Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Дерезенко Антона Вячеславовича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи протидії акустичним прихованим каналам витоку інформації*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	доц. к.е.н. Пілова Д.П.	92	Вілмінно	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Дерезенко А.В.* **Академічної групи** **125м-22-2**
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***
за освітньо-професійною програмою ***Кібербезпека***
на тему ***Методи протидії акустичним прихованим каналам витоку інформації***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-С

Розділ	**Зміст**	**Термін виконання**
Розділ № 1	*Огляд прихованих каналів витоку інформації, аналіз закону України та постановка задачі.*	15.11.2023
Розділ № 2	*Розробка моделі загроз, рекомендації щодо методів протидії.*	05.12.2023
Розділ № 3	*Розрахунок витрат пов'язаними з впровадженням методів захисту*	12.12.2023

Завдання видано_____ Кручінін О.В.
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Дерезенко А.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка:79 ст ,17 рис.,9 табл.,5 додатків,15 джерел

Предмет дослідження: розробка та аналіз заходів, спрямованих на запобігання або ускладнення несанкційованого витоку інформації через акустичні канали.

Методи дослідження: спостереження, аналіз, опис.

Мета проекту: Основною метою є аналіз моделі загроз та розробка методів протидії акустичним прихованим каналам витоку інформації. Це включає в себе ідентифікацію потенційних загроз, що випливають із використання акустичних прихованих каналів, а також розробку стратегій для мінімізації цих загроз.

Перша частина описує різні типи прихованих каналів, необхідність заходів протидії, підкреслюється значення законодавства яке встановлює правові основи для захисту інформації. Особливу увагу приділено акустичним каналам витоку інформації, які включають широкий спектр звукових сигналів. Вказано на потенційні "сліпі зони" в системах безпеки, де такі канали часто ігноруються, що може призвести до витоку конфіденційної інформації

Другий розділ описує загальну модель загроз, методи протидії акустичним прихованим каналам витоку інформації які були представлені у першому розділі та загальні поради щодо протидії цим каналам.

У третьому розділі розраховано витрати на впровадження даного методу протидії акустичним прихованим каналам витоку інформації, прорахована економічна доцільність створення та використання методів протидії цим атакам.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПРИХОВАНІ АКУСТИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МЕТОДИ ПРОТИДІЇ

ABSTRACT

Explonetory note:79 p.,17 fig.,9 tables,5 applications,15 sources.

Research Subject: Development and analysis of measures aimed at preventing or complicating unauthorized information leakage through acoustic channels.

Research methods: observation, analysis, description.

Project Goal: The main goal is to analyze the threat model and develop methods for counteracting acoustic hidden channels of information leakage. This includes identifying potential threats from the use of acoustic hidden channels and developing strategies to minimize these threats.

The first part describes various types of hidden channels, the necessity of countermeasures, highlighting the importance of legislation that establishes the legal framework for information protection. Special attention is given to acoustic channels of information leakage, encompassing a broad spectrum of sound signals. It points out potential "blind spots" in security systems where such channels are often overlooked, which could lead to the leakage of confidential information.

The second section outlines the general threat model, methods of counteracting acoustic hidden channels of information leakage as presented in the first section, and general recommendations for countering these channels.

The third section calculates the costs of implementing this method of counteracting acoustic hidden channels of information leakage and evaluates the economic feasibility of creating and using methods to counter these attacks.

INFORMATION SECURITY, SOUND COVERT CHANNELS OF INFORMATION LEAKAGE, THREAT MODEL, COUNTERMEASURES METHODS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ГП- графічний процесор

НД ТЗІ - нормативний документ технічний захист інформації

ОЗП - оперативний запам'ятовуючий пристрій

ПЗ - програмне забезпечення

ЦП - центральний процесор

ЗМІСТ

ВСТУП

Вплив сучасних технологій на наше життя не може бути переоцінений, і в цифровому світі конфіденційність і безпека інформації стають багатошаровими викликами. Серед загроз безпеці даних особливе місце посідають акустичні приховані канали витоку інформації. Ці канали використовують звукові сигнали для передачі конфіденційної інформації, часто непомітної для людського слуху, і створюють потенційні ризики для безпеки даних.

Дослідження актуальності та значення проблеми акустичних прихованих каналів витоку інформації та визначає необхідність розробки методів протидії цим загрозам.

Загострена увага на сучасних засобах спілкування, таких як смартфони, веб-камери, мікрофони та інші пристрої, призводить до збільшення можливостей для створення акустичних прихованих каналів. Це може бути використане як для шпигунства, так і для здійснення кібератак, що ставить під загрозу безпеку даних, які передаються через акустичні канали.

У цьому контексті, розробка ефективних методів протидії акустичним прихованим каналам стає надзвичайно важливою. Такі методи повинні забезпечити виявлення та блокування можливих каналів витоку інформації, зменшуючи ризик для безпеки даних і конфіденційності користувачів.

У наступних розділах дослідження ми розглянемо існуючи методи протидії прихованим каналам витоку інформації , їх переваги та недоліки.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз прихованих каналів витоку інформації

Приховані канали витоку інформації - це механізм, який не був призначений для комунікації, але який все ж може бути використаний для передачі інформації з високого рівня доступу до низького.[1] Ці канали особливо небезпечні, оскільки вони можуть бути використані для обходу стандартних засобів безпеки, таких як мережеві фільтри та моніторинг доступу.

Основні типи каналів які використовуються атаках за допомогою прихованих каналів витоку інформації представлені на рис. 1.1

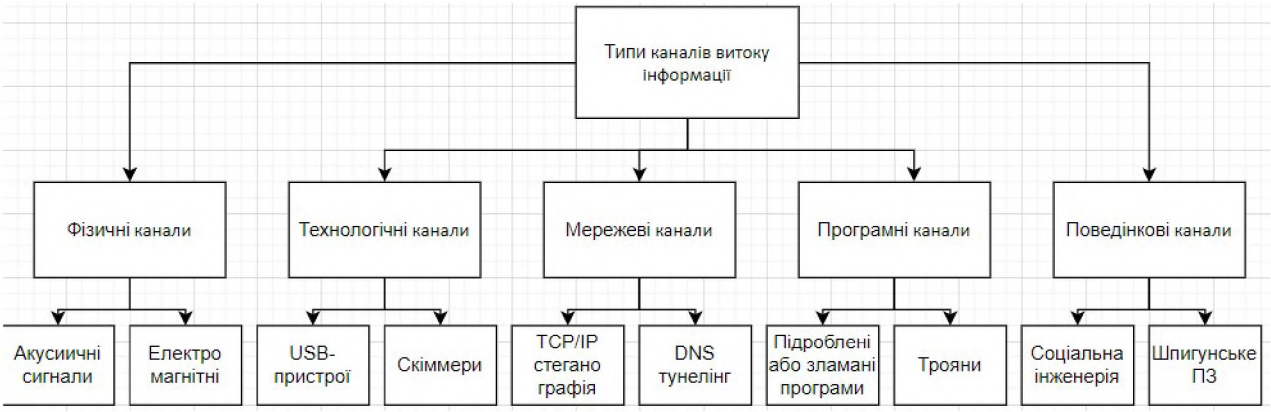

Рисунок 1.1 – Класифікація прихованих каналів витоку інформації

Фізичні канали включають в себе передачу даних через непомітні фізичні сигнали. Наприклад, акустичні канали можуть передавати інформацію через звуки, які не чути людському вуху, але які можуть бути виявлені спеціалізованим обладнанням.

Технологічні канали Включають в себе використання різних технічних засобів. Наприклад, за допомогою USB-пристроїв можливий непомітний витік інформації, коли вони підключені до системи.

Мережеві канали використовують стандартні мережеві протоколи для непомітної передачі даних. Наприклад, через DNS(система доменних імен) тунелювання можна передавати інформацію, маскуючи її під звичайні DNS запити.

Програмні канали включають в себе використання зловмисного ПЗ для витоку інформації. Трояни, наприклад, можуть збирати дані з системи та відправляти їх на віддалений сервер.

Поведінкові канали експлуатують людський фактор. Соціальна інженерія може бути використана для виманювання конфіденційної інформації від працівників або встановлення шпигунського ПЗ.

Переходячи від загального огляду класифікації прихованих каналів витоку інформації до більш спеціалізованої тематики програмних прихованих каналів, ми поглиблюємо наше розуміння різних методів та стратегій, які можуть бути використані для несанкційованої передачі даних. Приховані канали витоку інформації можуть бути розглянуті в широкому спектрі, починаючи від фізичних методів, таких як акустичні та електромагнітні випромінювання, до більш складних і підступних технік, які включають програмне забезпечення та цифрові технології.

Програмні приховані канали представляють собою один з найбільш витончених та складних видів витоку інформації. Ці методи передачі даних використовують звичайне програмне забезпечення або операційні системи для створення каналів, через які конфіденційна інформація може бути передана без відома користувача або адміністратора системи. Вони часто вимагають значних технічних знань та розуміння внутрішньої роботи систем, роблячи їх непомітними для стандартних методів виявлення.

Програмні приховані канали не є новим явищем у світі кібербезпеки. Їх історія налічує десятиліття, починаючи з ранніх днів комп'ютерних мереж та інтернету.

Програмні приховані канали витоку інформації використовують програмне забезпечення або програмні засоби для непомітного екстрагування або передачі даних. Ці методи можуть бути особливо складними для виявлення, оскільки вони часто маскуються під легітимні програмні процеси.

Класифікація цих прихованих каналів надана у табл.1.1

Таблиця 1.1 – Класифікація програмних прихованих каналів

Тип ПЗ	Опис	Приклади
Трояни	Зловмисне ПЗ, що видає себе за легітимну програму.	Спостерігачі за натисканням клавіш,троянські програми для віддаленого доступу
Руткіт(Rootkits)	ПЗ, яке приховує присутність зловмисного ПЗ в системі.	Загрузочні враження,Руткіти на рівні ядра
Бекдор(Backdoors)	Непомітні входи в систему, створені зловмисниками.	Підроблене адміністративне ПЗ.
Набір експлойтів	Набори інструментів для використання вразливостей.	Англер, Експлоіт-набір Нукліар
Зловмисне програмне забезпечення для викрадання даних(Data Exfiltration Malware)	ПЗ, розроблене для крадіжки даних.	Викрадачі інформації, Продвинуті постійні загрози
Захоплення каналу комунікації(Communication Channel Hijacking)	Перехоплення або маніпулювання легітимними комунікаційними каналами.	Атаки типу людина посередині,Захоплення сесії

Троян — шкідливе програмне забезпечення, яке приховує справжню мету своєї діяльності за допомогою маскування. Однак, на відміну від вірусу, він не здатний самостійно копіювати або інфікувати файли. Щоб проникнути на пристрій жертви, загроза використовує інші засоби, такі як приховане

завантаження, використання уразливостей, завантаження іншим шкідливим кодом або методи соціальної інженерії.[2]

Руткіт — це програма або набір шкідливих програмних інструментів, які надають зловмисникові віддалений доступ до комп'ютера або іншої системи та контроль над ними. Хоча цей тип програмного забезпечення має деякі легітимні використання, наприклад, для надання віддаленої підтримки кінцевому користувачу, більшість руткітів відкривають бекдор у системах жертв для введення шкідливих програм — включаючи віруси, програми-вимагачі, програми-кейлогери або інші типи шкідливого програмного забезпечення — або для використання системи для подальших атак на мережеву безпеку. Руткіти часто намагаються уникнути виявлення шкідливих програм, деактивуючи антивірусне та антималюарне програмне забезпечення на кінцевих точках.[3]

Бекдор – це зазвичай прихований метод обходу звичайної аутентифікації або шифрування в комп'ютері, продукті, вбудованому пристрої або його втіленні. Бекдор найчастіше використовуються для забезпечення віддаленого доступу до комп'ютера або отримання доступу до відкритого тексту в криптосистемах. Відтак вони можуть бути використані для отримання доступу до привілейованої інформації, такої як паролі, псування або видалення даних на жорстких дисках, або передачі інформації в автохаотичних мережах.[4]

Набір експлойтів: ці набори інструментів дозволяють зловмисникам використовувати відомі вразливості в програмному забезпеченні, зокрема для непомітної установки зловмисного ПЗ.

Зловмисне програмне забезпечення для викрадання даних: спеціалізоване ПЗ для витоку даних, таке як викрадач інформації, зосереджене на викраденні конфіденційної інформації. APTs (Advanced Persistent Threats) використовують складні методи для тривалого непомітного перебування в системі.

Захоплення каналу комунікації: такі атаки включають перехоплення та маніпулювання існуючими комунікаційними каналами для непомітного перенаправлення або перехоплення даних.

Після аналізу програмних прихованих каналів витоку інформації, стає зрозуміло, що ці загрози представляють собою значний виклик у сфері кібербезпеки. Однак, для повного розуміння потенціалу витоку інформації необхідно розширити наш аналіз та включити в нього технічні канали витоку. Ці канали часто базуються на використанні фізичних властивостей обладнання або технічних характеристик систем і можуть включати в себе різноманітні методи витоку, які виходять за рамки звичайного програмного забезпечення.

Технічні канали витоку інформації можуть бути значно складнішими для виявлення та блокування, оскільки вони часто вимагають спеціалізованих знань та обладнання для їх ідентифікації. Вони можуть включати в себе атаки через електромагнітне випромінювання, акустичні сигнали, оптичні маніпуляції, а також інші фізичні методи. Осмислення цих аспектів є ключовим для створення ефективних стратегій захисту, які охоплюють усі можливі шляхи витоку інформації. Розглянемо тепер більш детально різні види технічних каналів витоку інформації які представлені у табл. 1.2

Таблиця 1.2 – Класифікація різних видів технічних каналів витоку інформації за їх типами

Тип Каналу	Атака	Опис	Метод/Компонент
Акустичний	Fansmitter	Використовує шум вентилятора для передачі даних.	Модуляція швидкості вентилятора.
	DiskFiltration	Передає дані через звукові вібрації жорсткого диска.	Контроль швидкості обертання диска.
	MOSQUITO	Передача даних через ультразвук між мікрофоном і динаміком.	Ультразвукові сигнали.

Продовження таблиці 1.2

Електромагнітний	AirHopper	Витік даних через ЕМ хвилі, що генеруються відеокартою.	Електромагнітні хвилі від відеокарти.
Тепловий	BitWhisper	Передача даних через теплове випромінювання.	Теплове випромінювання між ПК.
	Thermanator	Відновлення паролів за допомогою теплових слідів на клавіатурі.	Теплові сліди на клавіатурі.
Оптичний	LED-it-Go	Використовує миготіння LED жорсткого диска для передачі даних.	Індикатор жорсткого диска.
	VisiSploit	Передача даних через швидкі візуальні сигнали, непомітні для ока.	Швидкі візуальні миготіння.
Фізичний	USBee	USB-пристрої для передачі даних через ЕМ хвилі.	ЕМ хвилі від USB-пристроїв.
	HeatHammer	теплове випромінювання від комп'ютера для передачі даних.	Теплове випромінювання процесора/ПЗУ.
Кінетичний	Seismokard	Передача даних через вібрації поверхні.	Вібрації поверхні від ударів.
	VibraPhone	Використовує вібрації мобільного телефону для передачі даних.	Вібрації мобільного телефону.

Отже, підсумовуючи аналізи прихованих каналів витоку інформації, ми можемо зробити висновок, що ці канали становлять собою різноманітну та комплексну загрозу інформаційній безпеці. Кожен тип має свої унікальні характеристики та вимагає специфічних заходів захисту.

Акустичні канали витоку інформації заслуговують на увагу з кількох причин. Вони охоплюють широкий спектр потенційних вразливостей, від простих людських розмов у незахищеному середовищі до складніших методів, таких як аналіз звуків клавіатури або роботи інших пристроїв. Це робить акустичні канали досить універсальними у своєму потенціалі для витоку інформації.

Однак, з появою і розвитком цифрових технологій, увага до акустичних каналів почала зменшуватися. В цей період відбулося зосередження на кіберзагрозах, таких як віруси, хакерські атаки, та фішинг. Технологічний прогрес призвів до посилення уваги на цифрові загрози, в той час як фізичні канали, включаючи акустичні, стали недооціненими. Це було також підсилено зміною робочих просторів та усвідомленням безпеки, що зосереджувалося на кібераспектах.

З часом стало зрозуміло, що ця недооцінка акустичних каналів витоку інформації може призводити до серйозних вразливостей. Сучасні дослідження та інциденти показали, що акустичні канали все ще можуть бути ефективними засобами для збору конфіденційної інформації. Таке усвідомлення спонукало фахівців з безпеки знову звернути увагу на акустичні канали як на важливу складову комплексного захисту інформації.

Загалом, акустичні канали витоку інформації представляють собою важливий аспект безпеки, який не можна ігнорувати або недооцінювати, незважаючи на зростаючу увагу до цифрових загроз. Сучасна безпека вимагає балансу між захистом від цифрових і фізичних каналів витоку інформації.

1.2 Необхідність заходів протидії прихованим каналам витоку інформації

Необхідність заходів протидії прихованим каналам витоку інформації формулюється як в законодавчих актах України, нормативних документах та рекомендаціях держспецзв'язку та інших відомств та організацій, що відповідають за національну безпеку та захист інформації. Вони включають ряд вимог та рекомендацій, спрямованих на запобігання та мінімізацію

ризиків, пов'язаних з використанням прихованих каналів для несанкційованого витоку інформації.

1.2.1 Загальні положення Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" є ключовим документом, який встановлює правові основи для захисту інформації в Україні. Цей закон визначає важливість і необхідність вжиття заходів протидії прихованим каналам витоку інформації.

Конфіденційність інформації яка обробляється в інформаційно-телекомунікаційних системах. Приховані канали витоку можуть становити значний ризик для цієї конфіденційності, дозволяючи несанкційований доступ до чутливих даних.

Закон вимагає від організацій застосування заходів для запобігання несанкційованого доступу до інформаційних систем. Приховані канали часто використовуються для обходу традиційних систем безпеки, тому їх ідентифікація та блокування є критично важливими.

Законодавство також вимагає регулярної оцінки та управління ризиками, пов'язаними з обробкою інформації. Це включає ідентифікацію потенційних прихованих каналів витоку та розробку стратегій для їх запобігання.

Закон наголошує на необхідності використання як технічних, так і організаційних заходів для захисту інформації. Це може включати в себе впровадження спеціалізованого ПЗ для виявлення та блокування прихованих каналів, а також навчання персоналу щодо загроз інформаційної безпеки.

1.2.2 Рекомендації Держспецзв'язку щодо прихованих каналів витоку інформації

Нормативні акти державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) грають важливу роль у формуванні політики безпеки інформації, особливо щодо заходів протидії прихованим

каналам витоку інформації. Ці нормативні акти встановлюють вимоги та стандарти, які спрямовані на забезпечення безпеки інформаційних систем від різноманітних загроз, у тому числі від прихованих каналів витоку.

Держспецзвязку розробляє та впроваджує стандарти та нормативні вимоги, які організації повинні дотримуватися для захисту своїх інформаційних систем.

Нормативні акти зазвичай включають методи оцінки ризиків, що дозволяють організаціям ідентифікувати потенційні вразливості, включаючи приховані канали витоку інформації.

Нормативи надають рекомендації та керівництво щодо впровадження ефективних заходів безпеки, включаючи технічні, адміністративні та фізичні контролі.

Заходи протидії:

1)Шифрування та контроль доступу:

Використання шифрування для захисту даних та систем контролю доступу для обмеження несанкційованого доступу до інформації.

2)Моніторинг та виявлення:

Встановлення систем моніторингу для виявлення незвичайних або підозрілих діяльностей, що можуть вказувати на використання прихованих каналів.

3)Регулярні перевірки та аудити:

Проведення регулярних аудитів та перевірок безпеки для ідентифікації та виправлення вразливостей.

4)Навчання персоналу:

Організація тренінгів для співробітників з метою підвищення обізнаності про ризики інформаційної безпеки та методи протидії загрозам.

1.2.3 Рекомендації НД ТЗІ щодо прихованих каналів витоку інформації

В нормативному документі ТЗІ 2.5-004-99 розглядається аналіз прихованих каналів витоку інформації. Ця діяльність виконується з метою

виявлення та усунення потоків інформації, які існують, але не контролюються іншими послугами.

Заходи протидії прихованим каналам витоку інформації:

1)Виявлення та аналіз прихованих каналів є важливим для виявлення потоків інформації, які можуть уникнути стандартних контрольних механізмів. Це особливо важливо у сучасних складних IT-системах, де різноманітність компонентів та взаємодій може приховувати неочевидні шляхи витоку даних.

2)Усунення вразливостей після ідентифікації прихованих каналів.необхідно розробити та впровадити заходи для їх усунення. Це може включати модифікацію системи, оновлення політик безпеки, використання спеціалізованого ПЗ для контролю та моніторингу.

3)Важливо застосувати комплексний підхід до безпеки, який охоплює не тільки технічні аспекти, але й організаційні та адміністративні заходи. Це включає навчання персоналу, розробку і дотримання процедур і стандартів безпеки.

4)Регулярні перевірки безпеки та аналіз прихованих каналів дозволяють своєчасно виявляти нові вразливості та адаптувати заходи безпеки до змінюваних загроз

Згідно з нормативним документом ТЗІ 2.5-004-99, послуги, пов'язані з протидією прихованим каналам витоку інформації, включають в себе наступні рівні:

1)Виявлення Прихованих Каналів (КК-1):

Цей рівень передбачає аналіз прихованих каналів у апаратному і програмному забезпеченні, а також у програмах ПЗП (периферійні засоби обробки). Основна задача полягає у документуванні всіх виявлених прихованих каналів та їх максимальної пропускної здатності, одержаної на підставі теоретичної оцінки або вимірів

2)Контроль Прихованих Каналів (КК-2):

На цьому рівні забезпечується реєстрація використання затвердженої підмножини знайдених прихованих каналів. Це включає моніторинг і контроль діяльності, яка може вказувати на використання цих каналів.

3)Перекриття Прихованих Каналів (КК-3):

Цей рівень передбачає заходи щодо усунення або обмеження знайдених прихованих каналів. Це може включати зміни в архітектурі системи, впровадження додаткових контрольних механізмів або використання спеціалізованих інструментів для блокування або обмеження цих каналів.

Кожен з цих рівнів відіграє важливу роль у забезпеченні захисту від прихованих каналів витоку інформації, пропонуючи комплексний підхід до виявлення, контролю та усунення цих загроз.

Але цей нормативний документ є загальним та не завжди може відповідати стрімкому розвитку технологій, тому з часом можливо будуть ставати актуальні інші канали які не наведені в цьому документі.

1.3 Аналітичний огляд акустичних прихованих каналів витоку інформації

Акустичні приховані канали витоку інформації представляють собою суттєву загрозу в контексті інформаційної безпеки, особливо у світлі сучасних технологічних розвитків. Ці канали можуть бути використані для перехоплення та витоку конфіденційної інформації через різні звукові сигнали та шуми.

Вони можуть включати в себе широкий спектр звукових сигналів, починаючи від розмов людей і закінчуючи звуками, які видають різні пристрої. Найбільш очевидним прикладом є витік інформації через прямі розмови, коли конфіденційна інформація обговорюється в незахищених місцях. Однак, існують і більш складні форми, такі як аналіз звуків клавіатури, де кожна клавіша має свій унікальний звуковий профіль, що може бути використане для відновлення введеного тексту.

Дослідження в цій області демонструють значний потенціал акустичних каналів для витоку інформації. Наприклад, дослідники з MIT і

інших університетів показали, що можливо відтворити введені на клавіатурі текстові послідовності, аналізуючи звуки клавіш. Інші дослідження зосереджуються на акустичному криптоаналізі, де шуми від електронних компонентів, таких як процесори та жорсткі диски, можуть надати інформацію про обчислювальні процеси, що відбуваються в пристрої.

Акустичні канали представляють собою унікальні ризики, оскільки вони часто ігноруються під час розробки систем безпеки. У багатьох організаціях існує свідомість щодо необхідності захисту від цифрових загроз, але фізичні аспекти, такі як акустичні канали, часто залишаються без уваги. Це створює потенційні "сліпі зони", де конфіденційна інформація може бути викрита без належного рівня захисту.

Усвідомлення існування та потенційної небезпеки акустичних каналів витоку інформації є важливим кроком у розробці ефективних заходів інформаційної безпеки. Це стосується не лише великих організацій, але й малих та середніх підприємств, а також індивідуальних користувачів. Розуміння ризиків, пов'язаних з акустичними каналами, може допомогти у виробленні більш комплексних та ефективних стратегій захисту інформації.

Переходячи від загального розгляду акустичних каналів витоку інформації до більш конкретних аспектів, важливо підкреслити, що акустичні канали не обмежуються лише очевидними джерелами, такими як розмови або звуки офісного обладнання. Вони включають в себе широкий спектр потенційних вразливостей, які варто розглянути детальніше.

Ця здатність перехоплювати і аналізувати інформацію, зашифровану в акустичних сигналах, відкриває нові можливості для зловмисників і водночас ставить нові виклики перед фахівцями з безпеки.

1.3.1 Fansmitter

Існуючі акустичні методи вимагають встановлення зовнішнього або внутрішнього динаміка в передавальному комп'ютері. Це вважається обмежувальною вимогою, оскільки у багатьох випадках використання динаміків заборонено на комп'ютерах, які ізольовані від зовнішніх мереж (air-

gapped), відповідно до регуляції та практик безпеки.[5] З іншого боку, цей метод не вимагає, щоб передавальний комп'ютер був оснащений аудіоапаратурою або внутрішнім чи зовнішнім динаміком.[5]

Фансміттер (Fansmitter) вносить свій вклад у галузь акустичних прихованих каналів, що представляють канали прихованого зв'язку поза смугою пропускання. Фансміттер пропонує такий метод як виведення інформації з комп'ютерів, ізольованих від зовнішніх мереж (air-gapped). Подібно до інших прихованих комунікаційних каналів, модель атаки ворога складається з передавача та приймача. Зазвичай у цих сценаріях передавачем є звичайний настільний комп'ютер, а приймачем - мобільний телефон поблизу. На початковому етапі передавач та приймач були б скомпрометовані нападником.Інфікування високозахищеної мережі може бути здійснене, як це було продемонстровано атаками, пов'язаними з Stuxnet[6] та Agent.Btz[7]. У нашому випадку, заражений комп'ютер повинен бути оснащений внутрішнім вентилятором ЦП(центрального процесору) або корпусу, що є характерним для майже кожного сучасного комп'ютера. Зараження мобільного телефону є набагато менш складним завданням і може бути виконане за допомогою багатьох різних векторів атаки, використовуючи електронні листи, SMS/MMS, шкідливі додатки тощо.Тоді скомпрометований комп'ютер збирає конфіденційні дані (наприклад, ключі шифрування) та модулює їх, передаючи за допомогою акустичних хвиль, які випромінюються внутрішніми вентиляторами комп'ютера. Поблизу розміщений мобільний телефон-приймач (також скомпрометований), оснащений мікрофоном, виявляє та приймає передачу, демодулює та декодує дані, а потім передає їх нападнику за допомогою мобільного зв'язку, SMS або Wi-Fi. [5]

Різні елементи комп'ютерної системи, включно з центральним процесором, оперативною пам'яттю та графічним процесором, генерують тепло під час їх роботи. Щоб уникнути перегрівання, яке може призвести до збоїв або навіть до фізичного пошкодження цих компонентів, необхідно підтримувати їх в оптимальному температурному режимі. Для цього у

комп'ютерних системах використовуються вентилятори, призначені для покращення охолодження через збільшення потоку повітря навколо цих елементів.

Настільні комп'ютери, як правило, оснащені трьома-чотирма типами вентиляторів (блоку живлення, корпусу, ЦП та необов'язковим вентилятором графічної карти).

Вентилятор корпусу. Цей вентилятор встановлений на бічній або задній частині комп'ютерного корпусу. Він зазвичай забирає холодне повітря ззовні комп'ютера та випускає його через верх або задню частину комп'ютера.

Вентилятор ЦП. Цей вентилятор встановлений на верхній частині роз'єму ЦП. Він охолоджує радіатор ЦП.

Цей тип атаки фокусується на вентиляторах ЦП та корпусу. Ці вентилятори гарантовано присутні в кожному комп'ютері, що робить Фансміттер загрозою майже для кожного комп'ютера.

Швидкість вентиляторів ЦП та корпусу може керуватися автоматично або вручну. З автоматичним управлінням швидкість вентилятора регулюється контролером на материнській платі. Контролер збільшує та зменшує швидкість вентилятора відповідно до поточної температури. Ручне управління може замінити поточну швидкість вентилятора та встановити її за допомогою вхідного сигналу керування вентилятором. Вручну встановлення швидкості вентилятора зазвичай виконується через інтерфейс BIOS або безпосередньо з ОС, якщо було встановлено відповідний драйвер для доступу до відповідної шини.[5]

Шум, що виникає від обертання комп'ютерного вентилятора, вимірюється в одиницях обертів за хвилину і випромінюється на різних частотах та силах. Типові швидкості обертання вентиляторів комп'ютера варіюються від кількох сотень до кількох тисяч обертів за хвилину. Шум виникає через рух лопастей вентилятора, кожна з яких виштовхує повітря на своєму шляху, і разом їхні рухи створюють хвилю стиску з деякою мірою рідкісності. Рівень шуму залежить від повітряного потоку, механіки та

вібрацій, які в основному визначаються місцем розташування, розміром, кількістю лопастей та поточною швидкістю обертання вентилятора. Оскільки місце розташування, розмір та кількість лопастей вентилятора є фіксованими, поточна швидкість обертання є основним фактором, який визначає рівень шуму. Відомо, що рівень шуму вентилятора (в дБ) зростає пропорційно до п'ятої ступені швидкості обертання вентилятора, тому зміни в обертанні вентилятора відразу викликають зміну випромінюваного шуму.[5]

Акустичний сигнал вентилятора процесора з різних дистанцій наведено на рис. 1.2

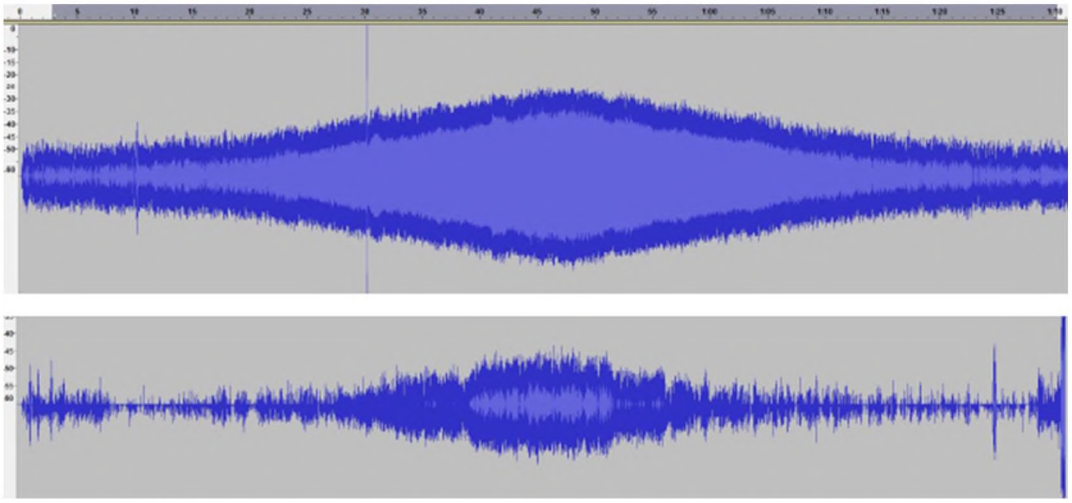

Рисунок 1.2 – Акустичний сигнал вентилятора процесора, отриманий мобільним телефоном з дистанції 1 метр(зверху) та 4 метра(знизу)[5]

Для кодування цифрової інформації через акустичний сигнал вентилятора дані мають бути модульовані. У нашому випадку модулюються бінарні дані через несучу звукову хвилю: форму хвилі звуку вентилятора. Використовується два типи схем модуляції: Амплітудна маніпуляція (ASK) та Частотна маніпуляція (FSK). Маніпуляція частотна маніпуляція є швидшою і більш стійкою до зовнішніх шумів, ніж амплітудна маніпуляція, але вона більш стійка до типу використовуваного вентилятора та його характеристик частоти проходження лопастей, ніж частотна маніпуляція. Загалом використовується частотна, коли заздалегідь відомий загальний тип передавального вентилятора, і амплітудна використовується, коли тип вентилятора або його властивості невідомі нападнику.

Тестування яке було проведено в середовищі яке складалося з кімнати зі звичайним фоновим шумом, двох робочих станцій, кількох мережевих комутаторів та активної системи кондиціонування повітря. Час передачі та швидкість передачі бітів був сильно залежний від зовнішнього шуму. Вищий рівень зовнішнього шуму знижує швидкість передачі бітів та ємність каналу. На рис. 1.2, рис. 1.3 та рис. 1.4 зазначені результати на відстані від одного до чотирьох метрів між передавачем і приймачем, та базуються на описаному вище тестувальному середовищі.

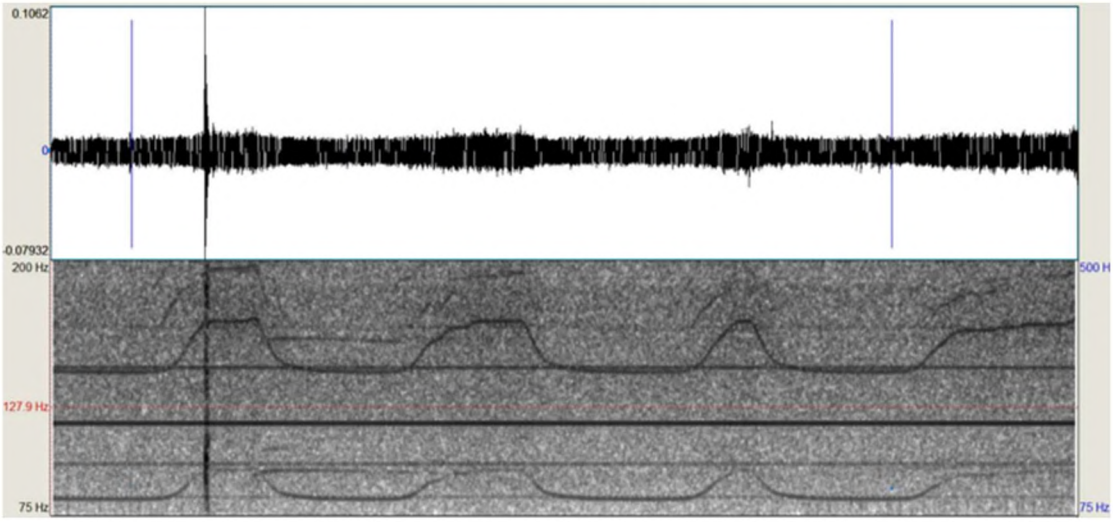

Рисунок 1.3 – Аудіоспектральний огляд ЦП(1000-1600 об/хв ,дистанція 1м)[5]

При дистанції 1м та 1000-1600 об/хв швидкість передачі даних 3 біта за хвилину.

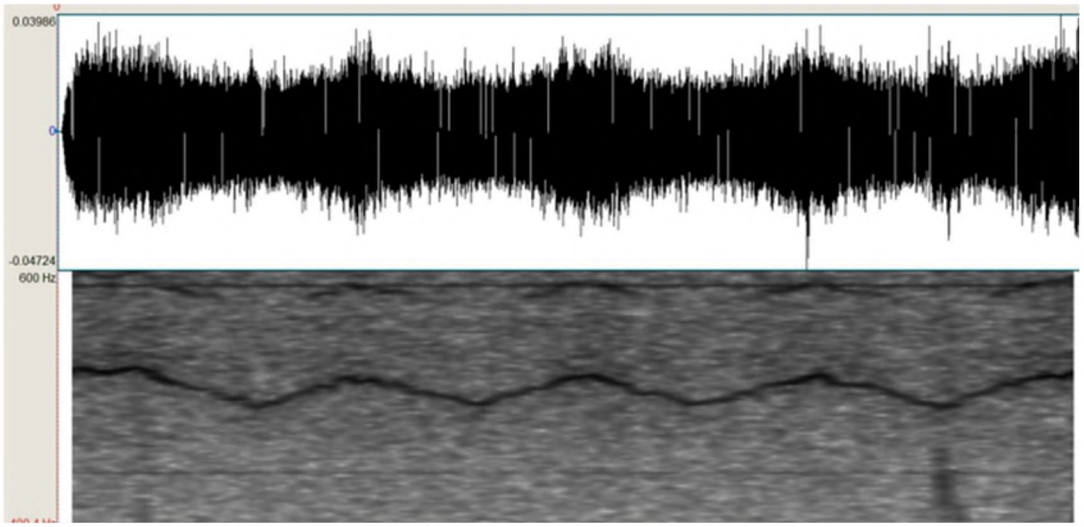

Рисунок 1.4 – Аудіоспектральний огляд ЦП(4000-4250 об/хв ,дистанція 1м)[5]

При дистанції 1м та 4000-4250 об/хв швидкість передачі даних 15 бітів за хвилину.

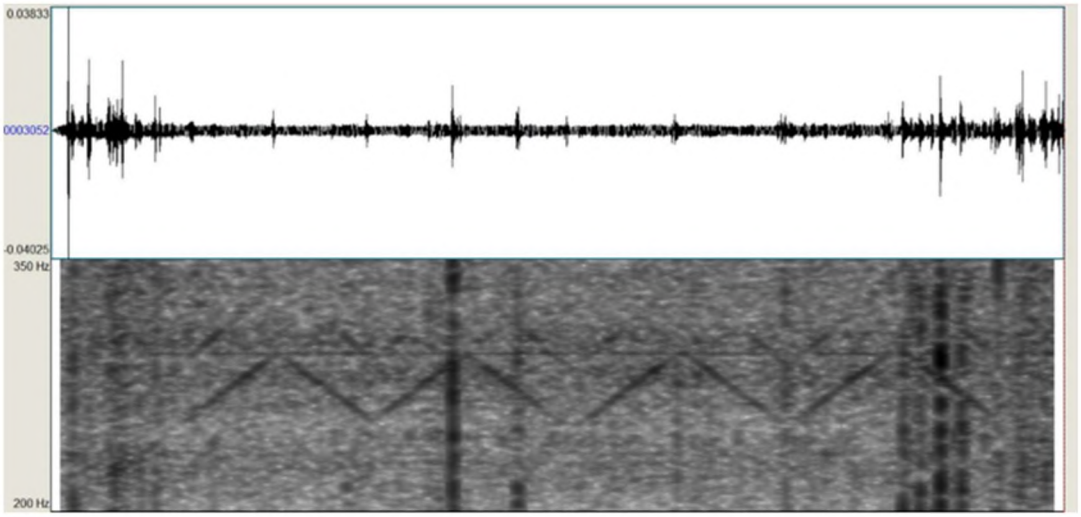

Рисунок 1.5 – Аудіоспектральний огляд ЦП(3100-3350 об/хв ,дистанція 4м)[5]

При дистанції 4 метра та 3100-3350 об/хв швидкість передачі даних 10 бітів в хвилину.

1.3.2 MOSQUITO

Ця атака зосереджена на можливостях шкідливого програмного забезпечення використовувати гучномовці/навушники/гарнітури, підключені

до комп'ютера, для запису аудіосигналів, і обговорює обмеження цього підходу.

Технічні знання які потрібні для розуміння цієї атаки:

1) Реверсивність гучномовця

Гучномовець, може також використовуватися як мікрофон, використовуючи принцип зворотної роботи. Якщо гучномовець перетворює електричний сигнал на акустичні хвилі, то мікрофон, навпаки, перетворює акустичні хвилі у електричні сигнали. У гучномовці змінне магнітне поле, що генерується електричним сигналом, змушує діафрагму рухатися, створюючи звук. Подібним чином, у мікрофоні мікроскопічна діафрагма вібрує під впливом звукового тиску, створюючи електричний сигнал. Цей двосторонній механізм дозволяє використовувати звичайний гучномовець як мікрофон шляхом підключення до мікрофонного входу, але слід врахувати, що якість запису з такого "мікрофону" буде досить низькою, оскільки гучномовці не розроблені для виконання цієї функції.[5]

2)Перепрограмування роз'ємів

Аудіочіпсети на сучасних материнських платах та звукових картах включають опцію зміни функції аудіороз'єму на програмному рівні, тип аудіопрограмування, іноді називаний "перепрограмуванням роз'єму"(Jack Retasking). Ця опція доступна на більшості аудіочіпсетів (наприклад, аудіочіпсетів Realtek), інтегрованих у материнські плати ПК сьогодні. Перепрограмування роз'єму, хоча й задокументоване у технічних специфікаціях, не дуже відоме.

Гучномовці, навушники, гарнітури фізично побудовані як мікрофони, разом із тим фактом, що роль аудіороз'єму в ПК може бути програмно змінена з вихідного на вхідний, створює уразливість, яку можуть використовувати нападники. Шкідливе ПЗ може непомітно переконфігурувати роз'єм навушників з лінійного вихідного на мікрофонний. В результаті підключений вихідний пристрій може функціонувати як пара записуючих мікрофонів,

перетворюючи комп'ютер на записуючий пристрій - навіть коли комп'ютер не має підключеного мікрофона.[8]

3)Пасивні гучномовці, навушники та гарнітури

Зворотність динаміків ставить обмеження, що динамік повинен бути пасивним, без підсилювачів переходів. У випадку активного динаміка між роз'ємом та динаміком є підсилювач; отже, сигнал не буде переданий з вихідного на вхідний бік . Навушники, гарнітури побудовані з пари пасивних динаміків і тому завжди зворотні. Однак, більшість гучномовців ПК сьогодні мають внутрішній підсилювач.[9] Пасивні гучномовці переважно існують в застарілих та міжкімнатних системах .[10]

Активні гучномовці не є зворотними і тому можуть виступати лише як передавальна сторона в нашому прихованому каналі. Приймаючою стороною має бути комп'ютер, підключений до пасивних динаміків, навушників або гарнітури.

Однією з можливостей реалізації такої атаки є формування бітових рамок(Bit-Framing).

Сформовані пакети бітів даних передаються у вигляді невеликих кадрів. Кожен кадр складається з 46 бітів і включає в себе преамбулу,корисний вантаж (payload) та циклічний контроль залишків(CRC), як показано на рис. 1.6

Преамбула передається на початку кожного пакета. Вона складається з послідовності шести чергуючих бітів ('101010'), які допомагають приймачу визначити властивості каналу, такі як частота несучої хвилі та період біту (швидкість передачі бітів). Крім того, заголовок преамбули дозволяє приймачу виявити початок передачі кожного пакета. Це важливо для прихованого каналу, оскільки у випадку ультразвукового прихованого каналу передача може бути перервана, наприклад, якщо комп'ютер був перезавантажений під час триваючої передачі.

Корисний вантаж – це 32 біти необробленої інформації, який містить сам пакет.

Циклічний контроль залишків(CRC) застосовується для виявлення помилок вставляється вісім бітів CRC-коду в кінці кадру. Приймач розраховує CRC для отриманого вантажу, і якщо воно відрізняється від отриманого CRC, виявляється помилка. У випадку помилки відправляється запит на повторну передачу пакета (лише у випадку двостороннього зв'язку).

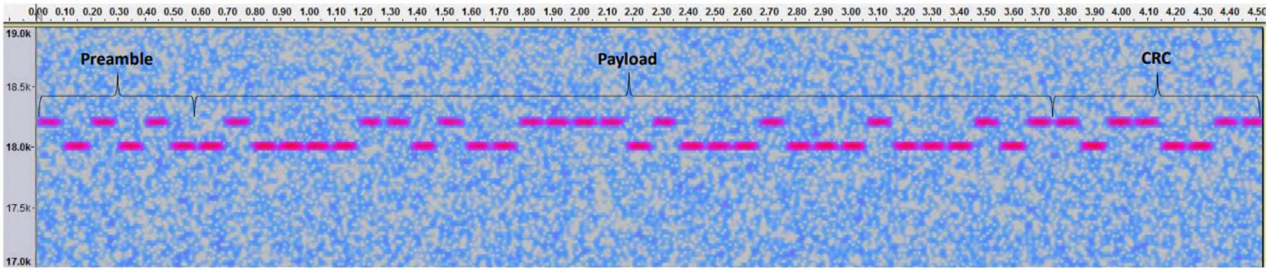

Рисунок 1.6 – Спектрограмма 46-бітного кадру(преамбула,вантаж, CRC)переданого зі швидкістю 10 біт /сек за допомогою модуляції B-FSK.[8]

Навушники, гарнітури та пасивні гучномовці не були розроблені для виконання ролі мікрофонів з точки зору якості та діапазону частот. У цьому розділі йде оцінка ефективність комунікації між гучномовцями та представлений емпіричний аналіз їх відповідної ємності каналу. Також Розповідаємо про різні практичні аспекти, пов'язані з ультразвуковим прихованим каналом. Переважно цікаві високочастотні області, які пропонують високу ємність каналу при одночасно низькій аудиторній усвідомленості.[8]

Розраховується ємність комунікаційного каналу, утвореного між двома гучномовцями, один з яких служить як передавач, а інший - як приймач. У цих експериментах грається десяти секундний синусоїдний сигнал із діапазоном від 1 Гц до 24 кГц від передавача та записується приймачем.

Тестування яке було наведене в джерелі [8] було розглянуто три пасивні гучномовці: Logitech Z523, Logitech Z213 та Philips SPA5300. Гучномовці підключалися до перепрограмованого аудіовихідного роз'єму настільного ПК Optiplex 9020. Свіп-сигнал відтворювався через гучномовець Logitech Z100, підключений до робочої станції Gigabyte GA-H97M-D3H (Intel Core i7-4790), що працює на Ubuntu 16.04.1 з ядром 4.4.0.

Сигнал аналізується в послідовних гауссових вікнах тривалістю 200 мілісекунд з перекриттям у 25% за часом. Використовується роздільна здатність частоти 100 Гц для кожної смуги, що дає 250 аналізованих смуг. SNR оцінюється для кожної частотної смуги як співвідношення потужності отриманого сигналу та вимірюваного шуму в цій смузі.

На рис. 1.7 представлено оцінену ємність каналу для всього діапазону частот. Для налаштувань 1 м, 4 м та 8 м теоретична верхня межа ємності каналу становить від 1200 біт/сек до 1800 біт/сек для чутних частотних смуг (нижче 18 кГц). Як і очікувалося, ємність каналу корелюється з відстанню між передавачем та приймачем. Ємність каналу значно погіршується в саббуферному діапазоні (до близько 60 Гц) та для високих частот (вище 18 кГц). У цих діапазонах теоретична верхня межа становить від 300 біт/сек до 600 біт/сек у більшості випадків. Причиною цього є те, що гучномовці, особливо домашнього рівня, були спроектовані та оптимізовані для людських аудиторних характеристик і тому більш реактивні на чутні діапазони частот.[8]

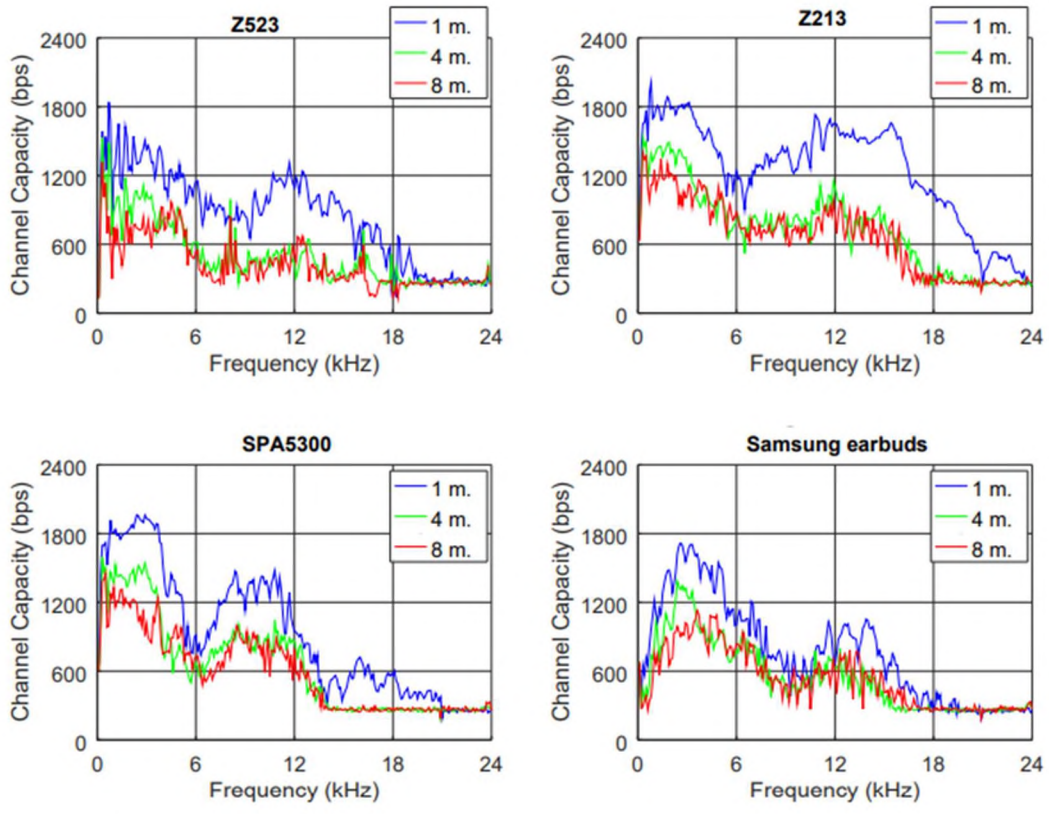

Рисунок 1.7 – Ємність каналу зв'язку між гучномовцями[8]

Відомо, що приховане спілкування може бути встановлено між двома сусідніми комп'ютерами, ізольованими від зовнішніх мереж, дозволяючи їм обмінюватися даними за допомогою ультразвукових хвиль. Однак, стандартна модель атаки вимагає, щоб обидва комп'ютери були оснащені як динаміками, так і мікрофонами. Таким чином, цей тип прихованого каналу не застосовний у безпечних установах, де зазвичай заборонено використання мікрофонів. Також багато настільних робочих станцій не мають мікрофонів, або мікрофони були фізично вимкнені або заглушені. Цей тип атаки має змогу обмінюватися даними за допомогою ультразвукових хвиль з комп'ютерів, ізольованих від зовнішніх мереж без мікрофонів.

1.3.3 POWER-SUPPLaY

Можливість створення акустичних сигналів через блоки живлення може бути важливим внеском у сферу створення прихованих акустичних каналів, незалежно від їхнього зв'язку з концепцією повітряного зазору. Розглядається ця можливість як спосіб передачі інформації з систем, що ізольовані від зовнішніх мереж та аудіо пристроїв. Аналогічно до інших методів прихованого зв'язку, сценарій атаки передбачає наявність відправника та одержувача. Зазвичай у таких випадках відправником виступає комп'ютер, а одержувачем - мобільний телефон, який може належати співробітнику або відвідувачу.

Технічне уявлення про перетворювачі комутації напруги (SMPS), акустичне випромінювання та опис генерації сигналу.

Комп'ютери споживають електроенергію зі своїх блоків живлення. Сучасні перетворювачі комутації напруги використовуються в усіх типах електронного обладнання, включаючи комп'ютери, телевізори, принтери, та вбудовані пристрої, а також зарядники для мобільних телефонів. Переваги перетворювача комутації напруги перед старішими лінійними блоками живлення включають високу ефективність, менший розмір і невелику вагу. Він перетворює енергію з джерела 220 В перемінного струму на кілька навантажень постійного струму, перетворюючи характеристики напруги та

струму. В них, енергія перемінного струму проходить через запобіжники та фільтр лінії, а потім випрямляється повний міст випрямлювача. Випрямлення напруги застосовується до модуля корекції коефіцієнта потужності та регулюється за допомогою постійного напруги до постійного напруги.[11]

Постачання постійного струму від випрямлювача або батареї подається на інвертор, де його включають і вимикають з високими швидкостями. Типова частота комутації блоку живлення комп'ютера знаходиться в діапазоні від 20 кГц до 20 МГц.

Частота комутації впливає, серед іншого, на такі компоненти як трансформатори та конденсатори. Вони є основними джерелами акустичного шуму, що генерується в перетворювачах комутаційної напруги.

Звуковий шум трансформаторів виробляється, оскільки він містить багато фізично рухомих елементів, таких як котушки, ізоляційні стрічки та бобіни. Струм у котушках, який відбувається на частоті комутації, створює електромагнітні поля, які генерують відштовхувальні та / або притягальні сили між котушками. Це може створювати механічні вібрації в котушках, сердечниках або ізоляційних стрічках.[11]

Звуковий шум конденсаторів є результатом вібрацій конденсатора на друкованій платі, які відбуваються в умовах нормальної роботи. Ці вібрації призводять до переміщення конденсатора. Частота і амплітуда переміщення визначають акустичну форму сигналу, що генерується конденсаторами. Коли частота вібрацій знаходиться в звуковому діапазоні, приблизно від 20 Гц до 20 кГц, її також може бути чутно як чутний гул. Діапазон від 20 кГц до 24 кГц розглядається як "близький до ультразвуку" і не може бути почутий більшістю людей.[11]

Типова частота комутації під час її нормальної роботи знаходиться в діапазоні від 20 кГц до 20 МГц. Тому акустичний сигнал, що генерується, в основному знаходиться в діапазоні від 20 кГц і вище. Цей діапазон знаходиться в верхній межі людського слуху і вважається нерозпізнаваним для дорослих осіб.

На фазі зараження передавач та приймач скомпрометуються нападником. У цьому випадку заражений комп'ютер повинен бути оснащений внутрішнім блоком живлення, який існує майже у кожній комп'ютеризованій системі. Крім того, мобільні телефони працівників можливо заразити за допомогою методів соціальної інженерії. Припускається, що працівники носять свої мобільні телефони на робочому місці. Ці пристрої потім заражаються, будь то онлайн, шляхом використання вразливостей пристрою, або за фізичного контакту, коли це можливо. Зараження мобільного телефону може бути виконане за допомогою різних векторів атаки, використовуючи електронні листи, SMS/MMS, шкідливі додатки, шкідливі веб-сайти тощо.[11]

У фазі виведення шкідливе ПЗ на скомпрометованому комп'ютері збирає конфіденційні дані, що представляють інтерес. Це можуть бути файли, журнал натискань клавіш, облікові дані (наприклад, паролі) або ключі шифрування. Після цього шкідливе ПЗ передає дані, використовуючи акустичні хвилі, що випромінюються блоком живлення комп'ютера (рис. 1.8). Сусідній заражений мобільний телефон виявляє передачу, декодує дані та передає їх нападнику через Інтернет, використовуючи мобільні дані або Wi-Fi.

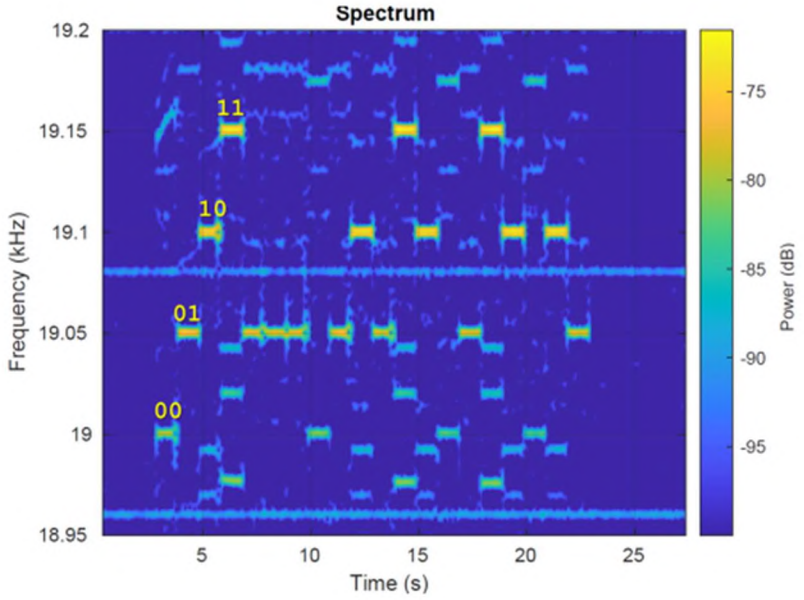

Рисунок 1.8 – Інформація про виведенні через приховані ультразвукові сигнали, що відтворююся з блоку живлення.[11]

Зловмисне програмне забезпечення, що працює на комп'ютері, може використовувати живлення як додатковий динамік. Код, який виконується в системі, може навмисно регулювати внутрішню частоту перемикання живлення, і, таким чином, контролювати форму сигналу, який генерується з його конденсаторів та трансформаторів. Ця техніка дозволяє генерувати звукові та ультразвукові аудіотони з різних типів комп'ютерів та пристроїв, навіть коли аудіоапаратура заблокована, вимкнена або відсутня. POWER-SUPPLaY може працювати з звичайного процесу користувача та не потребує доступу до апаратних ресурсів або привілеїв кореня. Цей метод не викликає спеціальних системних викликів або доступ до апаратних ресурсів і, отже, є дуже хитрим. Як наведено у роботі[8] за допомогою POWER-SUPPLaY можливо акустично витягнути дані з без звукових систем на сусідній мобільний телефон на відстані 2,5 метра з максимальною швидкістю передачі даних 50 біт/с.

1.3.4. DiskFiltration

DiskFiltration, як прихований акустичний канал, може використовуватися для витоку даних з комп'ютерів, ізольованих від зовнішніх мереж. Однак цей прихований канал також можна використовувати у випадку комп'ютерів, підключених до Інтернету (не ізольованих), в яких мережевий трафік інтенсивно моніториться системами виявлення вторгнень (IDS), запобігання вторгненням (IPS) та запобігання витоку даних (DLP). У цих випадках витік даних через Інтернет-трафік може бути виявлений, і тому нападник може вдатися до прихованого каналу зв'язку поза смугою пропускання.[12]

Жорсткий диск випромінює шум на різних частотах та рівнях інтенсивності, які виробляються рухами його внутрішніх частин. Незважаючи на кілька досліджень акустичних характеристик жорсткого диска, механізми випромінювання шуму та точне джерело таких випромінювань не були всебічно сформовані.[13]

Існує два основні джерела акустичного шуму всередині диска: мотор і актуатор. Ці джерела відповідають за два типи шумів, які пояснюються нижче.

Шум на холостому ходу визначається як шум, що генерується, коли жорсткий диск обертає пластину. Шум на холостому ходу в основному генерується шпиндельним мотором та кульковими підшипниками всередині мотора. Основна частота шуму на холостому ходу може бути розрахована за формулою $\mathrm{IdleMainFreq} = \mathrm{RPM}/60$, де RPM - швидкість обертання жорсткого диску. рис. 1.9 показує спектрограму шуму на холостому ходу, що генерується жорстким диском Western Digital, який обертається зі швидкістю 7200 об/хв. Основний тон генерується на частоті 7200/60 = 120 Гц, і можна побачити на спектрограмі як виділений безперервний пік частоти.[12]

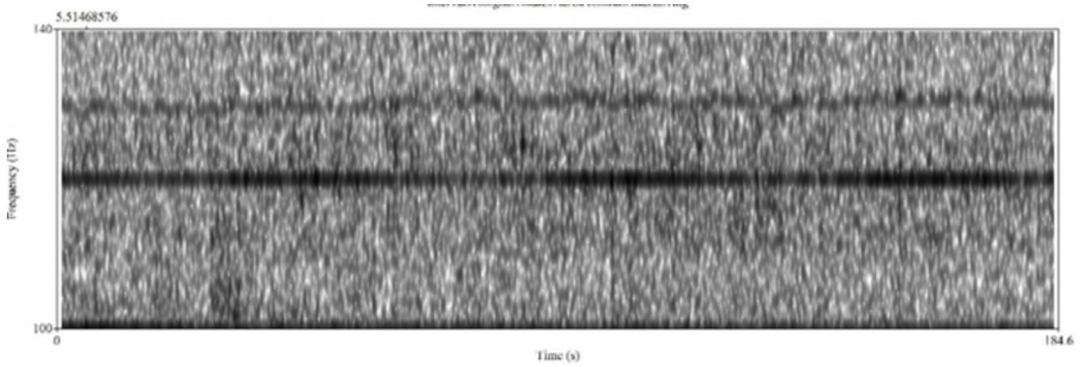

Рисунок 1.9 – Спектрограма акустичного шуму на холостому ходу, генерованого жорстким диском зі швидкістю обертання 7200 об/хв.[12]

Акустичний шум, який створюється від обертання диска на холостому ходу, є незмінним і не піддається контролю через програмне забезпечення. Проте, шум, що виникає через рухи актуатора, може бути використаний для модулювання бінарних даних. Шляхом керування послідовністю операцій зчитування, можна управляти акустичним сигналом, який випромінюється жорстким диском, дозволяючи модулювати бінарні '0' і '1'.

На Рисунку 1.10 представлені спектрограми акустичних хвиль, що генеруються жорстким диском під час операцій читання (зображення зліва) та запису (зображення справа), зафіксовані поза корпусом комп'ютера.Було прочитано 100 МБ бінарних даних у буфер у пам'яті та записано 100 МБ випадкових байтів на диск. Для забезпечення безпосереднього доступу до

диска було відключено всі рівні кешування. Під час операцій читання та запису спостерігаються акустичні піки (загальне підвищення частоти на короткий проміжок часу), але протягом більшої частини цих процесів читаюча головка залишається нерухомою.

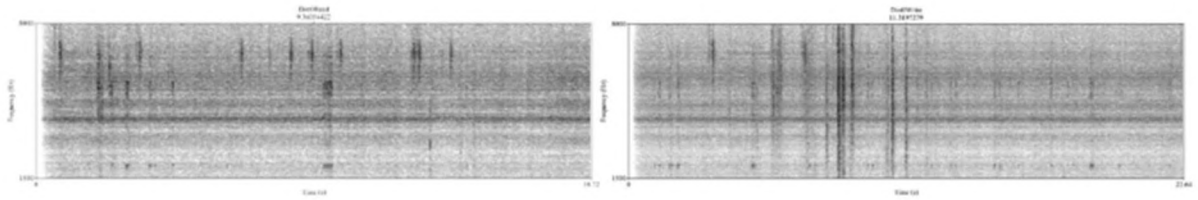

Рисунок 1.10 – Спектральний вигляд операцій читання(зліва) та запису(справа)[12]

Рисунок 1.11 демонструє спектрограму акустичного сигналу, який виробляється жорстким диском під час виконання операцій пошуку, зафіксовану зовні корпусу комп'ютера. У цьому експерименті головка диску була неодноразово переміщена між двома сусідніми доріжками, створюючи пошукові операції, що тривали протягом трьох секунд. На спектрограмі чітко видно окремі піки частот, що свідчать про наявність сильного акустичного сигналу в діапазоні частот між 1500 та 8000 Гц під час проведення цих пошукових операцій.

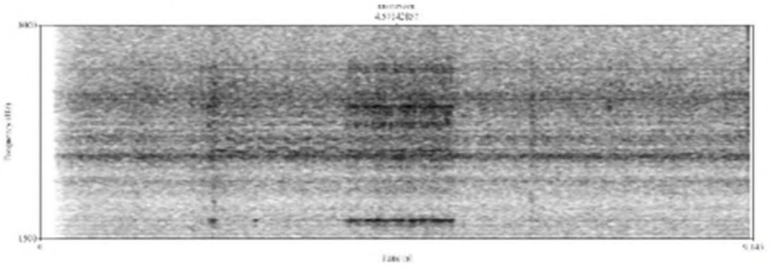

Рисунок 1.11 – спектральний вигляд операції пошуку[12]

Також вивчається акустичний шум, випромінюваний операціями пошуку, коли актуатор рухається між доріжками на різних відстанях. Рисунок 1.12 показує акустичну хвилю, генеровану з жорсткого диску під час операцій пошуку, записану ззовні корпусу комп'ютера. У цьому тесті виконується три типи операцій пошуку, повторне пошук та читання з перших і останніх секторів, пошук та читання між двома послідовними доріжками та пошук та читання між двома послідовними секторами. Операції пошуку та читання

викликають акустичний сигнал, який охоплює весь діапазон від 0 до 6000 Гц. Не було виявлено значних акустичних відмінностей (частот або амплітуди) між трьома типами операцій пошуку. Це вказує на те, що для створення помітного рівня шуму достатньо виконувати операції пошуку між будь-якими двома доріжками.

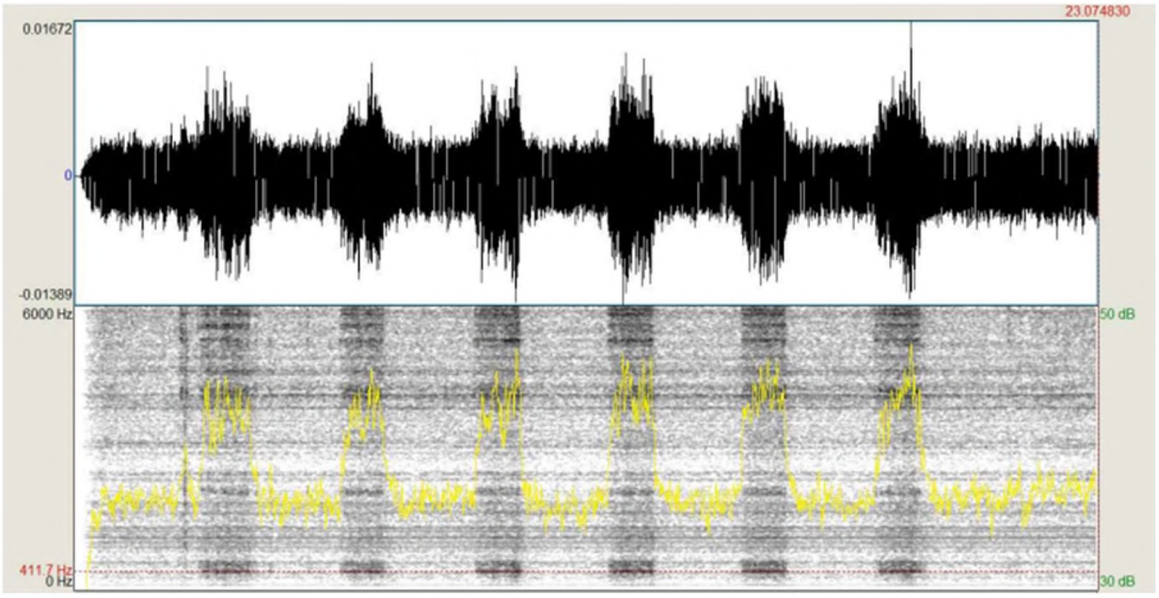

Рисунок 1.12 – Спектральний вигляд операції пошуку між різними доріжками[12]

За допомогою цього методу зловмисник може витікати бінарні дані з комп'ютерів за допомогою прихованих звукових сигналів, що виникають від жорстких дисків. На відміну від більшості існуючих акустичних прихованих каналів, DiskFiltration може працювати на комп'ютерах, які не обладнані динаміками або аудіоапаратурою. Зловмисний код, встановлений на комп'ютері, може виконувати намірені операції з переміщення, що викликають рух голівки жорсткого диска (актуатора) між різними доріжками. Механічні рухи генерують акустичні сигнали, які можна використовувати для модуляції '0' і '1'. Приховані сигнали можуть бути отримані із пристрою для запису,який знаходиться неподалік, таким як смартфон, смарт-годинник, ноутбук тощо.

За допомогою цього метода можливо досягти передачі даних зі швидкістю 180 біта в хвилину

1.4 Висновок

Акустичні приховані канали витоку інформації становлять значну загрозу в сфері інформаційної безпеки. Вони включають широкий спектр звукових сигналів, від людського голосу до шуму обладнання, і можуть бути використані для перехоплення та передачі конфіденційної інформації. Хоча такі загрози часто ігноруються під час розробки систем безпеки, вони створюють "сліпі зони", де інформація може бути викрита.

Оглянуті методи демонструють складність та різноманітність акустичних прихованих каналів витоку інформації. Вони вимагають від фахівців з безпеки розуміння цих загроз та розробки комплексних стратегій для їх виявлення та нейтралізації. Урахування цих аспектів є важливим для забезпечення ефективного захисту конфіденційних даних в сучасному цифровому світі.

Таблиця 1.3 надає порівняння між різними методами акустичного витоку інформації, демонструючи їхні особливості та потенційну ефективність. Важливо відзначити, що кожен із цих методів має свої переваги та обмеження, залежно від середовища та умов використання.

Таблиця 1.3 – порівняння основних характеристик акустичних прихованих каналів витоку інформації

Характеристика	Fansmitter	MOSQUITO	DiskFiltration	POWER-SUPPLaY
Опис	Використовує шум вентилятора для передачі даних.	Передача даних через ультразвук між мікрофоном і динаміком.	Передає дані через звукові вібрації жорсткого диска.	Генерує акустичні сигнали через блоки живлення.

Продовження таблиці 1.3

Метод	Модуляція швидкості вентилятора.	Ультразвукові сигнали.	Контроль швидкості обертання диска.	Використовує варіації у виробництві електроенергії
Діапазон	Залежить від моделі та типу вентилятора.	Високочастотний діапазон, який не чутний людському вуху.	Залежить від характеристик жорсткого диска.	Залежить від специфікацій блоку живлення.
Ефективність	Помірна, залежить від конфігурації системи охолодження.	Висока, особливо в тихих середовищах.	Помірна, обмежена фізичними характеристиками диска.	Залежить від конструкції та якості блоку живлення.
Виявлення	Відносно легко виявити зміни в шумі вентилятора.	Важко виявити без спеціалізованого обладнання.	Може бути виявлено за характерними звуковими вібраціями.	Може бути важко виявити без спеціального обладнання.

Хоч ці атаки і є маловірогідні, та не здатні до передавання великої кількості інформації, але вони реалізуємі, та здатні до викрадення інформації, нездатність легкого виявлення роблять ці атаки ще більш загрозливими.

1.5 Постановка задачі

Основною метою є аналіз моделі загроз та розробка методів протидії акустичним прихованим каналам витоку інформації. Це включає ідентифікацію потенційних загроз що випливають із використання акустичних прихованих каналів, та розробку стратегій для мінімізації цих загроз.

У результаті виконання цих завдань очікується отримання глибокого розуміння загроз, пов'язаних з акустичними прихованими каналами, та розробка ефективних стратегій їх нейтралізації. Це дозволить зменшити ризики витоку конфіденційної інформації та підвищити загальний рівень безпеки інформаційних систем.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель загроз витоку інформації акустичними прихованими каналам витоку інформації.

Загальна модель загрози передбачає наявність двох суб'єктів, які бажають обмінюватися інформацією незаконно в обхід політики безпеки, яка забороняє їм це робити прямо. Ця політика безпеки може бути представлена як проста багаторівнева політика безпеки або будь-яка інша загальна політика безпеки. Основною ідеєю є те, що відправник має вищий рівень безпеки і доступ до критичних активів, до яких одержувач не має доступу, і він намагається передати цю інформацію одержувачеві так, щоб це залишилося непоміченим.[14]

Акустичні приховані канали зазвичай працюють шляхом модуляції даних у акустичні сигнали, які потім передаються з одного пристрою на інший. Приймаючий пристрій, оснащений мікрофоном або подібним сенсором, захоплює ці сигнали, демодулює їх і отримує дані. Модуляція може виконуватися різними способами, наприклад, використанням частот, які не чутні для людини (ультразвукові) або шляхом приховування даних у звуках, які не легко розпізнати.

Таблиця 2.1 надає загальний огляд потенційних загроз, пов'язаних з акустичними прихованими каналами. Важливо розуміти, що контекст використання та специфічні умови можуть вимагати додаткових або альтернативних заходів безпеки.

Таблиця 2.1 – модель загроз для акустичних прихованих каналів витоку інформації

Компонент Загрози	Опис	Приклади	Заходи Захисту
Фізичні джерела	Джерела, які створюють акустичні сигнали, здатні несення інформації.	Вентилятори комп'ютерів, звуки клавіатури, системні звуки.	Використання шумопоглинаючих матеріалів, контроль фізичного доступу.
Технічні засоби перехоплення	Пристрої та технології для перехоплення акустичних сигналів.	Високочутливі мікрофони, лазерні мікрофони, стетоскопи.	Обмеження доступу до обладнання для перехоплення, застосування протишпигунських пристроїв.
Методи передачі	Способи та техніки передачі інформації через акустичні сигнали.	Модуляція звуку, навмисне створення шумів з інформаційним навантаженням.	Аналіз спектру акустичних сигналів, моніторинг незвичайних шумів.
Приймачі	Обладнання або методи для отримання та інтерпретації перехоплених сигналів.	ПК зі спеціалізованим ПЗ для аналізу акустичних даних, мобільні пристрої.	Забезпечення безпеки приміщень, де ведеться конфіденційна робота.

Продовження таблиці 2.1

Зовнішні фактори	Зовнішні умови, які можуть впливати на ефективність акустичних каналів.	Шум зовнішнього середовища, погодні умови, архітектура приміщення.	Застосування звукоізоляції, оптимізація розміщення обладнання.

Потенційні зловмисники для акустичних прихованих каналів витоку інформації можуть бути класифіковані як зовнішні та внутрішні.

Зловмисники які потенційно можуть напасти зовні такі як конкуруючи організації або корпорації: використовують акустичні приховані канали для перехоплення конфіденційної комерційної інформації, такої як плани розвитку нових продуктів, маркетингові стратегії або фінансові дані, щоб отримати конкурентні переваги. Кіберзлочинці які націлені на особисті дані, банківські реквізити або інші чутливі дані для подальшого вимагання викупу або продажу цієї інформації.

Внутрішні загрози виходять від незадоволених співробітників та шпигунами, зловживаючи своїм положенням можуть використовувати ці канали для отримання інформації до якої у них немає доступу встановлюючи зловмисне ПЗ.

Три різні моделі загроз, які можуть бути використані для обходу систем, ізольованих від мережі:

1)Кооперативна мережа між динаміком і мікрофоном (рис.2.1). У цій моделі загрози передбачається наявність двох різних пристроїв, які відокремлені один від одного ізольованою мережею. Один з пристроїв заражений шкідливим програмним забезпеченням. Пристрій відправник має динамік, а пристрій отримувач - мікрофон. Пристрій відправник передає дані до отримувача використовуючи динамік і мікрофон . Це базова і традиційна модель для виведення з ладу ізольованих систем.

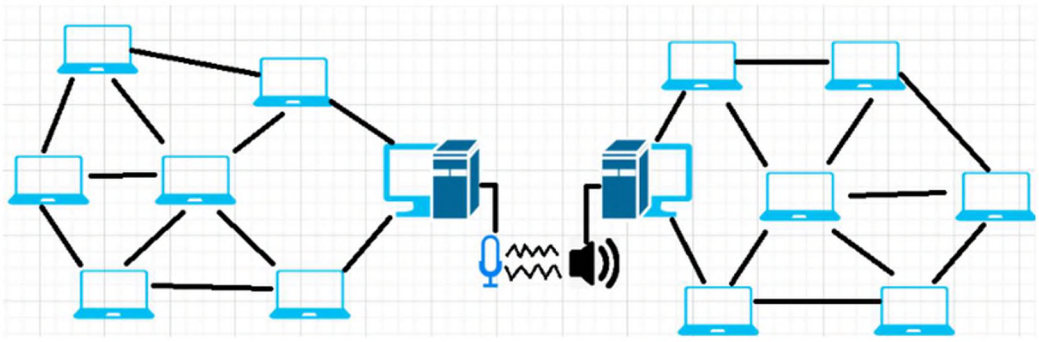

Рисунок 2.1 – Прихована мережа між мікрофоном та динаміком

2) Кооперативна мережа між динаміком і динаміком(рис.2.2). Ця модель розширює першу модель, замінюючи мікрофон на динамік у приймальному пристрої. У багатьох ситуаціях цільова система може не мати мікрофона. У таких випадках динамік може бути використаний як для передачі, так і для прийому даних, що забезпечує більш гнучкий підхід до атаки.

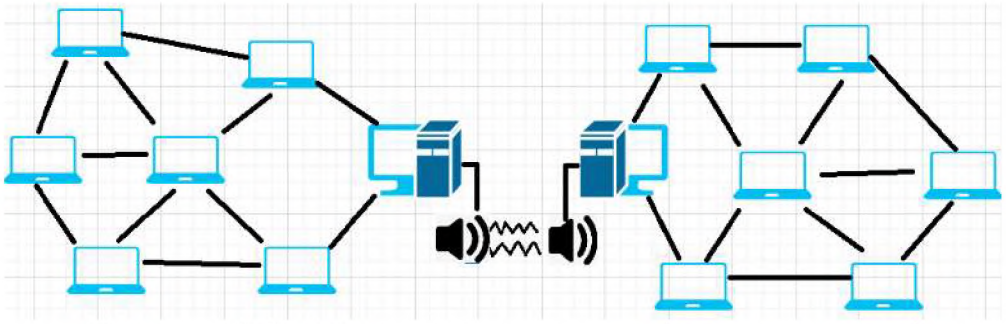

Рисунок 2.2 – Прихована мережа між двома динаміками

3)Кооперативна мережа між динаміком та централізовано керованим вбудованим динаміком(рис.2.3). У цій моделі мікрофони та динаміки з'єднані з близько розташованими терміналами або пристроями. Однак, якщо використовувати динаміки як приймальний пристрій, модель загрози може бути розширена. Наприклад, динаміки можуть бути окремо встановлені та підключені до інших динаміків через спільну лінію в будівлі та контролюватися центральним контрольним центром. У такому випадку, злочинець може передавати дані до системи, використовуючи спільні гучномовці, які розміщені на стіні. Цільовий термінал при цьому не обов'язково має бути поблизу від джерела передачі.

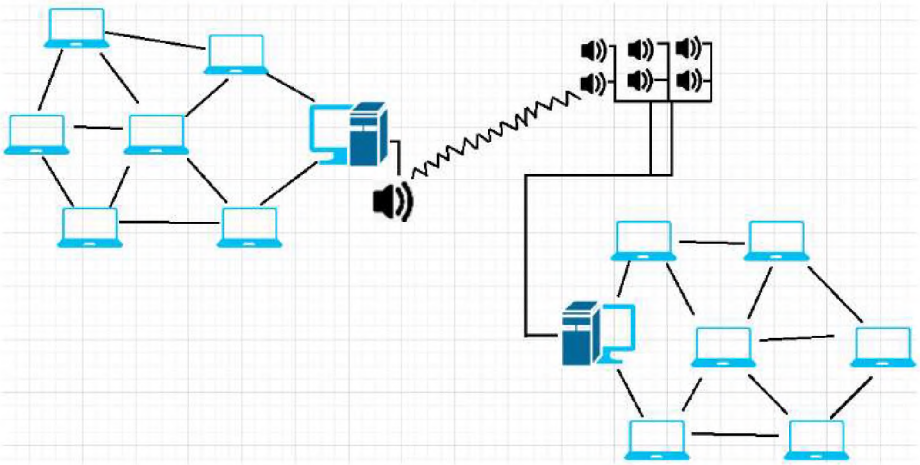

Рисунок 2.3 – Прихована мережа між мікрофоном та централізовано керованим динаміком

2.2 Методи протидії акустичним прихованим каналам витоку інформації представлених в першій частині

2.2.1 Методи протидії Fansmitter

Три основні категорії заходів протидії: процедурні, програмні та фізичні або на апаратному рівні.

Один з підходів включає створення спеціальних зон, де чутливі комп'ютери розміщуються в ізольованих просторах, з відсутністю мобільних телефонів, мікрофонів та іншого електронного обладнання. Цей метод, відомий як "чорно-червоне розділення", є ефективним проти різних акустичних, електромагнітних та оптичних загроз. Проте його застосування часто обмежене практичними причинами, такими як нестача простору.

Програмні заходи протидії включають використання захисних систем для кінцевих точок для виявлення зловмисної активності, а також програмне втручання в API управління вентиляторами та шинами даних. Ці методи можуть бути неефективними проти технік, які використовують руткіти та інші методи уникнення виявлення. Програмне регулювання швидкості вентиляторів може контролювати шум вентиляторів, але також може бути обійдене шкідливими програмами нижчого рівня.

Апаратні та фізичні заходи протидії охоплюють використання детекторів шуму для спостереження за звуковими хвилями на певних частотах.

Хоча ці пристрої існують, вони схильні до хибних спрацьовувань через навколишній шум. Іншим методом є глушіння сигналу вентилятора за допомогою створення фонового шуму, що може бути неефективним у тихих середовищах. Фізична ізоляція, яка передбачає виготовлення корпусу комп'ютера зі спеціального шумопоглинального покриття, є ефективною, але дорогою і непрактичною на велику шкалу. Заміна вентиляторів на тихіші або використання альтернативних систем охолодження, таких як водяне охолодження, може зменшити акустичне випромінювання, але це також менш практично для широкого застосування.

Заміна вентиляторів на спеціалізовані тихі вентилятори може обмежити рівень шуму, але навіть це не повністю запобігає випромінюванню шуму. Перехід на різні типи систем охолодження, такі як водяне охолодження або холодильні системи, може запобігти акустичне випромінювання, але це також менш практично для широкого впровадження. Таблиця 2.2 підсумовує перелічені заходи протидії разом з перевагами та недоліками кожного з них.

Таблиця 2.2 – Заходи протидії

Метод	Переваги	Недоліки
Розділення зон	Ефективна фізична ізоляція від зовнішніх загроз	Обмеження простору
Антивірус / моніторинг	Захист від відомих вірусів і шкідливих програм	Може бути обійдено руткітами або техніками ухилення
Регулювання вентилятора	Контроль шуму від вентилятора	Може бути обійдена низькорівневими шкідливими програмами
Виявлення шуму	Виявлення незвичайних акустичних сигналів	Хибно позитивні спрацьовування та тривоги
Перешкоджання сигналу	Глушіння потенційних витоків через шум	Генерація фонових шумів

Продовження таблиці 2.2

Заміна вентилятора,водяне охолодження тощо	Зниження рівня шуму, підвищення ефективності охолодження	Фінансові обмеження
Ізоляція корпусу	Ефективне блокування зовнішніх акустичних сигналів	Фінансові та просторові обмеження

2.2.2 MOSQUITO

Заходи протидії можна розділити на апаратні та програмні.

На високозахищених об'єктах часто практикується заборона використання будь-яких гучномовців (як пасивних, так і активних) для створення аудіорозриву між комп'ютерами. Це дозволяє уникнути передачі даних через акустичні канали. Більш м'які політики безпеки можуть забороняти використання мікрофонів, але допускають використання односторонніх гучномовців.

Одним із загальних рішень для гучномовців та навушників є інтеграція підсилювача прямо в аудіочіп. Інший метод включає використання ультразвукових глушилок, які створюють ультразвуковий фоновий шум для перешкоджання прихованим комунікаційним сигналам. Однак, такі глушилки не завжди ефективні, особливо на великих площах, оскільки їхня ефективність залежить від відстані до потенційних передавачів та приймачів, а радіус дії обмежується кількома метрами або однією кімнатою.

Для контролю ультразвукового діапазону вище 18 кГц рекомендується постійне сканування та аналіз цього діапазону. Однак, якщо пристрій для сканування знаходиться на значній відстані від джерела ультразвуку, цей метод може бути неефективним.

Програмні методи включають повне відключення аудіоапаратури в налаштуваннях UEFI/BIOS, що запобігає доступу шкідливого ПЗ до

аудіокодеку на рівні операційної системи. Така конфігурація, однак, унеможливлює використання аудіоапаратури, наприклад, для відтворення звуку, що може бути неприйнятним у деяких сценаріях. Інший варіант - це встановлення спеціалізованого HD аудіодрайвера, який запобігає зміні функцій аудіороз'єму або забезпечує жорстку політику щодо таких змін. Заходи загального захисту на програмному рівні також можуть включати використання систем проти шкідливих програм та систем виявлення вторгнення, які використовують моніторинговий драйвер для виявлення та блокування несанкційованих операцій переназначення гучномовця-мікрофона.

Ще одним підходом є фільтрація невловимих частот у діапазоні вище 18 кГц за допомогою низькочастотного або смугового фільтра, що дозволяє ефективно блокувати витік даних через ці частоти.

Таблиця 2.3 підсумовує перелічені заходи протидії разом з недоліками кожного з них.

Таблиця 2.3 – Заходи протидії

Захід	Переваги	Недоліки
Заборона використання навушників/гарнітури/колонок	Герметичний захист	Погана користувацька зручність
Використання активних колонок / вбудованих підсилювачів	Герметичний захист	Не застосовно до навушників та гарнітур
Відключення аудіокодека в BIOS/UEFI	Легко впровадити	Погана користувацька зручність
Виявлення переконфігурації роз'ємів / дотримання політик переконфігурації роз'ємів	Легко впровадити	Може бути обійдено складними вірусами та руткітами
Використання ультразвукових шумових передавачів (глушіння сигналу)	Універсальне рішення	Важко впровадити через шум, що генерується

Продовження таблиці 2.3

Виявлення ультразвукової передачі	Зовнішнє	Надійність
Низькочастотні фільтри (програмні/апаратні)	Універсальне рішення	Впровадження та додаткові витрати

2.2.3 DiskFiltration

Заходи для протидії цій атаці можна класифікувати на три категорії: апаратні, програмні та процедурні

Замінити традиційні жорсткі диски на твердотілі накопичувачі (SSD) може бути ефективним способом усунення загрози, оскільки вони не містять рухомих частин і виробляють мінімальний шум. Однак, така заміна в існуючих системах може бути непрактичною через високу вартість, а багато сучасних ПК, серверів, застарілих систем і ноутбуків все ще використовують жорсткі диски. Вибір жорстких дисків, що створюють менше шуму, або їх встановлення в спеціально розроблені корпуси також може зменшити рівень шуму.

Інші апаратні методи включають використання систем виявлення та глушіння шуму. Детектори шуму фокусуються на моніторингу фонового шуму в певних частотних діапазонах, але вони часто обмежені тихими середовищами та можуть бути неефективними у шумних умовах. З іншого боку, методи глушіння шуму, що створюють статичний фон, можуть бути непрактичними в робочих середовищах через дискомфорт, який вони можуть спричинити.

На рівні програмного забезпечення, сучасні жорсткі диски часто оснащені функцією автоматичного управління акустичним шумом, яка допомагає знижувати шум від роботи диска. Правильне налаштування цієї функції може допомогти обмежити радіус розповсюдження шуму. Використання систем виявлення вторгнень на хості (HIDS) та систем

запобігання вторгненням на хості (HIPS) також може допомогти виявляти та запобігати підозрілим діям на жорсткому диску, хоча віруси та руткіти на рівні ядра ОС можуть обійти такі системи. Розрізняти законні операції від зловмисних на жорстких дисках може бути складно.

Процедурні заходи, такі як фізичне відокремлення джерел сигналу від можливих приймачів, також є ефективними. Чутливе обладнання розташовується в обмежених зонах, де заборонено використання певних пристроїв. Зокрема, смартфони та інші записувальні пристрої не мають бути допущені поблизу чутливих комп'ютерів, щоб запобігти можливому витоку даних.Таблиця 2.4 підсумовує перелічені заходи протидії разом з недоліками кожного з них.

Таблиця 2.4 – Заходи протидії

Захід	Переваги	Недоліки
Заміна жорсткого диску на SSD	Зниження рівня шуму, вища швидкість	Висока вартість, складність заміни
Придбання тихих HDD	Зменшення рівня шуму	Обмежений вибір, можливі додаткові витрати
Встановлення спеціальних корпусів	Ефективне глушіння шуму	Додаткові витрати та складність установки
Детектори шуму	Моніторинг і виявлення несподіваних звуків	Обмежене використання в шумних середовищах
Пристрої глушіння сигналів	Запобігання передачі даних через шум	Перешкоди для робочого середовища
HIDS/HIPS	Захист від вторгнення та виявлення підозрілих дій	Можливість обходу вірусами, складність виявлення атак
Виявлення зловмисної діяльності	Раннє виявлення та запобігання атакам	Складність у розрізненні зловмисних дій

Продовження таблиці 2.4

Правильне налаштування автоматичного управління акустикою	Зменшення шуму від HDD	Потреба у точному налаштуванні
Зонове відокремлення	Фізична безпека обладнання	Обмеження доступу, складності в забезпеченні дотримання

2.2.4 POWER-SUPPLaY

Існують чотири основні категорії заходів, які можуть бути використані для захисту від запропонованого таємного каналу: зонове відокремлення, виявлення сигналів, глушіння сигналів та блокування сигналів.

В рамках процедурних заходів можливе використання стратегії зонування, де чутливі комп'ютери розміщуються у спеціалізованих зонах з обмеженням на використання мобільних телефонів, мікрофонів та іншого електронного обладнання. Проте, реалізація такого зонування може бути ускладнена обмеженнями простору та витратами. В таких зонах необхідно заборонити використання записувальних пристроїв на певній відстані від ізольованих систем.

Системи виявлення вторгнень на хості (HIDS) використовуються для моніторингу активності запущених процесів, щоб виявити підозрілі дії, такі як ненормальне регулювання частоти перемикання. Однак, цей метод може призводити до помилкових спрацьовувань, оскільки багато законних процесів використовують інтенсивні обчислення. Також віруси, які використовують техніки ухилення, можуть обійти ці системи.

Апаратні заходи включають детектори шуму для моніторингу спектру частот, але вони можуть спричинити помилкові спрацьовування через

зовнішні шуми. Глушіння сигналу блоку живлення за допомогою створення фонового шуму може бути неефективним у тихих середовищах.

Фізична ізоляція, яка включає використання спеціальних шумопоглинальних покриттів для корпусів комп'ютерів, є ефективною, але дорогою та непрактичною для масштабного застосування. Моніторинг аудіоканалу на наявність аномальних піків енергії може допомогти виявити приховані передачі, але його ефективність зменшується на великих відстанях від джерела сигналу. Таблиця 2.5 підсумовує перелічені заходи протидії разом з викликами кожного з них.

Таблиця 2.5 – Заходи протидії

Метод	Переваги	Недоліки
Процедурне зонування	Ефективна ізоляція чутливих систем	Обмеження простору і високі витрати
Системи HIDS/HIPS	Моніторинг підозрілих дій	Помилкові спрацьовування, можливість обходу
Апаратні детектори шуму	Виявлення акустичних сигналів	Помилкові спрацьовування, обмеження у використанні
Глушіння сигналу	Зменшення ризику перехоплення сигналів	Не застосовно в тихих середовищах
Фізична ізоляція	Ефективне блокування акустичних сигналів	Високі витрати, непрактично на великому масштабі
Моніторинг аудіоканалу	Виявлення прихованих передач	Обмежена ефективність на великій відстані

2.3 Методи протидії акустичним прихованим каналам витоку інформації

Протидія акустичним прихованим каналам витоку інформації є важливою частиною забезпечення інформаційної безпеки. Ось методи які я рекомендую для протидії цим каналам витоку інформації:

1) Контроль фізичного доступу: Обмеження доступу до приміщень, де знаходиться конфіденційна інформація, є ключовим. Також важливо контролювати пристрої, які можуть бути використані для запису або передачі акустичної інформації.

2) Аудіо маскування: Використання генераторів білого шуму або акустичних ширм може допомогти маскувати звуки, які містять конфіденційну інформацію, тим самим ускладнюючи їх перехоплення.

3) Аналіз акустичного середовища: Регулярний аналіз акустичного середовища може допомогти ідентифікувати потенційні приховані канали або незвичайну активність, що може вказувати на акустичні витоки.

4) Регулярне навчання персоналу: Навчання персоналу щодо ризиків акустичного витоку інформації та методів їхнього запобігання може значно знизити ймовірність ненавмисних витоків.

5) Технології виявлення витоків: Використання спеціалізованого обладнання для виявлення електронних пристроїв, які можуть бути використані для створення акустичних каналів.

6) Акустичне зонування: Розділення приміщень на зони з різним рівнем конфіденційності, щоб зменшити ризик витоку інформації через акустичні канали.

Ці методи можуть бути використані окремо або в комбінації для забезпечення більш ефективного захисту від акустичних прихованих каналів витоку інформації.

2.3.1 Контроль фізичного доступу

Контроль фізичного доступу є критичним для запобігання несанкційованому доступу до обладнання, даних та інших чутливих ресурсів.

Це не тільки допомагає запобігти потенційним акустичним витокам інформації, але й захищає від широкого спектру загроз безпеці, включаючи фізичне втручання, крадіжку, шпигунство тощо.

Важливо встановити Обмеження Доступу до Важливих Зон. Встановлення систем контролю доступу, таких як електронні картки, біометричні сканери або кодові замки.Визначення зон із високим рівнем конфіденційності та обмеження доступу до них тільки для уповноважених осіб.

Встановити камери спостереження для моніторінгу доступу до чутливих зон та регулярні перевірки безпеки для виявлення недозволених пристроїв або незвичайної активності.

Встановлення контрольованої зони, на якій унеможливлюється несанкційоване перебування сторонніх осіб. Створення фізичних бар'єрів, таких як замкнені двері або шумозахисні перегородки для запобігання несанкційованому доступу або прослуховуванню. Створення буферних зон, які відокремлюють конфіденційні простори від загальнодоступних або менш захищених зон.

Також важливо запровадити контроль персоналу та відвідувачів які заходять до чутливих зон.

Впровадження ефективного контролю фізичного доступу вимагає ретельного планування та оцінки ризиків. Важливо враховувати специфіку організації, розташування об'єктів, природу зберіганої інформації та потенційні загрози. Також важливо регулярно переглядати та оновлювати системи контролю доступу, щоб вони відповідали змінам у технологіях та загрозах безпеки.

2.3.2 Аудіо маскування

Аудіо маскування є ефективним методом для захисту від акустичного витоку інформації. Цей метод полягає в створенні звукового "шуму" або інших акустичних сигналів, які утруднюють або неможливо перехоплення та розуміння розмов, які відбуваються у захищеному просторі.

Аудіомаскування повинно виконуватися в широкому діапазоні частот, охоплюючи як чутний, так і ультразвуковий діапазони. Чутний діапазон(20Гц-20кГц) це стандартний діапазон частот, на яких людське вухо може сприймати звук. Аудіомаскування в цьому діапазоні допоможе приховати будь-які сигнали або інформацію, які можуть бути сприйняті або перехоплені через звичайні засоби слуху. Ультразвуковий діапазон хоча і виходить за межі сприйняття людського вуха, він може бути використаний для передачі даних через приховані канали. Маскування в ультразвуковому діапазоні є важливим для запобігання несанкційованого витоку інформації через такі технології.

Для цього можна використовувати генератори шуму які створюють невиразні звукові сигнали. Білий шум має рівномірний спектральний розподіл, що означає, що кожна частота має приблизно однакову потужність або інтенсивність, він використовується для маскування інших звуків у навколишньому середовищі. Рожевий шум має спектральний розподіл, де кожна октава (або будь-який інший логарифмічний інтервал) містить однакову кількість енергії. Це означає, що на нижчих частотах потужність більша, ніж на вищих. Коричневий (або червоний) шум характеризується ще більшою інтенсивністю на нижчих частотах порівняно з рожевим шумом. Синій і Фіолетовий Шуми мають більш високу інтенсивність на вищих частотах. Білий шум слід використовувати тому що він має рівномірний розподіл енергії по всьому частотному спектру, включаючи як чутний, так і ультразвуковий діапазон. Тому він більш універсальний, але у деяких випадках можливе використання й інших генераторів шуму.

Також генератори акустичних завад можуть бути ефективні, вони створюють більш динамічний та змінний шумовий сигнал, який може бути кращім у маскуванні певних типів сигналів особливо в ультразвуковому діапазоні. Але такі генератори можуть бути складними у налаштуванні та використанні.

Для маскування загального офісного шуму або мовлення генератори білого шуму можуть бути досить ефективними, але у випадку необхідності блокування специфічних акустичних сигналів або для захисту від складних акустичних атак, генератори акустичних завад можуть бути більш ефективними. Також можливо використовувати комбінацію цих генераторів для досягнення оптимального балансу

Ці звуки маскують голосову комунікацію, роблячи її менш зрозумілою для сторонніх слухачів або пристроїв перехоплення. Також звукові ширми які робляться з звукопоглинаючого матеріалу або конструкцій які ефективно блокують або розсіюють звук, запобігаючи його витоку за межі певної зони.

Загалом, для ефективного аудіомаскування важливо створити шумовий фон, який одночасно покриває широкий спектр частот. Це може включати генерацію білого шуму, який рівномірно розподіляє енергію по всьому частотному спектру, або інші типи шуму (наприклад, рожевий шум), які можуть бути більш ефективними для певних сценаріїв використання.

Аудіо маскування не є універсальним рішенням і має деякі обмеження. Наприклад, надмірний шум може бути некомфортним або відволікати співробітників. Також, цей метод може не бути ефективним проти дуже чутливих або розширених методів перехоплення.

Цей метод є важливою частиною комплексного підходу до забезпечення інформаційної безпеки, особливо в середовищах, де конфіденційність розмов є критичною. Воно може ефективно використовуватися разом з іншими заходами безпеки, такими як контроль фізичного доступу та шифрування даних.

2.3.3 Аналіз акустичного середовища

Аналіз акустичного середовища є ключовим компонентом у захисті від акустичних витоків інформації. Цей метод включає в себе вивчення та моніторинг акустичних умов у середовищі, де обробляється або зберігається

конфіденційна інформація, з метою ідентифікації та запобігання потенційним витокам.

Одним із аспектів аналізу акустичного середовища є виявлення чутливих зон. Потрібно ідентифікувати місця де обробляються конфіденційні дані, та оцінити ризики пов'язані з акустичним витоками у цих зонах. Також потрібно оцінити акустичні можливості середовища. Проаналізувати звукопоглинання та звукоізоляцію приміщень та вимірювання рівнів шуму та визначення джерел зовнішнього шуму, які можуть впливати на акустичну безпеку.

Ще один із аспектів це виявлення нестандартних акустичних сигналів. Потрібно проводити моніторинг на наявність нестандартних або підозрілих акустичних сигналів, які можуть вказувати на спроби несанкційованого прослуховування або встановлення пристроїв перехоплення.

Слід не забувати про регулярні перевірки та переоцінювання акустичного середовища для виявлення змін або нових потенційних загроз.

Для реалізації можливо використання спеціалізованого обладнання, таких як аудіо аналізатори, звукові метри та інші інструменти використовуються для точного вимірювання акустичних параметрів. Залучення акустичних інженерів або консультантів з безпеки для оцінки ризиків та рекомендацій щодо поліпшення акустичної безпеки та розробка чітких процедур та політик щодо акустичної безпеки, включаючи навчання персоналу.

Для аналізу акустичного середовища можна використовувати різноманітні прилади та обладнання, що дозволяють вимірювати, реєструвати та аналізувати звукові хвилі.

Звукоміри (Аудіометри) пристрої, які використовуються для вимірювання рівня звукового тиску. Вони можуть вимірювати гучність у децибелах (дБ) і часто використовуються у професійній аудіометрії, а також для моніторингу шуму в робочих та житлових зонах.

Спектроаналізатори прилади дозволяють аналізувати спектральний склад звукових сигналів, розкладаючи їх на окремі частоти. Вони корисні для детального аналізу звукового сигналу та визначення домінуючих частот.

Мікрофони з високою чутливістю для збору даних з акустичного середовища використовуються чутливі мікрофони. Вони можуть бути налаштовані на певні частотні діапазони та використовуватися разом з аналізаторами для точних вимірювань.

Полярні діаграми та антени використовуються для аналізу напрямку приходу звукових хвиль. Це може бути корисно для визначення джерела звуку в складних акустичних середовищах.

Аудіо інтерфейси та програмне забезпечення: Для цифрового запису та аналізу звуку можуть використовуватися аудіо інтерфейси, підключені до комп'ютера, на якому запущено спеціалізоване програмне забезпечення для аудіоаналізу.

Багатоканальні реєстратори: Для комплексного аналізу акустичного середовища можна використовувати реєстратори, які одночасно записують з декількох мікрофонів, розміщених у різних місцях.

Більш радикальним рішенням є зміна у дизайні приміщень для покращення звукоізоляції та зменшення ризику витоку інформації.

Для виявлення прихованого каналу також можливо застосувати телефон з встановленим на ньому додаток для аудіоспектрального аналізу. На рис. 2.4 та рис. 2.4 зображені спектрограми зняті з ноутбуку при швидкості вентилятора ЦП 3800 об/хв(рис. 2.4) та 4200 об/хв(рис. 2.5). На цих рисунках видно різницю шуму таким чином можна виявляти звичний шум, та наглядати, якщо появляться якісь стрибки у спектрограмі і при цьому робоча станція не виконує дії, це може ставити у підозру та почати перевіряти більш специфічним обладнанням

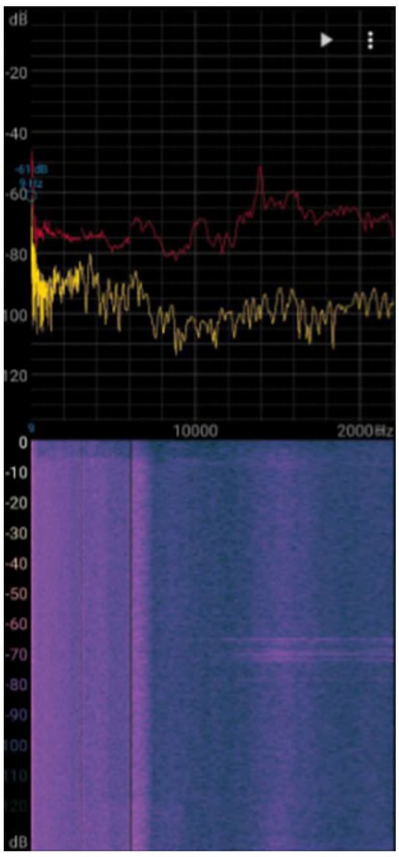

Рисунок 2.4 – Спектрограма акустичного шуму при 3800 об/хв вентилятора ЦП

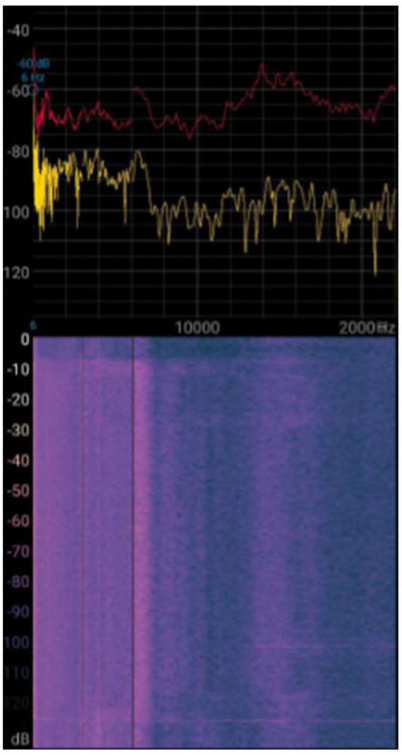

Рисунок 2.5 – Спектрограма акустичного шуму при 4200 об/хв вентилятора ЦП

Після виявлення прихованого каналу, можна почати процес глушіння, який генерує імпульсний потяг для блокування прихованого каналу. Ця послідовність модулюється для передачі як звуковий сигнал із несучою частотою, що використовується прихованим каналом, заважаючи розшифровці приймача.

Аналіз акустичного середовища є важливим елементом комплексної стратегії інформаційної безпеки в організації.

2.3.4 Регулярне навчання персоналу

Посилення обізнаності та освіти співробітників допомагає мінімізувати ризики, пов'язані з ненавмисним витоком інформації через акустичні канали.

Основними напрямками навчання будуть такі аспекти як:

Усвідомлення ризиків, розповісти персоналу, що таке акустичні приховані канали та як вони можуть бути використані для витоку інформації.

Ознайомлення з внутрішніми політиками безпеки, процедурами та кращими практиками та Навчання правильному поводженню з конфіденційною інформацією.

Обговорення фізичних заходів безпеки таких як значення контролю фізичного доступу, аудіо маскування та використання безпечних пристроїв для обговорення конфіденційних даних.

Важливо регулярно проводити навчання та тренінги щоб тримати персонал в курсі останніх загроз і технологій безпеки так як світ інформаційної безпеки постійно змінюється, і нові загрози вимагають оновлення знань і навичок. Регулярне навчання допомагає закріпити культуру безпеки в організації, де кожен співробітник усвідомлює свою роль у захисті інформації.

Регулярне навчання персоналу допомагає не тільки підвищити обізнаність працівників щодо потенційних загроз, але й надає їм інструменти та знання для ефективного запобігання та реагування на ці загрози.

Список тем які рекомендуються до розглядання на навчаннях надані у додатоку Ґ

2.3.5 Технології виявлення витоків інформації

Ці технології зосереджуються на ідентифікації та блокуванні можливих шляхів несанкційованого передавання інформації через акустичні сигнали.

Використання чутливих мікрофонів та аналітичного програмного забезпечення для виявлення незвичайних звуків або змін в акустичному середовищі, які можуть вказувати на спроби прослуховування.

Детектор безперервно спостерігає аудіосигнали за допомогою акустичного сенсора, наприклад, мікрофона. Він використовує фільтр смугового пропускання(Band Pass Filter) для фільтрації аудіосигналів поза спектром. Якщо амплітуда вихідного сигналу від перевищує поріг, вважається, що виявлено прихований канал.

Ідентифікація змін у звичайних акустичних умовах, які можуть свідчити про спроби несанкційованого прослуховування або встановлення прихованих пристроїв.

Також використовувати інструменти для виявлення нестандартної мережевої активності, яка може вказувати на витік акустичних даних, таких як системи виявлення вторгнень(IDS), система запобігання вторгнень(IPS), аналізатор мережевого трафіку або система управління подіями та інформацією безпеки(SIEM).

Ефективний захист від акустичних витоків часто вимагає комплексного підходу, який включає комбінацію різних технологій та методів. Наприклад, поєднання акустичного аналізу, радіочастотної детекції, фізичного огляду та кібербезпеки може забезпечити більш повний захист від потенційних загроз.

2.3.6 Акустичне зонування

Акустичне зонування в контексті захисту від атак акустичними прихованими каналами передбачає створення окремих зон у приміщенні або будівлі, кожна з яких має власний рівень акустичної безпеки. Це робиться для того, щоб мінімізувати ризик витоку конфіденційної інформації через неконтрольоване розповсюдження звуку. Наприклад, у найбільш захищених

зонах, де обговорюються або обробляються секретні дані, встановлюються високі стандарти звукоізоляції та використовуються технології аудіо маскування, як-от білий шум. Також може бути обмежений доступ персоналу та встановлені процедури для зберігання конфіденційності розмов. У менш чутливих зонах, де вимоги до конфіденційності не такі високі, заходи можуть бути менш суворими. Акустичне зонування дозволяє більш ефективно управляти ризиками, пов'язаними з витоком інформації через акустичні канали, і є важливою частиною комплексної стратегії інформаційної безпеки.

2.4 Висновок

У другому розділі було описано модель загроз, надано опис потенційних загроз та зловмисників які можуть нашкодити компанії. Було розглянено три різні моделі загроз такі як мережа між динаміком і мікрофоном, динаміком і динаміком та мікрофоном і централізованим керованим динаміком. Також представлені методи протидії акустичним прихованим каналам витоку інформації як конкретних атак так і в цілому

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА.

У сучасному світі, де інформація є ключовим активом будь-якої компанії або організації, забезпечення її безпеки набуває критичного значення. В контексті кібербезпеки особливу увагу слід звернути на акустичні приховані канали витоку інформації.

Економічна частина дослідження фокусується на аналізі витрат, пов'язаних із запобіганням та протидією акустичним прихованим каналам витоку інформації. Важливо зрозуміти, що інвестиції в заходи безпеки не лише захищають цінну інформацію, а й, в довгостроковій перспективі, можуть виявитися економічно вигідними, уникнувши значних збитків від потенційних інцидентів безпеки.

3.1 Визначення витрат на проектування та експлуатацію системи інформаційної безпеки

Основою для визначення витрат на створення систем інформаційної безпеки є концепція сукупності вартості володіння(Total Cost of Ownership), запропонована Gartner Group. У цій моделі враховуються наступні IT-витрати: фіксовані(капітальні) вкладення і поточні витрати.

Фіксовані(капітальні) витрати здійснюються на етапі створення системи інформаційної безпеки, поточні на етапі її функціонування. Варто зазначити, що вибір тієї або іншої апаратної й програмної платформи досить істотно впливає на наступні поточні витрати. Вагові частки статей витрат представлені у табл 3.1.

Таблиця 3.1 – Вагові частки статей витрат у сукупній вартості

Фіксовані вкладення	21%
Поточні витрати у т.ч.	79%
Керування системою	12%
Технічна підтримка й відновлення	21%
Активність користувача	46%

Капітальні(фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{аз} + К_{навч} + К_{н} \quad (3.1)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 6 тис. гри.

Проведення первинного аудиту безпеки для виявлення потенційних ризиків.

Розробка стратегії інформаційної безпеки та плану імплементації.

Консультації з експертами з кібербезпеки для оцінки потреб у захисті від акустичних прихованих каналів зв'язку.

Складання технічного завдання для вибору необхідного обладнання та програмного забезпечення

Кзпз — вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 5 тис. грн;

Придбання або оновлення антивірусного програмного забезпечення.(1000 грн)

Придбання або оновлення необхідних для роботи підприємства ПЗ (2000 грн)

Придбання ПЗ яке дозволяє контролювати та захищати конфіденційну інформацію таке як Symantec Data Loss Prevention (2000 грн)

Каз - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 9 тис. грн;

Закупівля мережевого обладнання, яке забезпечує захищене з'єднання та моніторинг трафіку.

Придбання спеціалізованого обладнання для знищення акустичних сигналів або апаратури активного шумозаглушення.

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу, 2 тис. грн;

Організація тренінгів з кібербезпеки для технічних фахівців.

Навчання персоналу основам безпеки, включаючи протидію соціальній інженерії та розпізнавання потенційних загроз.

Кн - витрати на встановлення обладнання та налагодження системи інформаційної безпеки 2,5 тис. грн;

Витрати на фізичне встановлення мережевого обладнання.

Налагодження та конфігурація захисного ПЗ та обладнання.

Первинна настройка систем шифрування та DLP.

За формулою 3.1 розраховуємо капітальні витрати

$$K= 6000+5000+9000+2000+2500= 24500$$

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

$$С = Св + Ск + Сак, тис. грн \quad (3.2)$$

Де $С_в$ – Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки.

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – «активність користувача», витрати викликані активністю користувачів системи інформаційної безпеки.

$С_в$ – орієнтовно визначимо виходячи із вагової частки статей витрат (21%) з сукупної вартості інформаційної системи

$$Св =24500*0.21= 5145$$

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$Ск = Сн + Са + Сз + Сєв + Сел + со + Стос, грн \quad (3.3)$$

Витрати на навчання адміністративного персоналу и кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо (Сн=2000 грн).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і

нематеріальних активів (ПЗ); Вартість купівлі ліцензійного ПЗ 5000 грн, мінімальний срок дії користування - 2 роки

Са=5000/2 = 2500 грн/рік

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_З$), складає:

$$Сз = Зосн + Здод, грн \quad (3.4)$$

Де $З_{осн}$ $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна Заробітна плата в місяць спеціаліста інформаційної безпеки становить ($З_{осн}$ = 20500 грн/місяць)

$$З_{дод} = 246000* 8\% =19680 \text{ грн}$$

$$С_З = 246000 + 19680 = 265680 \text{ грн}$$

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати (за узгодженням з консультантом економічної частини дипломного проекту)

$$С_{есв}= 31500 *0.22 = 6930 \text{ грн}$$

Вартість електроенергії', що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$Сел = Р * FP * Це, грн \quad (3.5)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$$Р = 0,7 *3 =2.1 \text{ кВт}$$

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (працює кожен день с 10:00 до 17:00 7 годин на добу);

Fр =1700 * 3 комп'ютера = 5040 годин.

Це – тариф на електроенергію, грн/кВт-годин. (Це = 2.64)

$$С_{ел} = 2.1 * 2.64 * 5040 = 27941 \text{ грн}$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу визначаються за даними організації. ($С_о = 1500$)

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$$K = 24500 \text{ грн}$$

$$С_{тос} = 24500 * 3\ \% = 735 \text{ грн}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними таблиці 3.1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

$$С_{ак} = 24500 * 46\% = 11270 \text{ грн}$$

Розрахуємо витрати на керування системою інформаційної безпеки за формулою 3.3:

$$Ск=2000+2500+265680+6930+27941+1500+735=307286 \text{ грн}$$

У кожному конкретному випадку можуть бути враховані й інші види поточних витрат, що визначаються специфікою експлуатації проектованої системи інформаційної безпеки.

Експлуатаційні витрати розрахуємо за формулою 3.2

$$С=5145+307286+11270=323701 \text{ грн}$$

3.2 Оцінка величини збитку

Для розрахунку вартості збитку необхідно застосувати спрощену модель оцінки

Необхідні такі дані для розрахунку:

$t_п$ - час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 годин;

$t_в$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 годин;

$t_{ви}$ - час повторного введення загубленої інформації співробітника атакованого вузла або сегмента корпоративної мережі, 2 годин

$З_с$ - заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 25000 грн на місяць

$З_о$ - заробітна плата обслуговуючого персоналу (адміністраторів та ін.) 21000 грн на місяць

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін. осіб) 2 особи

$Ч_с$ - чисельність співробітників атакованого вузла або сегменту корпоративної мережі, 4 осіб

О - обсяг продажів атакованого вузла або сегмента корпоративної мережі, 1250000 тис. грн у рік;

$П_{зч}$ - вартість заміни встаткування або запасних частин, 12000 грн;

і – число атакованих вузлів або сегментів корпоративної мережі 3;

n – середнє число атак на рік.10

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = Пп + Пв + V \quad (3.6)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (перевстановлення системи, зміна конфігурації та ін.),

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$Пп = \left(\frac{\sum Зс}{F}\right) * tп, грн \quad (3.7)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 25000 грн на місяць;

tп — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 годин;

Пп= ((25000/176)*3)*2= 852 грн

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$Пв = Пви + Ппв + Пзч \quad (3.8)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі,

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$: ($t_{ви}$ = 3)

$$Пви = \frac{\sum Зс}{F} * t_{ви} \quad (3.9)$$

Пви = ((25000/176)*3)*3 = 1278 грн

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки $t_В$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв = \frac{\sum Зо}{F} * tв \quad (3.10)$$

$П_{пв}$ = (21000/176)*2 = 238 грн

$П_в = 1278 + 238 + 12000 = 13516$ грн

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі: (О=750 000)

$$V = \frac{O}{Fr} * (t\text{п} + t\text{в} + t\text{ви}) \quad (3.11)$$

Де Fr – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий, тиждень 8-ми годинний робочий день) становить близько 2080 ч.

V = (1250000/2080) *(2+2+2) = 3605 грн

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

U = 852 + 13516 + 3605 = 17973 грн

Таким чином загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum i \sum n\, U \quad (3.12)$$

Де і – число атакованих вузлів або сегментів корпоративної мережі, 3;

n – середнє число атак на рік, 10;

B = 17973* 3 * 10 = 539190 грн

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B * R - C \quad (3.13)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. гри;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, 0,75 частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. гри.

$$E = 539190 * 0.7 – 323701 = 53732 \text{ грн}$$

3.3 Визначення та аналіз показників економічної ефективності

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

У цьому випадку необхідно порівняти сукупну вартість володіння, розраховану для двох варіантів проектного рішення щодо створення або удосконалення системи інформаційної безпеки, і вибрати варіант із найменшою з них.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$\text{ROSI} = \frac{E}{K}, \text{частка одиниці} \qquad (3.14)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, 53732 грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, 24500 гри.

Якщо порівнюється два варіанти системи інформаційної безпеки, то обирається варіант з більшим значенням ROSI.

$$\text{ROSI} = 53732 / 24500 = 2{,}1$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності Ен.

Проект системи інформаційної безпеки визнається доцільним за умови

$$\text{ROSI} > \text{Ен} \qquad (3.15)$$

При ROSI<E_H варіант є збитковим і більш економічним визнається відмова від його реалізації.

Розрахунок бажаного значення коефіцієнта ефективності виконується за узгодженням з консультантом економічної частини.

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій $T_р$.

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$\text{То} = \frac{K}{E} = \frac{1}{ROSI} \text{ років} \quad (3.16)$$

Якщо варіанти економічно рівноцінні, то приймається варіант, що забезпечує більш високу надійність, поліпшення умов праці.

$T_о$ = 1/2,1= 0.47 (приблизно 6 місяців)

3.4 Висновки

- Капітальні витрати складають: 24500грн

- Експлуатаційні витрати на впровадження інформаційної безпеки складають: 323701 грн

- Можливий збиток від атаки на вузол складають: 17973 грн

- Загальний ефект від впровадження системи інформаційної безпеки складає - 53732 грн

Термін окупності капітальних інвестицій - приблизно 6 місяців

Тому економічна доцільність впровадження інформаційної безпеки обґрунтована і може піти на користь підприємству.

ВИСНОВКИ

Робота зосереджена на аналізі загроз та розробці методів протидії акустичним прихованим каналам витоку інформації.

Було розглянуто різні приховані канали витоку інформації, серед них був зроблений вибір сфокусуватися саме на акустичних каналах витоку інформації.

Розглядається значення інформаційної безпеки у сучасному цифровому світі. Представлені такі документи як Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” та рекомендації Держспецзв'язку та НД ТЗІ щодо захисту цих каналів.

Проведено аналітичний огляд деяких акустичних каналів витоку інформації в яких було надано загальну інформацію щодо цих каналів та швидкість з якою кожний із цих каналів може передавати інформацію.

Аналізується модель загроз, яка передбачає наявність суб'єктів, що намагаються незаконно обмінюватися інформацією через акустичні приховані канали.

Представлено ряд методів для запобігання та протидії витоку інформації через акустичні канали, включаючи контроль фізичного доступу, аудіо маскування, аналіз акустичного середовища, регулярне навчання персоналу, та використання спеціалізованого обладнання для виявлення витоків.

Економічна частина аналізує витрати та ефективність заходів протидії, підкреслюючи економічну доцільність впровадження систем інформаційної безпеки.

Продемонстровано, що належне усвідомлення та протидія акустичним прихованим каналам витоку інформації є критично важливими для забезпечення інформаційної безпеки у сучасному світі.

ПЕРЕЛІК ПОСИЛАНЬ

1) Anderson R. J. Security Engineering: A Guide to Building Dependable Distributed Systems [Електронний ресурс] / Ross J. Anderson // Wiley Publishing, Inc. – 2008. – Режим доступу до ресурсу: https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf .

2) Троян [Електронний ресурс] – Режим доступу до ресурсу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/.

3) Rootkit [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/rootkit.

4) Backdoor (computing) [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Backdoor_(computing).

5) Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers. [Електронний ресурс] / Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. – 2016. – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf.

6) Marco De Falco. Stuxnet Facts Report [Електронний ресурс] / Marco De Falco. – 2012. – Режим доступу до ресурсу: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf.

7) Agent.btz: [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://securelist.com/agent-btz-a-source-of-inspiration/58551/.

8) MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication [Електронний ресурс] / Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. – 2018. – Режим доступу до ресурсу: https://arxiv.org/pdf/1803.03422.pdf.

9) Powered speakers [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Powered speakers.

10) https://cryptome.org/tempest-2-95.htm [Електронний ресурс] – Режим доступу до ресурсу: RED/BLACK INSTALLATION GUIDANCE.

11) Mordechai Guri. POWER-SUPPLaY: Leaking Data from Air-Gapped Systems by Turning the Power-Supplies Into Speakers [Електронний ресурс] / Mordechai Guri. – 2020. – Режим доступу до ресурсу: https://arxiv.org/pdf/2005.00395.pdf.

12) DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise [Електронний ресурс] / Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. – 2016. – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf.

13) Abdullah Al Mamun. Hard Disk Drive / Abdullah Al Mamun, GuoXiao Guo, Chao Bi. – Boca Raton: CRC Press, 2007. – 359 с. – (1st Edition).

14) Design, Implementation and Evaluation of Covert Channel Attacks. /Hamed Okhravi Stanley Bak Samuel T. King

15) Eunchong Lee. Various threat models to circumvent air-gapped systems for preventing network attack [Електронний ресурс] / Eunchong Lee, Hyunsoo Kim, Ji Won Yoon. – 2016.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Перший Розділ	32	
6	А4	Спеціальна частина	20	
7	А4	Економічний розділ	9	
8	А4	Висновки	1	
9	А4	Перелік використаних джерел	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1.ДерезенкоАВ_125м-22-2_ПЗ.docx

2. ДерезенкоАВ_125м-22-2_ПЗ.pdf

3. ДерезенкоАВ_125м-22-2_П.pptx

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2

Дерезенко Антона Вячеславовича

на тему: «Методи протидії акустичним прихованим каналам витоку інформації»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на ___ сторінках.

Метою кваліфікаційної роботи є розвиток методів протидії акустичним прихованим каналам витоку інформації.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази із протидії прихованим каналам; аналітичний огляд акустичних прихованих каналів витоку інформації; розглянуто модель загроз витоку інформації акустичними прихованими каналам.

Представлені заходи із захисту інформації від витоку акустичними прихованими каналами.

Практичне значення результатів кваліфікаційної роботи полягає у аналізі параметрів акустичних прихованих каналів витоку інформації.

До недоліків роботи відноситься:

- недостатньо структуровано викладення запропонованих рішень;
- відсутність експериментальної перевірки запропонованих рішень.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Дерезенко А.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки « добре ».

Керівник кваліфікаційної роботи, професор Корнієнко В.І.

Керівник спец. розділу, ст. викладач Кручінін О.В.

ДОДАТОК Г. Відгук керівника економічного розділу

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 92 б. («Відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Ґ Рекомендовані теми для навчання персоналу

1) Основи Прихованих Акустичних Каналів:

Роз'яснення концепції акустичних прихованих каналів витоку інформації та огляд історичних випадків та реальних прикладів використання акустичних каналів для витоку даних.

2) Методи та Техніки Витоку Інформації:

Обговорення різних методів, якими акустичні канали можуть бути використані для передачі даних (наприклад, через маніпуляцію звуку).

Перелік потенційних загроз та вразливостей у сучасних інформаційних системах.

3) Розпізнавання та Попередження Атак:

Навчання, як ідентифікувати потенційні ознаки акустичного витоку інформації та стратегії і практики для попередження та зменшення ризиків акустичного шпигунства.

4) Заходи Фізичної Безпеки:

Важливість фізичної ізоляції чутливих просторів та використання шумопоглинальних матеріалів і акустичних бар'єрів.

5) Політика Безпеки та Процедурні Заходи:

Роль політики безпеки у захисті від акустичних витоків та обговорення процедур, таких як регулярні перевірки безпеки та обмеження доступу до чутливих областей.

6) Технологічні Заходи Протидії:

Використання спеціалізованого обладнання для виявлення та блокування акустичних сигналів та перелік програмного забезпечення та інструментів для моніторингу та аналізу акустичного середовища.

7) Відповідальність та Свідомість Персоналу:

Наголос на важливості індивідуальної відповідальності кожного співробітника у захисті конфіденційної інформації.