

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

КОЛЕСОВ ІВАН СЕРГІЙОВИЧ

Допускається до захисту:

в. о. завідувача кафедри
прикладної математики та кібербезпеки,
д – р філософії з математики,

_____ А.В.Луценко

«__» _____ 20__ р.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:

Канд. техн. наук, доцент,

Старший викладач кафедри прикладної
математики та кібербезпеки,

Чернов Д.В.

Оцінка: ____ / ____ / ____

(бали за шкалою ЄКТС/за національною
шкалою)

Голова ЕК: _____

(підпис)

Вінниця - 2024

АНОТАЦІЯ

Колесов І. С. Захист інформації від витоку технічними каналами.
Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У даній кваліфікаційній (бакалаврській) роботі розглянуті питання технічного захисту інформації в приміщенні офісу комунального підприємства Вінницької міської ради та використання всіх існуючих рішень. Проаналізовано можливі канали витоку інформації на об'єкті та вироблені способи її запобігання.

Ключові слова: технічні канали витоку інформації, витік інформації, захист інформації в приміщенні. 40 с., 13 рис., 22 джерела.

ANNOTATION

Koliesov I. S. Protection of information from leakage through technical channels.
Specialty 125 "Cyber Security". Vasyl Stus Donetsk National University, Vinnytsia, 2024.

In this qualification (bachelor's) work, the issues of technical protection of information in the premises of the office of the utility company of the Vinnytsia City Council and the use of all existing solutions are considered. Possible channels of information leakage at the facility were analyzed and ways to prevent it were developed.

Keywords: technical channels of information leakage, information leakage, information protection in the premises. 40 pages, 13 figures, 22 sources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП.....	5
РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ	6
1.1. Технічний захист інформації.....	6
1.2. Загальне поняття технічних каналів витоку інформації	7
1.3. Кваліфікація технічних каналів витоку інформації	10
1.4. Технічні канали витоку мовної інформації	12
1.4.1. Акустичні канали витоку інформації	14
1.4.2. Акустовібраційні канали витоку інформації.....	15
1.4.3. Акустоелектричні канали витоку мовної інформації	16
1.4.4. Акустоелектронні канали витоку інформації.....	17
1.5. Технічні канали витоку інформації, що обробляються основними технічними засобами та системами	18
1.5.1. Канал побічних електромагнітних випромінювань ОТЗС	18
1.5.2. Канал наведень на лінії допоміжних технічних засобів та системах ..	19
1.5.3. Канал високочастотного нав'язування	20
РОЗДІЛ 2. ОПИС ПРИМІЩЕННЯ, В ЯКОМУ МОЖЛИВИЙ ВИТІК ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ	22
2.1. Обстеження приміщення	22
2.2. Опис діяльності підприємства “Центр”	23
2.3. Контрольована зона та існуючі ризики витоку інформації	25
РОЗДІЛ 3. СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ПРИМІЩЕННІ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ	29
3.1. Засоби для захисту інформації в кабінеті керівника	29
3.2. Захист інспекторської зали	31
3.3. Захист інформації від зйому направленим мікрофоном	33
3.4. Захист інформації від витоку лініями електромереж.....	35
ВИСНОВКИ	37
СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ	38

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ТЗІ – Технічний захист інформації

ОТЗС – Основні технічні засоби та системи

ДТЗС – Допоміжні технічні засоби і системи

ОІД – Об’єкт інформаційної діяльності

КЗ – Контрольована зона

ізОД – Інформація з обмеженим доступом

ТКВІ – Технічний канал витоку інформації

ЗТР – Засоби технічної розвідки

ПЕМВ – Побічні електромагнітні випромінювання

ВСТУП

Актуальність теми дослідження

З розвитком технологій та широким поширенням цифровізації, захист інформації стає одним із найважливіших аспектів інформаційної безпеки. Сучасні організації стикаються з численними викликами, оскільки кількість і складність загроз зростають. Кіберзлочинці використовують дедалі витонченіші методи, а атаки стають більш організованими та руйнівними. Важливо не лише захищатися від зовнішніх загроз, таких як хакерські атаки, віруси та фішинг, але й звертати увагу на можливі витoki інформації через технічні канали всередині приміщень. Окрім кіберзагроз, існують менш очевидні, але не менш небезпечні ризики витоку інформації через фізичні канали. Кожен із цих типів витоків може призвести до серйозних наслідків для організацій.

Враховуючи масштаби та серйозність можливих витоків, важливо розробляти комплексні рішення для захисту від усіх видів технічних загроз. Таким чином, сучасні технології та методи захисту інформації повинні розглядати усі можливі вектори атак та забезпечувати комплексну безпеку для захисту конфіденційної інформації всередині приміщень.

Мета роботи – організація захисту звукової інформації в приміщенні.

Завдання дослідження:

1. Аналіз технічних каналів витоку звукової інформації;
2. Моделювання можливих сценаріїв витоку звукової інформації з об'єкту інформаційної діяльності
3. Розробити систему захисту, використовуючи різний спектр методів та технологій

Об'єкт дослідження – процеси витоку інформації технічними каналами.

Предмет дослідження – засоби захисту інформації від її витоку технічними каналами.

РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

1.1. Технічний захист інформації

Технічний захист інформації (ТЗІ) - це діяльність, спрямована на забезпечення конфіденційності, цілісності та доступності інформації за допомогою інженерно-технічних заходів.

Інформаційна система - це організаційно-технічна система, яка реалізує інформаційні технології та включає в себе автоматизовану систему, комп'ютерну мережу або систему зв'язку. Вона складається з:

- обчислювальної системи;
- фізичного середовища;
- персоналу;
- оброблюваної інформації.

Конфіденційність - це здатність інформації бути захищеною від несанкціонованого доступу.

Цілісність - це здатність інформації бути захищеною від несанкціонованого зміни, руйнування або знищення.

Доступність — це здатність інформації бути захищеною від несанкціонованого блокування.

Витік інформації - це неконтрольоване розповсюдження даних, що призводить до їх незаконного отримання.

Однією з найбільш серйозних загроз для інформації, яка передається або обробляється на об'єктах інформаційної діяльності чи за допомогою технічних засобів, включаючи інформаційні (автоматизовані), телекомунікаційні, інформаційно-телекомунікаційні системи, є витік інформації через технічні канали. Такі витіки можуть мати значні наслідки для безпеки даних та загальної інформаційної безпеки організації [1].

1.2. Загальне поняття технічних каналів витоку інформації

Технічний канал витоку інформації - сукупність джерела інформації, лінії зв'язку (середовища поширення), по якій поширюється інформаційний сигнал, шумів, які перешкоджають передачі сигналу в лінії зв'язку, і технічних засобів перехоплення інформації (рис.1.1) [2].

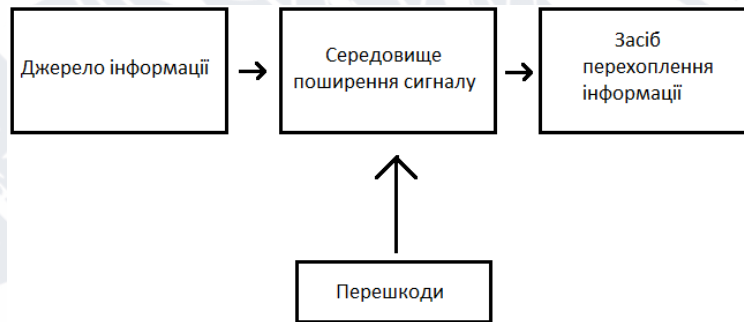


Рисунок 1.1 - Технічний канал витоку інформації

Витік інформації відбувається через певний канал витоку. Зловмисники зазвичай використовують технічні засоби розвідки, тому ці канали називаються технічними каналами. Технічний канал витоку інформації складається з декількох ключових компонентів [3]:

- 1) Джерело інформації: Це будь-який носій, що містить конфіденційні дані. До джерел інформації належать:
 - Голосовий апарат людини: Наприклад, розмови співробітників в офісі.
 - Випромінювачі систем звукопідсилення: Мікрофони, динаміки, аудіосистеми.
 - Текст, що друкується: Принтери, друкарські машини.
 - Радіопередавальні пристрої: Будь-які пристрої, що передають дані через радіохвилі.
 - Інші електронні пристрої: Комп'ютери, мобільні телефони, планшети.
- 2) Лінія зв'язку (середовище поширення): Це середовище, через яке передається інформаційний сигнал. Середовища поширення можуть включати:

- Повітряне середовище: Використовується для передачі радіохвиль, звукових хвиль.
- Водне середовище: Використовується для передачі звукових хвиль під водою.
- Фізичні середовища: Включають хімічні речовини, струмопровідні та пружні матеріали.
- Лінії електроживлення та зв'язку: Лінії електроживлення, заземлення, лінії зв'язку, сигналізації, управління.
- Інженерні комунікації: Спорудження, огорожувальні будівельні конструкції, світлопроникні елементи (вікна, двері), ґрунт, поверхня земної кори, рослинність.

3) Шуми, які перешкоджають передачі сигналу: Будь-які перешкоди, які знижують якість сигналу або роблять його менш помітним для злоумисників. Шуми можуть походити від природних або штучних джерел, таких як електромагнітні завади або фоновий шум у приміщенні.

4) Технічні засоби перехоплення інформації: Злоумисники використовують різні технічні засоби для перехоплення інформації, які можуть включати:

- Пристрої для перехоплення електромагнітних випромінювань: Антени, радіоприймачі.
- Акустичні пристрої: Мікрофони, стетоскопи.
- Тепловізори: Пристрої для виявлення теплового випромінювання.
- Оптичні засоби: Лазери, оптичні мікрофони.

Засіб перехоплення інформації – технічний засіб, який призначений для несанкціонованого здобування інформації.

Розглянувши можливі витoki інформації. Можна припустити, що на ОІД проводяться більшість інформаційних робіт, серед яких: накопичення носіїв інформації, мовне озвучування інформації, отримання технічними засобами та

системами інформації, представлення інформації. Витік інформації наведений на рис. 1.2.

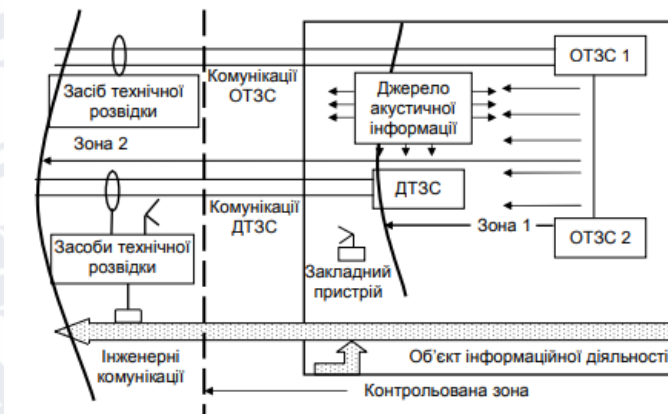


Рисунок 1.2 - Схематична можливість витіку інформації

В рамках інформаційної діяльності на об'єктах інформаційної діяльності (ОІД) можна виділити наступні основні джерела потенційно небезпечного сигналу:

- Людина, від якої надходить інформація у вигляді звуку, а також пристрої для відтворення звуку.
- Технічні засоби, які обробляють інформацію.
- Екрани моніторів електронно-обчислювальної техніки, деякі документи з написаним на них текстом та інші засоби, які відображують інформацію.

Середовища, через які може поширюватися небезпечний сигнал, включають:

- Відкритий простір.
- Комунікаційні мережі основних технічних засобів і систем (ОТЗС) та допоміжних технічних засобів і систем (ДТЗС), які виходять за межі контрольованої зони.
- Інженерні комунікації, які виходять за межі контрольованої зони.

За межами контрольованої зони можна використовувати засоби технічної розвідки, здатні перехоплювати небезпечний сигнал у відкритому просторі або шляхом прямого підключення до комунікацій ОТЗС, ДТЗС чи інженерних мереж. Це означає, що існують всі три складові технічних каналів витоку інформації, що унеможливорює створення деяких з цих каналів.

Основні технічні засоби та системи (ОТЗС) охоплюють обладнання і комунікації, призначені для обробки, зберігання і передачі конфіденційної інформації.

Допоміжні технічні засоби та системи (ДТЗС) включають обладнання, системи і комунікаційні засоби, які не призначені для обробки, зберігання або передачі конфіденційної інформації, але працюють разом з ОТЗС. Сюди відносяться системи радіозв'язку, кондиціонери та сигналізації.

1.3. Кваліфікація технічних каналів витоку інформації

Для організування захисту інформації від витоку технічними каналами їх класифікація здійснюється за певними ознаками, а саме:

- за типом інформаційної діяльності на ОІД,
- за принципом формування сигналу носія інформації,
- за середовищем поширення сигналу,
- за способом знаття сигналу засобами технічної розвідки.

За видом інформаційної діяльності на об'єкті існують такі типи ТКВІ:

- технічні канали витоку мовної інформації,
- технічні канали витоку інформації, що обробляється в ОТЗС,
- технічні канали витоку візуальної інформації,
- матеріально-речовинні канали витоку інформації.

Розглянемо систематизацію ТКВІ за принципами формування небезпечних сигналів, кола поширення небезпечних сигналів і методів перехоплення (зняття) небезпечних сигналів [2].

Технічні канали витоку мовної інформації поділяються на:

- Акустичні канали.
- Акустовібраційні (віброакустичні) канали.
- Акустооптоелектронні (лазерні акустичні) канали.
- Акустоелектричні канали.
- Візуально-оптичний канал витоку мовної інформації
- Канали витоку мовної інформації на основі закладних пристроїв.

Технічні канали витоку інформації, що обробляється в ОТЗС поділяються на:

- Канали побічних електромагнітних випромінювань.
- Канали побічних електромагнітних наведень.
- Канали "паразитної" модуляції сигналів ВЧ генераторів.
- Канали "паразитної" ВЧ генерації підсилювачів.
- Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.
- Канали перехоплення (зняття) інформації з каналів зв'язку.
- Канали ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).
- Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на:

- Візуальні канали.
- Візуально оптичні канали.
- Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації поділяються на:

- Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.

- Добування інформації з чернеток документів, з відходів виробництва, видавничої діяльності, діловодства тощо.
- Хімічні канали.

1.4. Технічні канали витоку мовної інформації

Як вже зазначалось вище, ТКВІ мовної інформації поділяються на:

- Акустичні канали.
- Акустовібраційні (віброакустичні) канали.
- Акустооптоелектронні (лазерні акустичні) канали.
- Акустоелектричні канали.
- Візуально-оптичний канал витоку мовної інформації

Звук має таку природу: коливання голосових зв'язок викликає механічні коливання молекул повітря, що передаються через простір за рахунок збудження коливань сусідніх молекул. Ці коливання називаються акустичними, а їх поширення від джерела інформаційного сигналу за межі контрольованої зони призводить до витоку інформації через акустичну хвилю. В акустичних каналах витоку інформації середовищем передачі мовних сигналів є повітря.

Такого типу коливання називають акустичним коливанням, а його поширення від джерела інформативного сигналу за межі контрольованої зони - спричиняє витік інформації акустичною хвилею. В акустичних каналах витоку інформації середовищем поширення мовних сигналів є повітря.

Витік акустичної інформації за межі огорожувальних конструкцій можливий:

- за рахунок “мембранного ефекту”. обумовлений коливанням тонких (відносно довжини) і відносно легких, елементів огорожувальних конструкцій (віконного скла, фанерних, гіпсокартонних, пластикових перегородок тощо), здатних прогинатися під дією звуку;

- через тріщини, отвори, щілини та інші акустичні отвори, тобто шляхом прямого поширенням 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 огорожувальної конструкції, перетворюється на віброакустичну, тобто в коливання твердих частинок матеріалу без перенесення речовини. Подолавши огорожувальну конструкцію, частина енергії віброакустичних коливань перетворюється на акустичну і випромінюється у вигляді акустичних коливань.

Несанкціоноване ознайомлення із мовною інформацією з метою її подальшого використання є можливим шляхом перехоплення її злоумисниками.

Для цього злоумисник може використовувати широкий арсенал портативних засобів акустичної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електро-акустичним та оптикоакустичним каналами.

Розрізняють два типи акустичних коливань середовища:

- дифузійне середовище, де молекули не мають пружних зв'язків;
- пружне середовище, в якому молекули жорстко та зв'язані між собою.

Коли канали витоку інформації утворюються в результаті поширення акустичних хвиль тільки в дифузійному середовищі, їх називають акустичними каналами витоку.

Якщо ж канали витоку виникають через поширення акустичних хвиль у пружному середовищі, вони називаються акустовібраційними (віброакустичними) каналами витоку інформації.

1.4.1. Акустичні канали витоку інформації

Акустичні канали створюються шляхом перехоплення мовних сигналів (акустичних полів) з об'єктів інформаційної діяльності (ОІД) за допомогою акустичних мікрофонів направленої дії або акустичних антен технічної розвідки. Ці пристрої розташовуються за межами контрольованої зони (КЗ), зазвичай в зоні прямої видимості до вікон або інших отворів приміщення ОІД.

Якщо ОІД являє собою приміщення, огорожене стінами з вікнами та дверима, стелею і підлогою, то акустичні хвилі можуть поширюватися через ці конструкції завдяки:

1. Парусності огорожувальних конструкцій. Якщо огорожувальна конструкція не достатньо масивна, то під дією акустичного тиску вона починає коливатися як мембрана акустичної системи та створює звуковий тиск за межами Об'єкту інформаційної діяльності.

2. Щілин (замкові отвори в дверях, щілини між дверми або рамами вікон та коробкою), мікрощілин (тріщини швів панелей, штукатурки), технологічні вікна, вікна вентиляції, тощо.

Поширення акустичних хвиль через щілини залежить від їх розмірів і форми. Чим довша щілина і менша її поперечна ширина відносно довжини хвилі, тим більше відбувається згасання сигналу. Великі отвори дозволяють акустичним сигналам проходити майже без перешкод.

Якщо контрольована зона невелика, а інколи і обмежена стінами приміщення, противник може використати ЗТР з направленими мікрофонами та перехопити інформативний сигнал.

Якщо контрольована зона обмежена невеликим простором або стінами приміщення, зловмисник може скористатися технічними засобами розвідки з направленими мікрофонами для перехоплення інформаційних сигналів. Коли необхідно підслухати розмови в приміщенні, доступ до якого, як і до сусідніх приміщень, неможливий, застосовуються спрямовані мікрофони та лазерні акустичні системи.

1.4.2. Акустовібраційні канали витоку інформації

Сутність акустовібраційних (віброакустичних) каналів витоку полягає у тому, що акустична хвиля інформативного сигналу, впливаючи на поверхню з твердого матеріалу (пружного середовища), спричиняє вібрацію - коливання його молекул, яке, в залежності від густини матеріалу, може поширюватись на досить великі відстані. Чим більша густина, тим більша дальність поширення сигналу. Класифікують такі основні види засобів технічної розвідки:

- малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки;
- спрямовані мікрофони;
- електронні стетоскопи;
- електронні пристрої для перехоплення мовної інформації (закладні пристрої) з мікрофонними та контактними датчиками передають перехоплену інформацію за допомогою радіоканалів, оптичних каналів (у інфрачервоному діапазоні хвиль), ультразвукових каналів, мереж електроживлення, телефонних ліній зв'язку, з'єднувальних ліній допоміжних технічних засобів або спеціально прокладених ліній;
- оптико-електронні (лазерні) акустичні системи та ін.

Портативні звукозаписувальні пристрої та закладні пристрої з мікрофонними датчиками (перетворювачі акустичних сигналів, що поширюються в повітряному та газовому середовищах) можуть бути встановлені під час неконтрольованого перебування посторонніх осіб безпосередньо в охоронюваних приміщеннях. Ця апаратура здатна реєструвати розмови середньої гучності на відстані 10-15 метрів від джерела звуку.

Електронні стетоскопи та закладні пристрої з контактними датчиками дозволяють перехоплювати мовну інформацію без фізичного доступу "агентів" до захищеного приміщення об'єкта інформаційної діяльності (ОІД).

На ОІД, де озвучується інформація, такими твердими тілами та пружними середовищами є конструкції приміщення (стіни з дверима та вікнами) та деякі

інші предмети інтер'єру, що піддаються змінному акустичному тиску, виходять за межі ОІД або мають щільний контакт з предметами за межами ОІД.

1.4.3. Акустoeлектричні канали витоку мовної інформації

Акустoeлектричні канали витоку виникають в результаті паразитного перетворення акустичних сигналів в електричні в елементах ДТЗС за принципом мікрофонного ефекту.

Практично в усіх електронних елементах в тій чи іншій мірі проявляється ефект акустoeлектричного перетворення.

Закладні пристрої для створення каналів витоку встановлюються переважно біля місць можливого витоку мовної інформації:

- мікрофонного типу (біля виходів кондиціонерів та вентиляційних каналів);
- контактного типу (перетворювачі віброакустичних сигналів, що поширюються по будівельних конструкціях споруд, інженерних комунікаціях та ін.) на зовнішніх поверхнях будівель, у віконних проїмах та рамах, у суміжних (службових і технічних) приміщеннях за дверними проїмами, на перегородках, трубах систем опалення та водопроводу, коробах вентиляційних та інших систем.

Прикладом прояву ефекту акустoeлектричного перетворення є конструкція електричного дзвінка телефонного апарату, лінії якого виходять за межі КЗ.

При покладеній трубці переговорна частина ТА знаходиться у відключеному стані.

До лінії постійно підключений лише приймач виклику - електромагнітний дзвінок. Такий ефект характерний також і для інших елементів, що містять котушки індуктивності. До них можна віднести реле, електромагніти (в годинниках), тощо.

1.4.4. Акустoeлектронні канали витоку інформації

На сьогодні найнебезпечнішими для витоку мовної інформації є акустооптоелектронні (лазерні акустичні) канали.

Акустооптичний канал формується шляхом віддаленого перехоплення вібраційних коливань поверхонь будівельних конструкцій або предметів інтер'єру ОІД за межами контрольованої зони за допомогою лазерних засобів акустичної розвідки. Ці вібрації викликані акустичним полем, тобто інформативним мовним сигналом. На ОІД, де озвучується інформація, під впливом інформативного акустичного сигналу знаходяться усі предмети.

Особливо небезпечними є предмети з відбивними властивостями, такі як скло або дзеркала. Якщо спрямувати лазерний промінь на таку віброуючу поверхню з-за меж ОІД, він відбиватиметься у вигляді променя, модульованого за амплітудою чи фазою вібраційним сигналом, і продовжить поширюватися далі.

Відбите випромінювання може бути перехоплене на певній відстані, демодульоване зловмисником, що дозволяє відновити початковий мовний сигнал. Найкраще для організації такого каналу підходить дзеркально відбите лазерне випромінювання. Однак на відстанях у кілька десятків або навіть сотень метрів можна використовувати і дифузне відбиття лазерного променя.

Для перехоплення мовної інформації через такі канали застосовуються складні лазерні системи, відомі як «лазерні мікрофони», що працюють переважно в ближньому інфрачервоному діапазоні (0.8-1.6 мкм). Найбільш перспективними є методи вимірювання вібрацій за допомогою лазерних систем з частотною модуляцією, які забезпечують високе співвідношення сигнал/шум.

1.5. Технічні канали витоку інформації, що обробляються основними технічними засобами та системами

Розглянемо шляхи утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами. Найнебезпечнішими для розголошення інформації, що обробляється основними технічними засобами та системами, є канали електромагнітних випромінювань та наведень (канали ПЕМВН).

1.5.1. Канал побічних електромагнітних випромінювань ОТЗС

Канал ПЕМВ ОТЗС виникає внаслідок перехоплення побічних електромагнітних полів приймачами засобів технічної розвідки. Ці поля генеруються навколо провідників та електронних компонентів ОТЗС при проходженні через них інформаційних сигналів і поширюються за межі контрольованої зони. В даному контексті електричний струм виступає як інформаційний сигнал [3].

Обробка та передача інформації у технічних засобах і системах здійснюється за допомогою провідних електричних струмів, які являють собою спрямовані потоки електронів. Оскільки ОТЗС складається з електронних елементів і провідників, навколо яких циркулюють електричні струми, що несуть інформацію, навколо них завжди присутні поля. Ці небажані випромінювання мають побічний характер і тому називаються побічними електромагнітними випромінюваннями.

Ці випромінювання можуть поширюватися у відкритому просторі і бути перехопленими приймачами технічної розвідки за межами контрольованої зони, створюючи таким чином канал ПЕМВ ОТЗС. (рис.1.3).

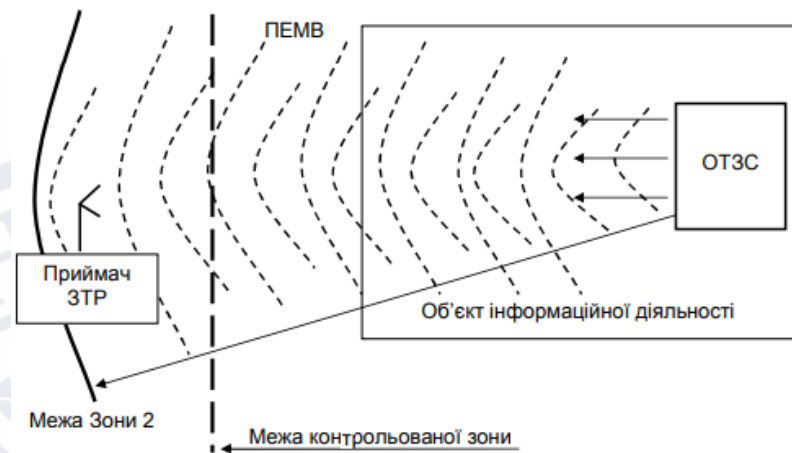


Рисунок 1.3 - Канал ПЕМВ ОТЗ

Запобігання витоку інформації каналом ПЕМВ ОТЗ досягається шляхом [4]:

- екрануванням ОТЗ або локального екранування електронних елементів та провідників ОТЗ;
- просторового електромагнітного зашумлення об'єкту.

1.5.2. Канал наведень на лінії допоміжних технічних засобів та системах

Витік інформації можливий за рахунок наведень електромагнітних випромінювань від ОТЗ на додаткові технічні засоби на ОІД, провідні лінії, розташовані на відносно незначній відстані від ОТЗ та подальше поширення лініями наведених сигналів за межі КЗ.

Крім з'єднувальних ліній ОТЗ і ДТЗС за межі КЗ можуть виходити проводи та кабелі, що до них не відносяться, але вони проходять через приміщення, де встановлені ОТЗ. Такі дроти, кабелі та струмопровідні елементи називаються сторонніми провідниками.

Спільно з заземлювальним пристроєм ДТЗС утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали.

В ґрунті навколо заземлювального пристрою виникає електромагнітне поле, яке також є джерелом інформації.

1.5.3. Канал високочастотного нав'язування

Існує можливість реалізації методів дистанційного знімання мовної ІзОД шляхом ВЧ нав'язування струмопровідними лініями, які виходять за межі КЗ.

Поряд з пасивними способами перехоплення інформації, що обробляється ОТЗ, можливе використання і активних способів, зокрема способу «високочастотного опромінення», при якому ОТЗ опромінюється потужним високочастотним гармонійним сигналом (для цих цілей використовується високочастотний генератор з спрямованою антеною, що має вузьку діаграму спрямованості).

При взаємодії опромінюючого електромагнітного поля з елементами ОТЗ відбувається модуляція вторинного випромінювання інформаційним сигналом. Перевипромінений сигнал приймається на приймальний пристрій засобом технічної розвідки і детектується.

Існує два способи ВЧ-нав'язування, а саме:

- **Контактний.** Високочастотний сигнал вводиться в електричне коло, що має паразитний зв'язок з технічним засобом, і при цьому використовується мікрофонний ефект.
- **Безконтактний.** Потужний ВЧ-сигнал зондує задану область простору.

Технічний канал витоку інформації через високочастотне нав'язування може бути створений шляхом несанкціонованого впровадження високочастотного струму від генератора, підключеного до лінії або кола, що має функціональний зв'язок з нелінійним або параметричним елементом ДТЗС. У цих елементах відбувається модуляція високочастотного сигналу інформаційним сигналом. Інформаційний сигнал з'являється в таких елементах внаслідок електроакустичного перетворення акустичних сигналів у електричні.

Параметричні або нелінійні елементи ДТЗС для високочастотного сигналу зазвичай є неузгодженим навантаженням. Відбитий від цих неузгоджень

промодульований високочастотний сигнал буде поширюватися в зворотному напрямку по лінії або випромінюватися. Для прийому таких відбитих або випромінених високочастотних сигналів використовуються спеціальні високочутливі приймачі.

Принцип роботи полягає у модуляції електромагнітного зонduючого сигналу мовним сигналом, коли вони одночасно впливають на елементи пристроїв, що створюють мікрофонний ефект. Після цього відбувається зворотне перевипромінювання модульованого зонduючого сигналу, його прийом і демодуляція, що дозволяє перехоплювати акустичну інформацію.

Висновки до розділу

Технічний захист інформації є критично важливою складовою загальної системи інформаційної безпеки організації. Його метою є забезпечення конфіденційності, цілісності та доступності інформації шляхом застосування інженерно-технічних заходів. Особливу увагу необхідно приділяти захисту від витоків інформації через технічні канали, які представляють собою фізичні шляхи поширення інформаційних сигналів, що можуть бути використані зловмисниками для несанкціонованого доступу до даних.

Витік інформації через технічні канали може мати серйозні наслідки для безпеки даних і загальної інформаційної безпеки організації. Тому важливо впроваджувати ефективні заходи ТЗІ, які включають регулярний моніторинг та аналіз потенційних каналів витоку, застосування відповідних технічних засобів захисту та забезпечення постійного контролю доступу до чутливої інформації.

РОЗДІЛ 2. ОПИС ПРИМІЩЕННЯ, В ЯКОМУ МОЖЛИВИЙ ВИТІК ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

2.1. Обстеження приміщення

Приміщення об'єкта інформаційної діяльності (ОІД), щодо якого спрямовані дії з метою захисту інформації від витоку технічними каналами, розташоване на другому поверсі будівлі по вулиці Соборній у місті Вінниця (рис.2.1). Цей ОІД є частиною підприємства, що має назву “Центр”.

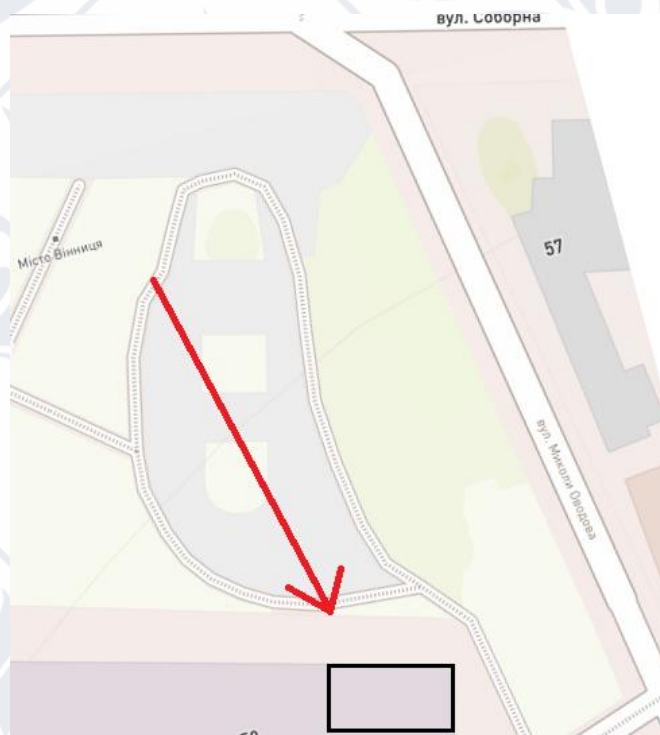


Рисунок 2.1 - Схема загального розташування будівлі

ОІД знаходиться на другому поверсі, що з одного боку забезпечує певну віддаленість від землі, але з іншого боку, створює ризики через можливий доступ злоумисників з вулиці.

Вікна ОІД виходять безпосередньо на вулицю, що може представляти потенційний ризик для перехоплення інформації через використання оптичних засобів або лазерних мікрофонів з боку злоумисників.

2.2. Опис діяльності підприємства “Центр”

Підприємство "Центр" спеціалізується на моніторингу та управлінні дорожньою ситуацією в місті Вінниця. Основне завдання підприємства полягає у відстеженні поточної ситуації на автомобільних дорогах з метою забезпечення безпеки та ефективності дорожнього руху. Для реалізації цієї задачі використовуються камери відеоспостереження, розташовані в різних точках міста, що дозволяє отримувати відеоінформацію в режимі реального часу.

Основні функції підприємства "Центр" охоплюють кілька ключових напрямків діяльності, що сприяють забезпеченню безпеки на автомобільних дорогах та тротуарах міста Вінниця.

Моніторинг стану автомобільних доріг міста здійснюється за допомогою розгалуженої мережі камер відеоспостереження. Ці камери стратегічно розміщені на основних вулицях та транспортних розв'язках, що дозволяє оператору "Центру" отримувати в реальному часі відеоінформацію про поточну дорожню ситуацію. Основними функціями в межах цього напрямку є фіксація дорожньо-транспортних пригод (ДТП), що дозволяє оперативно реагувати на інциденти та зменшувати їхні наслідки. Виявлення та реєстрація заторів допомагає у плануванні дорожнього руху та мінімізації затримок для водіїв. Окрім того, постійний моніторинг інших подій, що можуть впливати на безпеку та пропускну спроможність доріг, дозволяє вчасно вжити заходів для підтримання оптимального руху транспорту.

Інформаційне обслуговування є важливою складовою діяльності підприємства. "Центр" надає оперативну та достовірну інформацію державним органам та іншим зацікавленим сторонам. Це включає інформування відповідних органів, таких як поліція, служби порятунку та міська адміністрація, для прийняття оперативних рішень. Завдяки цьому можливо швидко реагувати на надзвичайні ситуації та забезпечувати безпеку міста. Окрім того, "Центр" готує та надає аналітичні звіти та рекомендації на основі зібраної інформації. Ці звіти допомагають у довгостроковому плануванні та розробці стратегій для

покращення дорожньої інфраструктури і управління рухом, що в свою чергу підвищує загальну ефективність транспортної системи міста.

Підприємство працює 5 днів на тиждень, з понеділка по п'ятницю, з 8:00 до 17:00. Прибирання приміщення відбувається в будні дні з 7:30 до 8:00, що дозволяє забезпечити чистоту та порядок перед початком робочого дня.

Територія будівлі охороняється цілодобово, що забезпечує високий рівень безпеки. При вході до будівлі знаходиться охоронець, який є працівником підприємства "Центр". Вхід до приміщень здійснюється за допомогою ключ-карт, що обмежує доступ сторонніх осіб. Приміщення має два входи, що дозволяє регулювати потік людей та забезпечити додатковий рівень контролю.

У "Центрі" працює 16 працівників, кожен з яких виконує конкретні функції, забезпечуючи ефективність роботи підприємства:

- Керівник (1 людина): Відповідає за загальне керівництво та управління підприємством, приймає стратегічні рішення та контролює їх виконання.
- Заступник керівника (1 людина): Допомогає керівнику в управлінні підприємством, виконує обов'язки керівника в його відсутність.
- Секретар (1 людина): Веде діловодство, координує зустрічі та виконує адміністративні завдання, забезпечує інформаційну підтримку керівника та заступника керівника.
- Оператори (10 людей): Відповідають за моніторинг відеокамер та обробку отриманої інформації, фіксують та реєструють події на дорогах, повідомляють про них відповідні служби.
- Охоронці (2 людини): Забезпечують безпеку приміщення та контроль доступу, працюють у змінному режимі, забезпечуючи цілодобову охорону.
- Прибиральниця (1 людина): Забезпечує чистоту та порядок у приміщеннях підприємства, проводить прибирання у визначений час перед початком робочого дня.

Завдяки злагодженій роботі команди та впровадженню сучасних технологій, підприємство "Центр" ефективно виконує свої завдання з моніторингу дорожньої ситуації та забезпечення безпеки на дорогах міста Вінниця.

2.3. Контрольована зона та існуючі ризики витоку інформації

Контрольована зона обмежена територією об'єкта інформаційної діяльності (ОІД). ОІД обладнано системою пожежної сигналізації, системою контролю доступу та камерами спостереження. На території ОІД знаходяться декілька видів систем комунікацій, які розписані у таблиці 2.1.

Таблиця 2.1 – Системи комунікації

Електроживлення	Підключено до підстанції для обслуговування споживачів.
Телефонна лінія	Підключена до «Vodafone», на офіс виділено два номери (для ресепшену, консультацій телефоном, приймальні керівника, керівника). Виходить за межі контрольованої зони.
Система водопостачання	Підключена до міського водоканалу, що виходить за межі контрольованої зони (пластикові труби, однотрубна система водопостачання).
Система вентиляції	Припливно-витяжна, штучна.

Об'єкт інформаційної діяльності складається з чотирьох приміщень: робочої інспекторської зали, кабінету керівника, кабінету для переговорів та санвузла. Робоча інспекторська зала є основним приміщенням, де виконуються повсякденні робочі завдання інспекторів. Вона обладнана робочими місцями, необхідною оргтехнікою та меблями, що забезпечують комфортні умови для

роботи співробітників. Кабінет керівника призначений для роботи керівника підприємства. Він обладнаний меблями для роботи та зберігання документів, а також технікою, необхідною для виконання управлінських функцій. Тут проводяться наради, прийом відвідувачів та вирішуються адміністративні питання. Кабінет для переговорів призначений для проведення зустрічей, нарад та переговорів. Санвузол – це приміщення, обладнане для гігієнічних потреб співробітників (Рис. 2.2).

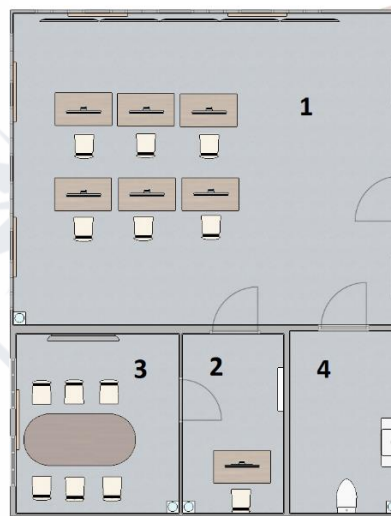


Рисунок. 2.2 - План приміщення ОІД

Таблиця 2.2 – нумерація приміщень підприємства

Номер	Назва приміщення
1	Робоча інспекторська зала
2	Кабінет керівника
3	Кабінет переговорів
4	Санвузол

Аналізуючи приміщення, характеристики та властивості ОІД, можна виділити деякі ризики витоку інформації.

1. Зловмисники можуть отримувати інформацію за допомогою спрямованих мікрофонів – спеціальних пристроїв, які дозволяють

прослуховувати слова з відстані десятків метрів. Ці мікрофони здатні вловлювати навіть слабкі звукові коливання, що робить їх ефективними для перехоплення розмов у приміщеннях, розташованих поруч із зовнішніми стінами чи вікнами.

2. У кабінеті керівника можуть відбуватись ділові зустрічі з сторонніми особами, що створює ризик підслуховування розмов або їх запису на звукопереносні пристрої. Зловмисники можуть застосувати різні заходи, такі як:
 - Телефонне вухо: Спеціальний пристрій, який підключається до телефонної лінії та дозволяє прослуховувати розмови.
 - Диктофон: Маленькі, приховані диктофони можуть бути залишені в приміщенні для запису розмов.
 - Провідний мікрофон: Мікрофони можуть бути заховані у кабінеті або поруч з ним, щоб записувати розмови.
3. Зловмисники можуть збирати інформацію, використовуючи стетоскопи – прилади, що знімають вібрації будівельних конструкцій, які виникають через розмову в приміщенні, та перетворюють їх на електричні сигнали звуку. Ці сигнали можна потім прослуховувати. Оскільки ОІД межує з вулицею, ймовірність прослуховування таким чином дуже висока.
4. Перехоплення інформації може здійснюватись за допомогою лазерного або інфрачервоного детектора. Цей метод не вимагає близького наближення до об'єкта розвідки і може виконуватись на відстані. Наприклад, під час розмови в приміщенні спостерігається дуже незначна вібрація віконного скла, викликана повітряними звуковими хвилями. Віконне скло модулюється цією розмовою. Якщо з протилежної будівлі на скло спрямувати лазерний промінь і отримати відображення, усі розмови можна почути та записати. Оскільки ОІД межує з вулицею і має віконні прорізи, ризик отримання інформації таким способом досить високий.

Висновки до розділу

У цьому розділі було досліджено ОІД підприємство "Центр", включаючи розташування та безпеку об'єкта інформаційної діяльності (ОІД), робочий графік та склад працівників, а також контрольовану зону та існуючі ризики витоку інформації. Було встановлено, що, незважаючи на наявність сучасних систем безпеки, підприємство стикається з кількома потенційними загрозами, пов'язаними з витоком інформації через технічні канали. Для забезпечення максимальної безпеки необхідно впровадити додаткові заходи захисту та підвищити обізнаність працівників про можливі загрози. Загалом, "Центр" ефективно виконує свої завдання, однак потребує вдосконалення системи інформаційної безпеки для зниження ризиків.

РОЗДІЛ 3. СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ПРИМІЩЕННІ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

3.1. Засоби для захисту інформації в кабінеті керівника

Щоб розробити систему захисту від витоку технічними каналами необхідно визначити місця, де буде озвучуватись найбільше важливої інформації. На першу думку спадає кабінет керівника в якому проводяться конференції та зустрічі.

Оскільки стіни кабінету не виходять на вулицю то для забезпечення конфіденційності інформації, яка озвучується в цьому приміщенні, можна зосередитися лише на звукоізоляції стін та дверей, що розділяють цю кімнату від сусідніх приміщень в якому можуть знаходитись відвідувачі “Центру” або інспектори для яких не призначена інформація.

Стіна, що розділяє кабінет переговорів від інших приміщень, повинна мати надійні звукоізоляційні властивості. Окрім стандартних матеріалів, які використовуються у будівництві, можна додатково застосувати спеціальні звукоізоляційні панелі або інші матеріали, що поглинають звук.

Особливу увагу слід приділити дверям, оскільки вони можуть стати слабким місцем у системі звукоізоляції. Для досягнення високого рівня звукоізоляції, двері повинні складатися зі сталевих листів. Проте важливо, щоб між цими листами був прокладений звукоізоляційний матеріал, інакше сталевий лист може посилювати шум, а не зменшувати його.

Хорошим варіантом для звукоізоляції є мембрана Tecsound FT, яка складається з двох пористих шарів войлоку і синтетичного полімерного покриття Tecsound (рис.3.1). Вона не містить бітуму, що забезпечує відмінні звукоізоляційні властивості. Для забезпечення ефективної звукоізоляції внутрішніх і зовнішніх стін необхідно вжити додаткових заходів [8].



Рисунок. 3.1 - Полімерне покриття Tecsound

Для внутрішніх стін рекомендується використовувати конструкції з двома облицюваннями, а замість одинарних каркасів - подвійні. Крім того, слід застосовувати не менше двох чи трьох шарів гіпсокартону (ГКЛ), заповнювати каркаси професійними звукопоглинальними матеріалами та використовувати пружні прокладки між будівельними конструкціями і напрямними профілями [9]. Для зовнішніх стін необхідно обрати відповідні звукоізоляційні матеріали. Зокрема, можна використовувати акустичні панелі з поролону Ecosound Tetras, які мають коефіцієнт звукового поглинання 0,85 (рис. 3.2) [10].

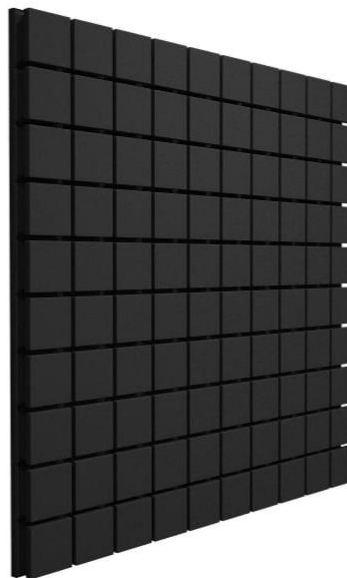


Рисунок. 3.2 – акустична панель Ecosound Tetras

Як вже було вказано раніше, у керівника можуть проходити ділові зустрічі з партнерами, тому необхідно забезпечити захист від потенційно пронесених в кімнату різних звукозаписуючих пристроїв та жучків.

Сучасні смартфони та диктофони, оснащені окремим мікрофоном з функцією шумозаглушення, можуть обійти стандартний акустичний захист від звичайного генератора шуму, для вирішення цієї проблеми можна використовувати ультразвуковий генератор шуму USPD (рис. 3.3).



Рисунок. 3.3 – ультразвуковий генератор шуму USPD

Цей пристрій захищає від практично всіх методів запису та прослуховування (мікрофонів вбудованих; диктофонів цифрових, аналогових, вбудованих у телефони та смартфони; жучків від мережі 220в, wi-fi, bluetooth, та gsm; лазерних пристроїв знімання інформації з вікон, стетоскопів) [11].

3.2. Захист інспекторської зали

Інспекторський зал безпосередньо знаходиться через стіну з коридором, тому важливо також розробити звукоізоляцію стін та дверей.

Оскільки працівники мають доступ до конфіденційної інформації, важливо створити умови, які запобігатимуть її витоку за межі контрольованої зони. Для цього необхідно, щоб кожен працівник, при прийомі на роботу, підписував договір про нерозголошення конфіденційної інформації.

Цей договір покладає на працівника відповідальність за збереження та нерозповсюдження будь-якої конфіденційної інформації, до якої він матиме доступ у процесі своєї діяльності.

Додатково, перед початком кожної робочої зміни, працівники та відвідувачі повинні залишати свої особисті пристрої, такі як мобільні телефони, планшети, ноутбуки та інші електронні гаджети, у спеціальному акустичному сейфі. Ці сейфи мають бути розташовані в охоронюваній зоні, забезпечуючи таким чином їхню безпеку та недоступність для сторонніх осіб.

Варіантом може бути використання ультразвукового сейфу ASU-6. (рис. 3.4). Цей пристрій блокує можливість запису на диктофон та прослуховування будь-якого смартфона. Для захисту від прослуховування потрібно буде лише покласти телефони у пристрій, і через декілька секунд розпочнеться ультразвукова перешкода завдяки якій, розмова стане повністю нерозбірливою. Робота приладу відбувається непомітно, без зайвого шуму, тому його використання залишиться непоміченим [12].



Рисунок. 3.4 – акустичний сейф для захисту від прослуховування ASU-6

Дотримання цих заходів є обов'язковою умовою для допуску працівників до їхніх робочих місць. Це допомагає не лише забезпечити збереження конфіденційної інформації, але й підвищити загальний рівень безпеки в організації.

3.3. Захист інформації від зйому направленим мікрофоном

Як вже описувалось вище, вікна операторської зали та кабінету для переговорів виходять безпосередньо на вулицю, даний факт означає що злоумисники можуть використати це собі на користь. Прикладом може бути аудіозйом інформації завдяки направленим мікрофонам. Оскільки ці мікрофони здатні вловлювати слабкі звукові коливання з відстані десятків метрів, то метод захисту повинен бути своєрідний. Звукоізоляційними вікнами не обійдеся.

Рішенням може бути використання генератора віброакустичного шуму DNG-2300 (Рис. 3.5). Цей пристрій створює шум, що розходить по всьому приміщенню [13]. Зазвичай його використовують разом із віброакустичними та акустичними випромінювачами.



Рисунок. 3.5 – генератор віброакустичного шуму DNG-2300

Генератор виробляє шум, який через підключені вібровипромінювачі та акустичні випромінювачі передається на конструкції і порожнини приміщення. Кількість перетворювачів і динаміків залежить від розмірів приміщення, можливих напрямків звукового спрямування та типу конструкцій (вікна, водопровідні труби, порожнини тощо). Вся захисна система складається з генератору та кількох віброакустичних та акустичних випромінювачів, встановлених у приміщенні на конструкціях і всередині повітряних порожнин.

Вібровипромінювачі передають шум на поверхні та конструкції, зупиняючи поширення звуку крізь них, тоді як акустичні випромінювачі заповнюють звуковими перешкодами порожнини та вентиляційні шахти, запобігаючи витоку звуку через повітря.

Перед встановленням системи потрібно ретельно вивчити приміщення на предмет можливих точок акустичного витоку та визначити найбільш чутливі місця для розміщення перетворювачів і динаміків. Коли генератор працює, вібровипромінювачі передають шум на конструкції, і частина вібрацій передається в повітря, що робить шум чутним для користувача.

Незважаючи на чутність, це лише невелика частина шуму, а основна частина енергії спрямовується в конструкції. Користувач може мінімізувати звукові перешкоди, налаштувавши оптимальний рівень шуму, який достатній для заглушення всіх пристроїв несанкціонованого прослуховування по периметру об'єкта.

Таким чином завдяки генератору віброакустичного шуму та випромінювачам мовну інформацію в приміщенні не зможуть підслухати.

Проти специфічних лазерних мікрофонів ситуація складніше, у подібних мікрофонах промінь відбивається від поверхні і потрапляє у приймач. Звукові хвилі створюють вібрації на поверхні об'єкта, які, своєю чергою, змінюють поведінку відбитого лазерного променя. Ці зміни реєструються приймачем й у результаті перетворюються на звукозапис розмови (рис. 3.6).

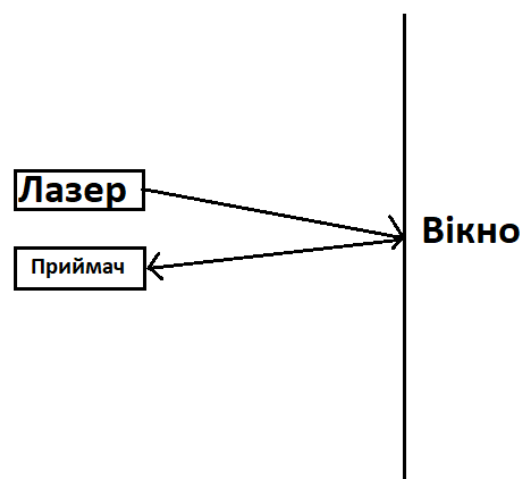


Рисунок. 3.6 - Зйом інформації лазерним мікрофоном

Захист від лазерних мікрофонів є складним завданням. Ці мікрофони використовують лазерний промінь, який відбивається від поверхні і потрапляє в приймач. Звукові хвилі викликають вібрації на поверхні, що змінюють поведінку відбитого лазерного променя. Приймач фіксує ці зміни та перетворює їх на звукозапис розмови.

Для захисту від такого прослуховування можна встановлювати додаткові вібровипромінювачі, але це дорого та створює сильні вібрації в приміщенні, які заважають під час розмов.

Одним з можливих рішень цієї проблеми є використання "захисного лазера", який працює зсередини приміщення (рис. 3.4).

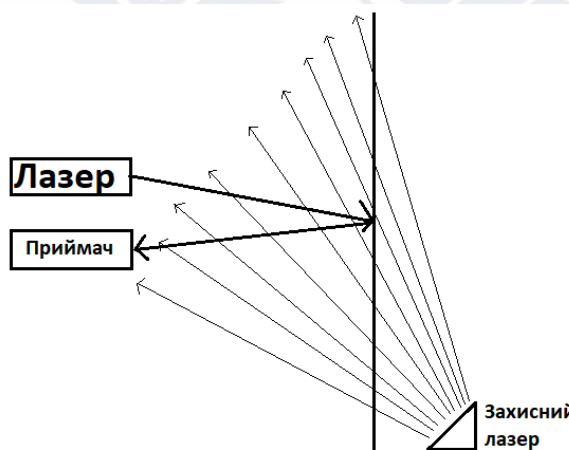


Рисунок. 3.7 – Приклад роботи захисного лазера

Такий лазер надсилає безліч променів на вікно, створюючи перешкоди для лазерного променя зломисників.

3.4. Захист інформації від витоку лініями електромереж

Не слід забувати про те, що на підприємстві встановлені технічні засоби телефонного зв'язку та система пожежної сигналізації. Ці системи включають стаціонарні та мобільні телефони, комутаційне обладнання, а також комплексну систему пожежної сигналізації.

Важливо враховувати, що ці засоби можуть стати джерелом витоку інформації через акустoeлектричний канал завдяки якому, зловмисники зможуть перехопити конфіденційну інформацію. Для захисту цього каналу потрібно використовувати:

- технічні засоби захисту в лініях ДТЗС, що затримують сигнали низького рівня;
- використання лінійного зашумлення.

Можна використати пристрій для захисту ліній електромереж Базальт-2ГС (рис. 3.7).



Рисунок. 3.7 - Захисний пристрій Базальт-2ГС

Пристрій призначений для захисту об'єктів від витоку мовної інформації з електромережі [15]. Забезпечує захист за допомогою придушення псевдовипадкової перешкодою акустoeлектричних перетворень і сигналів, що прослуховують і передають пристроїв, які можуть бути підключені до електромережі.

Живлення пристрою та подача псевдовипадкової перешкоди в мережу забезпечується через один стандартний шнур живлення. Пристрій формує вихідну напругу постійного струму живлення інших приладів.

Висновки до розділу

Враховуючи специфіку приміщення, було розроблено систему захисту інформації від витоку через технічні канали, використовуючи найефективніші засоби захисту. До цієї системи включено широкий спектр методів та технологій, спрямованих на мінімізацію ризиків та забезпечення максимальної безпеки інформаційних ресурсів.

ВИСНОВКИ

У ході роботи було розглянуто технічні канали витоку звукової інформації, яка озвучується в обстежуваному приміщенні. Було проаналізовано різні процеси, що можуть сприяти несанкціонованому витоку інформації за межі підприємства. Серед таких процесів були визначені:

- передача звукових хвиль через стіни, підлоги, стелі та системи вентиляції акустичними каналами;
- перетворення звукових коливань на електричні сигнали в кабелях і електронних компонентах акустоелектричними каналами;
- поширення вібрацій від звукових хвиль через конструктивні елементи будівлі, такі як стіни і стелі віброакустичними каналами;
- використання оптичних технологій для підслуховування, наприклад, лазерних мікрофонів, які зчитують вібрації зі скла вікон оптичними каналами;

На основі ідентифікованих каналів витоку та враховуючи специфіку приміщення, була розроблена система захисту інформації. Ця система включає в себе спектр методів та технічних засобів для забезпечення безпеки конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. ДСТУ 3396.2-97 [Електронний_ресурс] Режим доступу: <https://tzi.com.ua/478.html>
2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс]. Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content>
3. Прокоф'єв М. І., Стеченко В. М. Особливості оцінки рівня наведень побічних електромагнітних випромінювань в мережі електроживлення// Спеціальна техніка у правоохоронній діяльності. Матеріали 1У Міжнародної науково-практичної конференції (Україна, Київ, 26-27 листопада 2009 року)// с.195-196.
4. В. Стеченко, М. Прокоф'єв, Особливості розповсюдження сигналів ПЕМВН у мережі електроживлення і заземлення на високих частотах // XIII Міжнародної науково-практичної конференції, Київ, 2010р., с. 81–82.
5. В. Куліш, М. Прокоф'єв, В. Стеченко. Ще раз до проблеми захищеності мережі електроживлення // XIV Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах», Київ: 17–20 травня тези доповідей, 2010р., с. 57–58
6. Технічні канали витоку інформації [Електронний ресурс]. Режим доступу: <https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html>
7. Методики оцінки інформаційної захищеності телекомунікацій [Електронний_ресурс] Режим доступу до ресурсу : <https://metod.suitt.edu.ua/download/549>
8. Мембрана Tecsound [Електронний_ресурс] Режим доступу: <https://www.tecsound.com.ua/ru/products/tecsound-ft-40-75/>
9. Ефективна звукоізоляція. Основні правила [Електронний_ресурс] Режим доступу: <https://www.acoustic.ua/recommendations/743>

10. Панель Ecosound [Електронний_ресурс] Режим доступу:
<https://ecosound.kiev.ua/akusticheckii-diffuzor-tetras-wood-black>
11. Ультразвуковий генератор шуму [Електронний_ресурс] Режим доступу:
<http://gdekupit.com.ua/ultrazvukovoj-generator-shuma-uspd.html>
12. Захист від прослуховування мобільного телефону [Електронний_ресурс]:
<https://i-safe.com.ua/ua/p1808488790-akusticheskij-sejf-asu.html>
13. Генератор шуму USPD [Електронний_ресурс] Режим доступу:
<http://gdekupit.com.ua/ultrazvukovoj-generator-shuma-uspd.html>
14. Пристрій захисний Базальт 2-ГС [Електронний_ресурс] Режим доступу:
<https://usts.kiev.ua/prystrij-zakhysnyj-bazalt-2hs/>
15. Прокоф'єв М. І., Стеченко В. М. Дослідження поширення високочастотних сигналів в мережі електроживлення, „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, Випуск 2 (19) 2009, К., с. 88-94.
16. M. Tanaka, "High frequency noise power spectrum, impedance and transmission loss of power line in japan on intrabuilding power line communications,"IEEE Transactions on Consumer Electronics, vol. 34, no. 2, pp. 321--326, May 1988.
17. Radio noise. Recommendation ITU-R P.372-7, International Telecommunication Union, Geneva, 2001.
18. M. Prokofjev, V. Stechenko. Propagation of high frequency signals inducing in the power supply wires // "10th anniversary international scientific Conference "UNITEH'10 GABROVO", 19–20 November 2010, Proceeding, Volume 1, с. 1-148–1-154.
19. Journal of Electrical and Computer Engineering Volume 2013 (2013), Article ID 712376, 16 pages
20. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 29.08.2012 № 472.

21. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. Київ, 2016, 104с.
22. Combes P. F., and Mamesta H. J. The “Very-Near-Field” Region of Equiphas Radiating Apertures. IEEE Antennas @ Propagation Magazine, V. 47, N 4, 2005, p. 50 – 66.