу інформацію. Це дозволяє зменшити ризик поширення небезпечних сигналів через електричну інфраструктуру будівлі.

Підсистема заземлення є обов'язковою складовою електромагнітного захисту. Вона забезпечує правильну роботу екранів, фільтрів живлення та корпусів обладнання. Неправильно виконане або відсутнє заземлення може знизити ефективність захисту і створити додаткові шляхи поширення небезпечних сигналів. Узагальнений склад апаратури проєктованої системи наведено в таблиці 3.1.

Таблиця 3.1 – Складові апаратної частини проєктованої системи

Складова системи	Призначення	Канал витоку, на який впливає
Генератор шумових сигналів	Формування акустичних і віброакустичних завад	Акустичний, віброакустичний
Акустичні захищені колонки	Створення шумового поля у приміщенні	Акустичний
Вібровипромінювач для скла	Маскування коливань віконного скла	Віброакустичний
Вібровипромінювач для конструкцій	Маскування коливань стін, дверей, труб, меблів	Віброакустичний
Засоби екранування	Зменшення рівня побічних електромагнітних випромінювань	Електромагнітний
Екрановані кабелі	Обмеження випромінювання та наведень у кабельних лініях	Електромагнітний, електричний
Фільтри живлення	Обмеження поширення паразитних сигналів через електромережу	Електричний
Підсистема заземлення	Забезпечення роботи екранів і фільтрів	Електромагнітний, електричний

Апаратна частина проєктованої системи охоплює засоби активного захисту мовної інформації, елементи віброакустичного маскування, засоби електромагнітного захисту та допоміжну обчислювальну складову. Такий склад дозволяє досліджувати та перекривати основні канали витоку інформації.

3.2 Схеми блокування каналів витоку інформації

Після визначення складу апаратури проєктованої системи необхідно розробити схеми блокування основних каналів витоку інформації. Такі схеми показують не тільки перелік засобів захисту, а й місця їх розміщення, напрям дії та зв’язок із конкретними каналами витоку. У підрозділі окремо розглянуто блокування акустичного, віброакустичного та електромагнітного каналів.

Схеми блокування будуються для умовного службового приміщення, у якому проводяться переговори, використовується комп’ютерна техніка, є двері, вікно, вентиляційний канал, кабельні лінії живлення та передавання даних. Саме ці елементи є типовими джерелами або шляхами поширення небезпечних сигналів, тому вони відображаються на схемах.

Першою розглядається схема блокування акустичних каналів витоку інформації (рисунок 3.6). Основна загроза в цьому випадку полягає у поширенні мовного сигналу через повітряне середовище за межі контрольованої зони. Найбільш небезпечними напрямами є двері, вікна, вентиляційні канали, щілини у конструкціях та тонкі перегородки [11; 23].

На схемі акустичного блокування доцільно показати генератор шуму, акустичні випромінювачі, межу контрольованої зони та напрями можливого поширення мовної інформації. Акустичні випромінювачі розміщуються біля потенційних напрямів витоку: дверей, вікна, вентиляційної решітки та тонких перегородок. Таке розміщення дозволяє маскувати мовний сигнал саме в місцях його можливого виходу за межі приміщення.

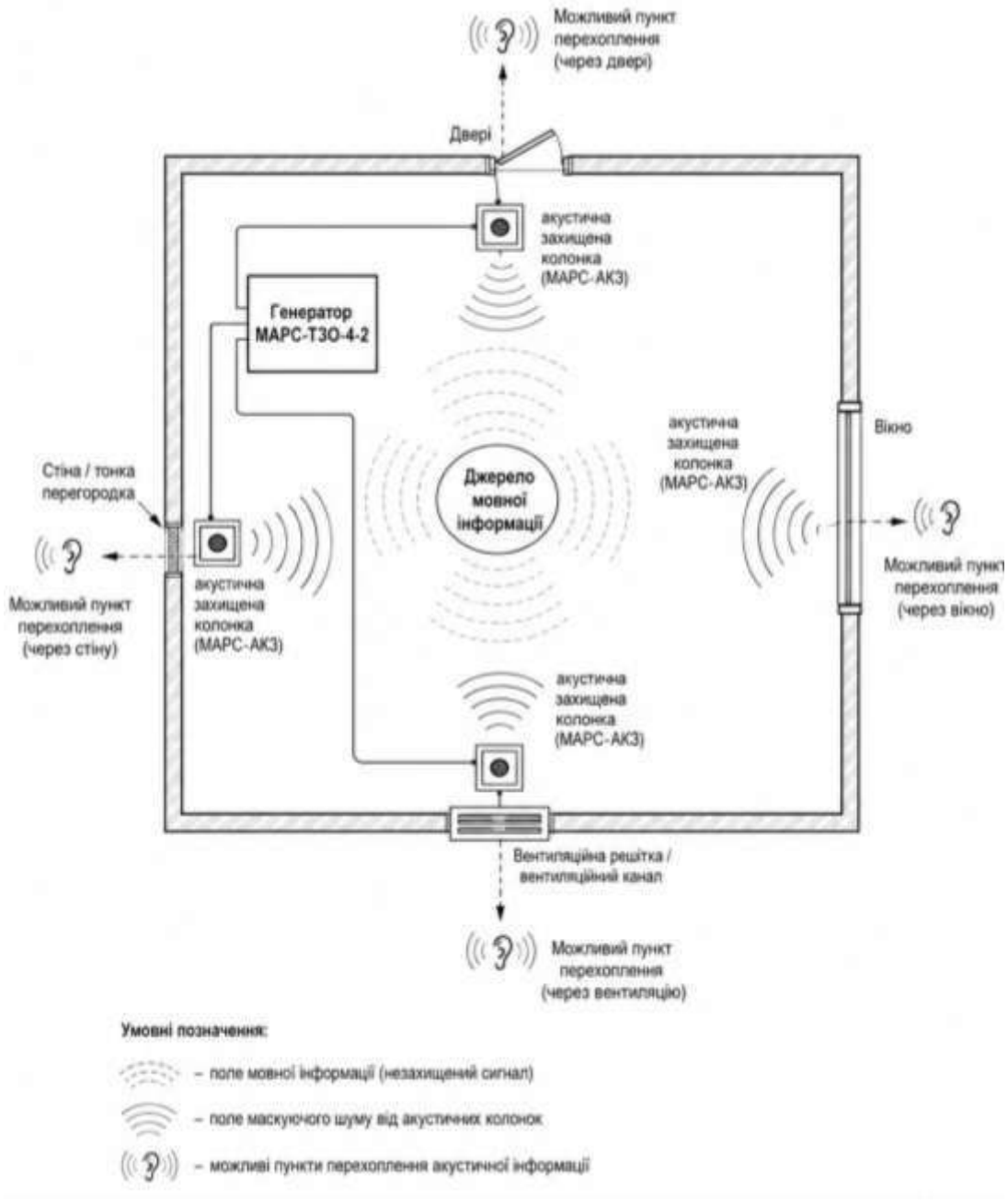


Рисунок 3.6 – Схема блокування акустичних каналів витоку інформації

Для підвищення ефективності акустичного блокування активні технічні засоби мають доповнюватися пасивними заходами. До них належать ущільнення дверей, використання щільних віконних конструкцій, застосування акустичних вставок у вентиляційних каналах та додаткове оздоблення поверхонь звукопоглинальними матеріалами. Генератор шуму в цьому випадку виконує роль активного засобу, а звукоізоляційні елементи зменшують рівень самого мовного сигналу.

Другою є схема блокування віброакустичних каналів витоку інформації (рисунок 3.7). Віброакустичний канал є складнішим, оскільки мовна інформація передається не тільки через повітря, а й через механічні коливання твердих конструкцій. До таких конструкцій належать віконне скло, дверне полотно, стіни, підлога, стеля, труби опалення, вентиляційні елементи та меблі [12; 25; 26].

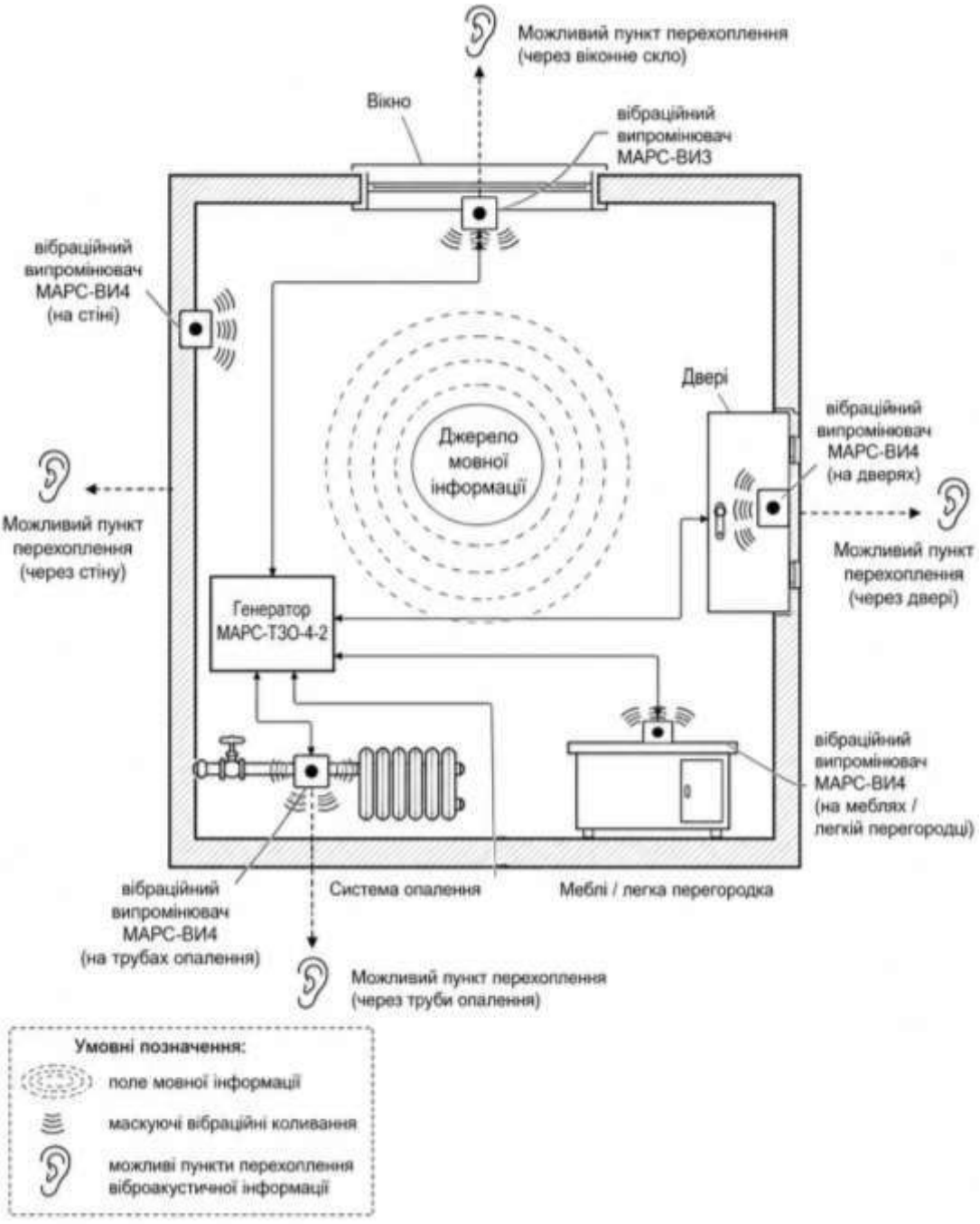


Рисунок 3.7 – Схема блокування віброакустичних каналів витоку інформації

Для блокування віброакустичного каналу використовуються вібровипромінювачі, які передають шумові коливання на потенційно небезпечні конструкції. На віконне скло доцільно встановлювати окремий вібровипромінювач для скляних поверхонь. На стіни, двері, труби опалення, підлогу або меблі можуть встановлюватися універсальні вібраційні випромінювачі з відповідними типами кріплення. Їхнє завдання полягає у створенні механічної завади, яка маскує корисні мовні коливання.

Особливу увагу на схемі варто приділити трубам опалення та віконному склу. Ці елементи можуть стати шляхом зчитування мовної інформації: скло коливається під дією звукового тиску, а труби опалення здатні передавати механічні коливання на значну відстань. Тому їх блокування є обов'язковим елементом системи віброакустичного захисту.

Третьою є схема блокування електромагнітних каналів витоку інформації (рисунок 3.8). У цьому випадку основними джерелами небезпечних сигналів є комп'ютери, монітори, мережеве обладнання, периферійні пристрої, кабельні лінії та електроживлення. Побічні електромагнітні випромінювання можуть поширюватися у просторі, а паразитні сигнали можуть виходити за межі контрольованої зони через кабелі або мережу живлення [16; 20].

Електромагнітний захист має проєктуватися не лише навколо окремого комп'ютера, а навколо всієї технічної інфраструктури приміщення. На схемі доцільно показати розміщення обладнання відносно меж контрольованої зони, напрям поширення побічних сигналів, екрановані кабелі, фільтри живлення, заземлення та точки можливого перехоплення.

Схема електромагнітного блокування пояснює, що захист повинен охоплювати не тільки самі технічні засоби, а й кабельні траси. Навіть якщо обладнання має прийнятні характеристики, неправильно прокладені кабелі або відсутність фільтрації живлення можуть створити додатковий канал витоку. Саме тому в системі передбачаються екранування, фільтрація, рознесення кабелів і контроль заземлення [33; 34].

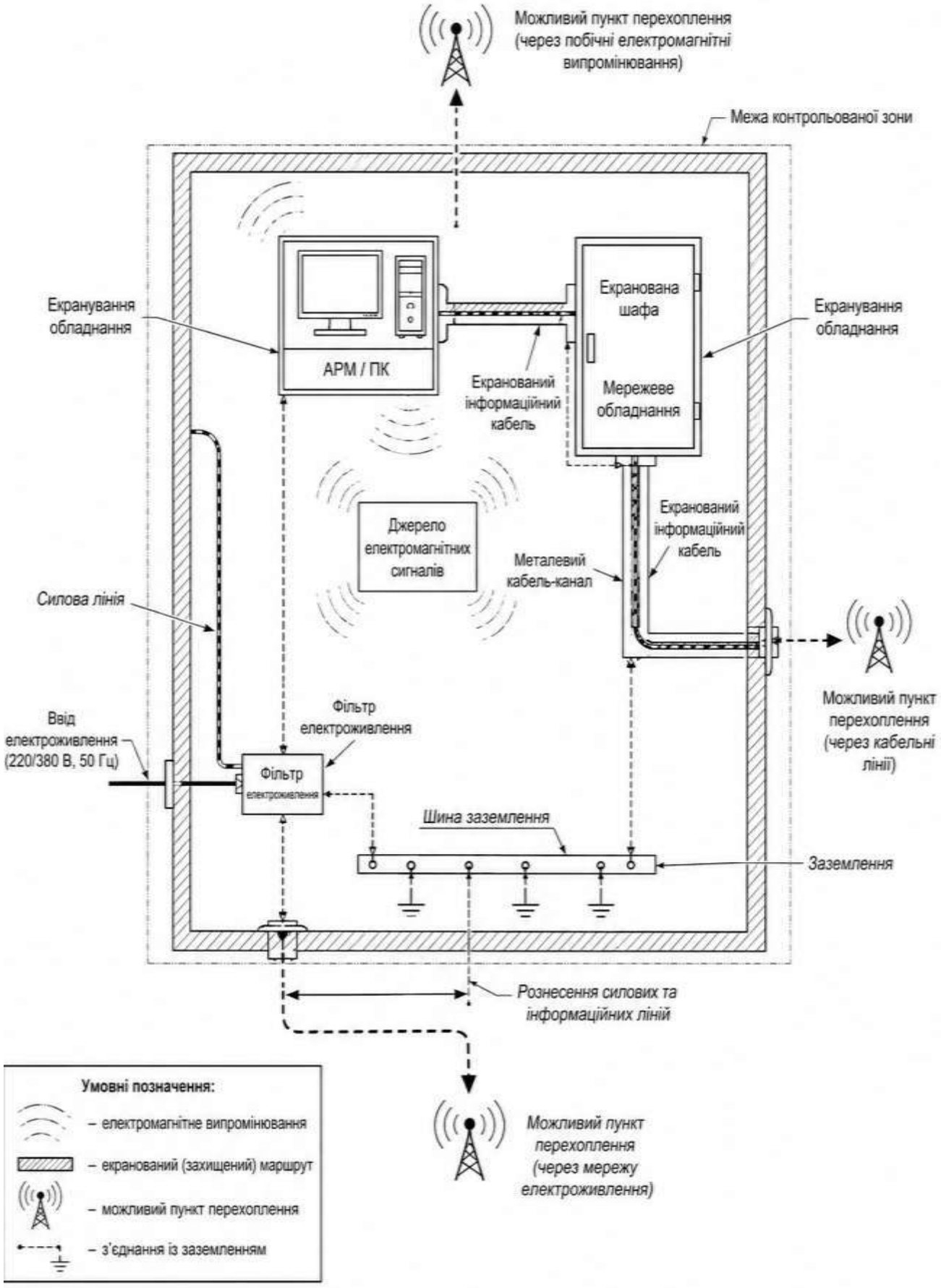


Рисунок 3.8 – Схема блокування електромагнітних каналів витоку інформації

Для більш наочного узагальнення відповідність каналів витоку, небезпечних елементів і засобів їх блокування зведено до таблиці 3.2.

Таблиця 3.2 – Відповідність каналів витоку та засобів їх блокування

Канал витоку	Небезпечний елемент	Засіб блокування	Місце застосування
Повітряний акустичний	Двері, вікна, вентиляція, щілини	Акустичні випромінювачі, звукоізоляція, ущільнення	Периметр приміщення
Віброакустичний через скло	Віконне скло	Вібровипромінювач для скла, демпфування	Віконна конструкція
Віброакустичний через конструкції	Стіни, двері, підлога, стеля	Вібровипромінювачі, демпфувальні матеріали	Тверді конструкції приміщення
Віброакустичний через комунікації	Труби опалення, вентиляційні елементи	Віброізоляція, віброшумове маскування	Інженерні комунікації
Електромагнітний	Комп’ютери, монітори, мережеве обладнання	Екранування, віддалення від меж контрольованої зони	Робоча зона
Електричний / кабельний	Лінії живлення, інформаційні кабелі	Фільтри живлення, екрановані кабелі, заземлення	Кабельна інфраструктура

Розроблені схеми блокування показують, як саме проєктована система впливає на кожен тип каналу витоку. Для акустичного каналу основна увага приділяється маскуванню мовлення та зменшенню його поширення через повітря. Для віброакустичного каналу важливим є створення шумових

механічних коливань у конструкціях. Для електромагнітного каналу головними є екранування, фільтрація, заземлення , правильна організація кабельних трас [19].

3.3 Розробка алгоритму оцінювання та підбору засобів захисту

Після визначення апаратної частини та схем блокування необхідно описати алгоритм оцінювання рівня захищеності інформації. У межах цієї роботи алгоритм розглядається як послідовність дій, яка дозволяє на основі характеристик приміщення, каналів витоку та наявних засобів захисту визначити орієнтовний рівень ризику [6; 19].

Алгоритм оцінювання не замінює спеціальних вимірювань рівня акустичного, віброакустичного чи електромагнітного сигналу. Його призначення полягає у попередньому аналізі стану захищеності та визначенні слабких місць у системі. У реальних умовах для остаточного підтвердження рівня захищеності потрібні вимірювальні роботи, але для проєктної частини достатньо формалізувати порядок оцінювання на основі обраних факторів ризику [6; 20].

Основою алгоритму є бальна модель. Кожному фактору, який підвищує ризик витоку, надається певна кількість балів. Кожному захисному заходу, навпаки, надається значення, яке зменшує підсумковий ризик. Після цього отриманий результат нормалізується до шкали від 0 до 100 %. Така шкала є зручною для подальшого відображення результатів у програмному модулі та для порівняння різних сценаріїв [19].

Загальна логіка алгоритму складається з кількох етапів. Спочатку користувач або виконавець аналізу визначає тип каналу витоку: акустичний, віброакустичний або електромагнітний. Далі вводяться параметри приміщення або технічного середовища. Після цього алгоритм перевіряє повноту та коректність даних. Якщо частина параметрів відсутня, оцінювання не виконується, оскільки результат буде неточним.

Після перевірки вхідних даних визначається базовий рівень ризику для

обраного типу каналу. Для акустичного каналу базовий ризик пов’язаний із поширенням мовної інформації повітрям. Для віброакустичного каналу він формується через можливість передавання коливань конструкціями. Для електромагнітного каналу базовий ризик визначається наявністю технічних засобів, кабельних ліній і ліній живлення, які можуть створювати побічні випромінювання або наведення.

Далі алгоритм аналізує фактори, які збільшують ризик. Для акустичного каналу такими факторами є тонкі стіни, неущільнені двері, вентиляційні канали, вікна без додаткового захисту, мала відстань до потенційної точки перехоплення та низький рівень фонового шуму.

Для віброакустичного каналу ризик підвищують великі скляні поверхні, труби опалення, жорстко закріплені конструкції та відсутність демпфування.

Для електромагнітного каналу ризик підвищують неекрановані кабелі, відсутність фільтрації живлення, неякісне заземлення та розміщення обладнання біля меж контрольованої зони.

На наступному етапі враховуються засоби захисту. Якщо в приміщенні застосовано звукоізоляцію, ущільнення дверей, акустичне маскування або захист вентиляційних каналів, ризик акустичного витоку зменшується. Якщо використано демпфування конструкцій, віброізоляційні вставки або віброшумові перетворювачі, зменшується ризик віброакустичного витоку.

Після розрахунку числового значення алгоритм визначає якісний рівень ризику. Для цього використовується три рівні: низький, середній та високий. Такий поділ зручний для практичного використання, оскільки користувач бачить не тільки відсоткове значення, а й зрозумілий висновок щодо стану захищеності.

Результат поділяється на три діапазони. Якщо значення ризику становить від 0 до 30 %, рівень вважається низьким. Якщо значення знаходиться в межах від 31 до 70 %, рівень вважається середнім. Якщо результат перевищує 70 %, ризик визначається як високий. Інтерпретацію отриманого значення ризику наведено в таблиці 3.3.

Таблиця 3.3 – Інтерпретація рівня ризику витоку інформації

Значення ризику	Рівень ризику	Характеристика стану захищеності
0–30 %	Низький	Основні канали витоку перекриті,
31–70 %	Середній	Частина каналів витоку залишається небезпечною,
71–100 %	Високий	Існує значна ймовірність витоку,

Після визначення рівня ризику алгоритм переходить до формування рекомендацій.

Рекомендації залежать від того, які саме фактори підвищили ризик:

– якщо високий ризик виник через вентиляційний канал, система повинна рекомендувати встановлення шумоглушників або акустичних вставок;

– якщо ризик пов’язаний із віконним склом, доцільно рекомендувати демпфування скла, застосування важких штор або віброшумових перетворювачів;

– якщо причиною є неекрановані кабелі, рекомендацією буде використання екранованих ліній, правильне рознесення трас і перевірка заземлення.

Таким чином, алгоритм пов’язує виявлені фактори ризику з конкретними засобами захисту і не зводиться лише до математичного розрахунку. Алгоритм приведенний в додатку А.

Запропонований алгоритм дозволяє перейти від загального опису системи захисту до формалізованого оцінювання її стану. Його перевагою є проста логіка та можливість реалізації у вигляді програмного модуля.

У подальшому цей алгоритм може бути розширений шляхом уточнення вагових коефіцієнтів, додавання нових факторів ризику та використання результатів реальних вимірювань.

3.4 Реалізація програмної візуалізації результатів роботи системи

Після розроблення апаратної частини системи, схем блокування каналів витоку та алгоритму оцінювання рівня захищеності доцільно реалізувати допоміжну програмну частину. Її основне призначення полягає не у безпосередньому технічному захисті інформації, а у зручному поданні результатів роботи алгоритму, фіксації перевірок, відображенні рівня ризику та формуванні рекомендацій щодо посилення захисту.

Програмний модуль у межах даної системи виконує роль інструмента візуалізації та підтримки прийняття рішень. Він дозволяє користувачу послідовно ввести параметри приміщення, обрати тип каналу витоку, запустити алгоритм оцінювання, отримати результат у відсотковому вигляді та побачити перелік рекомендованих засобів захисту. Тому наведені нижче рисунки демонструють не окремий вебсайт, а етапи роботи допоміжного модуля в складі системи захисту.

Важливо підкреслити, що програмна частина не замінює апаратні засоби захисту, такі як генератор шумових сигналів, акустичні випромінювачі, вібровипромінювачі, фільтри живлення, екрановані кабелі або підсистема заземлення. Її функція полягає в систематизації даних про стан захисту, спрощенні аналізу та поданні результатів у зрозумілій для користувача формі.

Для реалізації програмної частини використовується веб-інтерфейс, оскільки такий формат є зручним для демонстрації, роботи з формами введення та перегляду результатів. Користувачу не потрібно встановлювати окреме спеціалізоване програмне забезпечення: достатньо відкрити сторінку програмного модуля, заповнити необхідні поля та отримати результат аналізу.

Структурно програмний модуль складається з клієнтської частини, серверної частини та бази даних. Клієнтська частина відповідає за відображення інтерфейсу, форм введення, результатів аналізу, журналу перевірок і графічних елементів. Серверна частина обробляє введені дані, виконує алгоритм оцінювання, формує рекомендації та передає результат назад користувачу. База

даних використовується для збереження історії перевірок і подальшого формування статистики. Серверну частину доцільно реалізувати на основі Node.js [38] з використанням Express [39], а для передавання даних між клієнтом і сервером - Axios [37].

Для реалізації клієнтської частини доцільно використати React [32]. Ця технологія дозволяє створити інтерфейс у вигляді окремих компонентів: головної сторінки, форми аналізу акустичного каналу, форми аналізу віброакустичного каналу, форми аналізу електромагнітного каналу, сторінки результату, журналу перевірок і сторінки статистики. Для створення клієнтського проєкту та запуску середовища розробки використовується Vite [35]. Для оформлення сторінок застосовується Bootstrap 5 [36]. Загальний вигляд головної сторінки програмного модуля наведено на рисунку 3.9.

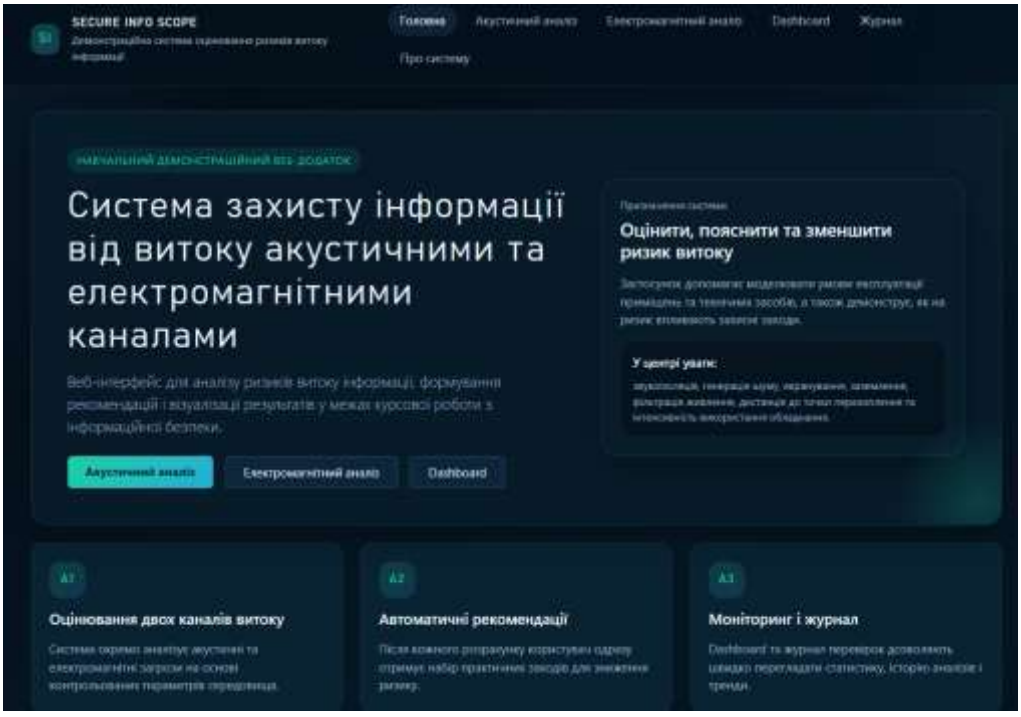


Рисунок 3.9 – Головна сторінка програмного модуля візуалізації результатів

На головній сторінці програмного модуля розміщується короткий опис призначення системи, основні типи каналів витоку та кнопки переходу до відповідних режимів оцінювання. Користувач одразу бачить, що модуль призначений для аналізу системи захисту інформації, а не є самостійним

технічним засобом блокування каналів. Передбачено три основні напрями аналізу: акустичний, віброакустичний та електромагнітний.

Для введення параметрів акустичного каналу створюється окрема форма. У ній користувач зазначає наявність дверей, вікон, вентиляційного каналу, рівень звукоізоляції, наявність генератора шуму, акустичних випромінювачів та інших засобів захисту. Ці параметри відповідають факторам, які були визначені під час проєктування акустичного захисту. Приклад форми введення параметрів акустичного каналу наведено на рисунку 3.10.

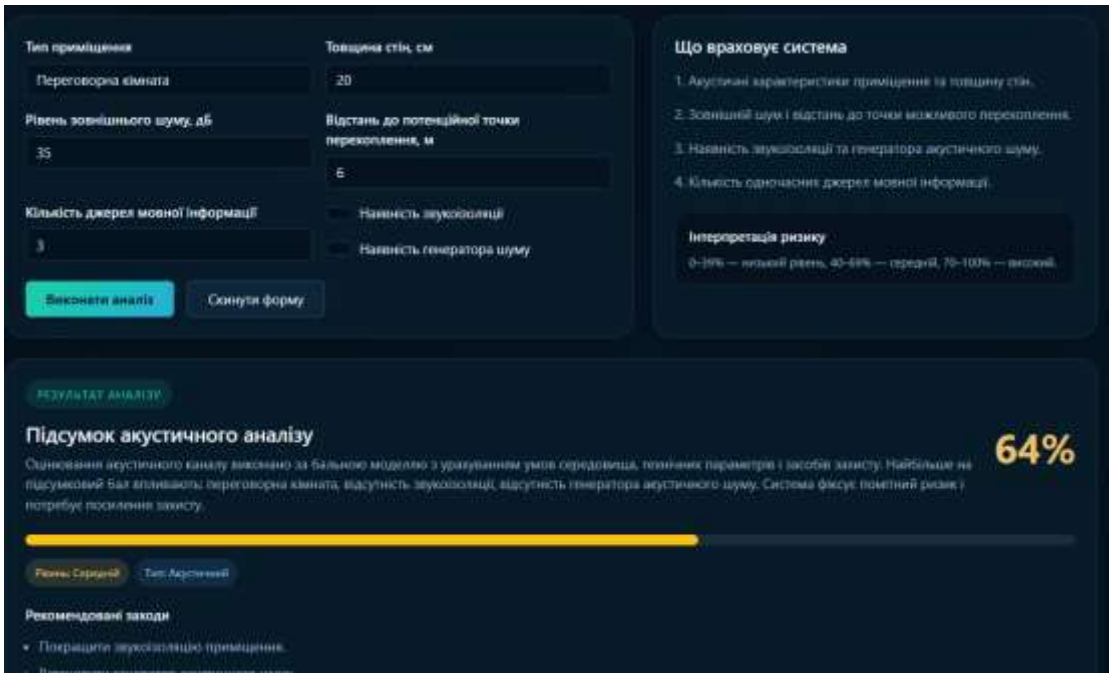


Рисунок 3.10 – Форма введення параметрів акустичного каналу витоку

Для віброакустичного каналу передбачається окрема форма, у якій враховуються конструктивні елементи приміщення. До таких елементів належать віконне скло, стіни, підлога, стеля, двері, труби опалення, вентиляційні елементи та меблі. Також користувач зазначає, чи застосовуються вібровипромінювачі, демпфувальні матеріали або віброізоляційні вставки. Приклад форми введення параметрів віброакустичного каналу наведено на рисунку 3.11.

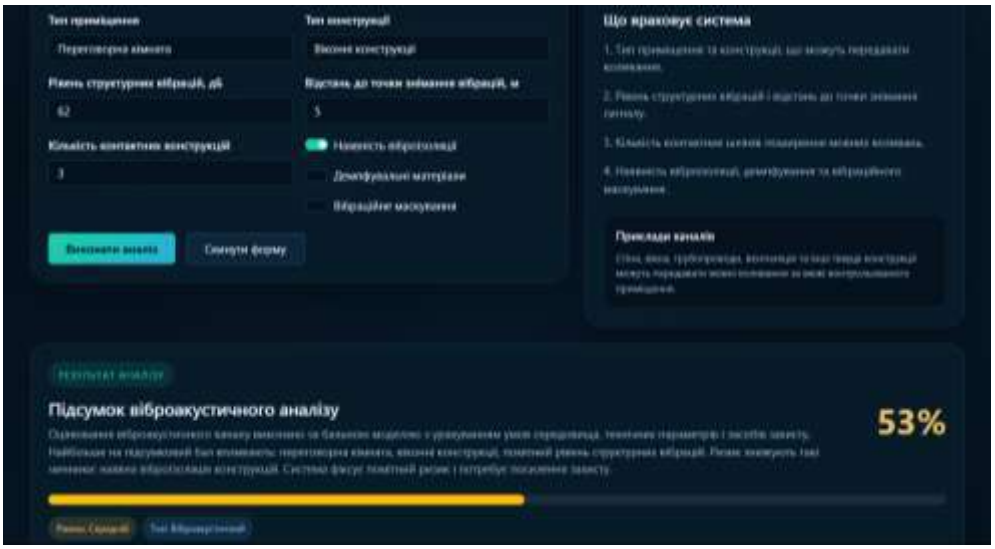


Рисунок 3.11 – Форма введення параметрів віброакустичного каналу

Для електромагнітного каналу форма введення містить параметри, пов’язані з технічним обладнанням і кабельною інфраструктурою. Користувач зазначає кількість технічних засобів, тип кабелів, наявність екранування, фільтрації живлення, заземлення, рознесення кабельних трас і контроль сторонніх електронних пристроїв. На основі цих даних алгоритм визначає ризик витоку через побічні електромагнітні випромінювання, наведення та лінії живлення. Приклад форми введення параметрів електромагнітного каналу наведено на рисунку 3.12.

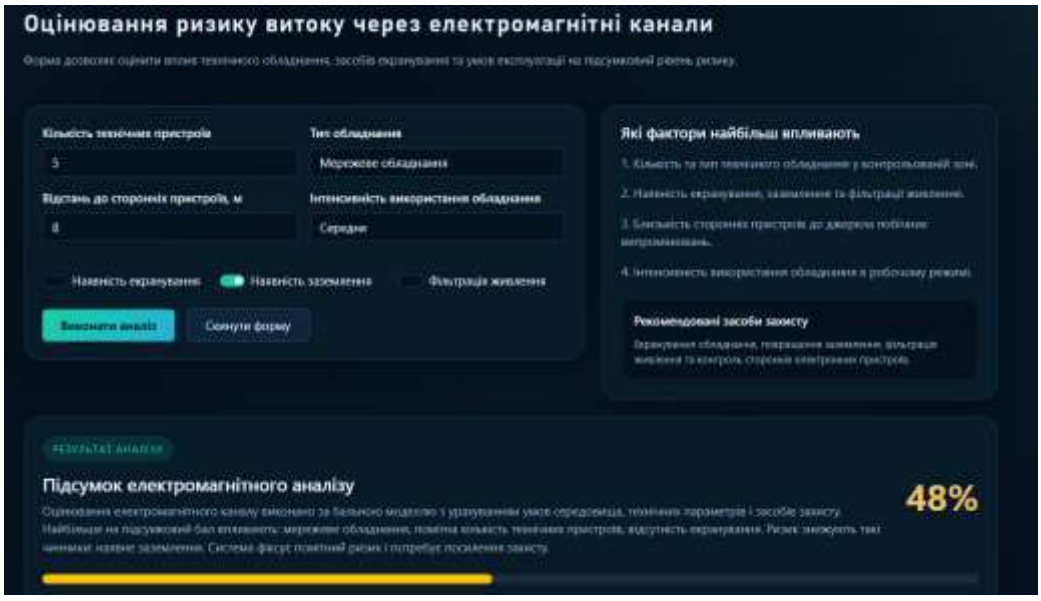


Рисунок 3.12 – Форма введення параметрів електромагнітного каналу витоку

Після заповнення форми користувач запускає оцінювання. Серверна частина отримує введені дані, перевіряє їх коректність, визначає базовий ризик, додає бали за небезпечні фактори, віднімає бали за наявні засоби захисту та формує підсумковий результат. Результат подається у вигляді відсоткового значення, текстового рівня ризику та переліку рекомендацій. Приклад відображення результату оцінювання рівня ризику наведено на рисунку 3.13.

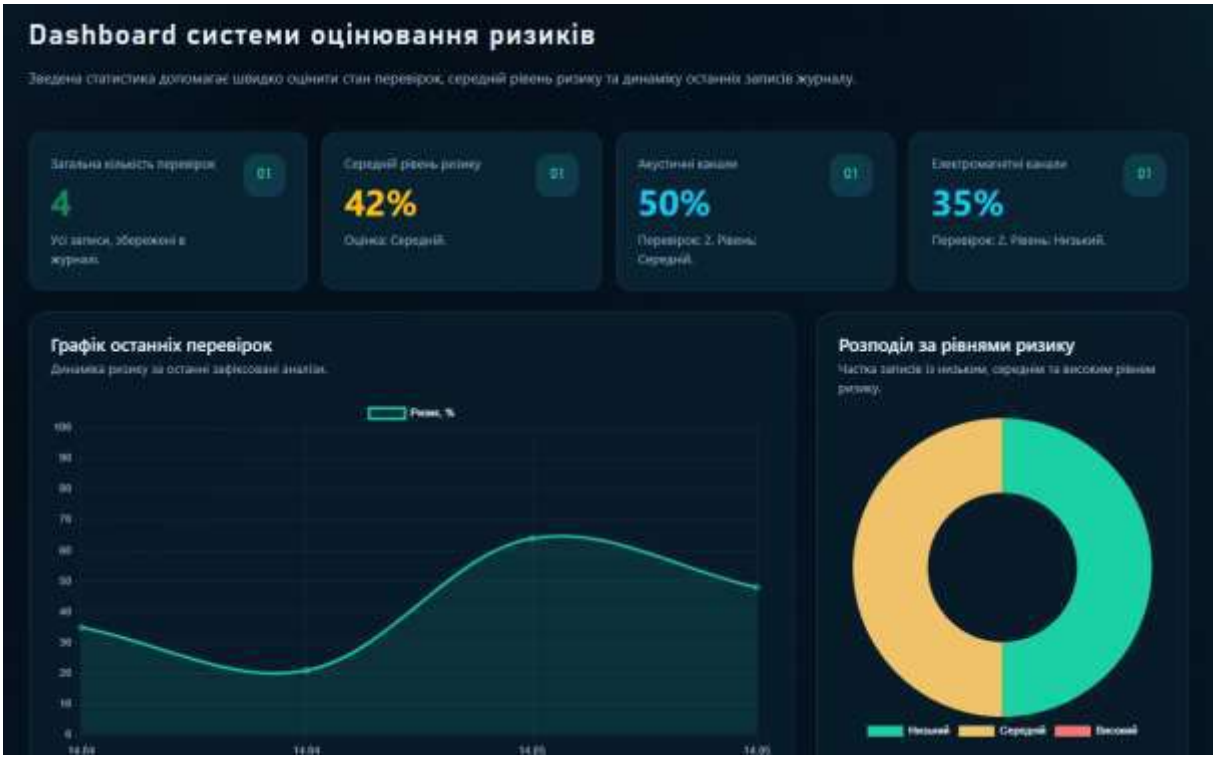


Рисунок 3.13 – Відображення результату оцінювання рівня ризику

На сторінці результату відображаються тип проаналізованого каналу, відсотковий рівень ризику, якісний рівень ризику, перелік факторів, які найбільше вплинули на результат, а також рекомендації щодо посилення захисту. Наприклад, якщо високий ризик сформувався через вентиляційний канал, система рекомендує акустичні вставки або шумоглушники. Якщо ризик пов’язаний із неекранованими кабелями, система рекомендує використання екранованих кабелів і перевірку заземлення.

Для збереження результатів використовується база даних. У ній зберігаються тип каналу, введені параметри, підсумковий ризик, рівень ризику,

сформовані рекомендації та дата проведення аналізу. Це дозволяє створити журнал перевірок, за допомогою якого можна переглядати попередні результати та порівнювати різні варіанти стану захисту.

Базу даних доцільно реалізувати на PostgreSQL [40], а для роботи з нею використовувати Prisma [41]. Приклад журналу результатів оцінювання наведено на рисунку 3.14.

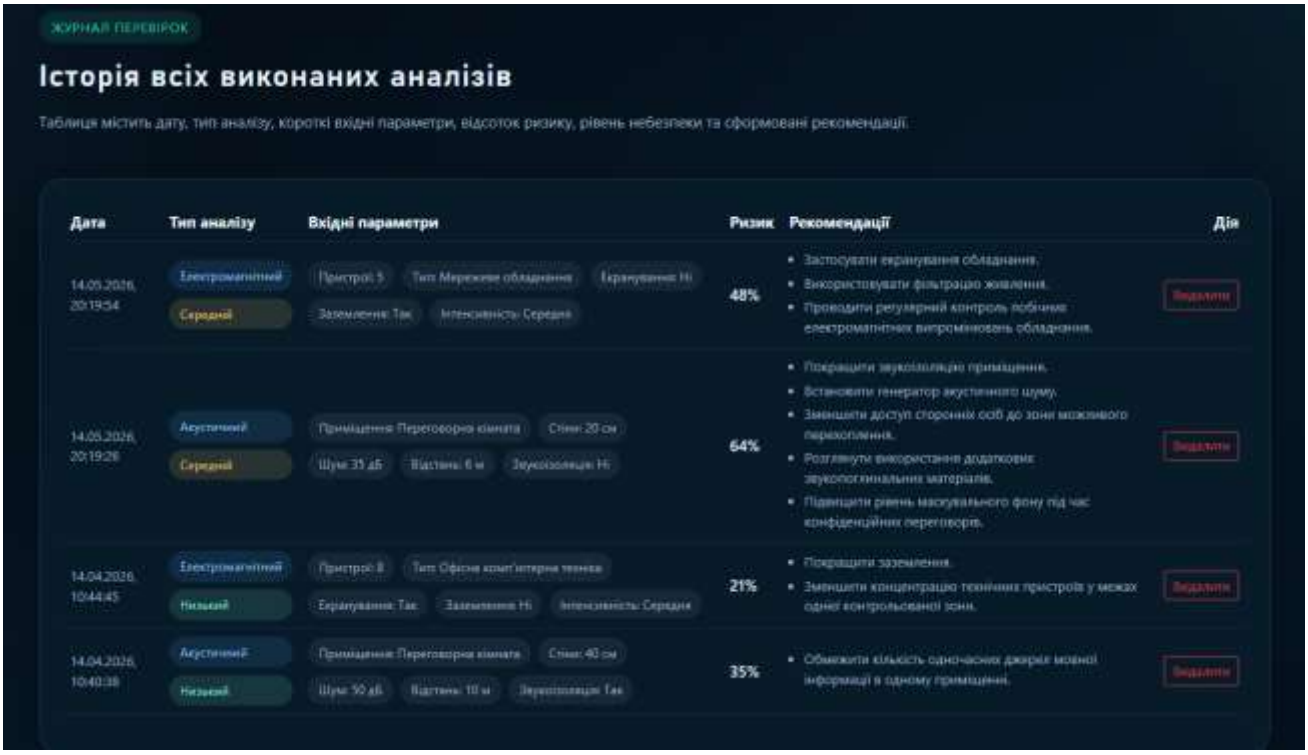


Рисунок 3.14 – Журнал результатів оцінювання системи захисту

Журнал перевірок має важливе значення для дослідження системи. Він дозволяє не просто один раз отримати результат, а відстежувати зміни після додавання нових засобів захисту. Наприклад, спочатку можна виконати оцінювання приміщення без генератора шуму, вібровипромінювачів або екранованих кабелів, а потім повторити оцінювання після додавання цих засобів і порівняти зміну рівня ризику.

Для графічного подання статистики може застосовуватися Chart.js [42].

3.5 Висновки

У третьому розділі було розроблено систему дослідження та оцінювання захисту інформації від витоку технічними каналами. Основну увагу приділено апаратним засобам, схемам блокування каналів витоку, алгоритму оцінювання ризику та програмній візуалізації результатів.

Було визначено склад апаратної частини проєктованої системи. До неї віднесено генератор шумових сигналів, акустичні випромінювачі, вібровипромінювачі для захисту скла та будівельних конструкцій, засоби електромагнітного захисту, екрановані кабелі, фільтри живлення, елементи заземлення та допоміжний комп’ютер для роботи програмного модуля.

Окремо було розглянуто схеми блокування акустичних, віброакустичних та електромагнітних каналів витоку інформації. У схемах показано, які елементи приміщення є потенційно небезпечними, де доцільно розміщувати засоби захисту і як ці засоби знижують ризик перехоплення інформації.

Було розроблено алгоритм оцінювання та підбору засобів захисту. Алгоритм передбачає вибір типу каналу витоку, введення параметрів приміщення та обладнання, перевірку коректності даних, визначення базового ризику, урахування небезпечних факторів, урахування наявних захисних заходів, розрахунок підсумкового рівня ризику та формування рекомендацій.

Допоміжний програмний модуль розглянуто як інструмент візуалізації результатів роботи системи. Він не виконує фізичного блокування каналів витоку, але забезпечує введення параметрів, запуск алгоритму, відображення рівня ризику, збереження результатів перевірок і формування рекомендацій.

У результаті виконання третього розділу сформовано завершену структуру проєктованої системи: апаратні засоби блокування каналів витоку, схеми їх розміщення, алгоритм оцінювання ризику та програмна візуалізація результатів. Програмна частина подана саме як допоміжний інструмент дослідження й оцінювання, а не як самостійна система захисту.

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто питання розробки системи захисту інформації від витоку акустичними, віброакустичними та електромагнітними каналами. Актуальність цієї теми обумовлена тим, що конфіденційна інформація може бути втрачена не лише через програмні атаки або несанкціонований доступ до інформаційних систем, а й через фізичні процеси, які супроводжують мовлення людини, роботу технічного обладнання, кабельних ліній та інженерних комунікацій. Саме тому захист інформації повинен враховувати не тільки програмні засоби безпеки, а й технічні канали витоку.

У першому розділі було проаналізовано основні поняття технічного захисту інформації та розглянуто класифікацію технічних каналів витоку. Було встановлено, що для службового приміщення найбільш характерними є акустичні, віброакустичні, електромагнітні та електричні канали. Акустичний канал пов’язаний із поширенням мовної інформації через повітряне середовище, двері, вікна, вентиляцію та нещільності конструкцій. Віброакустичний канал виникає тоді, коли мовна інформація передається через механічні коливання скла, стін, труб, перекриттів або меблів. Електромагнітний канал формується внаслідок побічних електромагнітних випромінювань і наводок, що виникають під час роботи комп’ютерної техніки, мережевого обладнання та кабельної інфраструктури.

Також у першому розділі було визначено основні загрози та фактори, які впливають на рівень захищеності інформації. До таких факторів належать конструктивні особливості приміщення, наявність вентиляційних каналів, тип дверей і вікон, розміщення технічних засобів, якість кабельної інфраструктури, наявність екранування, заземлення, фільтрації живлення та організаційного контролю. Проведений аналіз показав, що технічні канали витоку мають різну фізичну природу, тому їх неможливо ефективно перекрити одним універсальним засобом.

У другому розділі було виконано проєктування системи захисту інформації для службового приміщення. Було визначено об’єкт захисту, сформовано модель загроз і описано можливі шляхи реалізації витоку інформації. Система захисту була побудована як комплекс взаємопов’язаних підсистем: акустичної, віброакустичної, електромагнітної, підсистеми захисту електроживлення та організаційного контролю.

Для захисту від акустичного витоку було запропоновано використовувати звукоізоляцію, ущільнення дверей і вікон, захист вентиляційних каналів та акустичне маскування. Для віброакустичного захисту було обґрунтовано застосування демпфувальних матеріалів, віброізоляційних вставок і вібровипромінювачів, які створюють маскувальні коливання на конструкціях приміщення. Для електромагнітного захисту було запропоновано використання екранованих кабелів, металевих кабель-каналів, фільтрів електроживлення, заземлення та раціонального розміщення обладнання в межах контрольованої зони.

У результаті проєктування було сформовано структурну схему системи захисту інформації, яка поєднує технічні та організаційні заходи. Було показано, що ефективність системи залежить не від окремого пристрою, а від узгодженого застосування всіх елементів. Якщо не врахувати хоча б один із каналів витоку, загальний рівень захищеності може залишатися недостатнім. Наприклад, акустичне маскування не усуває електромагнітний витік, а екранування кабелів не захищає від прослуховування через вентиляційний канал. Тому система повинна мати комплексний характер.

У третьому розділі було розроблено систему дослідження та оцінювання захисту інформації від витоку технічними каналами. Було визначено склад апаратної частини, до якої входять генератор шумових сигналів, акустичні випромінювачі, вібраційні випромінювачі, засоби екранування, екрановані кабелі, фільтри живлення, заземлення та допоміжний комп’ютер для роботи програмного модуля. Для кожного апаратного елемента було визначено призначення та канал витоку, на який він впливає.

Окрему увагу було приділено схемам блокування каналів витоку інформації. Було розроблено схеми блокування акустичних, віброакустичних та електромагнітних каналів. На цих схемах показано, які елементи приміщення можуть бути джерелами або шляхами витоку, де доцільно розміщувати засоби захисту та як саме вони перекривають потенційні канали. Це дозволило перейти від загального опису засобів захисту до конкретного інженерного подання системи.

Також було розроблено алгоритм оцінювання та підбору засобів захисту. Алгоритм передбачає вибір типу каналу витоку, введення параметрів приміщення і технічного середовища, перевірку коректності даних, визначення базового рівня ризику, урахування факторів, що підвищують ризик, урахування засобів захисту, розрахунок підсумкового ризику, його нормалізацію до шкали 0–100 %, визначення рівня ризику та формування рекомендацій. Такий алгоритм дозволяє не просто перелічити засоби захисту, а встановити зв’язок між виявленими загрозами, каналами витоку та конкретними заходами протидії.

Для зручного подання результатів роботи алгоритму було передбачено допоміжний програмний модуль з веб-інтерфейсом. Його роль полягає у введенні параметрів, запуску алгоритму, відображенні рівня ризику, формуванні рекомендацій, збереженні результатів перевірок та візуалізації статистики. Програмний модуль не є самостійною системою захисту інформації, оскільки не блокує канали витоку фізично. Його призначення полягає у підтримці аналізу та демонстрації результатів роботи спроєктованої системи.

Практичне значення роботи полягає в тому, що запропонована система може бути використана як основа для навчального або дослідного стенда з вивчення технічних каналів витоку інформації. Вона дозволяє досліджувати, яким чином мовна та технічна інформація може виходити за межі контрольованої зони, які засоби потрібні для її захисту та як змінюється рівень ризику після впровадження відповідних заходів. Система також може бути використана для попереднього аналізу службового приміщення перед вибором конкретних засобів технічного захисту.

У результаті виконання кваліфікаційної роботи було досягнуто поставленої мети - розроблено комплексну систему захисту інформації від витоку акустичними, віброакустичними та електромагнітними каналами. У роботі було проаналізовано канали витоку, визначено основні загрози, спроєктовано підсистеми захисту, обґрунтовано вибір апаратних засобів, розроблено схеми блокування каналів, запропоновано алгоритм оцінювання ризику та передбачено програмну візуалізацію результатів.

Запропонована система відповідає інженерному характеру кваліфікаційної роботи, оскільки основна увага приділена не створенню окремого вебсайту, а проєктуванню засобів і методів захисту інформації від технічних каналів витоку. Програмний модуль у цій системі виконує допоміжну роль і використовується для зручного аналізу, документування та подання результатів. Комплексне поєднання апаратних, інженерно-технічних, організаційних і програмних рішень дозволяє знизити ризик несанкціонованого отримання інформації та підвищити загальний рівень захищеності службового приміщення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.04.2026).

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 15.04.2026).

3. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.04.2026).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.04.2026).

5. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. URL: https://kubg.edu.ua/images/stories/podii/2017/06_21_posylannia/dstu_8302.pdf (дата звернення: 17.04.2026).

6. Іванченко С. О., Гавриленко О. В., Липський О. А., Шевцов А. С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації : навч. посіб. Київ : ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

7. Яцків В. В., Кулина С. В. Технічні засоби захисту інформації : опорний конспект лекцій. Тернопіль : ЗУНУ, 2023. 88 с.

8. Костенко В. О., Сметанін І. М. Методи і засоби захисту інформації. Частина 1 : конспект лекцій. Запоріжжя : НУ «Запорізька політехніка», 2019. 66с.

9. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. Вип. 2(13). С. 88–95. URL: https://ela.kpi.ua/server/api/core/bitstreams/fb3cf41e-273c-424e-aa24-1fddfc51943f/content (дата звернення: 19.04.2026).

10. Технічні канали витоку інформації. URL: https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html (дата звернення: 19.04.2026).

11. Захист мовної інформації. URL: https://tzi.com.ua/zaxist-movno-nformacz.html (дата звернення: 20.04.2026).

12. Засоби віброакустичного захисту інформації. URL: https://tzi.com.ua/zasobi_vbrazaxistu.html (дата звернення: 20.04.2026).

13. Роїк О. М., Міронова Ю. В., Волкотруб О. П. Захист інформації від витоку акустичними каналами. Інформаційні технології та комп'ютерна інженерія. 2015. № 1. С. 48–54. URL: https://itce.vntu.edu.ua/index.php/itce/article/view/175 (дата звернення: 21.04.2026).

14. Данілов В. В., Котенко А. М. Напрями захисту акустичної інформації на об'єкті інформаційної діяльності. Сучасний захист інформації. 2020. № 4(44). С. 18–22.

15. Kriuchkova L., Tsmokanych I. Overview of Methods of Protection of Acoustic Information Against Leaks by Channels Formed by High-Frequency Impositions. International Journal of Innovative Technologies in Social Science. 2021. № 3(31). URL: https://rspublisher.org/index.php/ijitss/article/view/2123 (дата звернення: 22.04.2026).

16. Sydorkin P., Nesterenko S., Salnyk S., Konotopets M., Kulynich O., Smolkov O. Methods and Techniques of Protecting Information from Leakage by Technical Channels via Side Electromagnetic Radiation. Political Science and Security Studies Journal. 2021. Vol. 2, No. 3. P. 15–25.

17. Oleynikov A., Bilotserkivets O., Shirokyi O. Modeling the Acoustic Channel of Voice Information Leakage. MC&FPGA-2023 : V International Scientific and Practical Conference, Kharkiv, 2023. P. 17–18.

18. Павленко Я. С. Спеціальні дослідження з виявлення акустоелектричних каналів витоку інформації. Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнар. молодіж. форуму, Харків, 2024. Т. 3. С. 401–402.

19. Humeniuk I., Kosterev D., Sheihas V. Method of Optimizing the Blocking Means Number of Acoustic Information Leakage Channels at Information Activity Object. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, no. 2. P. 289–296. URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/19241 (дата звернення: 24.04.2026).

20. Zabolotnyi V. I. Technical Channel of Information Leakage by Side Electromagnetic Radiation. Radioengineering. 2024. URL: https://rt.nure.ua/article/view/318794 (дата звернення: 24.04.2026).

21. Генератор шумових сигналів МАРС-ТЗО-4-2. URL: https://tzi.com.ua/mars-tzo42.html (дата звернення: 25.04.2026).

22. Генератор шумових сигналів МАРС-ТЗО-4-2. URL: https://tzi.ua/ua/generator_shumovih_signalv_mars-tzo-4-2 (дата звернення: 25.04.2026).

23. Колонка акустична захищена МАРС-АКЗ. URL: https://tzi.com.ua/mars-ak3.html (дата звернення: 26.04.2026).

24. Колонка акустична захищена «МАРС-АКЗ». URL: https://www.mapc.com.ua/img/files/2Spik.pdf (дата звернення: 26.04.2026).

25. Вібровипромінювач ВИ3 для захисту віконного скла. URL: https://tzi.com.ua/vi3.html (дата звернення: 27.04.2026).

26. Вібровипромінювач ВИ4 для стін, підлоги, стелі та системи опалення. URL: https://tzi.com.ua/vi4.html (дата звернення: 27.04.2026).

27. Генератор шуму iProTech DNG-2300. URL: https://lockers.com.ua/generator-shuma-dng-2300/ (дата звернення: 28.04.2026).

28. Мобільний генератор шуму iProTech MNG-300 Rabbler. URL: https://lockers.com.ua/mobilnij-generator-shuma-mng-300-rabbler/ (дата звернення: 28.04.2026).

29. Пригнічувач диктофонів комплект Plux NOISE 3S. URL: https://lockers.com.ua/podavitel-diktofonov-komplekt-plux-noise-3s/ (дата звернення: 29.04.2026).

30. Вібраційний випромінювач TRN-2000 для DNG-2300. URL: https://lockers.com.ua/vibratsionnyj-izluchatel-trn-2000-6652-05-trn-2000/ (дата звернення: 29.04.2026).

31. Акустичний випромінювач OMS-2000. URL: https://lockers.com.ua/akusticheskij-izluchatel-oms-2000-6650-05-oms-2000/ (дата звернення: 30.04.2026).

32. React. Documentation. URL: https://react.dev/ (дата звернення: 01.05.2026).

33. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О. та ін. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

34. Павленко Я. С. Спеціальні дослідження з виявлення акустоелектричних каналів витоку інформації / Я. С. Павленко ; наук. керівник проф. А. М. Олейніков // Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 3. С. 401–402.

35. Vite. Guide. URL: https://vite.dev/guide/ (дата звернення: 01.05.2026).

36. Get started with Bootstrap. URL: https://getbootstrap.com/docs/5.3/getting-started/introduction/ (дата звернення: 02.05.2026).

37. Axios. Documentation. URL: https://axios-http.com/docs/intro (дата звернення: 02.05.2026).

38. Node.js. About Node.js. URL: https://nodejs.org/en/about (дата звернення: 03.05.2026).

39. Express. Node.js Web Application Framework. URL: https://expressjs.com/ (дата звернення: 03.05.2026).

40. PostgreSQL Documentation. URL: https://www.postgresql.org/docs/ (дата звернення: 04.05.2026).

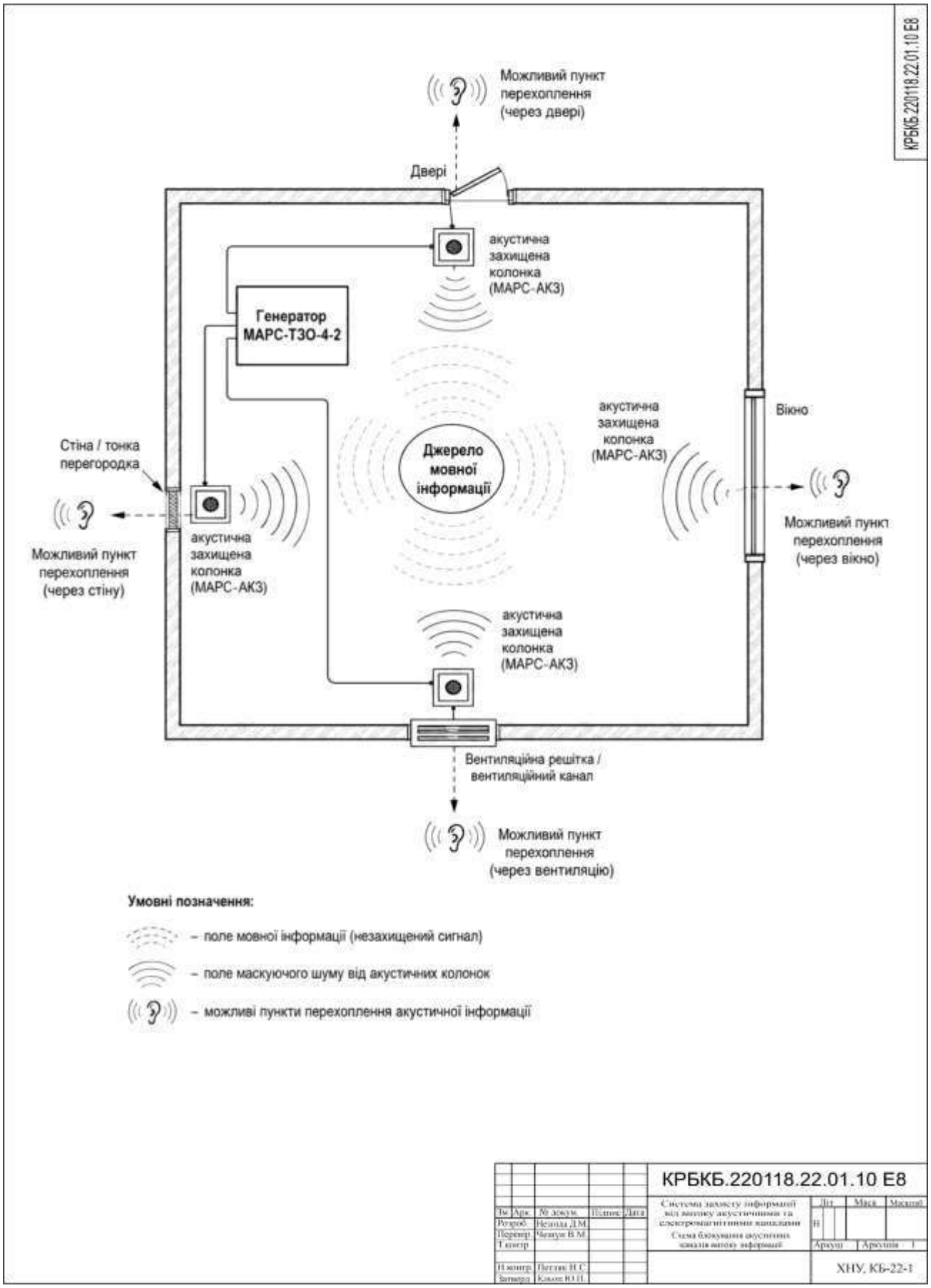
41. Prisma Documentation. URL: https://www.prisma.io/docs (дата звернення: 04.05.2026).

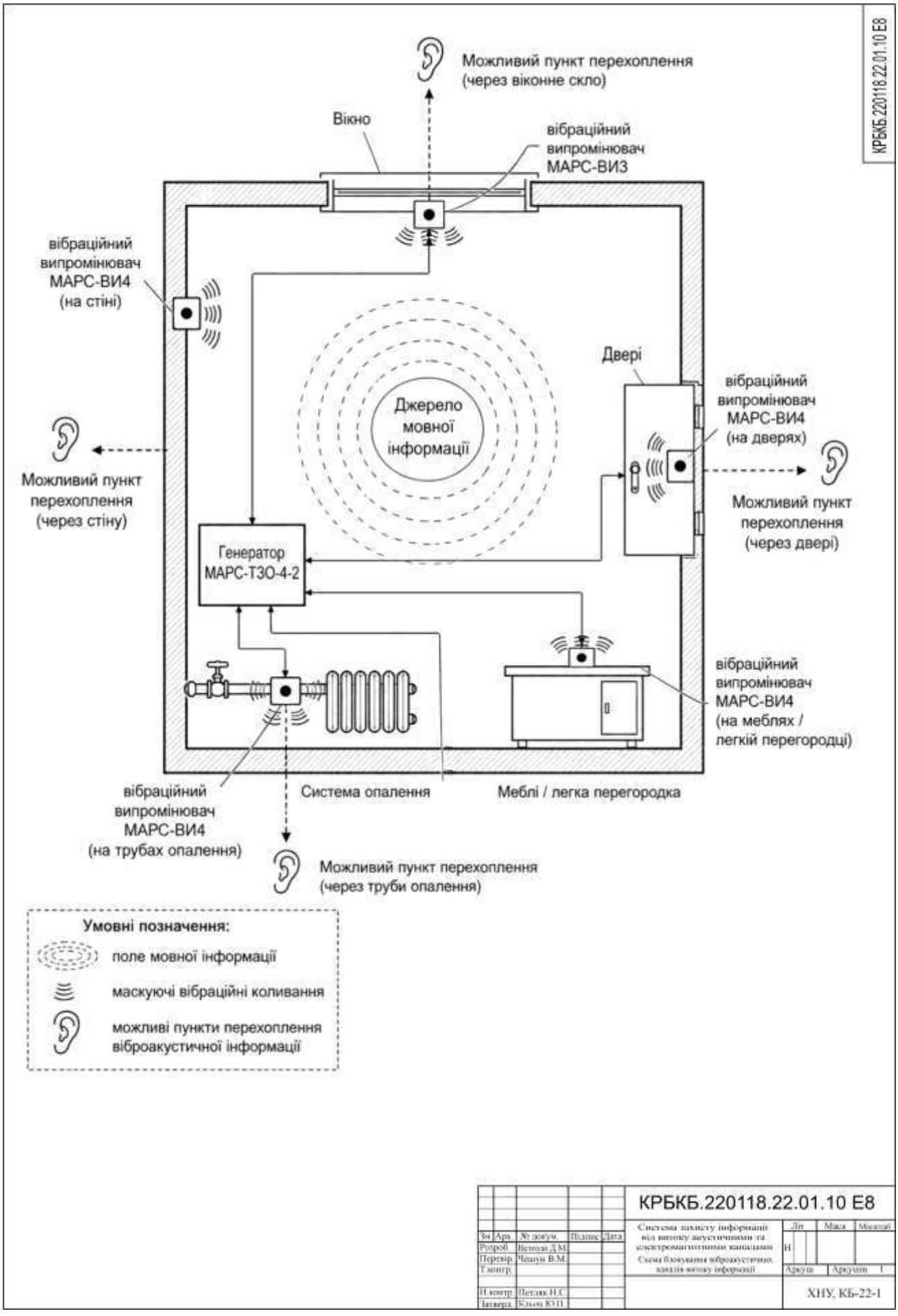
42. Chart.js Documentation. URL: https://www.chartjs.org/docs/latest/ (дата звернення: 05.05.2026).

Додаток А

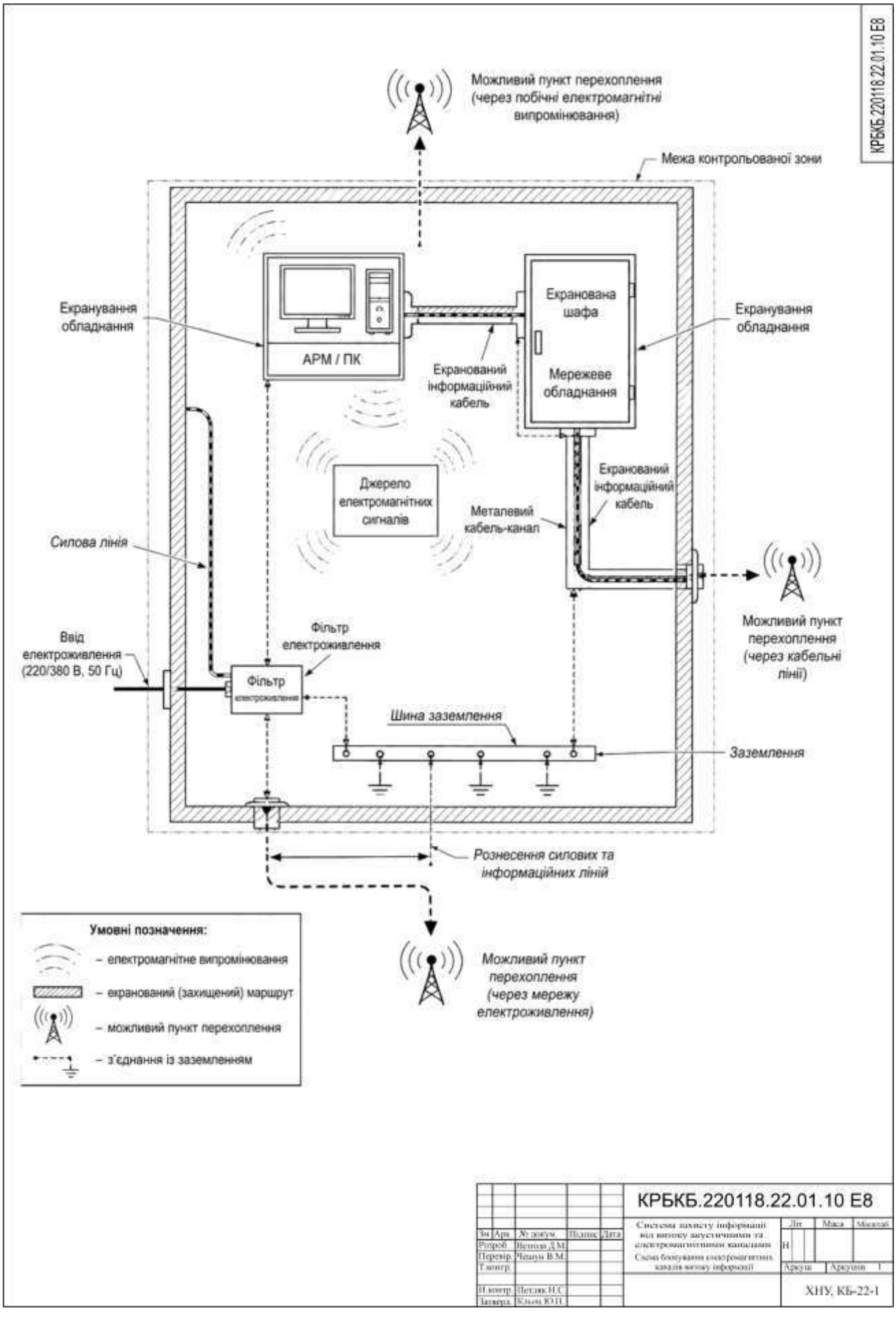
(обов’язковий)

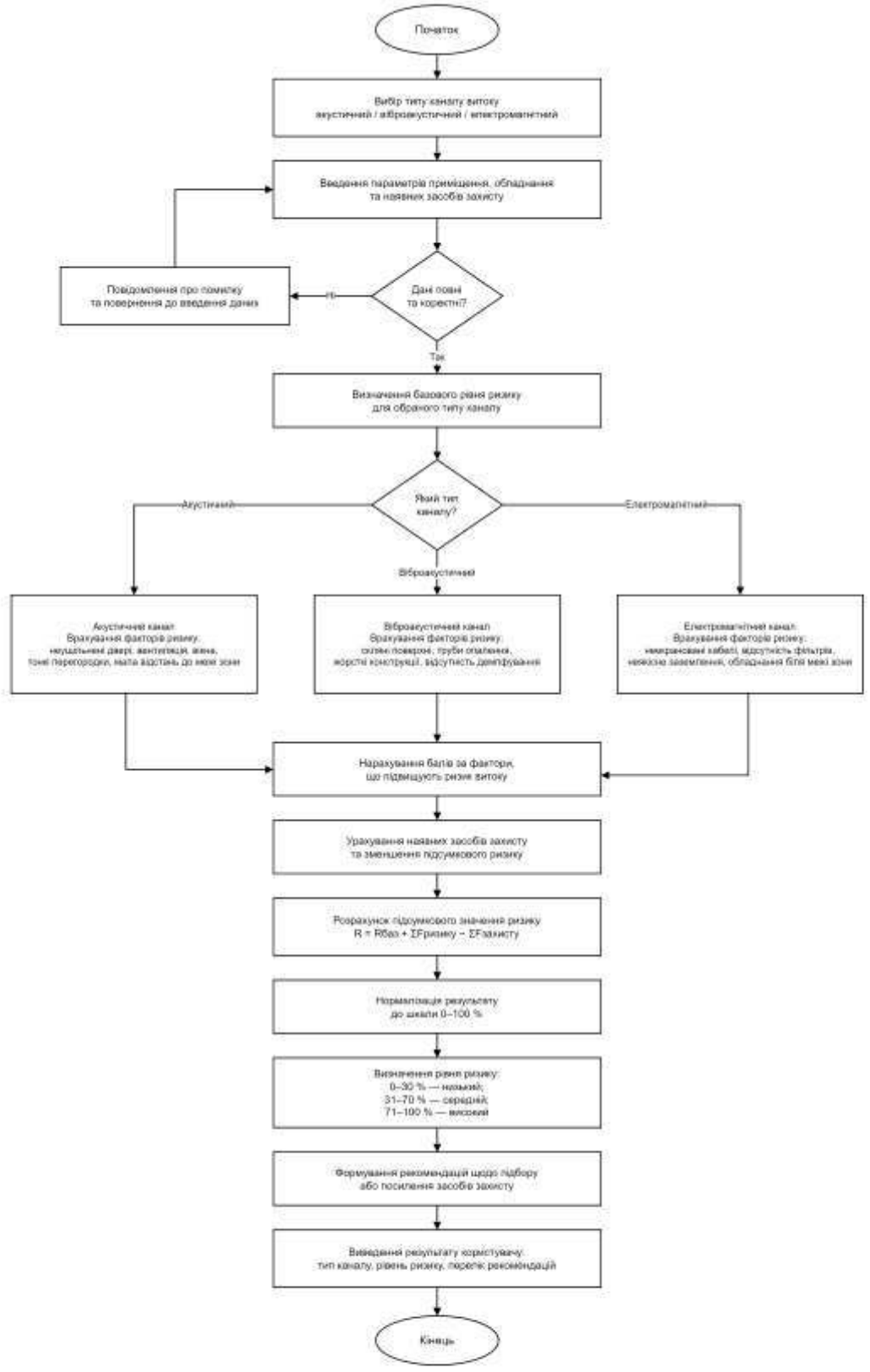
Копії графічної частини





					КРБКБ.220118.22.01.10 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інформації від витоку акустичними та електромагнітними каналами. Схема блокування віброакустичних каналів витоку інформації	Літ.	Маса	Масштаб
Розроб.		Негода Д.М.				Н		
Перевір.		Чешун В.М.						
Т.контр.						Аркуш	Аркушів	1
Н.контр.		Петлик Н.С.				ХНУ, КБ-22-1		
Затверд.		Кольо Ю.П.						


КРБКБ.220118.22.01.10 Е8
Можливий пункт перехоплення (через побічні електромагнітні випромінювання)
Межа контрольованої зони
Екранування обладнання
АРМ / ПК
Екранований інформаційний кабель
Екранована шафа
Мережеве обладнання
Екранування обладнання
Джерело електромагнітних сигналів
Металевий кабель-канал
Екранований інформаційний кабель
Силова лінія
Можливий пункт перехоплення (через кабельні лінії)
Ввід електроживлення (220/380 В, 50 Гц)
Фільтр електроживлення
Фільтр електроживлення
Шина заземлення
Заземлення
Рознесення силових та інформаційних ліній
Можливий пункт перехоплення (через мережу електроживлення)
Умовні позначення:
– електромагнітне випромінювання
– екранований (захищений) маршрут
– можливий пункт перехоплення
– з'єднання із заземленням
КРБКБ.220118.22.01.10 Е8
Система захисту інформації від витоку акустичними та електромагнітними каналами
Схема блокування електромагнітних каналів витоку інформації
Літ
Маса
Масштаб
Зм. Арк. № докум. Підпис Дата
Розроб. Нестуля Д.М.
Перевір. Чешун В.М.
Т.контр.
Н.контр. Петлик Н.С.
Затверд. Кільчик Ю.П.
Н
Аркуш
Аркушів 1
ХНУ, КБ-22-1



					КРБКБ.220118.22.01.10 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інформації від витоку акустичними та електромагнітними каналами	Літ.	Маса	Масштаб
Розроб.		Нестода Д.М.				Н		
Перевір.		Чешун В.М.			Алгоритм роботи	Аркуш	Аркушів	1
Т.контр.								
Н.контр.		Петлик Н.С.				ХНУ, КБ-22-1		
Затверд.		Клюєв Ю.П.						