Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Бакалаврська дипломна робота на тему:

«Система захисту приміщення від витоку інформації технічними каналами»

Виконав: студент 4 курсу групи 1БС-19 б
спеціальності 125 Кібербезпека
_____ Боднар І.І.

Керівник: к. т. н., доц. каф. ЗІ
_____ Дудатьєв А.В.
«19» червня 2023 р.

Рецензент: к. т. н., доц. каф. ПЗ
_____ Хошаба О.М.
«19» червня 2023 р

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінниця ВНТУ– 2023 року

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра захисту інформації

Рівень вищої освіти І (бакалаврський)

Галузь знань – 12 Інформаційні технології

Спеціальність – 125 Кібербезпека

Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗІ,

д. т. н., проф.

_____ В. А. Лужецький

«20» березня 2023 року

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ

студенту Боднару Іллі Івановичу

1. Тема роботи: «Система захисту приміщення від витоку інформації технічними каналами»

керівник роботи: Дудатьєв А.В., к. т. н., доц. каф. ЗІ.,
затверджені наказом ректора кафедри ЗІ від 20 березня 2023 року №67.

2. Строк подання студентом роботи 19 червня 2023 р.

3. Вихідні дані до роботи:
   - приміщення, де відбуваються конфіденційні перемовини;
   - методи захисту від витоку інформації ТКВІ;

4. Зміст текстової частини: Вступ. 1. Технічні канали витоку інформації. 2.Проектування апаратної реалізації пристрою. 3. Розробка та апаратна реалізація пристрою. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу:
Схема приміщення. Характеристика каналів витоку. Електрична принципова схема пристрою. Схема захищеного приміщення. Структурна схема системи захисту приміщення. Характеристика механізмів захисту, що складають систему.

6. Консультанти розділів роботи

Розділ	Прізвище , ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Дудатьєв А.В., к. т. н., доц. каф. ЗІ.	20.03.23	16.06.23
2	Дудатьєв А.В., к. т. н., доц. каф. ЗІ.	20.03.23	16.06.23
3	Дудатьєв А.В., к. т. н., доц. каф. ЗІ.	20.03.20	16.06.23

7. Дата видачі завдання 20.03.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	20.03.23 – 26.03.23	
2	Аналіз інформаційних джерел за напрямком бакалаврської дипломної роботи	27.03.23 – 09.04.23	
3	Розробка рішень, моделей, алгоритмів	10.04.23 – 23.04.23	
4	Практична реалізація, моделювання експериментування, результати	24.04.23 – 21.05.23	
5	Оформлення бакалаврської роботи	22.05.23 – 24.05.23	
6	Попередній захист БДР	25.05.23 – 31.05.23	
7	Виправлення зауважень, підготовка ілюстративного матеріалу	01.06.23 – 15.06.23	
8	Представлення БДР до захисту, рецензування	16.06.23 – 19.06.23	
9	Захист БДР	20.06.23 – 23.06.23	

Студент _____ Боднар І.І.

Керівник роботи _____ Дудатьєв А.В.

АНОТАЦІЯ

Бакалаврська дипломна робота складається з 55 сторінок формату А4, на яких є 9 рисунків, 11 таблиць, список використаних джерел містить 20 найменувань.

Бакалаврська робота присвячена розробці системи захисту від витоку інформації технічними каналами. Розглянуто об’єкти та технічні канали які можуть бути джерелом витоку інформації. Також розглянуто методи та засоби захисту інформації від витоку технічними каналами. Надано рекомендації щодо захисту інформації від перехоплення випромінювань технічних засобів – об’єктів інформаційної системи та сформовано основні рекомендаційні поради щодо розробки систем захисту. Проаналізовано приміщення що потребує захисту, розглянуто ймовірні загрози, які можуть виникнути на його території. В ході виконання роботи було представлено розробку засобу просторового зашумлення – генератор білого шуму.

Ключові слова: система захисту, канали витоку, перехоплення інформації, закладні пристрої, білий шум.

ABSTRACT

The bachelor's thesis consists of 55 pages of A4 format, on which have 9 pictures, 11 tables, the list of used sources contains 20 names

The bachelor's work is devoted to the development of a system of protection against information leakage through technical channels. Objects and technical channels that can be a source of information leakage are considered. Methods and means of protecting information from leakage through technical channels are also considered. Recommendations on protecting information from the interception of radiation of technical means - objects of the information system have been provided, and basic recommendations for the development of protection systems have been formed. The premises in need of protection were analyzed, possible threats that could arise on its territory were considered. In the course of the work, the development of a means of spatial noise was presented - a white noise generator

Key words: protection system, leakage channels, interception of information, embedded devices, white noise.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІзОД – інформація з обмеженим доступом;

ТКВІ – технічний канал витоку інформації;

ОІД – об’єкт інформаційної діяльності;

ОТЗС – основні технічні засоби та системи;

ДТЗС – допоміжні технічні засоби і системи;

ЗП – закладний пристрій;

ЗТР – засіб технічної розвідки;

ПНЧ – підсилювач низьких частот;

КЗ – контрольована зона

ТЗІ – технічний захист інформації;

ТЗПІ – технічні засоби прийому інформації;

ЕМС – електромагнітна сумісність;

ІТС – інформаційно-телекомунікаційна система;

АС – автоматизована система;

ПЕМВН – побічні електромагнітні випромінювання та наведення;

КСЗІ – комплексні системи захисту інформації.

ВСТУП

Зважаючи на широке поширення технічних засобів та зростаючу кількість даних, що перетинають мережі зв'язку, захист від витоку інформації є однією з найбільш актуальних проблем сьогодення. Дана проблема виникає, оскільки інформація може бути витіснена за допомогою технічних каналів, які дозволяють передавати інформацію під видом інших даних. Так, з розвитком інформаційних технологій та зростанням кількості цифрової інформації набуває особливої актуальності захист інформаційних ресурсів від несанкціонованого доступу, витоку або пошкодження. Це стосується як корпоративних інформаційних систем, так і приватної інформації, що зберігається на персональних пристроях.

Важливою частиною захисту інформаційних ресурсів є захист технічними каналами передачі інформації, які можуть стати метою атак хакерів або конкурентів. Українські науковці та інженери також працюють над розробкою ефективних методів захисту інформаційних ресурсів [1-5]. Наприклад, в Україні проводяться дослідження щодо захисту інформації від витоку за допомогою каналів звукової та вібраційної інформації, а також розробляються нові методи захисту від різних видів атак на інформаційні системи.

Наприклад, у Харківському національному університеті радіоелектроніки проводяться дослідження з проблем захисту інформації від різних видів атак на технічні канали передачі інформації. Також в Україні діє Національна академія наук України, де проводяться наукові дослідження з проблем кібербезпеки та захисту інформації.

Враховуючи це, розробка систем захисту приміщення від витоку інформації технічними каналами має велике значення в багатьох галузях, включаючи національну безпеку, захист комерційної та корпоративної інформації та приватності користувачів.

Згідно з дослідженням проведеного компанією Verizon у 2020 році [6], 70% кібератак на компанії мали місце через уразливості в цифрових системах, а більшість з них були пов'язані з технічними каналами. Зазначається, що компанії

недостатньо уважно ставляться до захисту технічних каналів, що може призвести до витоку конфіденційної інформації та порушення захисту персональних даних клієнтів.

Дана бакалаврська дипломна робота присвячена системі захисту приміщення від витоку інформації технічними каналами. Мета роботи полягає в підвищенні рівня захисту від зняття інформації технічними каналами витоку інформації та організації захисту в приміщенні що розглядається.

Для досягнення мети необхідно виконати такі задачі:

- провести порівняльний аналіз різних методів захисту інформації від витоку технічними каналами;
- дослідити ефективність наявних методів захисту ;
- розробка загальних вимог щодо захисту середовища в якому циркулює ІзОД;
- розробити та налаштувати генератор білого шуму, який забезпечуватиме ефективний захист інформації від зловмисних атак з використанням направлених мікрофонів.

Об'єктом у даній бакалаврській роботі є дослідження методів захисту приміщення інформації від витоку технічними каналами.

Предметом дослідження є система захисту для приміщення, в якому відбуваються конфіденційні перемовини.

Апробація. За результатами дослуджень було опублікована тизи на тему «витік технічними каналами витоку» на науково- технічній конференції факультету інформаційних технологій та комп’ютерної інженерії, Вінницького національно технічного університету [7].

1 ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

Обмін інформацією є невід'ємною частиною ділових процесів, безпека і захист конфіденційної інформації стають надзвичайно важливими завданнями. Однак, зростання технологічного розвитку і зростаюча залежність від інформаційних систем призводять до появи нових загроз, зокрема витоку інформації.

Під витоком інформації розуміється ситуація, при якій конфіденційна, таємна або службова інформація незаконно або несанкціоновано передається, виходить поза контроль або стає доступною для осіб, які не мають права на її отримання.

Витік інформації відбувається відповідним каналом витоку. Оскільки засоби розвідки противника, як правило технічні, то і канали витоку також називають технічними.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки(рис 1.1) [7].

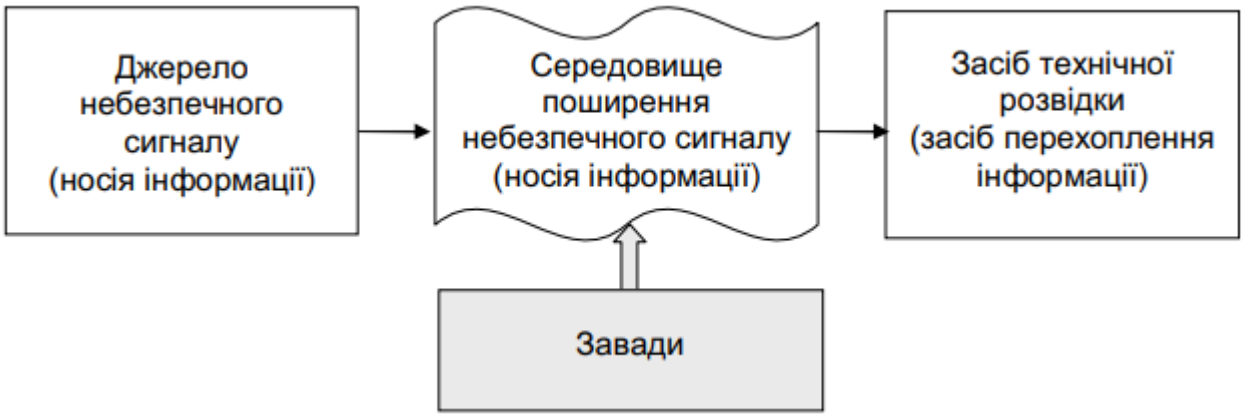


Рисунок 1.1 –Технічний канал витоку інформації

Для забезпечення технічного захисту в Україні створена система технічного захисту інформації. Вона являє собою сукупність організаційної інфраструктури, нормативно-правової бази, та матеріально-технічної бази, об’єднаних цілями та завданнями захисту інформації інженерними та технічними засобами

1.1 Класифікація каналів витоку інформації

Технічні канали витоку інформації становлять серйозну загрозу безпеці інформаційних систем. Зловмисники можуть використовувати різні методики та засоби для перехоплення та передачі небажаної інформації. Для ефективного захисту важливо класифікувати технічні канали витоку за різними ознаками, що дозволить усвідомити їх різноманітність, принципи дії та потенційні загрози.

Класифікувати ТКВІ можна за такими ознаками [7]:

- за видом інформаційної діяльності на об'єкті інформаційної діяльності ОІД;
- за принципом формування небезпечного сигналу ;
- за середовищем поширення небезпечного сигналу;
- за способом перехоплення(зняття).

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ:

1) Технічні канали витоку мовної інформації.
2) Технічні канали витоку інформації що обробляється в основних технічних засобах та системах (ОТЗС).
3) Технічні канали витоку візуальної інформації.
4) Матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за іншими трьома ознаками (за принципом, середовищем та способом перехоплення), буде проведено в межах вищезазначених типів.

Технічні канали витоку мовної інформації поділяються на:

1) Акустичні канали.
2) Акустовібраційні (віброакустичні) канали.
3) Акустооптоелектричні (лазерно акустичні) канали.
4) Акустоелектричні канали.
5) Відеоакустичні канали.
6) Канали ВЧ навязування (для зняття мовної інформації).

Технічні канали витоку інформації що обробляється в ОТЗС :

1) Канали побічних електоромагнітних випромінювань.

2) Канали побічних електромагнітних наведень.
3) Канали «паразитної» модуляції сигналів ВЧ генераторів.
4) Канали «паразитної» ВЧ генерації підсилювачів.
5) Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.
6) Канали перехоплення (зняття) інформації з каналів зв'язку.
7) Канали ВЧ нав'язування.
8) Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на такі:

1) Візуальні канали.
2) Візуально оптичні канали.
3) Канали витоку візуальної інформації, на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації

1) Добування інформації з магнітних та інших носіїв інформації, засобів електронно-обчислювальної техніки.
2) Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.
3) Хімічні канали.

За місцем перехоплення інформації засобами технічної розвідки противника відокремлюють такі типи ТКВІ

1) Канали перехоплення (зняття) інформації за межами КЗ.
2) Канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації (наприклад, канал ВЧ нав'язування).
3) Канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Дана класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про різні типи каналів та їхні особливості. Вона надає засоби для

категоризації каналів за різними ознаками, такими як носій інформації, принцип формування небезпечного сигналу, середовище поширення та спосіб перехоплення. Це допомагає уточнити розуміння та визначення заходів захисту від кожного типу каналу. Класифікація сприяє більш системному підходу до аналізу технічних каналів витоку інформації і створює основу для подальших досліджень та розробок в області інформаційної безпеки.

Оскільки переважна частина інформації яка циркулює в приміщенні де проводяться конфіденційні перемовини є мовною, то виникає потреба в більш глибокому аналізі каналів витоку акустичної інформації. Необхідно розглянути окремі варіації акустичних каналів, які спеціально спрямовані на перехоплення і передачу мовлення. Такі канали можуть використовувати спеціальне обладнання для вимірювання звукових коливань, аналізу та відтворення мовлення, що дозволяє зловмисникам отримувати доступ до конфіденційної інформації, яка передається через звукові сигнали.

1.1.1 Акустичний канал

Акустична інформація – інформація, носієм якої є акустичний сигнал. Вона включає в себе мовлення, звуки оточуючого середовища, музику, звукові ефекти та інші звукові сигнали.

Акустичний сигнал – це звуковий сигнал, який передається через середовище у формі звукових хвиль. Він може мати різні характеристики, такі як амплітуда (сила звуку), частота (кількість коливань за одиницю часу), фаза (положення у часі) та інші параметри, що визначають його властивості.

Акустичний канал витоку інформації реалізується в наступному:

- підслуховування розмов на відкритій місцевості і в приміщеннях, перебуваючи поруч або використовуючи спрямовані мікрофони (бувають параболічні, трубчасті або плоскі;
- негласний запис розмов на диктофон (в тому числі цифрові диктофони, що активізуються голосом);
- підслуховування розмов з використанням виносних мікрофонів.

Мікрофони, які використовуються в радіо закладках, можуть бути вбудованими або виносними і мають два типи: акустичні (чутливі в основному до дії звукових коливань повітря і призначені для перехоплення мовних повідомлень) і вібраційні (перетворюють в електричні сигнали коливання, що виникають в різноманітних жорстких конструкціях).

В акустичних каналах витоку інформації середовищем поширення мовних сигналів є повітря. Виток акустичної інформації за межі огороджувальних конструкцій можливий трьома шляхами [8]:

- за рахунок «мембранного ефекту». Так званий «мембранний ефект» обумовлений коливанням тонких (відносно довжини) і, як правило відносно легких, елементів огороджувальних конструкцій (віконного скла, фанерних, гіпсокартоних, пластикових перегородок тощо), здатних прогинатися під дією звуку;
- через тріщини, отвори, щілини та інші акустичні отвори, тобто прямим розповсюдженням акустичних коливань;
- за рахунок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні. У даному випадку частина енергії акустичних коливань (частина відбивається), падаючи на поверхню огороджувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення речовини. Подолавши огороджувальну конструкцію, частина енергії віброакустичних коливань (частина відбивається) перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

Схематично шляхи витоку акустичної інформації за межі огороджувальних конструкцій відображені на рисунку 1.2

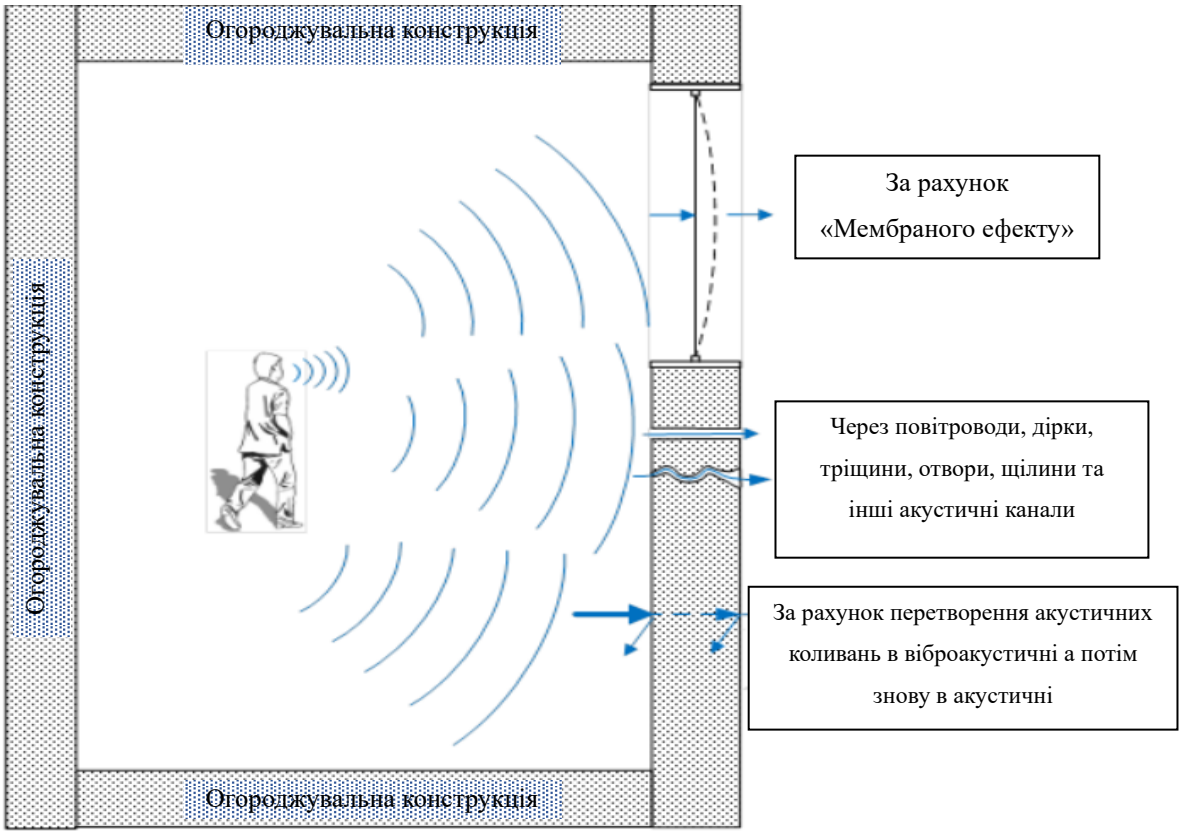


Рисунок 1.2 – Можливі шляхи витоку акустичної інформації

Для перехоплення акустичної інформації можуть використовуватися високочутливі мікрофони. Якщо немає можливості застосувати такі мікрофони використовуються спрямовані мікрофони, тобто таки, які мають вузьку діаграму спрямованості.

Перехоплена мовна інформація може записуватися на портативні записуючі пристрої (диктофони) або передаватися по радіоканалу, мережі електроживлення, оптичному каналу з'єднувальним лініям, стороннім провідникам, інженерним комунікаціям тощо.

1.1.2 Віброакустичний канал

У віброакустичних каналах витоку інформації середовищем поширення мовних сигналів є огороджувальні будівельні конструкції приміщень (стіни, вікна, двері, перекриття тощо) та інженерні комунікації.

Сутність віброакустичних каналів витку полягає в тому, що акустична хвиля небезпечного сигналу. Впливаючи на поверхню твердого матеріалу (пружного се-

редовища), приводить його до вібрації – коливання його молекул, яке, в залежності від густини матеріалу може розповсюджуватись на досить великі відстані. Чим більша густина, тим більша дальність розповсюдження сигналу.

Для перехоплення мовних сигналів у цьому випадку використовують контактні мікрофони (акселерометри). Вібродатчик, з'єднаний з електронним підсилювачем називають електронним стетоскопом (далі – ЕС). ЕС дозволяє здійснювати прослуховування мови за допомогою голосових телефонів та її запис.

Шляхи витоку інформації віброакустичними каналами наведено на рис. 1.3

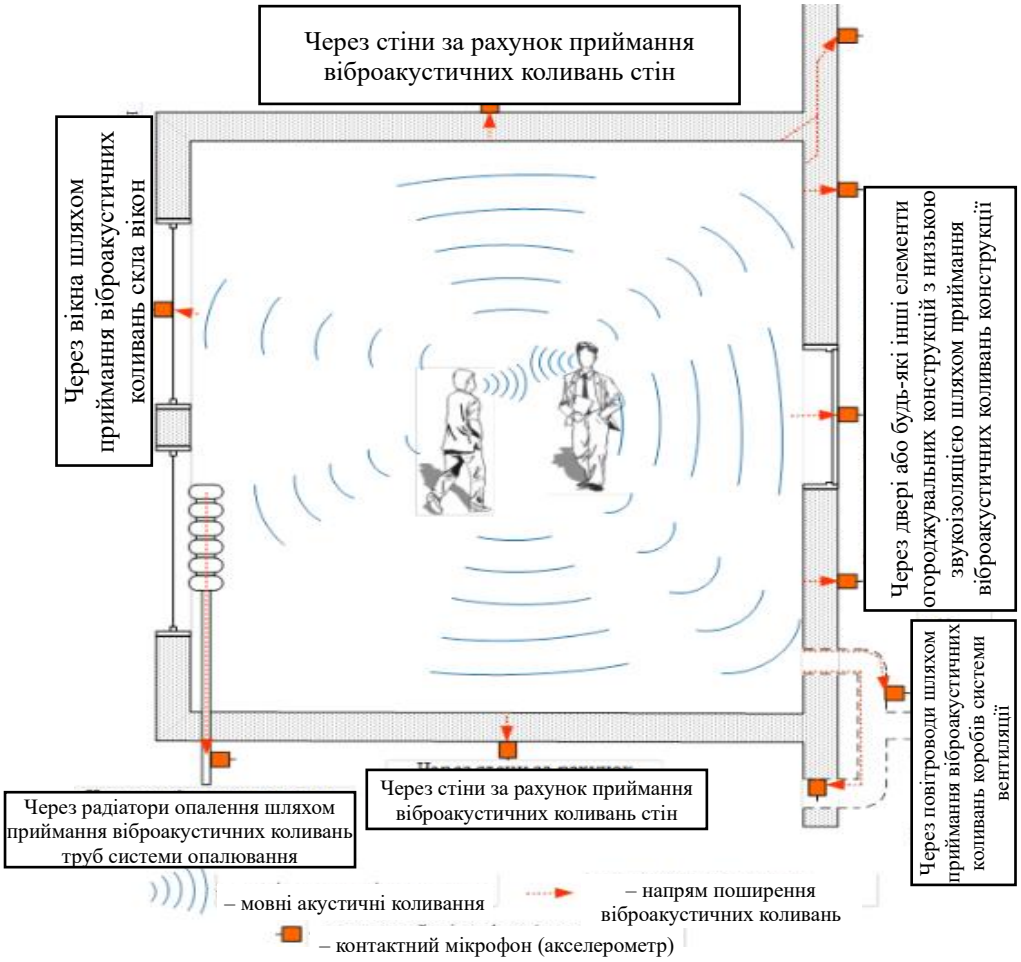


Рисунок 1.3 – Віброакустичні канали витоку інформації

По віброакустичному каналу також можливо перехоплення інформації з використанням ЗП. Для передачі інформації часто використовується радіоканал, тому такі пристрої часто називають радіостетоскопами. Можливе використання ЗП з пе-

редачею інформації по оптичному каналу в ближньому інфрачервоному діапазоні довжин хвиль, а також по ультразвуковому каналу (по інженерним комунікаціям).

1.1.3 Акустоелектричні канали

Акустоелектричні канали витоку інформації виникають за рахунок перетворень акустичних каналів в електричні.

Деякі елементи допоміжних технічних засобів і систем (ДТЗС), у тому числі трансформатори, котушки індуктивності, електромагніти вторинних годинників, телефонних дзвінків апаратів і тощо, мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу.

Зміна параметрів призводить або до появи на даних елементах електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам згідно із змінами електричного поля [8].

ДТЗС, крім зазначених елементів, можуть містити безпосередньо акустоелектричні перетворювачі. До таких відносяться деякі типи датчиків пожежної та охоронної сигналізації, гучномовці ретрансляційної мережі тощо. Ефект акустоелектричного перетворення іноді називають «мікрофонним ефектом».

Перехоплення акустоелектричних коливань в даному каналі витоку інформації здійснюється шляхом безпосереднього підключення до з'єднувальних ліній ДТЗС спеціальних високочутливих ПНЧ.

Для прикладу розберемо ефект акустоелектричного перетворення в конденсаторі пристрою ДТЗС. Як правило, всі електронні схеми технічних засобів і систем містять конденсатори. Будь-яку схему ДТЗС можна представити у виді схеми заміщення (рис. 1.4).

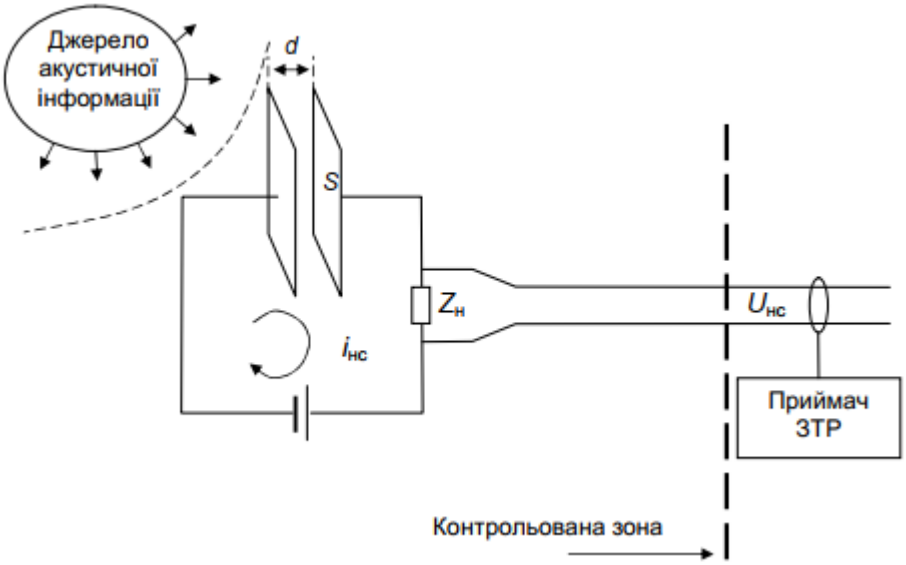


Рисунок 1.4 – Акустоелектричні перетворення на прикладі конденсатора пристроїв ДТЗС

Якщо на конденсатор в схемі впливає акустичний тиск, то він призводить до вібрації пластинки конденсатора, в результаті чого поміж ними змінюється відстань та , відповідно, його ємність. В результаті коливання ємності на пластинках конденсатору при фіксованій різниці потенціалів відбувається перерозподіл заряду, а в електричному ланцюгу, що з’єднує ці пластини, утворюється електричний струм. Останній, в свою чергу, приводить до падання напруги на опорі навантаження. Якщо лінія, що зв’язана зі схемою з кондесатором, виходить за межі КЗ та ОІД, то противник може перехоплювати небезпечний сигнал [7].

Технічний канал витоку інформації з використанням «високочастотного електромагнітного нав'язування» може бути здійснено шляхом несанкціонованого контактного введення струмів високої частоти від генератора в лінію, що має функціональні зв'язки з нелінійними або параметричними елементами ДТЗС, на яких відбувається модуляція високочастотного каналу інформаційним сигналом. Інформаційний сигнал у даних елементах ДТЗС з'являється внаслідок акусто-електричного перетворення акустичних сигналів в електричні. Промодульований сигнал відбивається від зазначених елементів і поширюється у зворотному напрямку або випромінюється.

1.1.4 Оптико електронний (лазерний) канал

Оптико-електронний (лазерний) канал витоку інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відбивається (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузійні або дзеркальне) модулюється по амплітуді й фазі (за законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Для організації такого каналу є кращим використання дзеркального відбиття лазерного променю. Якщо ззовні ОІД на поверхню скла, дзеркала, що вібрують спрямувати лазерний промінчик, то він віддзеркалиться від поверхні у вигляді промінчика, модульованого тремтінням від сигналу вібрацій, і розповсюджуватиметься далі (рис. 1.4). Тремтіння віддзеркаленого промінчика може бути перехоплене противником, здійснена його демодуляція (виділене тремтіння) і відновлений початковий інформаційний мовний сигнал [7].

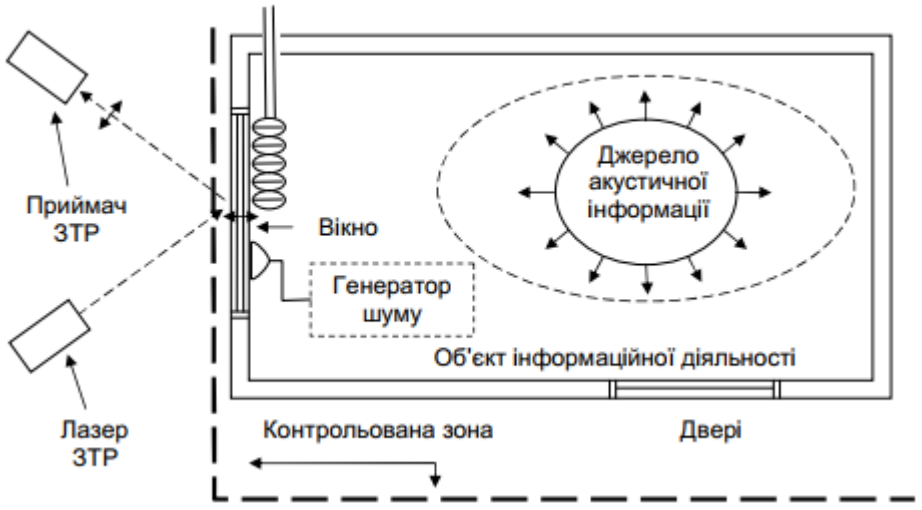


Рисунок 1.4 – Акустооптоелектричний канал витоку інформації

Однак, при невеликих відстанях до поверхонь, що відбивають (порядку декількох десятків метрів) може бути використано дифузне віддзеркалення лазерного випромінювання [8].

Для перехоплення мовної інформації з даного каналу використовуються складні лазерні системи – «лазерні мікрофони», які працюють, як правило в ближньому інфрачервоному діапазоні довжин хвиль.

1.2 Способи захисту інформації

В сучасному цифровому світі, де інформація є однією з найцінніших ресурсів, захист конфіденційної інформації стає надзвичайно важливим завданням для організацій і осіб. Існує безліч способів захисту інформації, але вони можуть бути систематизовані в три основні категорії: правові, організаційні та інженерно-технічні.

Правові способи захисту інформації передбачають використання законодавчих норм і правил для регулювання доступу до конфіденційної інформації та покарання незаконних дій щодо її витоку. Основні аспекти правового захисту інформації включають:

1) Законодавчі акти: Уряди країн встановлюють закони та нормативно-правові акти, що стосуються захисту інформації. Ці акти визначають правила обробки, зберігання та передачі інформації.
2) Авторські права: Авторські права захищають інтелектуальну власність, включаючи літературні, музичні, художні твори та інші.
3) Патенти і товарні знаки: Інноваційні розробки та технічні винаходи можуть бути захищені патентами, що надають власнику ексклюзивні права на їх використання.
4) Конфіденційність і нерозголошення: Угоди про нерозголошення (NDA) та інші конфіденційні угоди можуть бути використані для захисту конфіденційної інформації, забороняючи її розголошення третім особам.
5) Міжнародні стандарти: Існують міжнародні стандарти, такі як ISO 27001, що встановлюють вимоги до систем управління інформаційною безпекою і сприяють створенню ефективних заходів захисту інформації.

Ці правові заходи допомагають створити правову основу для захисту інформації, регулюючи правила та вимоги до обробки, зберігання та передачі конфіденційної інформації.

Організаційні заходи є важливою складовою частиною стратегії захисту інформації. Нижче наведено деякі основні аспекти організаційних заходів, які забезпечують безпеку інформації:

1) Проектування і будівництво приміщень: Служба безпеки взаємодіє з відповідними структурами під час проектування і будівництва приміщень, щоб врахувати вимоги до забезпечення безпеки. Це включає створення спеціальних перекриттів і каналів повітряної вентиляції, екранування окремих кімнат та інші заходи.
2) Підбір персоналу: Служба безпеки бере участь у підборі персоналу і перевіряє їх кваліфікацію та надійність.
3) Організація пропускного режиму: Служба безпеки встановлює та контролює пропускний режим, що включає систему обліку та контролю доступу працівників і гостей до об'єктів.
4) Охорона приміщень і територій: Служба безпеки організовує охорону приміщень і територій, встановлює системи безпеки.
5) Зберігання і використання документів: Служба безпеки встановлює процедури зберігання, обліку та використання конфіденційних документів, а також планує регулярні перевірки для забезпечення їх цілісності і захисту.

Виконання організаційних заходів вимагає постійного моніторингу, навчання персоналу та впровадження розрахункових процедур. Вони доповнюють інші заходи безпеки і створюють загальну культуру безпеки в організації.

Інженерно-технічні заходи є важливими для забезпечення захисту інформації. Основні складові інженерно-технічного захисту включають:

1) Апаратні засоби захисту: системи контролю доступу, біометричні системи ідентифікації, пристрої для шифрування інформації, фізичні бар'єри і обмеження доступу до приміщень і серверних кімнат.

2) Програмні засоби захисту: програмне забезпечення для виявлення і відсіювання шкідливих програм, брандмауери для контролю мережевого трафіку, програми шифрування для захисту даних від несанкціонованого доступу тощо.
3) Математичні методи захисту: криптографічні методи, які включають шифрування даних, використання цифрових підписів та інших алгоритмів, які дозволяють зберігати і передавати дані в безпечному форматі.

Ці три складові інженерно-технічного захисту взаємодіють і співпрацюють між собою для створення комплексного підходу до захисту інформації в системах та мережах. Комбінація правових, організаційних і інженерно-технічних заходів дозволяє ефективно захищати конфіденційну інформацію та запобігати її витоку.

Мовний сигнал створюється голосовим апаратом людини і являє собою обурення повітряного середовища. Енергія мовного сигналу зосереджена в діапазоні 300 – 4000 Гц [10].

Захист інформації від витоку технічними каналами забезпечують проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв [11].

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів відносять:

- залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області ТЗІ;

- категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;

– використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

– встановлення КЗ навколо об'єкта;

- залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;

– організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

– введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;

– відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи – це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал /завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

Пасивні заходи захисту інформації спрямовані на підвищення звукоізоляції огороджувальних конструкції (далі – ОК) ОІД (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючої підлоги», встановлення акустичних фільтрів у повітроводи тощо) [12].

До технічних заходів із використанням пасивних методів відносять такі:

1) контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення (установлення на об'єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу);
2) локалізація випромінювання:

– екранування ТЗПІ та з'єднувальних ліній;

– заземлення ТЗПІ та екранів їх з'єднувальних ліній;

– звукоізолювання виділених приміщень;

3) розв'язування інформаційних сигналів:

– установлення спеціальних захисних засобів типу Граніт, Рікас у ДТЗС із мікрофонним ефектом і таких, що мають вихід за межі КЗ;

– установлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі КЗ;

– установлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);

– установлення в мережах електроживлення ТЗПІ, а в лініях освітлювальної та розеткової мережі виділених приміщень;

- завадоподавляючих фільтрів типу ФП, ФСП, ФС-2.

Активні заходи захисту інформації спрямовані зниження співвідношення сигнал/завада до норми шляхом створення акустичної\віброакустичної завади на межі огороджувальних конструкцій ОІД [12].

Активні методи захисту здійснюються шляхом використання електромагнітних генераторів псевдовипадкових шумів. Виділяють два типи таких генераторів. А саме:

– генератори просторового зашумлення – призначенні для створення електромагнітних коливань визначеного діапазону частот для створення завад типу «білий шум» або псевдовипадковий шум;
– лінійного зашумлення – забезпечують маскування інформаційного сигналу, що був наведений в ДТЗС або сторонніх провідниках.

1) просторове зашумлення:

– просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами (за умови виявлення та з'ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ);
– створення акустичних і вібраційних завад із використанням генераторів акустичного шуму – шумотронів;
– подавлення працюючих у режимі запису диктофонів за допомогою подавляючих пристроїв.

2) лінійне зашумлення:

– мереж електроживлення та кіл заземлення;

– сторонніх дротів та з'єднувальних ліній ДТЗС, що виходять за межі КЗ.

3) знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів «жучків»).

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об'єктів ТЗПІ та виділених приміщень.

Для виявлення закладних пристроїв використовують:

1) пасивні методи:

- установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах);
- установлення стаціонарних детекторів диктофонів;
- розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно-апаратних комплексів контролю;
- організація радіоконтролю (постійно або на час проведення конфіденційних заходів) побічних електромагнітних випромінювань ТЗПІ.

2) активні методи:

– спеціальна перевірка виділених приміщень із використанням нелінійних локаторів;

– спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

До системи просторового зашумления, застосовуваної для створення електромагнітних перешкод, що маскують, пред'являються наступні вимоги [13]:

- система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань ТСПІ;
- створювані перешкоди не повинні мати регулярної структури;

- рівень створюваних перешкод (як по електричної, так і по магнітної складового поля) повинен забезпечити відношення с/ш на границі контрольованої зони менше припустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;
- система повинна створювати перешкоди як з горизонтальної, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);
- на границі контрольованої зони рівень перешкод, створюваних системою просторового зашумления, не повинен перевищувати необхідних норм по ЕМС.

Ціль просторового зашумлення вважається досягнутої, якщо відношення небезпечний сигнал/шум на границі контрольованої зони не перевищує деякого припустимого значення, що розраховує по спеціальних методиках для кожної частоти інформаційного (небезпечного) побічного електромагнітного випромінювання ТЗПІ.

Висновки до розділу

У данному розділі було розглянуто сучасний стан теоритичної та практичної реалізації проблеми захисту інформації різними каналами витоку. Проаналізовано класифікацію каналів витоку інформації. Детально розглянуто технічні канали витоку акустичної інформації та методи захисту від витоків. Захист інформації від витоку мовними каналами є складним завданням, яке потребує комплексного підходу і використання різних методів захисту.

Для запобігання просочування інформації акустичними і віброакустичними каналами використовують пристрої просторового та лінійного зашумлення, впроваджуються заходи щодо шумопоглинання і звукоїзоляції. В більшості випадків для несанкціонованого знімання інформації з приміщення зловмисник застосовує відповідні задуму заставні пристрої. Для перешкоджання цьому виконуються дії щодо їх виявлення та знешкодження

2 АНАЛІЗ ПРИМІЩЕННЯ

2.1 Аналіз фізичного середовища

Для того аби система захисту була комплексною та повною потрібно проаналізувати структуру приміщення згідно НД ТЗІ 3.7 [14]. Приміщенням, яке підлягає аналізу є простора конференц зала. В даній залі відбуваються конфіденційні перемовини та наради між керуючими ланками підприємства.

В приміщенні наявні базові системи для комфорту роботи співробітників та безпеки фізичного та інформаційного простору.

Приміщення офісу має тепло- та шумоізоляцію. Забезпечено доступ природньому освітленню та додатково оснащено лампами денного світла. Наявна пожежна сигналізація, вогнегасники та план евакуації з будівлі.

Приміщення має один вхід, Та подвійні вхідні двері між якими утворюється тамбур. двері мають щільну підгонку до дверної коробки та гумові прокладки для ущільнення. Поверхня тамбура облаштована звукопоглинаючими матеріалами.

Стіни та перегородки даного ОІД багатошарові. Перший шар являє собою цегляну кладку , завтовшки 120 мм, після нього прокладено мінеральну вату ,яка зверху зашита гіпсокартоном. Дана багатошаровість має гарні звукопоглинаючі та теплоізоляційні властивості.

Стеля окрім декоративної функції також підвищує звукоізоляцію. Підвісна стеля зроблена зі звукопоглинаючих плит. При цьому є змога легко оглядати простір над і під стелею, та немає закритих порожнин доступ та огляд яких ускладнений.

Підлога багатошарова на основі паркетної дошки із звукопоглинаючим матеріалом всередині. Побудована за принципом „плаваючої підлоги”.

В приміщенні є два металопластикові вікна, які мають дві камери (три скла) для підвищення звукоізоляції. На вікнах встановлені жалюзі, , які не дозволяють оглядати приміщення ззовні.

Будівля в якій облаштована конференц зала знаходиться в районі з низькою сейсмічною активністю та рівнем злочинності.

Об’єкт підключено до наступних елементів комунікацій та систем життєзабезпечення, що мають вихід за межі контрольованої зони:

- електроенергія;
- система кондиціонування повітря;
- інтернет.

Також наявне заземлення, виконане за рахунок металевих провідників з’єднаних з землею та заземлюючих провідників, які з’єднують заземлювані частини електроустаткування.

2.2 Аналіз інформаційного середовища

Інформаційне середовище являє собою ту інформацію яка виноситься в порядку денному конкретне засідання ради директорів. Інформація що циркулює та функціонує в даному приміщені може різнитись в залежності від мети кожної з нарад, які проводяться. Здебільшого являє собою конфіденційну інформацію щодо стратегії роботи підприємства, цілей які ставляться керівництвом та обговоренням шляху їх досягнення.

Підприємство яке використовує аналізовану конференц залу має свою локальну мережу. Доступ до неї в межах розглянутого приміщення здійснюється з комп’ютера оператора за допомогою традиційної авторизації « логін та пароль». Реалізований TRIPLE-A захист з підключенням протоколу Radius. З даного ПК вся інформацію передається на інші мультимедійні пристрої які знаходяться в приміщенні (проектор, монітори). На ОІД Встановлено ліцензійне програмне забезпечення .

Носії інформації, які присутні використовуються для зберігання інформації переважно стаціонарні та паперові. Також використовується VLAN стандарту 802.1q – він дозволяє зберігати доступ до мережі Інтернет та ізолювати комп’ютер від інших машин на підприємстві.

2.3 Аналіз середовища користувачів

Кількість користувачів даного ОІД може налічувати до 25 осіб. Легітимність знаходження користувачів підтверджується ключ картою та сесійним токеном.

Основний користувач, який має найбільшу взаємодію з інформаційними потоками є оператор. Вимоги до кваліфікації даної особи найвищі.

На підприємстві присутній різнорівневий захист інформації. Системи розмежування прав доступу, система ААА, ліцензійне антивірусне забезпечення, системи відеоспостереження та сигналізації.

В кожного користувача даного середовища є принаймні один смартфон, який може бути внесеним та в подальшому винесений за межі контрольованої зони, що розширює діапазон можливостей зловмисників.

2.4 Ідентифікація загроз та розробка моделі порушника

Наступним кроком потрібно визначити загрози, які можуть виникнути на об’єкті інформаційної діяльності, який розглядається. Було визначено 23 потенційні загрози, які можуть призвести до перехоплення інформації противником. Перелік даних загроз наведено нижче:

1. Витік за рахунок структурного звуку в стінах і перекриттях;
2) Знімання інформації з використанням відео-закладок;
3) Радіо-закладки в стінах і меблях;
4) Знімання інформації за системою вентиляції;
5) Лазерне знімання акустичної інформації з вікон;
6) Виробничі і технологічні відходи;
7) Знімання інформації за рахунок наведень і „нав'язування”;
8) Дистанційне знімання відео інформації (оптика);
9) Знімання акустичної інформації з використанням диктофонів;
10) Високочастотний канал витоку в побутовій техніці;
11) Знімання інформації направленим мікрофоном;

12) Знімання з клавіатури по акустичному каналу;
13) Знімання з дисплея по електромагнітному каналу;
14) Наведення на лінії комунікацій і сторонні провідники;
15) Витік через лінії зв'язку;
16) Витік по ланцюгах заземлення;
17) Витік по охоронно-пожежній сигналізації;
18) Витік по мережі електроживлення;
19) Витік по мережі опалювання.

Наступним кроком потрібно розробити модель порушника. Порушник – це особа, яка може отримати доступ до роботи з включеними в склад АС засобами. Порушники поділяються на два типи: внутрішні та зовнішні.

Зовнішні порушники працюють за територією підприємства не маючи прямого фізичного доступу до компонентів які розташовані на його території. Як правило зовнішні порушники використовують непрямі методи втручання в ІТС підприємства. Через системи комунікацій/життєзабезпечення тощо. Внутрішні мають повний або частковий доступ до функціональних компонентів підприємства. Як правило порушники такого типу є співробітниками підприємства.

Порушення на підприємстві можуть бути обумовлені низкою факторів, починаючи від людського – де користувач створює перепону на підприємстві через власну необачність закінчуючи корисливими або самоствердження.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості.

Порушення безпеки АС може бути викликано корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до інформації в АС. Навіть якщо АС має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Після того як дано характеристику зовнішнього і внутрішнього порушника можемо приступити до розробки моделі. Специфікацію моделі порушника за ознакою наведено в додатку А.

Модель внутрішнього порушника наведено в таблиці 2.2 . При її розробці визначено мотив рівень знань та навичок щодо роботи з ІТС, специфікацію за місцем та часом дії. Також визначено сумарний рівень загрози такого порушника.

Таблиця 2.2 – Модель внутрішнього порушника

Визначення категорії	Мотив порушення	Рівень кваліфікації та обізнаності щодо АС.	Можливості використання засобів та методів подолання системи захисту.	Специфікація моделі порушника за часом дії	Специфікація моделі порушника за місцем дії	Сумарний рівень загрози
Шпигун, який влаштувався на посаду оператора	М4	К5	З5	Ч4	Д4	17

Аналогічно до моделі внутрішнього порушника розроблено модель зовнішнього (табл. 2.3).

Таблиця 2.3 – Модель зовнішнього порушника

Визначення категорії	Мотив порушення	Рівень кваліфікації та обізнаності щодо АС.	Можливості використання засобів та методів подолання системи захисту.	Специфікація моделі порушника за часом дії	Специфікація моделі порушника за місцем дії	Сумарний рівень загрози
Противник, за межами контрольованої зони	М4	К3	З2	Ч3	Д1	12

Отже після формування моделі порушника, як результат можем побачити що внутрішній і зовнішній порушники однаково небезпечні хоча кожен має свої переваги та недоліки.

Як приклад внутрішнього порушника взято особу-шпигуна, якого впровадили та заглибили в середовище під виглядом оператора. Дана особа має високий рівень класифікації, мотив перехоплення інформації є професійний обов'язок , адже задля цього й було потрібно проникнути на ОІД. Оператор має доступ до приміщення в якому циркулює ІзОд. Необмежений за часом впливу, та має можливості взаємодії з локальною мережею.

Зовнішній порушник в даному випадку є противник за межами контрольованими зонами. Після емпіричного аналізу особи за межами контрольованої зони, можна дати експертну оцінку середнім можливостям такого порушника. Кваліфікація такого порушника є вище середньої. Місце дії обмежується територією за межами контрольованої зони. Час активності такого порушника випадає лише на період діяльності АС, так як під час її бездіяльності в нього не буде змоги з нею взаємодіяти.

Висновки до розділу

В даному розділі було проаналізоване приміщення, яке потребує захисту, було визначено що в приміщенні наявні базові пасивні методи захисту, але не більше. Наступним кроком було визначено перелік загроз, які можуть виникнути в межах контрольованої зони. Також було розроблено модель внутрішнього та зовнішнього порушника та дано оцінку рівню небезпеки, який несуть.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ ПРИМІЩЕННЯ

Після того як проведено аналіз приміщення та виявлено загрози, які можуть виникнути на ОІД можна дійти висновку що потрібно приділити увагу наступним аспектам захисту ТКВІ:

- Встановити контрольовану зону навколо об’єкта
- Сформувати організаційні методи захисту приміщення для контролю пропускного режиму та забезпечення охорони приміщення.
- Забезпечити планову перевірку приміщення з використанням технічних засобів на предмет наявності закладних пристроїв
- Розробити технічні заходи для захисту інформації витік якої може відбутися лініями комунікацій які виходять за межі КЗ.
- Реалізувати просторове зашумлення, як активний захист з метою безпеки циркулювання акустичної інформації
- Встановити контроль та обмеження доступу на територію об’єкта технічних пристроїв які можуть бути джерелом витоку (зі злим умислом або ненавмисне)

3.1 Організаційні методи захисту приміщення та контрольована зона

Контрольована зона – територія об’єкта на якій виключено неконтрольоване знаходження осіб що не мають постійного або разового доступу.

Межі контрольованої зони повинні визначатись керівництвом компанії виходячи з конкретних обставин та можливостей перехоплення засобами технічної розвідки.

Для обмеження доступу до контрольованої зони доцільно встановити двері з електронними картками. Доступ до приміщення надаватиметься ключ картою лише вповноваженим особам. Додатковою підставою для доступу в конференц залу модна реалізувати програмну видачу сесійного ключа(токену) особам які повинні бути присутні на тому чи іншому зібранні на запланований проміжок часу.

Технічний персонал, який займатиметься організаційно-технічними аспектами, по типу підготовки приміщення до наради абощо, матиме спеціалізований ключ технічного персоналу.

Візуальний контроль за контрольованою зоною вестиметься за допомогою системи відеоспостереження, камери потрібно розташувати в стратегічних місцях щоб охоплювати всю КЗ, також потрібно уникати появи мертвих зон, які не захоплюються жодною камерою. Система відеоспостереження повинна мати функцію запису. Відеоматеріали записів зберігатимуться щонайменше місяць після цього видалятимуться, а на їх місце записуватимуться нові.

В межах КЗ потрібно встановити систему сповіщення, яка буде автоматично сповіщати про будь-яку недозволену або підозрілу діяльність у контрольованій зоні. Це можуть бути сигналізаційні системи, повідомлення на мобільні пристрої або сповіщення до служби безпеки.

До робіт із встановлення та монтування всієї апаратури доцільно залучати організації з відповідними ліцензіями та консультуватись з ними щодо відповідних рішень.

Підбір персоналу: для контролю співробітників та виключення можливості проникнення шпигунів службою безпеки повинна виконуватись перевірка персоналу, що наймається на ту чи іншу посаду.

В випадках коли противник працевлаштовується на посаду з доступом до захищуваного ОІД, наслідки можуть бути критичними для компанії. В залежності від проміжку часу за який діє шпигун до моменту його виникнення, шкода заподіяна ним зростатиме.

Утилізація паперових носіїв та відходів повинно бути реалізоване таким чином що порушник не міг скористатись ними для отримання інформації. Способи знищення паперових носії, зміст яких не підлягає розголошенню:

- Шредерування;
- Спалювання;
- Хімічна обробка;

Один з відомих способів знищення паперових носіїв інформації полягає в процесі подрібнювання їх до стану, що унеможливлює їх читання, недоліком цього способу є те що для утилізації великих обсягів інформації займає великий проміжок часу.

Іншим способом знищення є спалювання. Можливі два методи спалювання: на відритому повітрі або в спеціальній печі. Процес спалювання на відкритому повітрі включає в себе два етапи: підготовка документів і безпосередньо спалювання. На етапі підготовки документи просочуються спец. сумішшю (50% бензину, 50% дизельного палива). Папки занурюють в розчин витримують деякий час потім укладають так аби між теками були повітряні прошарки що забезпечували ю краще горіння і повне згорання. Цей метод давно не використовують через те що він є найменш раціональним та екологічним рішенням. Спалювання документів на спеціальному обладнанні потребує відповідних дозволів та покупки дороговартісного устаткування, що також є ірраціонально для тих об’ємів які має дане підприємство [16].

Хімічний спосіб утилізації. При цьому способі знищення документів використовують обробку хімічно активними речовинами. Вони впливають на папір, розкладаючи її і перетворюючи в однорідну масу. До переваг способу відноситься надійність – після обробки відновленню документи вже не підлягають. Але він досить витратний – потрібне спеціальне обладнання та реактиви. Крім того, виконавець повинен суворо дотримуватися правил техніки безпеки [16].

Найдоцільніше буде використати метод шредерування так як обсяги паперових носіїв не є великими, і покупка машини для шредерування є менш затратне в порівнянні з іншими методами. Більш того, уклавши договір з компаніями по переробці паперу, нарізані смужки можна здати на вторинну сировину для переробки. Цей крок допоможе зберегти екологію та поверне невелику суму коштів.

Також на момент проведення переговорів вимагається вимикати всі елементи та лінії комунікацій що виходять за межі контрольованої зони, для запобігання витоку інформації за допомогою підключення то них передавачів.

3.2 Контроль доступу технічних пристроїв в ОІД

Мобільні пристрої або інші технічні пристрої, які можуть бути пронесені на територію ОІД користувачами несуть загрозу для безпеки інформації. Використовуючи вразливості програмного забезпечення, шкідливі програми або незаконне дистанційне керування, зловмисник може за допомогою мобільного телефону виконувати несанкціонований збір або передачу конфіденційної інформації.

Для виключення даної загрози пропонується залишати всі технічні пристрої за межами конференц зали. Пристрої будуть залишатись в камері схову, яку можна облаштувати в тамбурі перед конференц залом. Дана камера повинна бути зі звукоізолюючих матеріалів для унеможливлення запису акустичної інформації ззовні, та екранована металом або металевою сіткою для того аби унеможливити проникання ПЕМВН назовні.

Після того як технічні пристрої будуть залишені в камерах схову користувачі можуть пройти крізь другі двері тамбуру. Перед цим дверима встановлені магнітні рамки, які реагуватимуть на пристрої, які не здані користувачами в камери схову. Також службою безпеки проводитиметься додаткова перевірка користувачів на наявність жучків за допомогою детекторів, які реагують на частотне випромінювання навіть якщо жучок вимкнений.

На моменти проведення переговорів в приміщенні конференц зали працюватиме пошукова система і в режимі сканування. Тому в випадках коли попередні етапи перевірки не виявили ЗП та порушник все ж таки проніс жучок на контрольовану зону, система оповіщатиме службу безпеки про виявлений підозрілий сигнал.

3.3 Протидія закладним пристроям

Одна з можливостей перехоплення інформації є витік каналами на основі закладних пристроїв. Їх принцип роботи полягає в тому що розміщений на ОІД «жучок» приймає (перехоплює) інформацію та передає її противнику. Засоби несанкціонованого перехоплення приховано встановлюють та камуфлюють під інші об’єкти з метою ускладнити їх виявлення.

З метою виявлення закладних пристроїв потрібно регулярно проводити візуальний огляд приміщення. При перевірці потрібно приділити увагу важкодоступним місцям таким як кути, ніші, вентиляційні отвори. Повинні враховуватись архітектурні та конструкційні особливості приміщення. Фальш стелі, підвісні стелі, предмети інтер’єру, щілини часто використовуються як місце де встановлюють «закладки». Також потрібно звертати увагу на електричні пристрої та комунікації. Розетки, вимикачі, розподільчі панелі, кабелі можуть бути місцями встановлення закладних пристроїв.

Окрім візуального огляду також потрібно залучати до перевірки технічні засоби, сканери, детектори, локатори та пошукові системи які спрощують задачу. Такі пристрої проводять сканування приміщення та виявляють підозрілі сигнали та їх джерело. Пошукові системи можуть реагувати на аналогові та цифрові пристрої які працюють постійно або з деякою періодичністю. Сканування проводиться в широкому діапазоні частот, в видимому та ІЧ діапазоні, ультразвук .

3.4 Екранування приміщення

На високих частотах застосовується винятково електромагнітне екранування. Дія електромагнітного екрана заснована на тім, що високочастотне електромагнітне поле послабляється ним же створеним (завдяки вихровим струмам, що утворяться в товщі екрана) полем зворотного напрямку. Теорія і практика покатують, що з погляду вартості матеріалу і простоти виготовлення перевага на боці екранованого приміщення з листової сталі. Однак при застосуванні сітчастого екрана можуть

значно спроститися питання вентиляції і освітлення приміщення. У зв'язку з цим сітчасті екрани також знаходять широке застосування.

Для виготовлення екрана доцільно використовувати такі матеріали [17]:

- сталь листова декапірованна ДСТУ 1386-47 товщиною (мм) 0.35; 0.50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистова оцинкована ДСТУ 7118-54 товщиною (мм) 0,35; 0.50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75;2,00;
- сталь тонколистова оцинкована ДСТУ 7118-54 товщиною (мм) 0.51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;
- сітка сталева ткана ДСТУ 3826-47 номер 0,4;0,5;0,7,1,0;1,4;1.6:1,8;2,0;2.5;
- сітка сталева плетена ДСТУ 5336-50 номер 3; 4, 5; 6;
- сітка з латунного дроту марки Л-80 ДСТУ 6613-53 0,25, 0,5; 1,0; 1,6; 2.0; 2,5.

Металеві аркуші чи полотнища сітки повинні бути між собою електрично з'єднані по всьому периметрі. Для суцільних екранів це може бути здійснено пайкою чи електрозварюванням. Шов пайки чи електрозварювання повинен бути суцільним для того, щоб одержати суцільнозварну конструкцію екрана.

Для сітчастих екранів придатна будь-яка конструкція шва, що забезпечує гарний електричний контакт між сусідніми полотнищами сітки не рідше чим через 10... 15 мм. Для цієї мети може застосовуватися пайка чи точкове зварювання.

Екран, виготовлений з лудженої низьковуглецевої сталевої сітки з вічком 2,5...3мм, дає ослаблення порядку 55.„60 дБ, а з такою же подвійною (з відстанню між зовнішньою і внутрішньою сітками 100 мм) -близько 90 дБ. Екран, виготовлений з одинарної мідної сітки з вічком 2,5 мм, має ослаблення порядку 65...70 дБ.

3.5 Реалізація просторового зашумлення

Білий шум – стаціонарний шум, спектральні складові якого рівномірно розподілені по всьому діапазону задіяних частот. Прикладами білого шуму є шум близького водоспаду (віддалений шум водоспаду – рожевий, так як високочастотні

складові звуку загасають в повітрі сильніше низькочастотних), або дробовий шум на клемах великого опору, або шум стабілітрона, через який протікає дуже малий струм. Назву отримав від білого світла, що містить електромагнітні хвилі частот всього видимого діапазону електромагнітного випромінювання. Крім білого, існують шуми багатьох кольорів.

Акустичним генератором називається пристрій, призначений для наведення перешкод у місцях яких проводяться секретні переговори. Акустичний генератор формує "білий" шум у всьому діапазоні звукової частоти. Передача акустичних коливань здійснюється, як правило, п'єзоелектричними вібраторами та акустичними колонками. В генераторах шуму використовується білий шум, так як навіть сучасними способами обробки сигналів цей шум погано фільтрується.

В схемі наведеній нижче (рисунок 3.1) джерелом шуму є напівпровідниковий елемент, а саме стабілітрон VD1 (КС168А). Цей стабілітрон функціонує в режимі лавинного пробою при дуже невеликому струмі. Сила струму що протікає крізь даний стабілітрон дорівнює всього-на-всього близько 100 мкА .

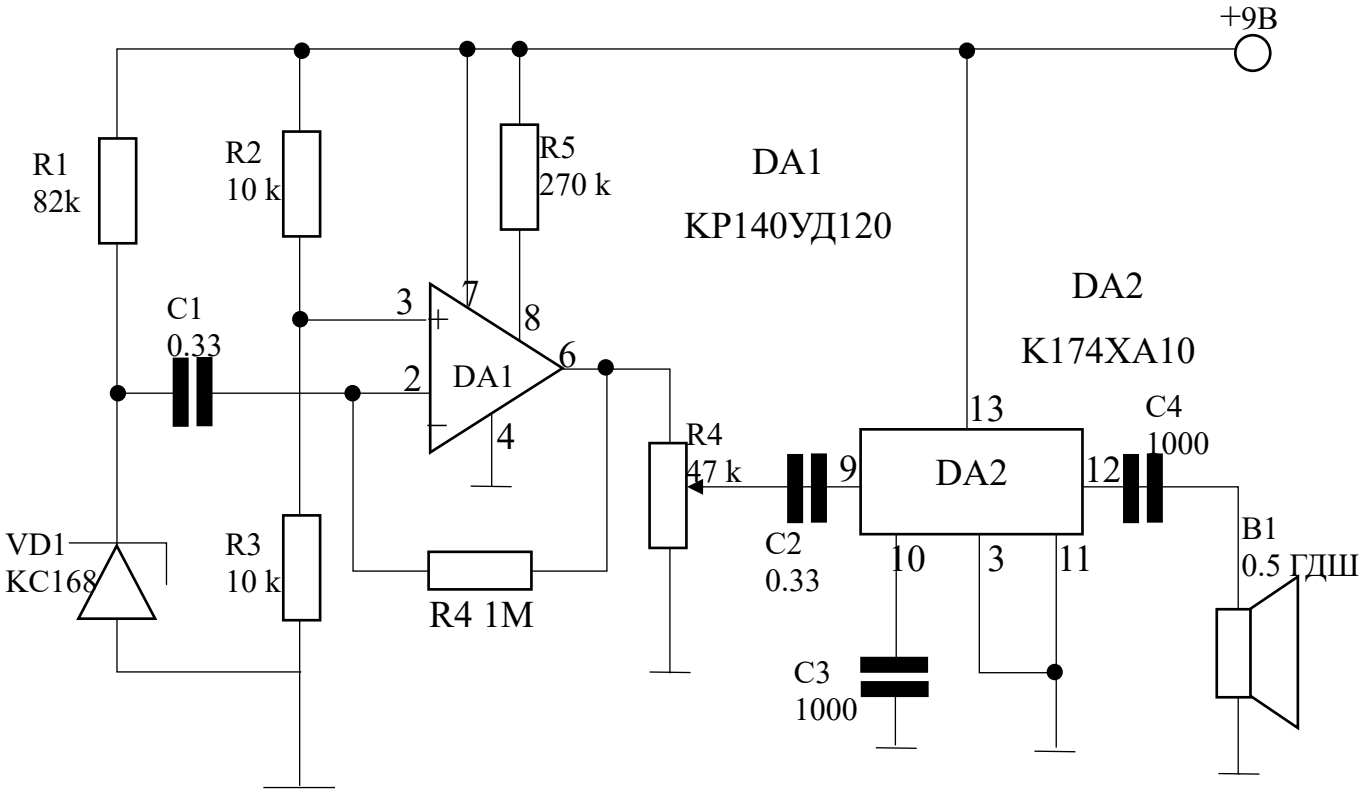


Рисунок 3.1 – Схема генератора білого шуму

Електронний шум, як цінний сигнал, приймається з катода стабілітрона VD1 і крізь неполярний конденсатор C1 йде на інвертується вхід 2 DA1 операційного підсилювача (КР140УД1208). З дільника напруги складається з резисторів R2 і R3 напруга зсуву надходить на другий вхід 3 DA1 цього ж підсилювача.

Порядок роботи мікросхеми DA1 обумовлюється опором резистора R5, а коефіцієнт посилення опором резистором R4. Навантаженням підсилювача DA1 є змінний резистор R6. З нього виділений сигнал йде на підсилювач потужності DA2, побудований на мікросхемі К174ХА10 .

Посилений сигнал з виходу DA2 через полярний конденсатор C4 йде на малогабаритну динамічну головку B1. Ступінь шуму регулюється змінним резистором R6. Стабілітрон VD1 створює шум в великому діапазоні частот від декількох герц до декількох десятків мегагерц. Проте, практично він обмежений АЧХ операційного підсилювача і динамічної головкою відтворює сигнал .

3.6 Вибір середовища моделювання

Для моделювання електричної схеми генеротора білого шуму було використано середовище Proteus Professional 8.5.

Proteus Professional – це потужне інтегроване середовище для моделювання електронних схем і систем. В порівнянні з іншими середовищами моделювання, Proteus Professional має декілька переваг [18]:

1) Інтегрованість: Proteus Professional забезпечує повний набір інструментів для проектування, моделювання, симуляції і візуалізації електронних схем. Він включає в себе редактор схем, симулятор, моделі поведінки компонентів, а також інструменти для автоматичної трасування друкованих плат і перевірки правильності проекту.
2) Симуляція в реальному часі: Proteus Professional дозволяє виконувати симуляцію електронних схем в реальному часі. Це означає, що ви можете

перевірити реакцію вашої схеми на зміну вхідних сигналів у реальному часі, що допомагає виявляти можливі проблеми і покращувати проект.

3) Велика бібліотека компонентів: Proteus Professional має велику бібліотеку стандартних і спеціалізованих компонентів, які можуть бути використані у вашому проекті. Ви можете легко вибрати потрібний компонент і включити його в свою схему без необхідності створення його моделі з нуля.
4) Імпорт і експорт даних: Proteus Professional підтримує імпорт і експорт даних у різних форматах, що дозволяє взаємодіяти з іншими середовищами моделювання і проектування. Ви можете імпортувати готові моделі компонентів або експортувати дані для подальшого аналізу або використання в інших програмах.
5) Зручний інтерфейс користувача: Proteus Professional має дружній інтерфейс користувача, який дозволяє легко створювати, редагувати і симулювати електронні схеми. Інтуїтивно зрозумілі інструменти та налаштування спрощують роботу з програмою і зменшують час, потрібний для розробки проекту.

Відмінність від аналогічних за призначенням пакетів програм, наприклад, Electronics Workbench Multisim, MicroCap, Тіна і т.п. у розвиненій системі симуляції (інтерактивної налагодження в режимі реального часу і покрокової) для різних сімейств мікроконтролерів: 8051, PIC (Microchip), AVR (Atmel), та ін Протеус має обширні бібліотеки компонентів, в тому числі і периферійних пристроїв: світлодіодні і РК індикатори, температурні датчики, годинник реального часу – RTC, інтерактивних елементів введення-виведення: кнопок, перемикачів, віртуальних портів і віртуальних вимірювальних приладів, інтерактивних графіків, які не завжди присутні в інших подібних програмах [18].

Загалом, Proteus Professional є потужним і зручним середовищем моделювання, яке дозволяє ефективно проектувати і перевіряти електронні схеми та системи. Його функціональність, бібліотеки компонентів і можливість симуляції в реальному часі роблять його привабливим вибором для інженерів і розробників.

3.7 Моделювання схеми пристрою

Моделювання електричної схеми:

- в якості мікросхеми КР140УД1208 була вибрана модель LT1222;
- в якості мікросхеми К174ХА10 була вибрана модель 10159;
- в якості резисторів було обрано модель RESISTOR.

Як було обрано у попередніх підрозділах моделювання пристрою, а саме вузла керування буде проводитись у Proteus Professional 8.5. Схема змодельованого пристрою представлено на рисунку 3.2.

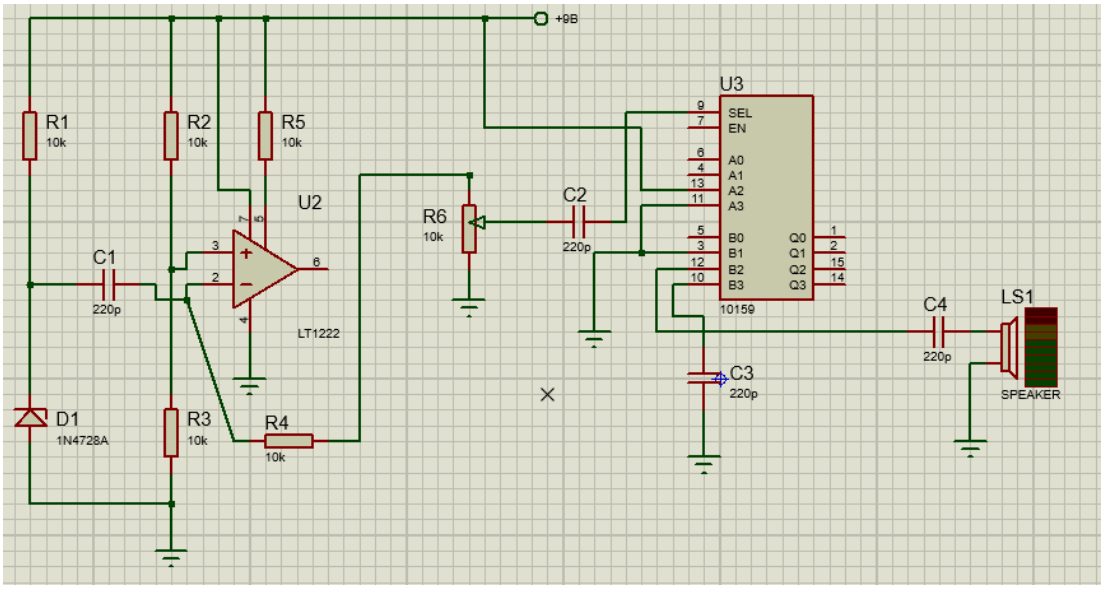


Рисунок 3.2 – Електрична схема пристрою

Пристрій складається з таких компонентів:

1) Блок живлення;
2) Напівпровідниковий елемент, а саме стабілітрон (КС168А);
3) Операційний підсилювач, побудований на мікросхемі (КР140УД1208);
4) Підсилювач потужності, реалізований на мікросхемі (К174ХА10);
5) Динамічна головка.

Перелік всіх необхідних елементів для реалізації змодельованого пристрою наведено в таблиці 3.1.

Таблиця 3.1 – Перелік елементів використаних у розробці пристрою

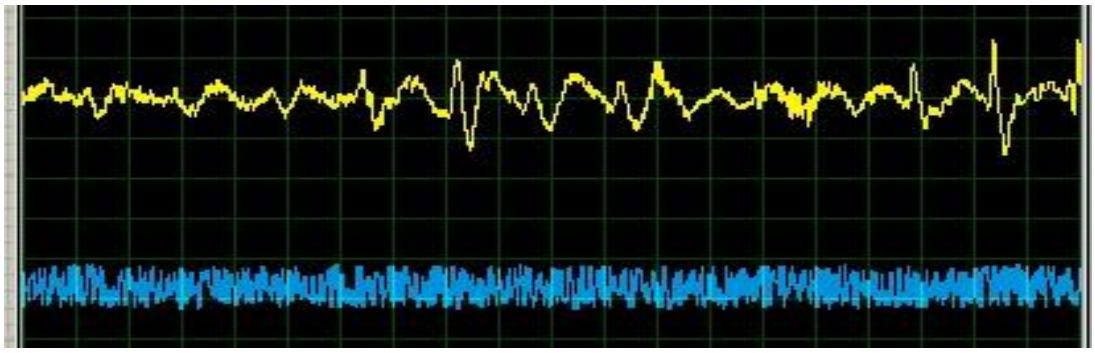
Види елементів	Найменування	Кількість
Мікросхеми		
	КР140УД1208	1
	К174ХА10	1
Стабілітрон		
	КС168А	1
Транзистори		
	КТ315	1
Резистори		
	МЛТ-82 кОМ	1
	МЛТ-10 кОМ	2
	МЛТ-270 кОМ	1
	МЛТ-1 мОм	2
Конденсатори		
	С1 – 0,33 мкф	2
	С2 – 100 мкф	2

Струм з блоку живлення протікає через стабілітрон, після чого інвертується і потрапляє в операційний підсилювач, після обробки струму резисторами, виділений сигнал йде на підсилювач потужності.

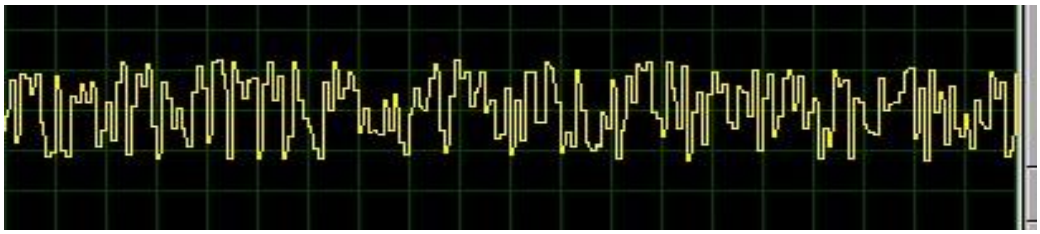
У ході виконання роботи було здійснено моделювання та розроблення пристрою, який генерує білий шум. Мета роботи полягала у створенні пристрою, який буде генерувати білий шум, для захисту інформації від витоку інформації від мікрофону направленої дії.

Даний пристрій працює на частотах від 3000 Гц до 5000 Гц, даний звук дуже шкідливий для людського вуха і тому для покращення пристрою було використано заміну динаміку , що дозволяє пристрою працювати на частоті від 12000 – 15000 Гц. Також даний пристрій являється персональним, тому було використано акумулятор «Крона», для його портативності.

Після моделювання пристрою було проведення тестування. Метою тесту було замірювання сигналу що передається, за допомогою осцилографа. Результати тестування представлено на рисунку 3.3.



а)



б)

Рисунок 3.3 – Результати тестування: а – сигнали до накладання б – сигнал отриманий в момент роботи пристрою

На рисунку 3.3,а жовтим кольором показано сигнал джерелом якого є мова людини, синій колір відображає сигнал який генерується розробленим генератором шуму. На рисунку 3.3,б наведено результат накладання двох сигналів один на інший, тобто продемонстровано сигнал який буде перехоплено записуючим пристроєм в момент роботи генератора

Розроблений пристрій повністю виконує свою функцію, а саме здійснює генерацію білого шуму на високих частотах.

Ще однією особливістю розробленого пристрою є зміна частоти.

Отже, можна зробити висновок, що реалізація запропонованого технічного пристрою виконана успішно.

3.8 Створення цільової функції

Для того аби зібрати всі вище описані рішення щодо методів захисту в одне ціле, доцільно створити цільову функцію. Для розробки цільової функції було

визначено та проаналізовано загрози даного підприємства. На основі даних досліджень буде створено цільову функцію.

Розглянемо показники цільової функції в аналітичному вигляді:

- вартість ($C < N$), де N – максимальний ресурс, виділений на створення КСЗІ;
- надійність ($N \geq 30000$ год.).

Базуючись на тезі: «вартість системи безпеки не повинна перевищувати можливих збитків» та ресурсів які може виділити підприємство, визначено що на підготовку КСЗІ буде виділено 610 000 грн.

Для створення КСЗІ було проведено аналіз середовища та оцінку ризиків. В результаті було висунуто наступні вимоги:

- Ресурс, виділений на створення КСЗІ не повинен перевищувати 610000грн.
- Показник надійності вказує кількість годин які повинен працювати технічний засіб без порушень роботи.

В результаті аналізу загроз було визначено, що для захисту приміщення необхідними є такі елементи:

- камера схову для технічних пристроїв користувачів;
- додаткові камери відеоспостереження в тамбурі;
- пошукова система закладних пристроїв;
- детектор ЗП;
- широкосмуговий сканер ;
- генератор білого шуму;
- шредер для знищення паперових носіїв;
- екранування.

3.9 Порівняльний аналіз та вибір рішень

3.9.1 Камера схову

При проведені пошуку готових рішень щодо камери схову, яка б задовольняла вимоги поставлені раніше результатів знайдено не було. Через це пропонується використати звичайну камеру схову та провести її модифікацію. Для того аби ПЕМВН залишених технічних пристроїв не проникало в контрольовану зону, комірку зберігання потрібно екранувати ззовні. Екранування використовуватиме принцип дії клітки Фарадея. Також камеру потрібно звукоізолювати, аби при наявності замаскованих технічних пристроїв в камері схову унеможливити запис звуку. Перелік потрібного обладнання представлено в таблиці 3.2.

Таблиця 3.2 – Перелік обладнання

Обладнання	Ціна	Примітка
Камера схову	7 000	1,5х1,5х0,5м.,16 комірок
Екранування	3 000	Оцинкований лист 0,55мм.
Звукоізоляція	2 000	
Всього	12 000	

Як результат можемо бачити що отримана камера схову задовольнятиме вимоги підприємства. Перехоплення інформації суттєво ускладнене встановленими модифікаціями до звичайної камери схову.

3.9.2 Камери відеоспостереження:

При аналізі фізичного середовища було зазначено що в приміщені конференц зали наявні 4 камери відеоспостереження. Для того аби мати змогу контролювати тамбур перед конференц залою потрібно встановити додаткові камери в ньому, щоб виключити будь-які зони які не фіксуються відеоспостереженням. У табл. 3.3 наведено можливі варіанти засобів відеоспостереження

Таблиця 3.3 – Порівняльний аналіз камер відеоспостереження

Назва	Кут огляду	Роздільна здатність	Ціна (2шт)
IMOU IPC-T42EP	90	2560x1440	6 000
Hikvision DS-2CD2T43G2-4I	103	2560x1440	13 000
Reolink RLC-810A	90	3840x2160	8 600

IP-камера Reolink RLC-810A – 8-мегапіксельна камера з роздільною здатністю 3840x2160. Завдяки технології Power over Ethernet (PoE) ця зовнішня камера може передавати відео та отримувати живлення через один мережевий кабель. 18 потужних інфрачервоних світлодіодів цієї камери безпеки 4K випромінюють невидиме світло, яке проникає в темряву на відстані до 30 метрів. Щойно камера виявить щось підозріле, вона надішле миттєве push-повідомлення та електронний лист із знімком виявлення на ваш пристрій. Розумна IP-камера PoE RLC-810A підтримує цілодобовий безперервний запис, запис руху та запис за розкладом.

3.9.3 Пошукова система закладних

При проведені конфіденційних перемови доцільно використовувати пошукову систему в режимі сканування приміщення, для виявлення закладних пристроїв або підозрілих сигналів. При виявленні підозрілої активності надходитиме сповіщення службі охорони. А таблиці 3.4 наведено результати аналізу пошукових систем.

Таблиця 3.4 – Порівняльний аналіз пошукових систем

Назва	Частотний діапазон	Цифрові стандарти	Ціна, грн
Delta X 100/4	40кГц-4400МГц	GSM, 3G, 4G/LTE, 5G (<6GHz), Bluetooth, Wi-Fi, DECT	250 000
Delta X 100/12	100 кГц-12400 МГц		350 000
Delta S STANDARD	57-6000 МГц	GSM, 3G, 4G/LTE, 5G, Bluetooth, Wi-Fi, DECT та інші стандарти в діапазоні до 6 ГГц.	530 000

Delta X 100/12 – один із варіантів професійного обладнання, яке використовують фахівці для виявлення прослуховуючих пристроїв та інших «жучків». Виявляє приховану передачу інформації в мережі змінного струму, через проводи телефону, у проводах Ethernet, сигналізації та інших кабелях, а також перевіряє інфрачервоний діапазон за допомогою багатофункціонального зонду, що поставляється в комплекті [19].

3.9.4 Широкосмуговий сканер

При огляді приміщення на наявність закладних пристроїв пропонується використовувати широкосмуговий сканер. Детектор жучків – це електронний пристрій, який використовується для виявлення та локалізації прихованих або нелегально встановлених пристроїв з вбудованими мікрофонами або камерами, таких як акустичні або оптичні жучки. Варіанти даних пристроїв наведено в таблиці 3.5.

Таблиця 3.5 – Порівняльна характеристика детекторів ЗП

Назва	Частотний діапазон	Чутливість виявлення	Ціна, грн
Детектор жучків G318	1-8000 МГц	≤0. 003 кВ/м	1 500
BugHunter Professional BH-02	50-3000 МГц	≤ 50 мВ/м	10000
Bughunter DR-45 Memory Professional	25 – 5 800 МГц	≤ 70 мВ/м	7 500

BugHunter Professional BH-02 – простий і зрозумілий детектор жучків, відрізняється розширеним діапазоном робочих частот і вбудованим GSM-фільтром для відсіювання фонових радіоперешкод.

3.9.5 Шредер для знищення паперових носіїв

Для знищення паперових носіїв інформації було обрано метод шредирування. Даний метод є найбільш безпечним з точки зору екології та безпеки здоров’я. Інформаційна безпека різниться від типу самого обладнання а саме розміром

вихідної маси після знищення документів які містять ІзОД. Порівняння апаратури шредерування наведено в таблиці 3.6 .

Таблиця 3.6 – Порівняльна характеристика апаратури шредирування

Назва	Рівень безпеки	Розмір фрагментів	Швидкість знищення	Ціна
Шредер Agent 115 X	P4	3.8x40 мм	3 м/хв	17 000
Шредер DA MDM215	P5	2 x 15 мм	2.5 м/хв	27 000
Шредер DA TP-6212MD	P5	2.5 x 10 мм	1.8 м/хв	13 000

MDM215-60L – потужний знищувач для середнього та великого офісу в металевому корпусі з інформативною сенсорною системою керування. Знищує 15 аркушів за один раз (80 г/м2). Додатково знищує скоби, кредитні картки та CD-диски [20].

3.9.6 Екранування

Для того аби унеможливити витік ПЕМВН на території контрольованої зони потрібно екранувати приміщення. Для екранування буде використовуватись оцинкована сталь. Екран виготовлений з оцинкованої сталі товщиною 0,55мм забезпечує ослаблення сигналу порядку 90дБ. Необхідна ефективність екрана в залежності від його призначення і величини рівня випромінювання ПЕМВН звичайно знаходиться в межах 60-120 дБ. Тому можна дійти висновку що даний матеріал задовольняє вимоги. Вартість екранування наведено в таблиці 3.7 .

Таблиця 3.7 – Витратні матеріали для екранування

Площа кімнати	102 $м^2$
Ціна матеріалу ($м^2$)	500 грн
Вартість матеріалу	111 000 грн
Монтажно-будівельні роботи (70% вартості матеріалу)	77 000 грн
Додаткові витрати	10 000 грн
Всього	198 000 грн

Під додатковими витратами розуміється забезпечення захисту технологічних та комунікаційних отворів в екранованому приміщенні. Приклади

технологічних та комунікаційних отворів це вікна двері та решітки вентиляції. Для запобігання витоку ПЕМВН повз щілини у місцях контакту металевих дверей з металевою коробкою краєві контури обрамлюють за допомогою ущільнюючих профілів виконаного з пружного діелектричного матеріалу з значним процентним вмістом електропровідного матеріалу що має низький питомий опір та забезпечує надійне ущільнення з замиканням ПЕМВН по контуру стику закритих дверей з металом дверної коробки, запобігаючи витоку ПЕМВН. Для вікон ж застосовується нанесення на поверхню віконного скла прозорого електропровідного покриття з низьким поверхневим опором.

3.9.7 Генератор білого шуму

Для запобігання запису конфіденційних перемовин під час нарад, постає питання просторового зашумлення приміщення. Щоб задовільнити дану потребу було розроблено генератор білого шуму який працює на мікросхемах. Перелік потрібних елементів було наведено на етапі моделювання пристрою. В таблиці 3.8. наведено розрахункову вартість пристрою.

Таблиця 3.8. – Розрахунок вартості генератора білого шуму

Вид елементу	Ціна, грн
КР140УД1208	12
К174ХА10	22
КС168А	4
КТ315	0,5
МЛТ-82 кОМ	1
МЛТ-10 кОМ	2,4 (2 шт.)
МЛТ-270 кОМ	2
МЛТ-1 мОМ	4,8 (2 шт.)
С1 – 0,33 мкф	20 грн (2 шт.)
С2 – 0,100 мкф	30 грн (2 шт.)
Всього	100 грн

В результаті маємо працюючий пристрій зашумлення приміщення. Вартість виготовлення суттєво менша за існуючі варіанти готових зразків які є в продажу.

В процесі аналізу було розглянуто конкурентні варіанти засобів захисту, аналіз проводився за параметрами на які рекомендовано звертати увагу при виборі

кожного з перелічених засобів. Кінцевий перелік необхідного обладнання для створення оптимальної системи захисту в приміщенні яке розглядається наведено в таблиці 3.9.

Таблиця 3.9 – Перелік необхідного обладнання

Обладнання	Ціна, грн
Камера схову	12 000
Камери відеоспостереження Reolink RLC-810A	8 600
Пошукова система Delta X 100/12	350 000
Детектор жучків BugHunter Professional BH-02	10 000
Шредер DA MDM215	27 000
Екранування приміщення	198 000
Генератор білого шуму	100
Всього	605 700

Для об’єкту захисту було розроблено структурну модель напрацювання на відмову системи. При розробці було розглянуто загрозу витоку інформації за допомогою технічних каналів розвитку. Розроблена модель наведена на рис. 3.3.

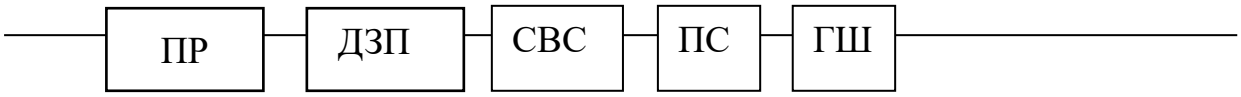


Рисунок 3.3 – Структурна модель елементів системи

На структурній схемі відображено блоки, які відповідають за унеможливлення встановлення та функціонування закладних пристроїв на території об’єкта інформаційної діяльності. Перше з чим стикається зловмисник при спробі встановлення це пропускний режим (ПР). У разі подолання першого бар’єру, закладний пристрій скоріш за все буде виявлено за допомогою детектора ЗП (ДЗП). В випадку коли вдалось оминути другий бар’єр, порушник стикнеться з системою відеоспостереження, яка найімовірніше зафіксує встановлення «жучка». Наступний етап захисту являє собою пошукову систему (ПС), яка працює в моменти проведення переговорів, даною системою проводиться сканування

приміщення на наявність шкідливих та підозрілих сигналів та сповіщається служба безпеки в разі їх виявлення. Якщо всі попередні бар'єри було пройдено то при передачі закладним пристроєм сигналу, на нього накладатиметься шум який випромінює генератор шуму (ГШ), що приглушає корисний сигнал, який потрібен зловмиснику.

Для системи, також було проведено розрахунок середнього напрацювання на відмову ($t_{ср}$). Вхідні дані для розрахунку, були наступними: ймовірність безвідмовної роботи (P(t)) більша рівна 0,99, протягом 400 год.. Розрахунки проводились за експоненціальним законом розподілу. Нижче наведені розрахунки.

$$P(t) = e^{-t/t_{cp}}$$

Прологарифмувавши вирази отримуємо наступне:

$$-\frac{400}{t_{cp}} = \ln(0{,}99)$$

$$t_{cp} = \frac{-400}{\ln(0{,}99)} = \frac{-400}{-0{,}01} = 40 * 10^3 \text{ год.}$$

В результаті розрахунків було встановлено, що середнє напрацювання на відмову досліджуваної системи дорівнює 40 тисяч годин.

Висновки до розділу

В даному розділі було сформовано загальні поради щодо створення системи захисту від витоку технічними каналами. В середовищі моделювання Proteus Professional розроблено та протестовано пристрій просторового зашумлення приміщення. Розроблено цільову функцію, та Обрано засоби захисту для розгнянутого приміщення, в якому циркулює ІзОД.

ВИСНОВКИ

В даній бакалаврській дипломній роботі було розглянуто проблематику витоку інформації технічними каналами витоку. Розглянуто класифікацію даних каналів та методи їх захисту.

Підводячи загальні підсумки роботи, варто відмітити, що дотримання безпеки інформації є критично важливим завданням для підприємств у сучасному світі. У роботі було розглянуто проблему витоку інформації технічними каналами витоку та проаналізовано різноманітні засоби технічної розвідки та перехоплення інформації, які стають все більш поширеними.

Отже, результати проведених досліджень показують, що проблема витоку інформації технічними каналами є серйозною і потребує вивчення та застосування заходів захисту. Розроблені методи та система захисту, а також прототип генератора білого шуму, можуть бути використані в реальних умовах для забезпечення безпеки інформації з обмеженим доступом.

При розробці системи захисту від витоку інформації технічними каналами, виконано аналіз приміщення відповідно до існуючих нормативних документів. Дане дослідження дозволило визначити потенційні загрози і вразливі місця, які можуть призвести до витоку конфіденційної інформації.

На основі використання прикладу конкретного приміщення було досліджено найпоширеніші методи перехоплення інформації і сформульовано загальні поради та вимоги для забезпечення конфіденційності інформації з обмеженим доступом.

Загальний результат аналізу приміщення дав можливість врахувати особливості його конструкції та виявити потенційні загрози безпеці інформації. Це дозволило ефективніше розробити систему захисту, враховуючи особливості самого приміщення та мінімізувати ризик витоку інформації через технічні канали. Система була оцінена з точки зору надійності та середнього напрацювання на відмову за допомогою математичних розрахунків.

Також у рамках досліджень було запропоновано власну модель розробки генератора білого шуму для просторового зашумлення приміщення з метою перешкоджання роботі мікрофонів направленої дії. Запропонований засіб було промодельовано в середовищі моделювання Proteus Professional, а також протестовано за допомогою вбудованих інструментів. В результаті було отримано працюючий аналог генератора білого шуму, який виконує свої функції та відповідає поставленим вимогам.

Отже, проведені дослідження показали, що система захисту, розроблена на основі встановлених вимог та цільової функції, є ефективним інструментом для запобігання витоку інформації через технічні канали. Крім того, впровадження запропонованого генератора білого шуму дозволяє забезпечити додатковий рівень захисту шляхом перешкоджання перехопленню звукової інформації.

Загальний обсяг досліджень у цій бакалаврській дипломній роботі зміцнює наше розуміння проблематики витоку інформації через технічні канали та надає практичні рекомендації для покращення безпеки і збереження конфіденційності інформації з обмеженим доступом. Результати досліджень можуть бути використані в різних сферах, де важлива захист інформації від технічного витоку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Методи та засоби захисту інформації в комп’ютерних системах та мережах / С.В. Шахов, А.В. Жуков, В.В. Безкоровайний. – Київ: ВПЦ "Київський університет", 2007. – 300 с.
2) Захист інформації: навч. посіб. / О. В. Глоба, С. В. Білецький, А. А. Чубар. – Київ: НАУ, 2016. – 184 с.
3) Охорона інформації в системах зв'язку та інформаційних технологій: навчальний посібник / Л.І. Герасимова, В.П. Бакланов, Л.А. Торба та ін. – Київ: НАУ, 2012. – 364 с.
4) Захист інформації в інформаційних системах: навчальний посібник / С.В. Шахов, А.В. Жуков, В.В. Безкоровайний. – Київ: ВПЦ "Київський університет", 2012. – 324 с.
5) Захист інформації: підручник / О.В. Глоба, С.В. Білецький, А.А. Чубар та ін. – Київ: НАУ, 2018. – 430 с.
6) "2020 Data Breach Investigations Report" | Version [Електронний ресурс]. : URL : https://enterprise.verizon.com/resources/reports/dbir/2020/ (дата звернення: 24.05.23)
7) Боднар І.І. витік інформації технічними каналами витоку// Матеріали тезів LII наук.-техн. конф. ФІТКІ, ВНТУ. Вінниця. 2023 – 3 С.
8) Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко , О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016 – 101с
9) Технічні канали витоку інформації [Електронний ресурс]. : URL :https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html
10) В. В. Сінюгін, В. С. Катаєв, і А. В. Грицак, «МОДУЛЬНИЙ ГЕНЕРАТОР ШУМУ ДЛЯ БЛОКУВАННЯ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ», Вісник ВПІ, вип. 6, с. 158–164, Груд. 2021.

11) Захист мовної інформації [Електронний ресурс]. : URL : https://tzi.com.ua/zaxist-movno-nformacz.html (дата звернення: 27.05.23)
12) Василюк, В. Об'єкти захисту інформації. Методи та засоби захисту інформації / науково-технічний збірник. — Київ : НТУУ «КПІ» – 2006. – С. 88-95.
13) Захист інформації від витоку технічними каналами [Електронний ресурс]. : URL :https://tzi.com.ua/zaxist-nformacz-vd-vitoku-texnchnimi-kanalami.html (дата звернення: 30.05.23)
14) Активні методи захисту інформації [Електронний ресурс]. : URL :https://vuzlit.com/1019550/aktivni_metodi_zahistu_informatsiyi (дата звернення: 2.06.23)
15) Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. – [Затверджений наказом ДСТСЗІ СБ України від 28.04. 1999 р. № 22]. – К.: ДСТСЗІ СБ України, 1999. – 41 с.
16) Спосіб знищення грифованих документів на паперових/пластикових носіях інформації: пат. 97089 Україна: МПК: F23G 5/00, F23G 5/12. №201411095; заявл. 13.10.14; опубл. 25.02.15 Бюл. №4. 10 с.
17) Конспект ТЗІ [Електронний ресурс]. : URL: https://studylib.net/doc/25648785/konspekt-tz%D1%96 (дата звернення: 07.06.23).
18) Встановлення Proteus Proffesional 8.5 [Електронний ресурс]. : URL: https://dnipro.lvivservice.com.ua/vstanovlennya-proteus-8-professional (дата звернення: 4.06.23)
19) Delta X – Посібник користувача [Електронний ресурс]. : URL: https://www.das-ua.com/wp-content/uploads/2020/10/Delta-X-1.221-%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D0%B0-1.pdf (дата звернення: 07.06.23)
20) Знищувач документів MDM215-60L [Електронний ресурс]. : URL: https://da.ua/ru/product/unictozitel-dokumentov-mdm215-60l (дата звернення: 07.06.23)

ДОДАТКИ

Додаток А

Специфікація моделі порушника за ознакою

Позначення	**Мотив порушення**	**Рівень загрози**
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок	4
Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи	1
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем	2
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки	3
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості	3
К6	Є розробником програмних та	4

	програмно-апаратних засобів захисту або системного програмного забезпечення	
Позначення	**Характеристика можливостей порушника**	**Рівень загрози**
З1	Використовує лише агентурні методи одержання відомостей	1
З2	Використовує пасивні засоби (технічні засоби переймання без модифікації компонентів системи)	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Застосовує методи та засоби дистанційного (з використанням штатних каналів та протоколів зв'язку) упровадження програмних закладок та спеціальних резидентних програм збору, пересилання або блокування даних, дезорганізації систем обробки інформації.	3
З5	Застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних).	4

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	До впровадження АС або її окремих компонентів	1
Ч2	Під час бездіяльності компонентів системи (у неробочій час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.)	2
Ч3	Під час функціонування АС (або компонентів системи)	3
Ч4	Як у процесі функціонування АС, так і під час призупинки компонентів системи	4
Позначення	**Характеристика місця дії порушника**	**Рівень загрози**
Д1	Без доступу на контрольовану територію організації	1
Д2	З контрольованої території без доступу у будинки та споруди	1
Д3	Усередині приміщень, але без доступу до технічних засобів АС	2
Д4	З робочих місць користувачів (операторів) АС	2
Д5	З доступом у зони даних (баз даних, архівів й т.ін.)	3
Д6	З доступом у зону керування засобами забезпечення безпеки АС	4

Додаток Б

ПРОТОКОЛ ПЕРЕВІРКИ БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Система захисту приміщення від витоку інформації технічними каналами

Автор роботи: Боднар Ілля Іванович

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 70,9%. Схожість – 29,1%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Боднар І. І.

Керівник роботи _____ Дудатьєв А. В.

ІЛЮСТРАТИВНА ЧАСТИНА

СИСТЕМА ЗАХИСТУ ПРИМІЩЕННЯ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

(Назва бакалаврської кваліфікаційної роботи)

Виконав: студент 4 курсу групи 1БС-19 б

спеціальності 125 Кібербезпека

_____ Боднар І.І.

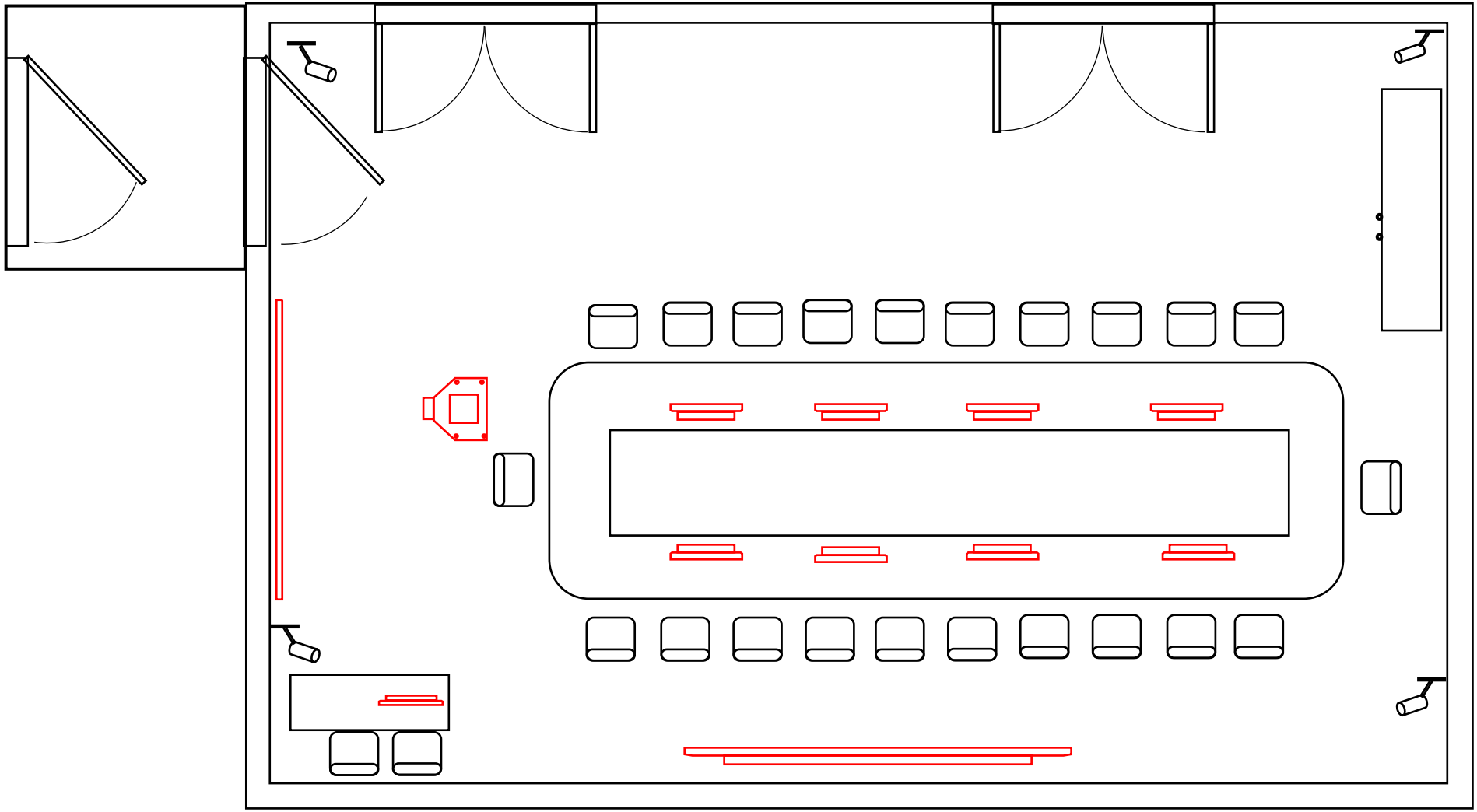
19 червня 2023

Керівник: к. т. н., доц. каф. ЗІ

_____ Дудатьєв А.В

19 червня 2023 р.

Схема приміщення



Характеристика каналів витоку

Канали	**Носій інформації**	**Середовище поширення**	**ЗТР**
Акустичний	Звукові хвилі	Повітря	Направлені мікрофони, диктофони, записуючі пристрої
Віброакустичний	Вібрації твердих тіл	конструкційні елементи споруд і будівель	контактні мікрофони, електронні стетоскопи, радіостетоскопи
Акустооптоелектричні (лазерно акустичні).	Акустичний(мовний) сигнал	Повітря, скло	«лазерні мікрофони», оптичні датчики
Акустоелектричні	Акустичні хвилі	Трансформатори, котушки індуктивності, електромагніти годинників тощо	Акустичні датчики ретранслятори
Відеоакустичні	Зображення, звук	Повітря, тверді тіла	Відеокамери, мікрофони
Електромагнітні	Електромагнітні хвилі	Повітря, простір, провідники	Антени, приймачі, аналізатори сигналів
Електричні	Електричні сигнали	Провідники	Електричні датчики
Параметричні	Параметричні сигнали	Електричні, оптичні канали	Параметричні датчики
Візуальні	Зображення	атмосфера; оптичні світловоди	Візуальне спостереження
Візуально-оптичні	Зображення, світло	Повітря, оптичні середовища	Фото-, теле-, кіноапаратура
Магнітні та інші носії інформації, засоби ЕОТ	Магнітні сигнали	Повітря, тверді тіла	Магнітні сенсори, приймачі
чернетки документів, видавницька діяльность, діловодство	Інформація на папері	Тверді тіла, папір	Оптичні сканери, копіювальні пристрої, аналізатори паперу
Хімічні канали	Хімічні речовини, запахи	Повітря, рідини, тверді тіла	Хімічні сенсори, аналізатори запахів

Електрична принципова схема пристрою

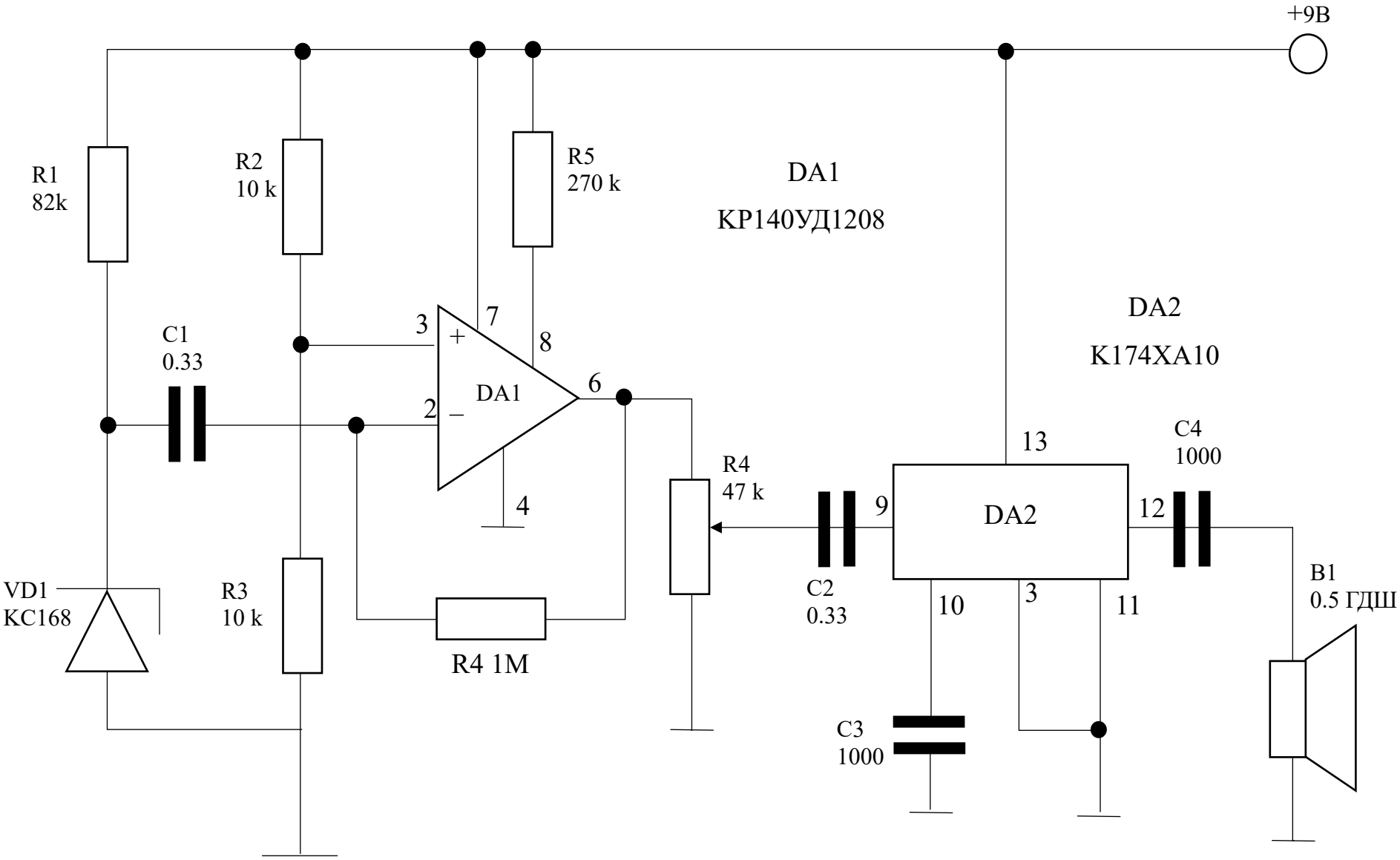
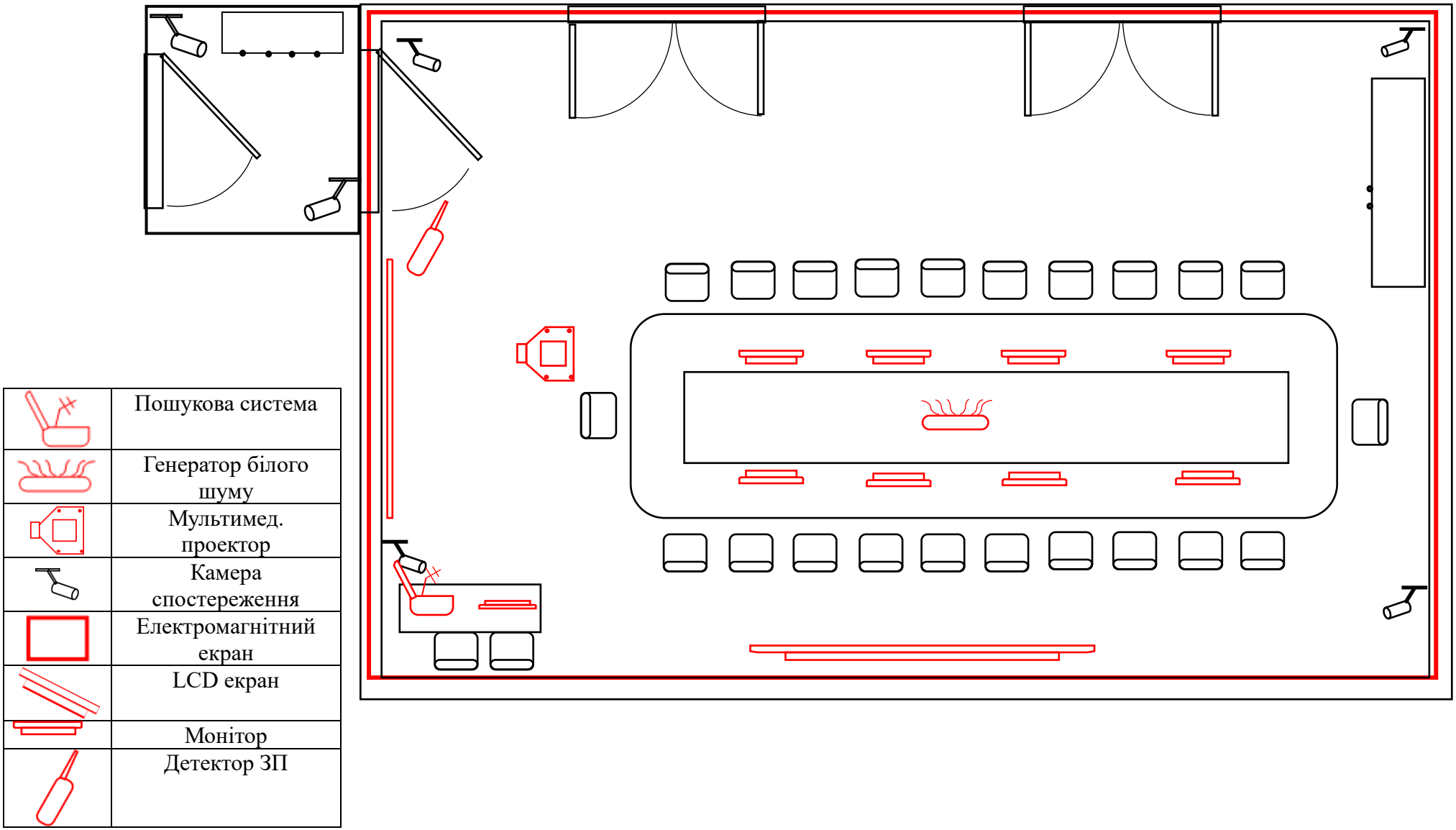
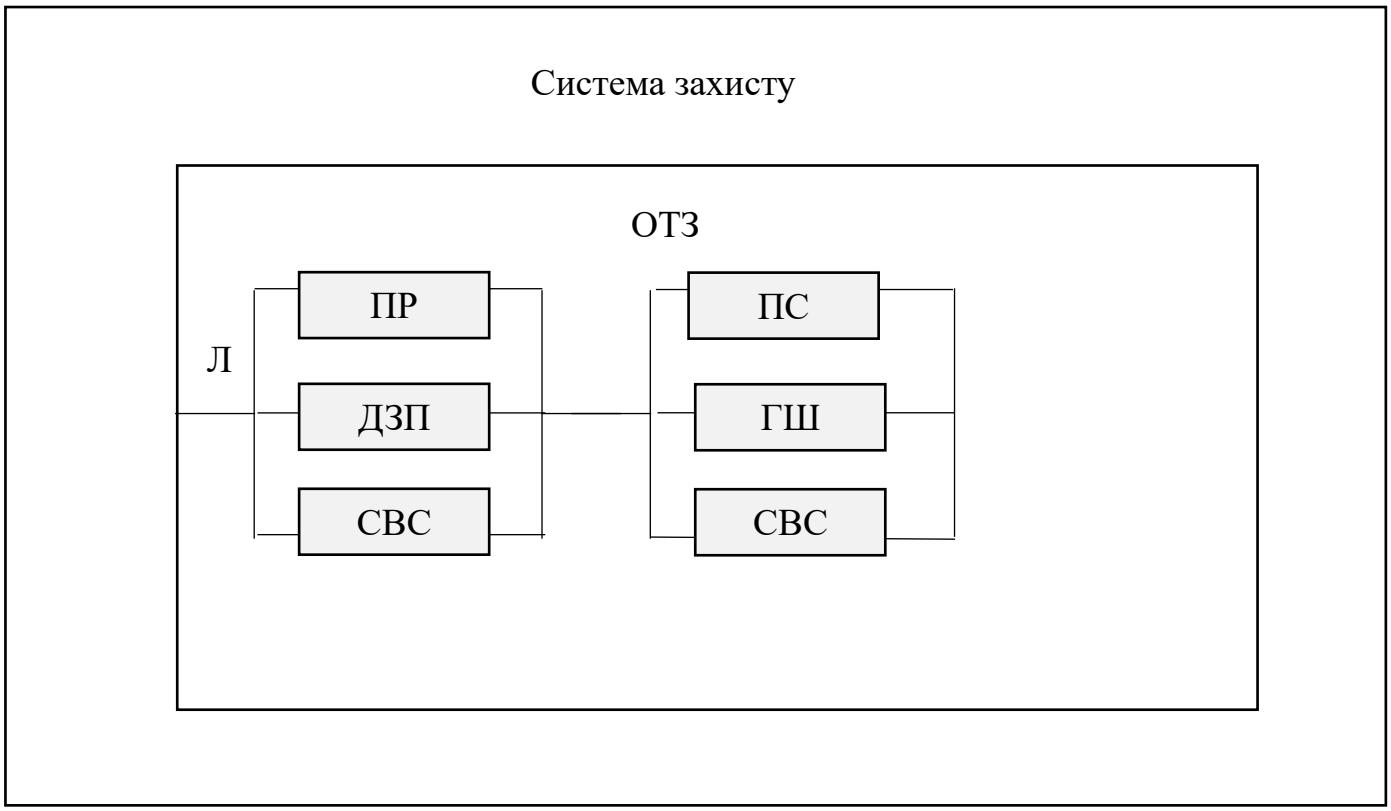


Схема захищеного приміщення



	Пошукова система
	Генератор білого шуму
	Мультимед. проектор
	Камера спостереження
	Електромагнітний екран
	LCD екран
	Монітор
	Детектор ЗП

Структурна схема системи захисту приміщення



ПР – пропускний режим;

ДЗП – детектор закладних пристроїв;

СВС – система відеоспостереження;

ПС – пошукова система;

ГШ – генератор білого шуму;

ОТЗ – організаційно-технічні заходи.

Характеристика механізмів захисту, що складають систему

Камера відеоспостереження			
Назва	Кут огляду	Роздільна здатність	ціна
Reolink RLC-810A	90	3840x2160	8 600
Пошукова система			
Назві	Діапазон частот	Цифрові стандарти	ціна
Delta X 100/12	100 кГц-12400 МГц	GSM, 3G, 4G/LTE, 5G (<6GHz), Bluetooth, Wi-Fi, DECT	350 000
Широкосмуговий сканер			
Назва	Діапазон частот	Чутливість	ціна
BugHunter Professional BH-02	50-3000 МГц	≤ 50 мВ/м	10000

Шредер				
Назва	Рівень безпеки	Розмір фрагментів	Швидкість роботи	Ціна
Шредер DA MDM215	P5	2 x 15 мм	2.5 м/хв	27 000

Елемент	Ціна
Камера схову	12 0000
Екранування	200 000