Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Засоби удосконалення комплексу технічного захисту інформації

Виконавець: студент IV курсу, групи КБ-42

_____ **Валерій РУДЕНКО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-42** (група) **Валерію Миколайовичу Руденку** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби удосконалення комплексу технічного захисту інформації

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Технічні канали витоку інформації, комплекси технічного захисту інформації, засоби технічного захисту інформації

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з технічними каналами витоку інформації, їх класифікацією, каналами витоку інформації, ознайомитись з комплексами технічного захисту інформації, їх визначенням, засобами, які використовуються, розробити рекомендації удосконалення комплексу технічного захисту інформації

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Аналіз існуючих засобів комплексу технічного захисту

інформації.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Валерій РУДЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 11.02.2023	*виконано*
2	Аналіз літератури	11.02.2023 – 28.02.2023	*виконано*
3	Обґрунтування вибору рішення	28.02.2023 – 01.03.2023	*виконано*
4	Огляд технічних каналів витоку інформації	01.03.2023 – 16.03.2023	*виконано*
5	Опис засобів витоку інформації	16.03.2023 – 01.04.2023	*виконано*
6	Аналіз вимог щодо створення комлпексу технічного захисту інформації	01.04.2023 – 26.04.2023	*виконано*
7	Збір відомостей щодо технічних засобів, які використовуються при створенні комплексу захисту	26.04.2023 – 21.05.2023	*виконано*
8	Розробка напрямків удосконалення комплексу технічного захисту інформації	21.05.2023 – 05.06.2023	*виконано*
8	Оформлення пояснювальної записки	05.06.2023 – 7.06.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	12.06.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Валерій РУДЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Розробка рекомендацій щодо удосконалення комплексу технічного захисту інформації» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 76 сторінки. Робота містить 23 рисунків, 1 таблиць. Список використаних джерел включає 22 джерела.

Об’єкт дослідження – процес захисту інформації в автоматизованих системах.

Мета роботи – дослідження напрямків удосконалення комплексу технічного захисту інформації

Предмет дослідження – засоби, які здатні удосконалити комплекс технічного захисту інформації

Практичне значення роботи полягає в удосконаленні комплексу технічного захисту інформації.

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Напрямки подальших досліджень: аналіз технічних каналів інформації для створення більш захищених комплексів технічного захисту інформації.

Ключові слова: технічний захист інформації, канали витоку інформації, комплекс технічного захисту інформації, засоби технічного захисту, вимоги до комплексів технічного захисту інформації, об’єкт інформаційної діяльності, інформація з обмеженим доступом.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

КТЗІ	–	Комплекс технічного захисту інформації
ТЗІ	–	Технічний захист інформації
ОІД	–	Об’єкт інформаціної діяльності
ІзОД	–	Інформація з обмеженим доступом
КЗЗ	–	Комплекс засобів захисту
ПЕОМ	–	Персональна електронно-обчислювальна машина
ДТЗС	–	Допоміжні технічні засоби і системи
ОТЗС	–	Основні технічні засоби і системи
ВОК	–	Візуально-оптичні канали

ЗМІСТ

ВСТУП

Розвиток комерційної та підприємницької діяльності призводить до збільшення масштабів використання технічних засобів захисту інформації. Ці засоби починають грати все більшу роль, і тому їх використання для захисту інформації, комп'ютерної техніки та хмарних обчислень стає все більш масштабним. Ці технології збирають значну кількість інформації, часто конфіденційної або з обмеженим доступом.

Сучасні системи обробки даних стають все потужнішими та обробляють великий об'єм інформації. Вони дозволяють передавати інформацію між пристроями майже непомітно, що ускладнює виявлення витоків інформації.

Дана кваліфікаційна робота є актуальною, оскільки сучасний світ все більше стикається з фінансовими та репутаційними втратами через втрату цінної інформації. Крадіжки даних стають все поширенішим явищем, що привертає велику увагу з боку бізнесу та суспільства в цілому. Через це люди переймаються можливими фінансовими втратами, які можуть призвести до банкрутства чи через можливість появи публікацій негативної особистої інформації або просто починають цікавитись професійним аспектом захисту інформації. Витоки інформації зростають, що спричиняє більший тиск на компанії, як фінансовий так і моральний. Найбільш складним є реалізація захисту інтелектуальної власності чи військових технологій, що несуть шкоду країні. Застосування систем технічного захисту інформації дозволяє знаходити та ліквідовувати більшість спроб несанкціонованого отримання даних та зменшення витрат від витоків або зменшити кількість шкоди від взловмисників.

Об'єкт дослідження – процес захисту інформації в автоматизованих системах

Мета роботи – дослідження напрямків удосконалення комплексу технічного захисту інформації

Враховуючи, що метою роботи було дослідження напрямків удосконалення комплексу технічного захисту інформації, для її досягнення визначено наступні завдання:

- Провести дослідження технічних каналів витоку інформації на об’єктах інформаційної діяльності
- Проаналізувати вимоги керівних документів щодо створення комплексу технічного захисту інформації
- Провести аналіз технічних засобів, які використовуються в процесі створення комплексу технічного захисту
- Розробити рекомендації для удосконалення захисту інформації на об’єктах інформаційної діяльності

Предмет дослідження – засоби, які здатні удосконалити комплекс технічного захисту інформації

Методи дослідження: – структурний аналіз, класифікація.

Практичне значення роботи полягає в удосконаленні комплексу технічного захисту інформації.

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Напрямки подальших досліджень: аналіз технічних каналів інформації для створення більш захищених комплексів технічного захисту інфор

РОЗДІЛ 1
АНАЛІЗ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

1.1 Інформація та її технічний захист

Згідно з Законом України "Про Інформацію" [1], інформація це будь-які відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Згідно цього ж самого закону захистом інформації являється сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження та цілісність інформації та належний доступ до неї.

Певні види інформації потребують обов’язкового захисту, а саме та інформація яка є з обмеженим доступом (таємна, конфіденційна та службова) або, яка відноситься до державних інформаційних ресурсів. Захист інформації являє собою діяльність, яка направлена на забезпечення трьох головних аспектів, а саме доступності, цілісності та конфіденційность. Вимога щодо захисту такого виду інформації під час її обробки в телекомунікаційних, інформаційно-телекомунікаційних та інформаційних системах встановлена відповідними законами України [2].

Одним з різновидів захисту інформації є технічний захист інформації, який буде розглянутий безпосередньо в ході виконання кваліфікаційної роботи. Технічний захист інформації (ТЗІ) – це діяльність, яка спрямована на забезпечення інженерно-технічними заходами організацію конфіденційності, цілісності та доступності інформації [3]. Даний захист здійснюють на об’єктах інформаційної діяльності та на інформаційно-телекомунікаційних, інформаційних та телекомунікаційних системах. Використовують технічний захист інформації для запобігання витоку інформації через технічні канали інформації та для запобігання здійснення несанкціонованого доступу до інформації. Проте здійснення базовго технічного захисту інформації може бути не достатньо ефективним в деяких моментах.

1.2 Визначення технічних каналів витоку інформації

Однією з потенційних та небезпечних загроз для оброблювальної інформації в технічних засобах включаючи інформаційно-телекомунікаційні, інформаційні та телекомунікаційні системи чи яка озвучується на ОІД є витік інформації через технічні канали.

Під каналом витоку інформації ми підрозуміваємо явище, що являє собою не контрольноване здійснення поширення інформації, що надає змогу до несанкціованого одержання. Поняття каналу витоку інформації відображено на рисунку 1.1.

Якщо для перенесення інформації використовуються технічні засоби, такий канал витоку називається технічним. Технічний канал витоку інформації – це канал, яких складається з трьох основних компонентів, а саме: засобу технічної розвідки сукупності джерела небезпечного сигналу та середовища поширення цього сигналу.

Рисунок 1.1 - Схема каналу витоку інформації

Небезпечний сигнал – це сигнал якогось фізичного походження в якому міститься ІзОд та яку можуть перехопити засобами технічної розвідки.

Носій інформації (наприклад електричний струм, світло, акустичне поле, тощо) – сигнал, який містить інформацію з обмеженим доступом.

Середовище поширення небезпечного сигналу – це якесь фізичне середовище в якому може бути поширений небезпечний сигнал.

Засоби технічної розвідки – це такі технічні засоби за допомогою яких можливо виконати здійснення несанкціонованого перехоплення інформації з обмеженим доступом.

Джерелом небезпечного сигналу, який має змогу розповсюджуватись в просторі на велику дистанцію і може бути перехопленим засобами технічної розвідки зловмисника поза межами контрольованої зони виступають основні технічні засоби та системи. Для ОТЗС визначено дві небезпечні зони, а саме:

- Зона 1 – це територія, яка охоплює область навколо основних технічних засобів та в межах якої відбувається наведення небезпечних сигналів на інші технічні засоби та системи їх комунікації. Ця зона характеризується радіусом R1, який встановлює граничну відстань від ОТЗ до межі, поза межами якої прийнято здійснення наведення небезпечних сигналів на технічні засоби вважається неможливо.
- Зона 2 – це територія, яка знаходиться навколо технічних засобів обробки інформації поза межами, якої перехоплення небезпечного сигналу вважається неможливим та характеризується радіусом R2, який встановлює найбільшу можливу відстань від технічних засобів обробки інформації до межі, поза якою електричне та магнітне поле небезпечного сигналу відносно шумових завад не перевищують нормоване значення.

Зону 1 та зону 2 можливо визначити за допомогою експериментально-розрахункового методу при дослідженнях ОТЗС. Перехоплення інформації може бути здійснене лише в зоні 2, але за її межами перехоплення інформації здійснити не можливо (радіуси зон відрізняються, і як правило радіус зони 2 є більшим, ніж радіус зони 1).

В реальних умовах навколишнього простору можуть бути різноманітні перешкоди, як природного, так і штучного походження, які можуть значно ускладнювати прийом і передачу сигналів для традиційних систем зв'язку. Однак, для захисту технічних засобів від витоку інформації по технічним каналам, такі перешкоди можуть бути корисними і нерідко створюються спеціально.

Технічні канали витоку інформації мають найбільший потенціал інформативность в яких для отримання інформації з обмеженим доступом використовують технічні засоби. Структура будь-якого технічного каналу витоку інформації, що утворюється через перехоплення інформації, можливо представити, як систему передачі інформації.

Інформаційні сигнали залежать від середовища їх поширення та від фізичної природи їх утворення, тому технічні канали витоку інформації поділяються на декілька видів наведених на рисунку 1.2.

Рисунок 1.2 - Види технічних каналів витоку інформації.

В залежності від місця в якому здійснюється перехоплення інформації за допомогою засобів технічної розвідки зловмисника, можливо виділити декілька різних типів технічних каналів витоку інформації [4]:

— Канали в яких перехоплення інформації здійснюється за межами КЗ. Перехоплення інформації відбувається поза контрольованим простром КЗ.

— Канали в яких перехоплення інформації здійснюється за межами КЗ з використанням активного впливу на наявні параметри ТКВІ. Використовуються активні методи впливу на параметри технічного каналу, щоб отримати доступ до інформації.

— Канали в яких перехоплення інформації здійснюється за допомогою засобів технічної розвідки, які були розміщені заздалегідь на ОІД. Реалізація можливого встановлення технічних засобів розвідки на ОІД.

1.3 Електромагнітні технічні канали витоку інформації

Електромагнітні канали витоку інформації - це канали витоку інформації, які надають можливість неправомірного перехоплення конфіденційної інформації шляхом інтерпретації електромагнітних сигналів, які передаються між електронними пристроями. Наприклад, це можуть бути бездротові сигнали, передача по кабелю сигналу або випромінювання електричного сигналу, що надходить від електронного пристрою.

До складу технічних засобів перехоплення інформації (ТЗПІ) та девіантних технічних засобів спостереження (ДТЗС), які можуть включають в себе різноманітні високочастотні генератори, зокрема:

— генератори тактових імпульсів;

— генератори, які призначенні, щоб підмагнічувати магнітофони та для стирання;

— Електронні генератори електричних коливань (гетеродини), які широко використовуються в радіоприймальних і телевізійних пристроях для можливості здійснення перетворення вхідних радіо- або відеосигналів на потрібні інтермодуляційні частоти;

— генератори для вимірювальних приладів та інші.

Електромагнітний технічний канал витоку інформації може виникнути через дію різних видів небажаних електромагнітних випромінювань, наприклад таких як:

— Випромінювання елементів ТЗПІ;

— Випромінювання вискочастотних генераторів ТЗПІ на їх частотах;

— Випромінювань на частотах самозбудження підсилювачів низької частоти ТЗПІ.

Види на які поділяються електромагнітні канали витоку іфнормації представлені в таблиці 1.1.

Таблиця 1.1

Класифікація електромагнітних каналів витоку

За природою виникнення	За діпазоном випромінювання	За середовищем поширення
Електромагнітні випромінювання; Паразитні зв'язки і наведення; Акукстичні перетворювачі.	Короткі хвилі; Середні хвилі; Довгі хвилі; Понаддовгі хвилі; Ультракороткі хвилі.	Повітряний простір; Безповітряний простір; Земне середовище; Водне середовище; Направляючі системи.

В ТЗПІ (Технічні засоби прийому інформації) носієм інформації виступає електричний струм в якому змінюються параметри згідно законів інформаційного сигналу. При пропусканні цього струму через струмопровідні елементи ТЗПІ виникнуть електричне та магнітне поля навколо них. Через це можна розглядати ці елементи, як випромінювачі електромагнітного поля, що модулюється відповідно за законом інформаційного сигналу.

В результаті зовнішнього впливу інформаційного сигналу на елементах високочастотних генераторів відбуваються електричні сигнали. В них приймачем електричного поля будуть виступати наприклад проводи високочастотного ланцюга чи якісь інші елементи. В свою чергу приймачем магнітного поля будуть виступати дроселі в ланцюгах електроживлення, котушки індуктивності, тощо.

Електромагнітні випромінювання на частотах самозбудження ПНЧ ТЗПІ (наприклад системи гучномовного зв'язку, магнітофони, тощо) відбуваються за рахунок здійснення випадкових перетворень індуктивних чи ємнісних зв'язків в паразитивно позитивні, що в свою чергу призведе до здійснення переведення підсилювача з його режиму посилення в режим автоматичної генерації сигналів [5]. Сама ж частота самозбудження буде знаходитись в рамках межі робочої частоти нелінійних елементів (напівпровідникових приладів, тощо). Самозбудження частіше за все спостерігається, при переході ПНЧ в режим перевантеження.

Зона в якій здійснюється перехоплення побічних електромагнітних випромінювань та наступна розшифровка перехопленої інформації, що міститься в них називається зоною 2. Ця зона охоплює діапазон, де відбувається перехоплення побічних електромагнітних випромінювань технічних засобів прийому інформації за допомогою засобів радіотехнічної чи радіо розвідки, які розміщуються за контрольованою зоною.

1.4 Акустичні канали

Акустичні канали витоку інформації - це канали витоку, які надають можливість отримати доступ до конфіденційної інформації за допомогою перехоплення або запису звукових сигналів, які будуть передаватись під час комунікації.

Переносником інформації в акустичних каналах виступає безпосередньо мова чи звуки, які знаходяться, в даних каналах, в діапазоні від 20кГЦ до інфразвукового діапазону.

Акустичний канал витоку інформації формується за допомогою коливних або вібруючих об’єктів та за допомогою механізмів, таких як телефонні апарати, звукопідсилювальні системи, тощо.

Джерела акустичних коливань можна розділити на наступні категорії:

1. Первинні джерела – являють собою якісь механічні коливальні системи, наприклад, музичні інструменти, звук якоїсь працюючої техніки та інші механічні пристрої, що породжують звук.

2. Вторинні джерела - електроакустичні перетворювачі, такі як телефони, мікрофони та інші пристрої, що здатні перетворювати акустичні коливання в електричні та навпаки та якісь інші технічні прилади в яких дані перетворюючі мають застосування.

Акустичні канали витоку інформації утворюються декількома способами, а саме:

— Завдяки поширенню акустичних коливань у вільному просторі (наприклад відкриті вікна двері;переговори на вулиці;вентиляційні канали,квартирки).

— Завдяки дії звукових коливань які впливають безпосередньо на елементи конструкцій будівель тим самим викликаючи у них вібрації (наприклад, стіни, стелі, двері, труби водопостачання, тощо).

— За допомогою звукових коливань можна впливати на технічні засоби, які приймають участь в обробці інформації (наприклад, шляхом акустичної модуляції волоконно-оптичних ліній передачі інформації або використовуючи мікрофонний ефект).

В акустичних каналах витоку інформації безпосереднім середовищем в якому поширюються мовні сигнали виступає повітря [6]. Через огороджувальні конструкції витік акустичної інформації можливий наступними шляхами (рисунок 1.3):

1. Із застосуванням мембранного ефекту. Данний ефект створюється шляхом здійснення коливання тонких і як правило легких елементів огороджувальних конструкцій, які можуть прогинатись під дією звуку тим самим призводячи до передачі акустичної інформації;

2. За допомогою наявного прямого розповсюдження акустичних коливань через тріщини, отвори тощо в огороджувальних конструкціях, великі пройми в свою чергу будуть дозволяти створення безперешкодної можливості передачі акустичного сигналу;

3. Шляхом перетворення акустичних коливань у віброакустичні коливання, а потім знову переходить в акустичні коливання. В даному випадку акустичні коливання падаючи на поверхню огороджувальної конструкції переходять у віброакустичні коливання, а вже подолавши конструкції перетворюються в акустичні коливання.

Схематичне відображення витоку інформації через огороджувальні конструкції відображено на рисунку 1.3.

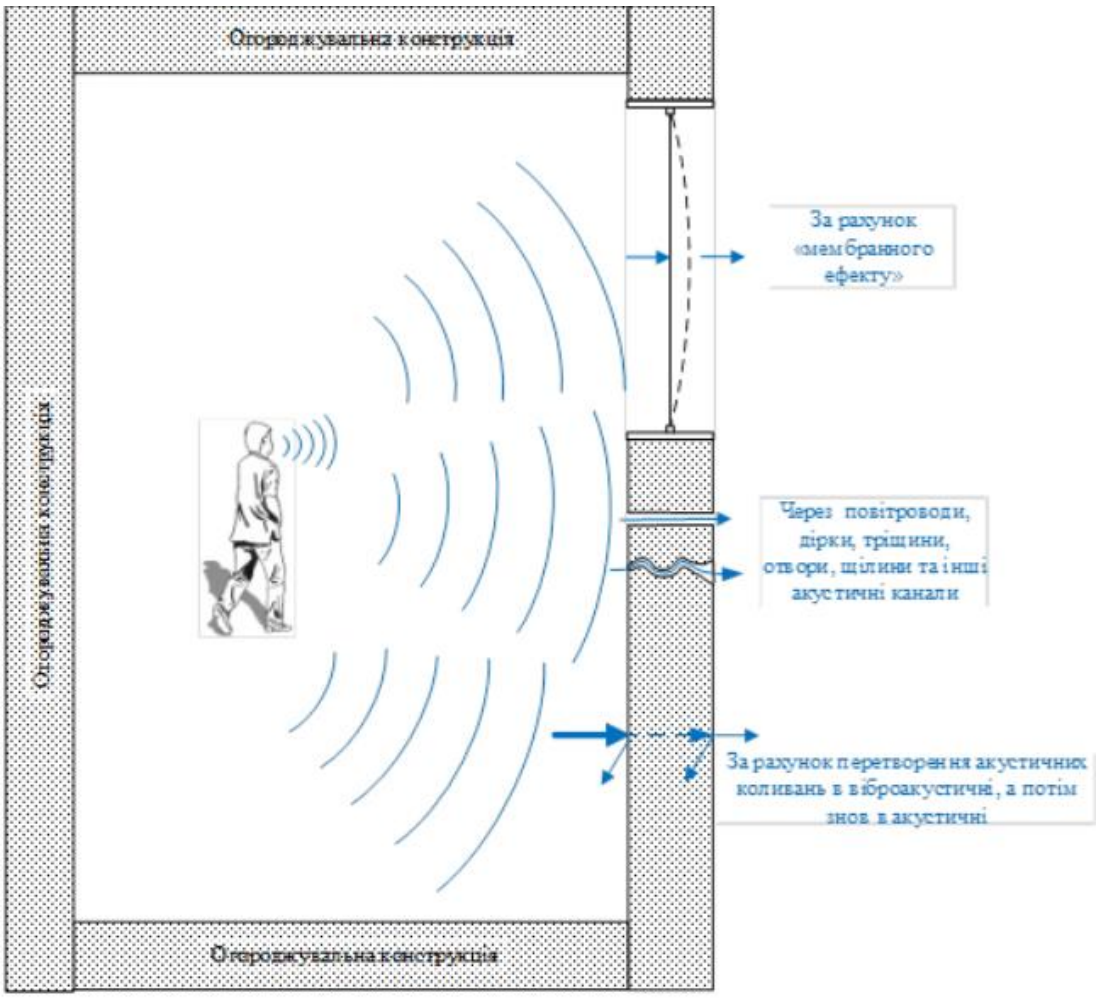

Рисунок 1.3 - Шляхи витоку інформації через огороджувальні конструкції

Акустичну інформацію можливо приймати, як і з засобами технічної розвідки так і без засобів технічної розвідки, а саме при випадковому прослуховуванні (не важливо чи це були умисні чи не умисні дії, спрямовані на отримання конфеденційної інформації).

Інформацію, яка передається через акустичні канали можна записувати на високочутливі мікрофони або спрямовані мікрофони, які мають вузьку діаграму спрямованості.

Мовна інформація в свою чергу може бути записана безпосередньо на диктофони або передана через різні канали зв'язку, такі як радіоканали, інженерні комунікації тощо.

Схема каналів витоку акустичної інформації відображена на рисунку 1.4.

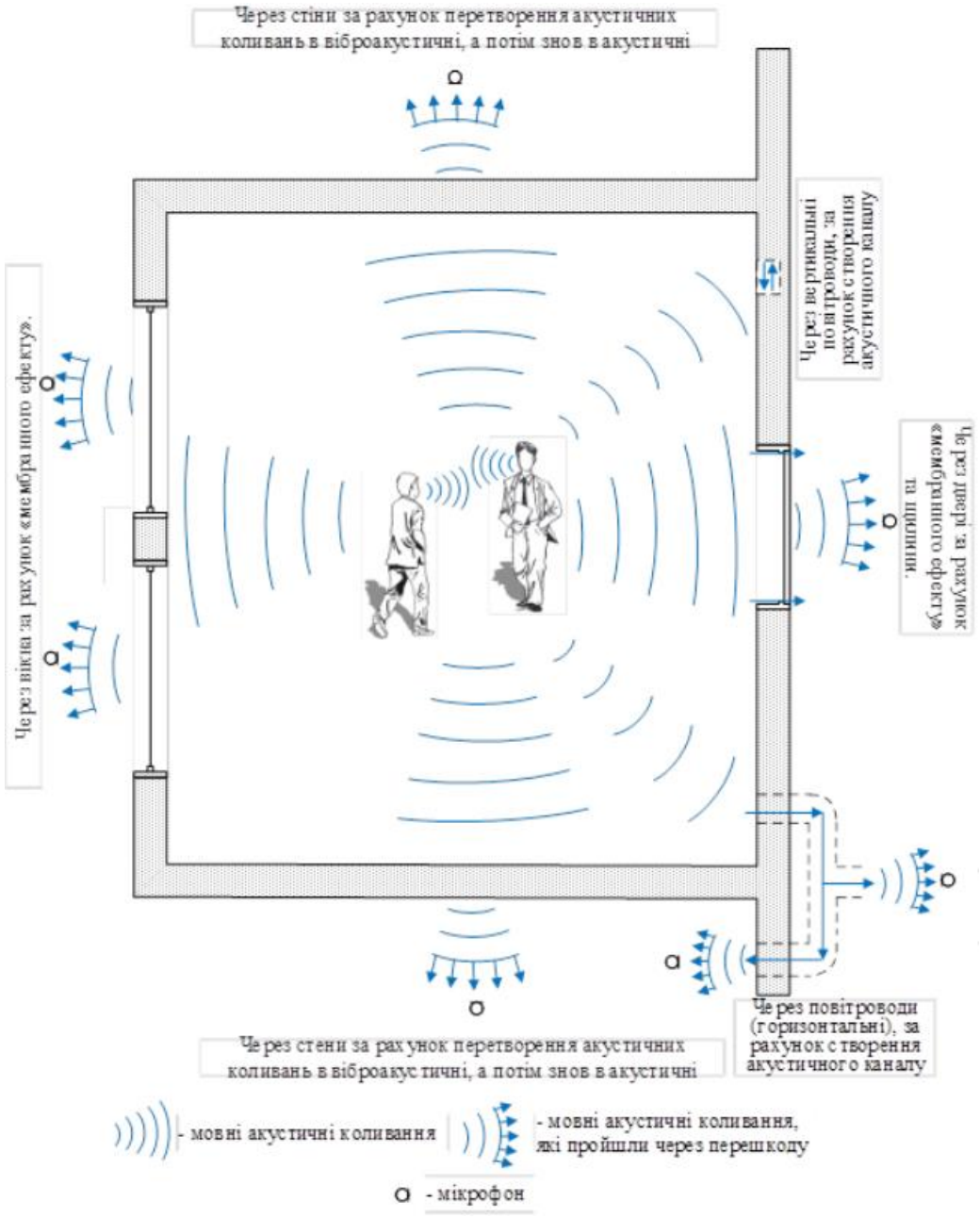

Рисунок 1.4 - Канали витоку акустичної інформації

1.4.1 Віброакустичні канали

Віброакустичні канали витоку інформації - це канали витоку, які надають можливість отримання доступу до конфіденційної інформації за допомогою перехоплення або запису вібрацій, які передаються в ході комунікації або роботи пристроями чи системами.

Схема віброакустичних каналів витоку інформації відображена на рисунку 1.5.

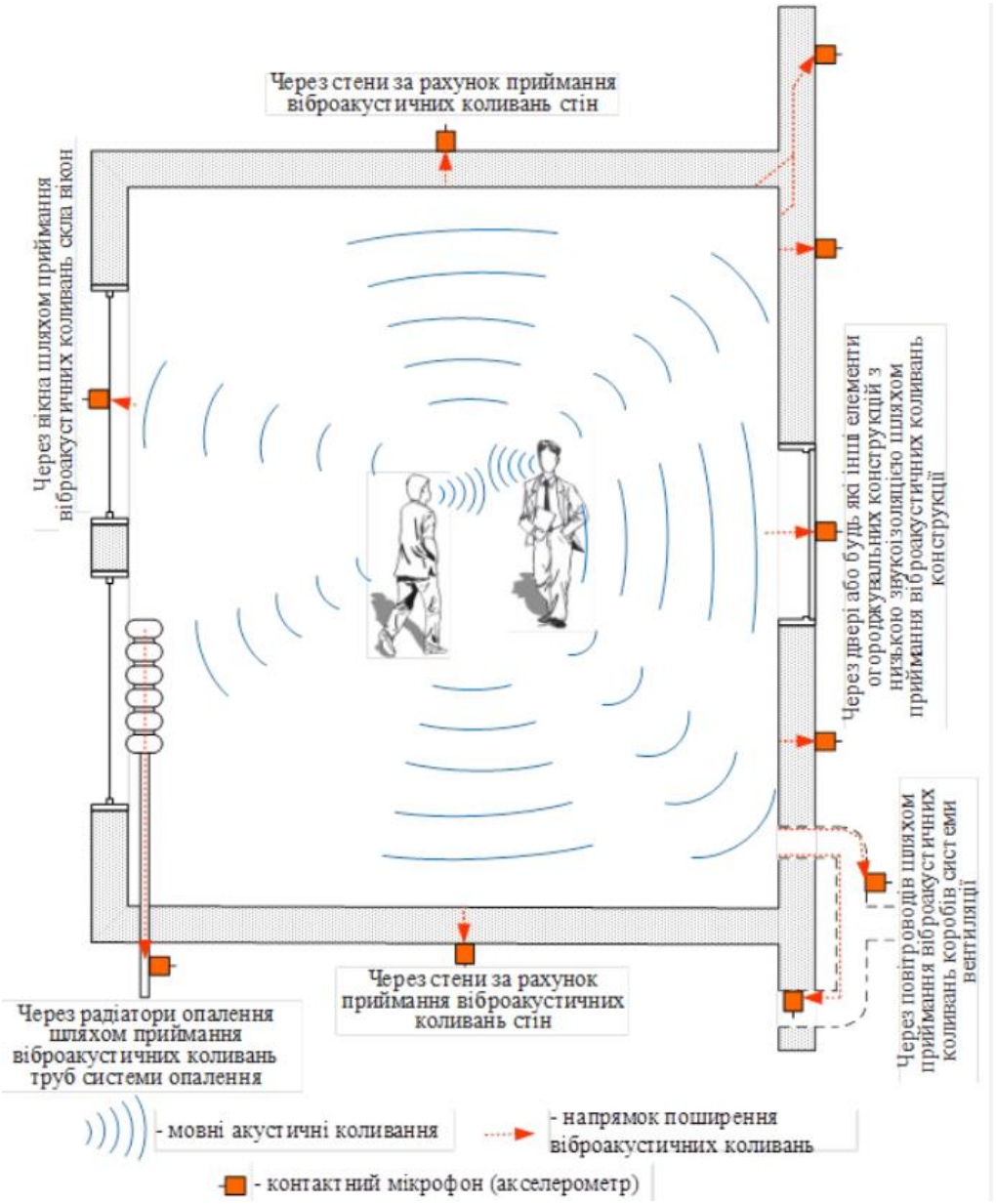

Рисунок 1.5 - Віброакустичні канали витоку інформації

У віброакустичних каналах витоку інформації середовищем через, яке відбувається поширення акустичних сигналів виступають будівлі, спорудження, труби, каналізації, тощо. Для перехоплення даних коливань в цьому випадку будуть використовувати стетоскопи (контактні мікрофони). Електронний стетоскоп (ЕС) - це пристрій, який складається з вібродатчика та електронного підсилювача. ЕС може використовуватись для прослуховування мови через голосові телефони, а також для запису звуку.

По віброакустичному каналу витоку інформації можливо здійснювати перехоплення інформації з використанням засобів перехоплення [7].

По віброакустичному каналу також можливо перехоплювати інформацію за допомогою різних засобів перехоплення. Для передачі інформації зазвичай використовується радіоканал, ці пристрої також часто називають радіостетоскопами. Крім того, можливе використання ЗП для передачі інформації по наявним оптичним каналам в ближньому інфрачервоному діапазоні довжин хвиль, а також по ультразвуковому каналу, який застосовують в інженерних комунікаціях.

Один з прикладів віброакустичного каналу витоку інформації є запис вібрацій на поверхні столу, на якому розміщений смартфон або інший пристрій, який надсилає конфіденційну інформацію. Хакер може використовувати спеціальне обладнання для перехоплення цих вібрацій та отримання конфіденційної інформації.

1.4.2 Електроакустичні канали

Електроакустичні канали витоку інформації – це канали витоку, які надають змогу отримання доступу до конфіденційної інформації за допомогою запису електричних сигналів або перехопленням під час комунікації. Ці канали можуть виникати за рахунок перетворення акустичних сигналів на електричні шляхом електроакустичних перетворень. Перехоплення акустичних коливань здійснюється шляхом “високочастотного нав’язування” та через ВТСС (мікрофонний ефект).

Під дією акустичного поля, яке створюється джерелом мовного сигналу деякі елементи технічних засобів і систем можуть змінити свої параметри (опір, індуктивність). Зміна яка утворюється під час цього призводить до модуляції струмів, які протікають по цим елементами або до появи електрорушійної сили на цих елементах.

Деякі елементи допоміжних технічних засобів і систем, в тому числі котушки індуктивності, телефонні двізнки апаратів, трансформатори та інші, що мають здатність змінювати свої параметри безпосередньо під впливом акустичного поля, яке створено джерелом мовного сигналу. Зміна параметрів може призводити до появи електрорушійної сили (ЕРС) на цих елементах або до модуляції струмів, що протікають через ці елементи згідно із змінами електричного поля. В ДТЗС також

можуть бути розміщені безпосередньо акустоелектричні пертворювачі, такі як: датчики охоронної чи пожежної сигналізації, гучномовці, тощо.

Схематиче відображення витоку інформації за допомогою електроакустичних перетворень наведено на рисунку 1.6.

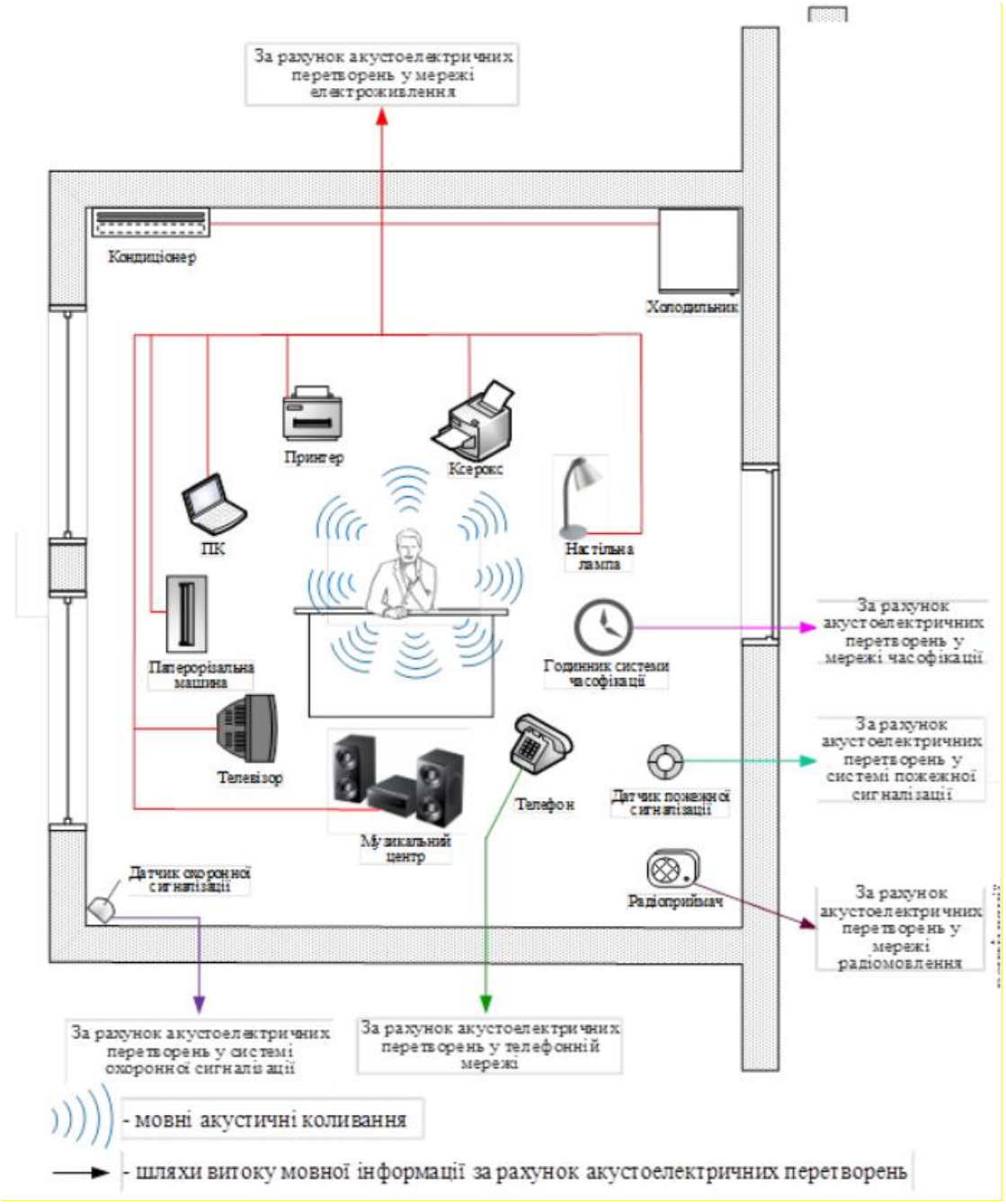

Рисунок 1.6 - Канали витоку за допомогою електроакустичних перетворювань.

Перехоплення даних у вигляді електроакустичних коливань в цьому каналі здійнюється безпосереднім підключення до з'єднувальних ліній девіантних технічних засобів спостереження спеціальних високочутливих УНЧ.

Електроакустичний канал витоку інформації із застосуванням високочастотного електромагнітного нав’язування можливо створити шляхом несанкціонованого введення струму високої частоти напряму від генератора в лінію, що має функціональний зв’язок з параметричними або з нелійними елементами ДТЗС, на котрих буде відбуватися модуляція високочастотного каналу інформаційним сигналом. Даний сигнал в елементах ДТЗС з’являється в результаті електроакустичного перетворення акустичних сигналів в електричні у вигляді наслідку. Промодульований сигнал поширюється в зворотному напрямку або випромінюється при відбиванні від елементів ДТЗС.

1.5 Візуально-оптичні канали витоку інформації

Візуально-оптичні канали витоку інформації – це канали в основі яких лежить будь-який процес передачі інформації за допомогою світла або оптичного випромінювання. Дані види випромінювання називаються електромагнітним випромінюванням довжина хвиль якого у вакуумі становить від 170 до 380 нм.

Візуально-оптичні канали утворюються від об’єкта, як оптичний шлях до зловмисника. Для утворення даного каналу зловмиснику знадобляться технічні пристрої (наприклад шпигунські камери, бінокулярів, тощо) та якісь просторові, тимчасові або енергетичні умови.

Об’єкт інформації не можливо буде виявити, якщо він погано видимий, зливається з навколишнім середовищем, час перебування в полі зору буде замалий або, якшо він знаходиться в темряві і не підсвічується.

Класифікація візуально-оптичних каналів витоку інформації:

1) За природою виникнення:

— За рахунок відбиття світлової енергії;

— За рахунок власного випромінювання об’єкту.

2) За природою випромінювання:

— Видима область;

— ЧК-область;

— Уф-область.

3) За середовищем поширення:

— Вільний простір;

— Направляючі лінії.

Для здійснення візуально-оптичного спостереження в інфрачервоному діапазоні необхідно конвертувати невидиме для людського ока зображення в інфрачервоному діапазоні, що має довжину хвилі понад 0,76 мкм, в зображення, яке можна побачити в видимому діапазоні. Для спостереження в умовах низької освітленості і відображення об'єктів у інфрачервоному діапазоні використовуються прилади нічного бачення (ПНВ).

Об’єкт до якого відбувається спостереження в оптичному каналі витоку інформації являю собою одночасно джерело інформації та сигналу, тому що світлові промені, які надають інформацію по видових ознаках об’єкта, являє собою власні випромінювання або відображення променів зовнішнього джерела об’єкта [8].

Інформація отримана завдяки відбитому від об’єкта світлу буде надавати зловмиснику інформацію про видові ознаки, а випромінення об’єктом світла надасть інформацію про ознаки сигналів. Запис даної інформації відбувається в момент відобрежання світла шляхом зміни його яскравості та спектрального складу. Випромінюване світло буде надавати інформацію про спектральний склад джерела видимого світла.

1.6 Матеріально-речові канали витоку інформації

Матеріально-речові канали витоку інформації - це канали в яких можливо отримати доступ до конфіденційної інформації за допомогою отримання фізичного доступу до носіїв інформації.

Матеріально-речові канали поділяються на наступні види [9]:

1) За фізичним станом:

— Рідини;

— Газоподібні речовини;

— Тверді маси.

2) За фізичною природою:

— Хімічні;

— Біологічні;

— Радіоактивні.

3) За середовищем поширення:

— У землі;

— У воді;

— В повітрі.

Матеріально-речові канали витоку інформації можуть бути спричинені можливістю противника отримувати доступ до ІзОД, яка міститься на різних носіях, таких як магнітні диски та інші засоби електронної обробки і збереження інформації, які вийшли з ладу, видавницька діяльність, з чорновиків від документів, тощо. Також до даних каналів витоку інформації може відноситись можливість противника до аналізу структури, речовини та хімічного складу використаних матеріалів, що мають гриф інформації з обмеженим доступом. Такою інформацію може бути, для прикладу, технологія виробництва зброї, отруйних речовин, структура матеріалу носіїв інформації та іншу інформаці з обмеженим доступом. Отримання фізичного доступу до такої інформації надасть взловмиснику повну змогу до отримання засекреченої інформації з носіїв.

Один з прикладів матеріально-речового каналу витоку інформації - це крадіжка документів або збір інформації з використаних паперових документів. Іншим прикладом може бути фізичний доступ до електронного пристрою, наприклад, витівка до комп'ютера або мобільного телефону з метою отримання конфіденційної інформації з нього.

А одним з видів небезпечних загроз є отримання доступу до інформації з магнітних носіїв, які вважаються стертими, саме тому використані магнітні носії потребують фізичного знищення.

Магнітні носії є популярними засобами зберігання інформації, оскільки їх можна легко зчитувати та записувати. Ідея застосування магнітних носіїв полягає у

використанні магнітної головки, яка рухається над поверхнею магнітного середовища і за допомогою поля запису впливає на орієнтацію доменів. Коли на магнітний носій застосовується зовнішнє магнітне поле, напрямок силових ліній поля змінюється, що може призвести до повороту доменів у відповідному напрямку. За рахунок ефекту гістерезису, домени залишаються у своєму новому положенні після зняття поля, що дозволяє запам'ятовувати поля намагнічування. Для зчитування інформації з магнітного носія, головка пересувається над його поверхнею та реєструє магнітні поля, створені намагніченими доменами. Після цього, відповідний сигнал передається в інформаційну систему для подальшої обробки.

Цей принцип дозволяє створювати різні типи магнітних носіїв, які використовуються в засобах електронно-оптичних технологій. Сучасні технології виготовлення магнітних носіїв забезпечують високу щільність запису, яка зростає з часом і дозволяє зберігати великі об'єми даних.

Всі жорсткі та гнучкі магнітні носії, що використовуються в засобах електронно-обчислювальної техніки, побудовані на основі принципу запису інформації на магнітних середовищах. Сучасні технології виготовлення магнітних носіїв дозволяють забезпечити високу щільність запису, яка постійно зростає з часом, що дозволяє зберігати великі об'єми даних.

Висновки за розділом 1

Інформація, яка обробляється на об’єктах інформаціної діяльності, яка має статус інформації з обмеженим доступом потребує захисту. Одним з видів захисту є організація технічного захисту інформації, для цього створюються комплекси ТЗІ, які можуть захистити інформацію від несанкціонованого доступу технічними каналами витоку інформації.

В даному розділі було виконано перше завдання поставлене до кваліфікаційної роботи, а саме, проведено дослідження технічних каналів витоку інформації на об’єктах інформаціної діяльності. В ході виконання даного завдання було наведено визначення каналу витоку інформації та наведено складові таких каналів. Також було

наведено визначення безпосередньо технічних каналів витоку інформації та наведено їх види.

Під час роботи було проаналізовано різні види технічних каналів витоку інформації, які може задіяти зловмисник, а саме наступні види ТКВІ: акустичні, електромагнітні, матеріально-речові, візуально-оптичні. Дані канали було детально досліджено, наведено їх визначення, класифікацію за якою вони розподіляються. Також було наведено яким чином здійснюється витік інформації в кожному виді та наведено.

РОЗДІЛ 2
КОМПЛЕКС ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Визначення комплексів технічного захисту інформації

Технічний захист інформації (ТЗІ) є важливою складовою забезпечення національної безпеки в сфері інформації. Основна мета ТЗІ полягає в застосуванні інженерно-технічних заходів для забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється на об’єктах інформаційної діяльності, інформаційно телекомунікаційних та автоматизованих системах.

Досягнення основної мети ТЗІ можливе шляхом побудови комплексу захисту інформації, що буде являти собою організовану сукупність засобів та методів забезпечення технічного захисту інформації. Організація здійснюється поетапно [10]:

1. Етап визначення та аналізу загроз.
2. Етап розробки системи захисту інформації
3. Етап реалізації плану захисту інформації
4. Етап керування системою захисту інформації та контроль її функціонування.

Правова основа забезпечення ТЗІ в Україні становить [11]:

1. Конституція України;
2. Закони України “Про основи національної безпеки”, “Про інформацію”, “Про доступ до публічної інформації”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про державну таємницю”, “Про науково-технічну інформацію”;
3. Інші нормативно-правові акти;
4. Міжнародні договори України, що стосуються сфери інформаційних відносин.

Комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

В складі КСЗІ на об’єктах інформаціної діяльності створюють комплекси технічного захисту інформації для протидії технічним каналам витоку інформації та несанкціонованому доступу до інформації [12].

Комплекс ТЗІ – це сукупність заходів, технологій та засобів, що мають на меті забезпечення технічного захисту конфеденційної інформації на об’єкті інформаційної діяльності [11].

Комплекси технічного захисту інформації створюються на об’єктах інформаційної діяльності, де передбачаються наступні аспекти:

— Обговорення конфеденційної інформації при проведенні нарад на підприємстві з застосування звукових чи відео технологій

— Обробка інформації з обмеженим доступом за допомогою технічних засобів, що включає записування, зчитування, зберігання, отримання, тощо

— Переміщення інформації з обмеженим доступом в рамках проектування будівництва, виробництві технічних засобів, тощо.

Створення технічного комплексу захисту інформації на об’єкті інформаційної діяльності являє собою складне завдання, адже воно вимагає від суб’єкта виконавця певної кваліфікації та зобов’язань. Для реалізації відповідних завдань у процесі створення КТЗІ та розподілу юридичною відповідальності виділяють наступні суб’єкти:

— Установа-замовник: установа, в інтересах якої створюється комплекс технічних засобів захисту інформації і яка є замовником цього проекту.

— Підрозділ-заявник: структурний підрозділ в установі на який покладається аргументація необхідності створення комплексу технічних засобів захисту інформації та, який відповідає за подання заявки на створення даного комплексу.

— Організатор КТЗІ: структурний підрозділ, який відповідає за організацію та супроводження робіт зі створення комплексу ТЗІ в установі, включаючи технічні засоби захисту інформації, а також може бути суб'єктом господарської діяльності.

— Підрозділ, відповідальний за здійснення спеціальних досліджень КТЗІ: структурний підрозділ, який несе відповідальність за проведення спеціальних досліджень технічних засобів захисту інформації.

— Відділ виконавчих робіт: структурний підрозділ, який є відповідальним за здійснення реалізації комплексу заходів направлених на впровадження технічних засобів захисту інформації.

— Відділ атестації: структурний підрозділ, який є відповідальним за проведення атестації комплексу технічних засобів захисту інформації.

Створення комплексу технічного захисту інформації на об’єкті інформаціної діяльності передбачає наступні основні етапи:

1. Виконання передпроектних робіт.

На цьому етапі відбуваються передпроектні роботи в ході яких виконується обстеження ОІД і розробляється завдання щодо створення на ньому комплексу ТЗІ. Окрім цього виконується розробка звіту про виконання передпроектних робіт та наводяться технічні вимоги до захисту ІзОД для виконання робіт з метою створення КТЗІ.

2. На наступному етапі відбувається розробка та впровадження заходів з захисту інформації на ОІД.

3. На останньому етапі відбуваються випробування та атестація вже готового комплексу ТЗІ. Під час даного етапу створюються комісія замовником, яка приймає комплекс ТЗІ, а виконавець в той час забезпечує атестацію комплексу.

Для проведення атестації комплексу ТЗІ залучаються суб’єкти господарської діяльності, які будуть долучені повинні мати ліцензію з надання послуг в галузі технічного захисту інформації. Після завершення атестації заповнюється технічний паспорт на комплекс технічного захисту інформації [13]. В даному паспорті буде зафіксований результат проведеної атестації, опис КТЗІ та його основні функціональні можливості.

2.2 Етапи створення комплексу технічного захисту інформації

Згідно нормативного документу НД ТЗІ 3.3-001-07 [14], процес створення комплексу ТЗІ передбачає два етапи. Під час першого етапу необхідно виконати наступні кроки:

1. Виконується обстеження діючої інформаційної системи на об’єкті інформаціної діяльності..

2. Виконується розробка моделі загроз ІзОД, що має вказати на перелік можливих загроз або виконується доповнення до вже діючої ОІД згідно положень НД ТЗІ.

3. Виконується розробка технічного завдання, яке безпосередньо направлене на створення комплексу ТЗІ.

На другому етапі згідно даного стандарту виконавець робіт виконує створення комплексу ТЗІ вимоги до якого затверджено технічним завданням. В ході даного етапу необхідно розробити пояснювальну записку з ТЗІ в якій виконавець зазначає перелік, терміни виконання робіт по створенню комплексу ТЗІ, зміст та склад документів, які будуть розробленні під час створення комплексу [15].

Крім того, виконавець робіт з ТЗІ також має виконати наступні пункти:

1. Розрообити проектно-кошторисну документацію відповідно до вимог, які описані в ДБН А.2.2-2 та ДБН А.2.2-3.

2. Виконати відповідні будівельні, монажно-налагоджувальні роботи та після операційно технічного контролю щодо до повноти їх виконання

3. Придбання необхідних технічних засобів забезпечення ТЗІ, які були наведені в ході створення технічного завдання

4. Виконання розробки проекту паспортів на комплекс ТЗІ.

При створення КТЗІ на ОІД також слід дотримуватись вимог НД з питань ТЗІ та виконати організаційні, технічні та інженерні заходи. Такі заходи включають наступні пункти:

— Архітектурно-будівельні заходи

— Заходи з оргіназації активного захисту ІзОД

— Заходи з організації пасивного захисту ІзОД

При створенні комплексу найбільше уваги слід надавати заходам організації пасивного захисту ІзОД та архітектурно-будівельним заходам.

2.3 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Для реалізації будь-якого комплексу засобів захисту інформації представляється ряд вимог, а саме [16]:

1. Реалізоване КЗЗ має забезпечувати безперервний захист на об’єкті інформаційної діяльності від взлому, несанкціонованої модифікації та витоку інформації. На ОІД не повинно бути можливості отримання доступу до об’єкту критичної системи в обхід КЗЗ. Жодна критична система не може вважатись безперервно захищеною, якщо в ній апаратні та програмні механізми, які задіяні для реалізації функції захисту та політики безпеки будуть виступати суб’єктами для несанкціонованої модифікації.

2. Важливим пунктом є наявність модульної структури комплексу засобів захисту. Модульність підрозуміває під собою на рівні архітектури критичної системи здійснення реалізації набору відносно незалежних частин. Кожна з цих незалежних частин повинна взаємодіяти одна з одною лише за допомогою добре визначених інтерфейсів.

В свою чергу на рівні архітектури КЗЗ “модульність” означає, що комплекс засобів захисту має представляти собою ретельно розроблений набір програмного та апаратного забезпечення, яке організоване таким чином, щоб утворювались логічні групи, які будуть направлені на вирішення конкретно заданих завдань. Будь-яка взаємодія компонентів повинна бути здійснення лише через описані канали, але за умови забезпечення відповідних гарантій реалізації можливе використання глобальних змінних допускається проте воно не рекомендується до здійснення на практиці.

Посилення вимог до модульності КЗЗ в свою чергу призведе до необхідності побудови комплексу засобів захисту з дотриманням принципів пошарової архітектури, що в свою чергу означає здійснення проектування КЗЗ, як набір груп функцій, які будуть взаємодіяти між сусідніми верхніми та нижніми шарами відповідно.

2.4 Загальні положення та вимоги щодо розміщення режимних приміщень

Проектування режимних приміщень в яких функціонує ІзОД має бути реалізована відповідно до вимог. На етапі розробки проектної документації на будівництві або реконструкції ОІД на якому є режимне приміщення, потрібно враховувати вимоги та рекомендації чинних нормативних документів в галузі будівництва, а також нормативних актів стосовно приміщень в яких постійно перебувають люди. чи реконструкції. При цьому також важливо дотримуватись вимог державних нормативів та правил, для забезпечення високого рівню захисту інформації в разі, якщо підприємство використовує в приміщеннях персонально електронно-обчислювальні машини за умови, якщо ці вимоги не будуть суперечити іншим нормам та правилам..

У разі, якщо в приміщеннях на ОІД є персональні електронно-обчислювальні машини (ПЕОМ), необхідно керуватись вимогами Державних нормативів та правил, за умови, що ці вимоги не суперечать іншим нормам та правилам.

При розміщенні режимного приміщення треба враховувати, що воно не повинне перебувати поруч з вікнами біля, яких будуть наявні пожежні драбини, балкони, покрівлі, прибудови, тощо через наявність можливості проникнення в приміщення через вікно сторонніми особами. Також дане приміщення має бути розташоване не вище перед останнього та не нижче другого поверху, якщо воно знаходиться в багатоповерхових будівлях, але в рахунок не буде братись технічний поверх.

Якщо режимні приміщення на ОІД взаємопов’язані між собою за функціональними ознаками то їх необхідно групувати та розміщувати таким чином, існували загальні входи зі сторони загального коридору для цих взаємопов’язаних груп.

Необхідно забезпечувати розташування обладнання та технічних засобів у приміщеннях згідно з вимогами технічного захисту інформації, санітарних норм,

безпеки праці та пожежної безпеки та переконуватися, що ці вимоги весь час дотримуються.

2.4.1 Вимоги до будівельних конструкцій режимних приміщень

До будівельних конструкцій безпосередньо відносяться їх перекриття (стеля, підлога), перегородки (стіни) та вікна і двері режимних приміщень. Перекриття та перегородки режимних приміщень, які відповідають за їх відокремлення між іншими приміщеннями мають бути залізобетонними або бетонними та мати товщину, яка не буде меншою за 80мм або не менше 120мм, якщо стіна буде зроблена з цегли. Також, цегляні та бетонні конструкції необхідно армувати.

В режимних приміщеннях необхідно встановлювати вхідні двері з використання двох різних замків, які матимуть не менше ніж два комплекта ключів.

Індекс ізоляції шуму в приміщенні стінами, дверима та перекриттям, які відокремляють його від інших приміщень, повинен становити не менше ніж 60ДБ. У випадку, якщо конструкція дверей не може забезпечити мінімального індексу ізоляції то передбачено використання подвійних дверей, які зможуть забезпечити даний індекс.

Для забезпечення захисту від візуальнооптичних каналів витоку інформації на вікнах мають передбачатись пристрої (жалюзі, штори, тощо), які унеможливлять огляд приміщення зовні в незалежності від того на якій висоті знаходить ОІД та наявності інших будівель напроти. У випадку якщо будуть існувати якісь особливості конструкції будівлі, які можуть дозволяти здійснення несанкціонованого проникнення на ОІД то необхідно здійснити встановлення на вікна стальних грат, які матимуть прути з діаметром в 16мм та на відстані 150мм між кожним прутом, а якщо стальні прути будуть розміщуватись горизонтально то відстань не має перевищувати 400мм між ними.

Обгрунтування необхідності встановлення контрольно-пропускних пунктів, турнікетів, тощо має бути зазначене в завданні на проектування.

Через режимні приміщення на ОІД заборонено прокладати повітропроводи, трубопроводи, комунікації, які не будуть мати необхідних вставок з використанням ізоляційного матеріалу чи якихось інших засобів, що реалізують технічні захист інформації, відповідно до вимог НД ТЗІ.

2.4.2 Вимоги щодо сигналізації в режимних приміщеннях

Для захисту переметру інформаціної системи на ОІД створюються наступні системи:

— Система охоронної сигналізації;

— Система пожежної сигналізації;

— Система цифрового відеоспостереження;

— Система контролю та керування доступом.

Режимні приміщення мають бути оснащенні охоронною системою, яка має бути доступною пультом на пості охорони ОІД. Дана сигналізація має мати автономний вид джерела живлення на випадок надзвичайних ситуацій в яких буде відсутнє основне джерело живлення та здійснювати перехід на автономне джерело живлення автоматичним чином. Крім охоронної сигналізації має бути передбачена пожежна сигналізація, яка буде працювати в автоматичному режимі.

Необхідність використання якихось додаткових спеціальних видів оптичного, електронного чи акустичного захисту а також якісь інші види сигналізацій мають передбачуватись безпосередньо в завданні на проектування КТЗІ.

2.5 Технічні засоби захисту

Комплекс технічного захисту інформації містить в собі різні засоби захисту інформації, які направлені на забезпечення захисту в залежності від конкретної ситуації та від потреб самого користувача. Питання технічного захисту інформації (ТЗІ) можливо розбити на два великих класи задач, а саме:

1. Організація захисту інформації від несанкціоноваго доступу;

2. Організація захисту інформації від технічних каналів витоку інформації.

Захист від цих двох класів здійснюється різними засобами захисту інформації.

Від несанкціонованого доступу до інформації використовуються наступні засоби захисту:

— Засоби апаратного рівня;

— Засоби прикладного та програмного рівнів;

— Засоби моніторингу та аудиту;

— Засоби фізичного захисту.

Від технічних каналів витоку інформації будуть використовуватись наступні засоби:

— Засоби активних систем генерації шуму;

— Екранування приміщень, кабелів та використання екранованого обладнання;

— Засоби віброакустичного захисту;

— Мережеві фільтри

— Застосування високочастотних фільтрів на лініях зв’язку;

— Фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв’язку, системи директорського та диспетчерського зв’язку.

Системи простороовго зашумлення використовуються за для уникнення перехоплення побічних електромагнітних випромінювань, які можуть виникнути по електромагнітному каналу. В свою чергу генератори лінійного зашумлення використовуються для запобігання несанкціонованого доступу до інформаційних сигналів через сторонні провідники та через з’єднувальні лінії [17].

2.6 Фізичні засоби захисту

Для забезпечення захисту інформації від несанкіонованого фізичного доступу, матеріально-речових каналів витоку та для охорони периметру ОІД застосовуються різного роду фізичні засоби захисту. Дані засоби передбачають в собі контроль за

доступом до зон в яких обробляється ІзОД, технічний контроль, застосування фізичних перешкод для потрапляння на ОІД, тощо. Найбільш поширеними засобами фізичного захисту зараз є:

1. Фізичне обмеження доступу: картки доступу, огороджувальні конструкції, замки та інші види засобів захисту, що передбачають в собі обмеження фізичного доступу до ОІД.

2. Системи сигналізації: датчики, які реагують на проникнення для виявлення спроби несанкціонованого доступу до ОІД.

3. Камери відеоспостереження: передбачають контроль та запис діяльності, яка відбувається на ОІД для подальшого контролювання дій відносно технічних пристроїв, тощо.

4. Шифрування інформації: передбачає в своїй основі використання алгоритму шифрування, який забезпечить захист інформації, якщо зловмисник отримає доступ до пристрою. В перевірених засобах від Держспецзв’язку відповідають два види шифрування, а саме симетричне та асиметричне і в нашому випадку більш доцільне використання саме симетричного шифрування, тому що воно працює швидше та надає більшу захищеність.

Перевагами таких засобів захисту є:

—Забезпечення високої надійності від несанкціонованого доступу до інформації;

—Можливість застосування даних засобів на будь-якому етапі розробки та впровадження комплексів ТЗІ.

Недоліками цих засобів захисту є наступні аспекти:

—Збільшення витрати часу на обробку інформації;

—Збільшені витрат на впровадження, управління фізичнх засобів захисту та регулярну перевірку.

можуть бути збільшення часу на обробку інформації, витрати на впровадження, управління фізичних засобів захисту та регулярну перевірку.

Мінімальними вимогами до захисту від матеріально-речових каналів може бути застосування засобів для контролю доступа до ОІД в яких функціонує ІзОД, а також

забезпечення фізичного захисту обладнання, яке приймає участь в обробці інформації.

2.7 Засоби захисту від витоку через візуально-оптичні канали.

Від візуально-оптичних каналів витоку інформації загалом існує два види захисту, а саме активний та пасивний.

До пасивних засобів від витоку інформації через ВОК відноситься фізичні бар'єри, які перешкоджають несанкціонованому доступу. До фізичних бар'єрів можуть бути віднесені різного виду перегородки, жалюзі, різноманітні екрани, які перешкоджаються доступу до розгляду моніторів, кімнати, тощо.

До активних засобів від витоку інформації через ВОК можливо віднести використання систем, які відповідають за контролювання рівня освітленості у приміщенні. Такі системи містять в собі спеціальні датчики, які будуть реагувати на всі зміни освітленості, які відбуваються у приміщенні. Ці засоби можуть автоматично вимикати світло для захисту від зчитування інформації з екрана або знижувати чи підвищувати яскравістьу приміщенні тим самим ускладнюючи можливість зчитування інформації з дисплеїв.

Для організації захисту достатньо використання пасивних засобів захисту від ВОК, щоб зменшити ймовірність витоку ІзОД та збору даних про наявні пристрої та засоби захисту в приміщенні. З наявних недоліків лише збільшення вартості та складності КТЗІ.

Недоліками такого захисту буде:.

—Низька ефективність захисту.

—Ефективність пасивних засобів захисту може залежати від конкретної фізичної структури приміщення або обладнання, що використовується. Наявність отворів, щілин або інших слабких точок може створювати можливість для витоку інформації.

—У деяких випадках, використовуючи спеціалізоване обладнання або технології, можливо обійти або подолати пасивний захист і отримати доступ до витікаючої інформації.

2.8 Засоби віброакустичного захисту

Для захисту приміщень, які призначаються для проведення конфеденційних заходів в ході яких буде оброблятись ІзОД найбільш ефективним засобом виступає віброакустичний захист, який забезпечить захист від знімання інформації через стіни, труби, вікна, тощо. Даний вид захисту запобігає зняттю інформації шляхом прослуховування мікрофонами, запусуючими пристроями, тощо.

Система віброакустичного захисту являє собою внесення віброакустичних шумових коливань в діапазоні звукових частот, що запобігає прослуховуванню. Складається, як правило такий захист з набору акустичних, вібраційних випромінювачів та генератору шуму.

Генератор шуму (рис 2.1) створює “білий” шум, який поширюється в діапазоні звукових частот [18]. За допомогою електромагнітних вібраторів, які мають елементи кріплення до огороджувальних конструкцій і через, які здійнюється передача акустичних коливань на огороджувальні конструкції. В тей же час, вібропереторювачі генерують віброколивання в тих же самих конструкціях, що і електромагнітні вібратори, забезпечуючи цим самим мінімальний рівень перешкод акустичного сигналу в приміщенні.

Рисунок 2.1 Вигляд генератора акустичного шуму

Акустичні випромінювачі, які є передбаченими в більшості приладів в свою чергу відповідають за “зашумлення” вентиляційних каналів та за потреби можуть регулювати рівень шумового акустичного сигналу.

Випромінювачі віброакустичні «БАЗАЛЬТ-4ДВМ» призначения для створення віброакустичних завад на конструкціях будівлі в складі активних засобів технічного захисту інформації. Використовуються в автоматизованих системах класу 2 для захисту інформації від витоку через акустичні та віброакустичні канали.

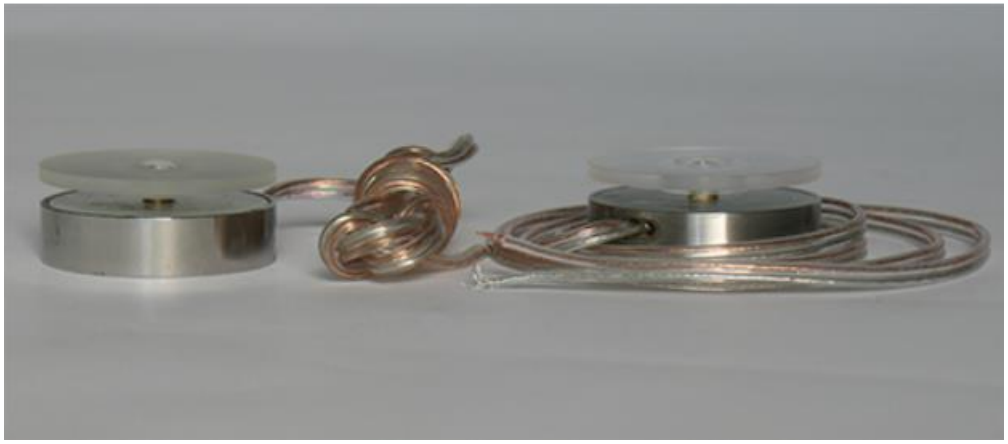

Рисунок 2.2 Вібровипромінювач "БАЗАЛЬТ-4ДВМ"

Згідно наданих даних, характеристики випромінювача віброакустичного "БАЗАЛЬТ-4ДВМ" такі:

Забезпечує передачу віброізольованій приєднаній стальній масі 10 кг віброприскорень у вказаному діапазоні частот із такими значеннями:

—Центральна частота октави 250 Гц: не менше 41 дБ

—Центральна частота октави 500 Гц: не менше 33 дБ

—Центральна частота октави 1000 Гц: не менше 30 дБ

—Центральна частота октави 2000 Гц: не менше 33 дБ

—Центральна частота октави 4000 Гц: не менше 36 дБ

Загалом, ці характеристики описують здатність випромінювача передавати вібрації на цільовий об'єкт з визначеною силою в широкому діапазоні частот, маючи компактні розміри та невелику масу. Також відоповідно до цих характеристик можливо оцінити випромінювач віброакустичний наступним чином:

Здатність передавати віброізольовані віброприскорення до сталевої маси 10 кг з використанням "білого" шуму в широкому діапазоні частот від 100 до 8000 Гц є перевагою цього випромінювача. Це означає, що він може надійно передавати вібрації на цільовий об'єкт з потрібною силою.

Вхідний опір у формі ємності 0,033 мкФ може вплинути на ефективність випромінювача. Його низький опір може призводити до втрат сигналу та спотворень при передачі.

Компактні габаритні розміри (не більше Ø50х18 мм) і невелика маса (не більше 0,12 кг) роблять цей випромінювач зручним для встановлення і використання.

Враховуючи ці характеристики, випромінювач віброакустичний може бути ефективним інструментом для передачі вібрацій на об'єкт з точністю і необхідною силою. Однак, слабкими сторонами можуть бути низький вхідний опір та обмежена пропускна здатність у відповідному діапазоні частот.

До загальних переваг засобу віброакустичного захисту КТЗІ можливо віднести:

1. Ефективність: організація ефективного захисту приміщень від звуку, який передається через огороджувальні конструкції.
2. Низький рівень шуму: можливе застосування засобів шумоізоляції, для зниження рівню шуму в приміщенні і зниження вірогідності прослуховування.
3. Можливість застосування в різних умовах.

До недоліків засобу віброакустичного захисту можна віднести:

1. Висока вартість: достатньо дорогі засоби захисту при придбанні, встановленні чи реконструкції будівлі.
2. Складність встановлення: вимагає спеціальнох кваліфікації працівників по встановленню.
3. Потреба у регулярному обслуговуванні.

2.9 Генератори шуму

Одним з видів генераторів шуму є «МАРС-ТЗО-4-2» - генератор, який створює шумовий сигнал в широкому діапазоні частот від 180 Гц до 5600 Гц і використовується для здійснення активного захисту інформації від витоку через акустичні та віброакустичні канали [19]. Оснащений даний генератор двома незалежними каналами, які і формують окремі шумові сигнали, вигляд зображено на рисунку 2.3.

Рисунок 2.3 - Генератор шумових сигналів «МАРС-ТЗО-4-2»

Переваги генератора шумових сигналів «МАРС-ТЗО-4-2» відносно наведених характеристик:

—Широкий діапазон частот шумового сигналу від 180 Гц до 5600 Гц дозволяє використовувати генератор для різних досліджень та застосувань, що вимагають роботи у різних частотних діапазонах.

—Високе ефективне значення вихідної напруги кожного каналу на опорі навантаження 4 Ом (не менше 3,5 В) забезпечує достатню потужність вихідного сигналу для різних застосувань, таких як випробування та тестування акустичних систем.

—Зазначена висока віброприскорення, що передається від вібровипромінювача ВИ4 ізольованій масі 10 кг в усій смузі шумового сигналу (не менше 50 дБ) дозволяє використовувати генератор для випробування вібраційної стійкості об'єктів.

—Високий рівень звукового тиску, що створюється колонками акустичними захищеними «МАРС-АКЗ» у вільному полі на відстані 1 м в діапазоні робочих частот (не менше 80 дБ), дозволяє використовувати генератор для звукових випробувань та налаштування акустичних систем.

—Зазначена глибина регулювання рівнів шумових сигналів на виходах (не менше 20 дБ) дозволяє точно налаштовувати рівні шуму відповідно до потреб дослідження чи випробування.

Недоліки генератора шумових сигналів «МАРС-ТЗО-4-2»:

—Середнє напрацювання на відмову 10000 годин може бути недостатнім для деяких довготривалих застосувань, де потрібна довготривала неперервна робота.

—Несумісність з іншими частотами живлення, відмінними від 50 Гц та 60 Гц, може обмежити можливості використання генератора в окремих країнах або в специфічних умовах.

—Хоча габарити генератора компактні (225 мм х 142 мм х 48 мм) і його маса невелика (не більше 1,5 кг), в деяких ситуаціях може бути необхідне більше компактне та легке рішення.

Загалом, генератор шумових сигналів «МАРС-ТЗО-4-2» є ефективним засобом активного захисту інформації від витоку через акустичні і віброакустичні канали. Він здатен створювати шумові сигнали в широкому діапазоні частот, що забезпечує надійний захист конфіденційної інформації. Також він відповідає стандартам НД ТЗІ та є рекомендованим засобом Держспецзв’язку.

2.10 Екранування

Через наявність технічних засобів обробки інформації на ОІД , поміж побічних ефектів електронної апаратури можуть виникнути побічні електромагнітні випромінювання. Через наявність таких випромінювань може бути створений додатковий електромагнтіний канал витоку інформації, який можуть використати несанкціоновані особи для отримання доступу до ІзОД.

На інформацію електромагнітне випромінювання може здійснювати вплив наступним чином:

1 За допомогою зовнішнього силового електромагнітного поля може бути порушена цілісніть та конфеденційність інформації;

2 Можливе застосування технічних засобів для здійснення радіоелектронної розвідки чи використання закладних пристроїв;

3 Утворення паразитних чи побічних випромінюваннь;

4 Ненавмисні опромінення ОІД електромагнітними полями техногенних джерел можуть вплинути на їх роботу.

Дані проблеми можливо усунути завдяки екрануванню приміщень на ОІД, в яких розташовуються системи обробки даних, що є досить ефективним засобом захисту від електромагнітного каналу витоку інформації. Електромагнітний екран, який встановлюється буде відповідати безпосередньо за зниження рівня електромагнітного випромінювання, яке генерується технічними засобами в межах екранованого приміщення та запобігає поширенню даного випромінювання в навколишній простір. Схематичний вигляд екранованого приміщення наведено на рисунку 2.2.

Рисунок 2.4 - Схематичний вигляд екранованого приміщення

Екранування забезпечує безпеку засобів обробки інформації та персоналу завдяки зменшенню зовнішнього навмисного електромагнітного випромінювання завдяки якому може викликати порушення конфеденційності та цілісності через несанкціонований доступ до інформації [2].

Перевагами екранування виступають наступні аспекти:

1. Забезпечення захисту від витоку інформації через електромагнітний канал;
2. Збереження приватності;
3. Зменшення рівня електромагнітних випромінювань;
4. Зменшення негативного впливу від зовнішнього навмисного електромагнітного випромінювання на персонал та обладнання для обробки інформації;
5. Електромагнітна безпека об'єкта.

Однак, екранування також має свої недоліки:

1. Високі витрати на установку екранів;
2. Складність технічного обслуговування екранів;
3. Потребує відповідної технічної експертизи та планування під час будівництва або реконструкції приміщення;
4. Зниження якості прийому радіосигналів в екранованому приміщенні.

Проте задля забезпечення максимальної ефективності даного засобу захисту потрібно екранувати не лише саме приміщення де обробляється ІзОД, але й екранувати також пристрої та кабелі.

Кабелі екранують з метою забезпечення захисту від додавання якихось сигналів до жили, а також для перешкоджання виходу сигналів із жили. Також екранування кабелів дозволяє зменшити рівень електромагнітного випромінювання, яке впливає на якість передачі сигналів тим самим зменшуючи ризик несанкціонованого доступу до інформації.

Екранування пристроїв в свою чергу використовується задля зменшення випромінювання електромагнітної енергії, яке може викликати перешкоди в роботі інших пристроїв. Також дане екранування забезпечує захист ІзОД, яка обробляється в електронних пристроях. Реалізується даний вид екранування за допомогою покриття електромагнітної зони якимось металом з високою електропровідністю або просто використання металевих корпусів.

2.11 Мережеві фільтри

Використання мережевих фільтрів для блокування витоку мовної ІзОД обумовлене збільшення використання електронними пристроями імпульсних джерел живлення та високошвидкісних цифрових схем, які під час роботи генерують високочастотні сигнали. Створення даних сигналів може мати негативний вплив на працездатність нормальної роботи пристроїв.

Мережеві фільтри використовують для запобігання потраплянню високочастотних сигналів на кабель живлення пристроїв, які використовуються та запобігти впливу шуму від мережі змінного струму на пристрій. Без наявності мережевих фільтрів відповідати стандартам електронної сумісності буде майже не можливо [21]. Вигляд мережевого фільтру представлений на рисунку 2.3.

Рисунок 2.5 - Вигляд мережевого фільтру

Основними функціями мережевого фільтра є:

1. Уникнення потрапляння на пристрій високочастотних сигналів (шуму) від мережі змінного струму.

2. Уникання потрапляння високочастотних сигналів, що генеруються в пристрої, на кабель живлення.

Дерспецзв'язком пройшов перевірку наступний мережевий філтьтр «ФЕМ-25», який використовується в автоматизованих системах та призначений для здійснення захисту інформації, яка оброблюється в інформаційних та телекомунікаційних системах від витоку електромагнітним каналом витоку інформації та для фільтрації електричних перешкод мережі електроживленння. Вигляд даного фільтру представлений на рисунку

Рисунок 2.6 - Вигляд мережевого фільтру «ФЕМ-25»

Фільтри "Фем-25" здійснюють захист від електромагнітних каналів витоку інформації, які можуть бути утворені через мережу електроживлення. Їх застосування забезпечує безпеку обробки інформації в АС, де є важливою характеристикою збереження конфіденційності та надійності передачі інформації.

Перевагами фільтру згідно його характеристики є:

Згасання електричних сигналів:

1. У смузі частот 0,01-0,15 МГц для несиметричних та симетричних перешкод без робочого струму затухання складає не менше 20 дБ.

2. У смузі частот 0,01-0,15 МГц для несиметричних та симетричних перешкод при проходженні робочого струму затухання складає не менше 20 дБ.

3. У смузі частот 0,15-1000 МГц для несиметричних та у смузі 0,15-30 МГц для симетричних перешкод без робочого струму затухання складає не менше 60 дБ.

4. У смузі частот 0,15-1000 МГц для несиметричних та у смузі 0,15-30 МГц для симетричних перешкод при проходженні робочого струму затухання складає не менше 60 дБ.

Падіння напруги:

1. Падіння напруги при робочому струмі 25 А не перевищує -5 В.

Недоліками фільтра "ФЕМ-25" є:

Обмеження по робочому струму: Фільтр розрахований на робочий струм навантаження до 25 А. Це може бути недостатньо для деяких великих навантажень, які вимагають більшої потужності.

Обмежений діапазон згасання: Хоча фільтр забезпечує ефективне згасання електричних сигналів у вказаних діапазонах частот, він може бути менш ефективним у вищих частотних діапазонах або при зустрічі зі складнішими сигналами.

Загалом, фільтр "ФЕМ-25" демонструє високу ефективність у затуханні електричних сигналів у широкому діапазоні частот та забезпечує стабільну роботу з мінімальним падінням напруги. Він відповідає стандартним значенням напруги та частоти мережі, має стійкість до температурних та вологостних умов та має компактні розміри, що робить його зручним для використання в різних системах. Також даний фільтр відповідає вимогам НД ТЗІ в обсязі функцій, які зазначені в документі згідно оприлюдненого списку затверджених засобів захисту від Держспецзв’язку

Також для даного засобу захисту є в край важливим не тільки електрична конструкція, а також і встановлення самого фільтра, спосіб, яким підведено провода та його місце розташування. Мережеві фільтри для блокування витоку мовної конфіденційної інформації колами електроживлення змінного (постійного) струму слід розміщувати там, де кабель живлення постійного струму входить в корпус для запобігання електромагнітному зв’яку з відфільтрованим шнуром живлення. Фільтр має бути встановлений таким способом, аби його металевий корпус був

безпосередньо підключений прямим контактом до корпусу потрібного нам пристрою, що забезпечить усунення будь-якої додаткової індуктивності в послідовності з внутрішніми конденсаторами класу Y. Рекомендується прокладати дроти, які будуть пролягати між фільтром і джерелом живлення безпосередньо до корпусу пристроя аби зменшити шанс на прийом сигналу. Також вхідні дроти фільтра не мають бути прокладені поблизу вихідних дротів живлення змінного струму, оскільки це впливає на збільшення можливості утворення паразитного ємнісного зв’язку та не мають бути поруч з іншими сигнальними дротами.

Якщо ж розглядати мережеві фільтри загалом то основними перевагами цього засобу захисту є:

— Стабільна робота обладнання: фільтри забезпечують більш стабільну роботу обладнання забезпечуючи зменшення ризику збоїв та знижуючи рівень шуму в електричній мережі

— Ефективного захист проти зовнішніх електромагнітних впливів.

— Більш стабільна робота обладнання в умовах електромагнітних перешкод: забезпечення захисту електронного обладнання шляхом зменшення впливу електромагнітного впливу на них.

Недоліками цього засобу захисту є:

— Висока вартість: мережеві фільтри зазвичай можуть бути досить дорогоми, що може стати проблемою при потребі в широкому використанні.

— Обмежений діапазон частот: наявні високі параметри фільтрації для діапазону мережевої частоти, але може бути не ефективним даний засіб, якщо робота буде здійснюватись з високими частотами.

— Складність налаштування та встановлення: ефективність безспореньо залежить від правильного встановлення та налаштування фільтрів, адже не правильне налаштування може призвести до втрат даних.

— Ефективність при захисті декількох пристроїв:при підключення до фільтра більш ніж одного пристрою загальна ефективність знизиться.

Мережеві фільтри, які призначеня для блокування витоку мовної ІзОД передбачають різні конструктивні варіанти та можуть бути використані для захисту

різного за типом обладнання, наприклад, телефони, промислові машини, комп’ютери та інше. Також дані фільтри можуть встановлюватись не ре лише на вхідній стороні, а й на вихідній стороні електронного пристрою.

Отже, мережеві фільтри можуть використовуватись для захисту обладнання від деяких видів шуму та коли проти витоку мовної ІзОД. Однак треба враховувати, що ці фільтри не можна використовувати, як універсальний засіб захисту та слід враховувати бюджет підприємства та недоліки даних фільтрів.

2.12 Фільтри-обмежувачі та спеціальні абонентські пристрої

Фільтри обмежувачі – пристрій, якій встановлюється на лініях зв’язку для подальшої фільтрації шумів, перешкод та для обмеження частотного діапазону мовної інформації. Функціональна схема фільтрів обмежувачів наведена на рисунку 2.4. Їх основна функція полягає в зменшенні рівня вихідної мовної інформації на вихідній лінії для забезпечення безпечного рівня шуму, який буде захищений від несанкціонованого доступу до інформації (прослуховування) [22].

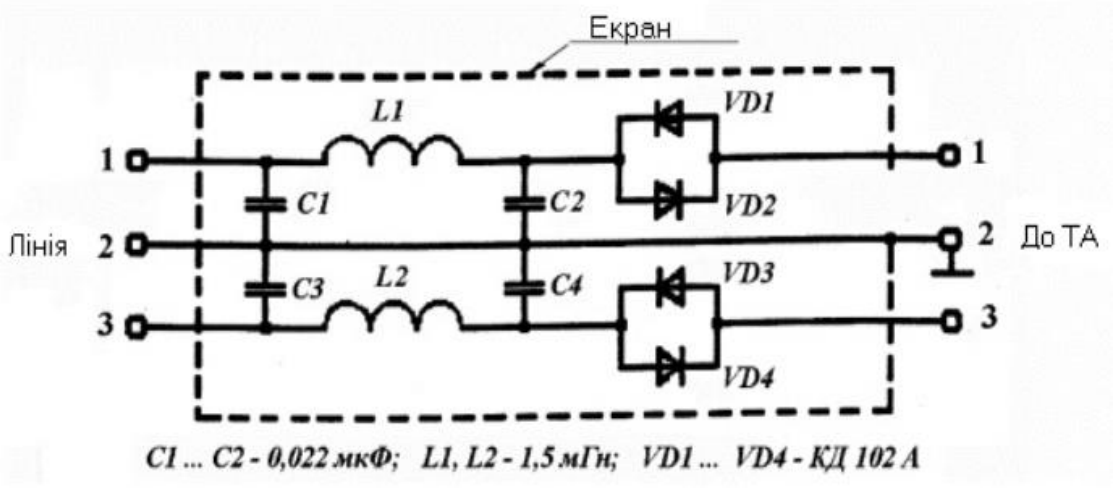

Рисунок 2.7 - Схема фільтру обмежувача.

В свою чергу спеціальні абонентські пристррої захисту – пристрої, які необхідно встановлювати на абонентському обладнанні і основна функція, яких полягає в забезпеченні захисту від витоку мовної інформації через двопровідні лінії зв’язку [21].

Основними перевагами даних засобів захисту є:

1. Збільшення рівня конфеденційності та захисту мовної інформації від несанкціонованого доступу.
2. Ефективний захист від технічних каналів витоку інформації.
3. Легкі у використанні та у встановленні.
4. Зменшення рівня відбитих сигналів на лінії.

Недоліками даних засобів захисту є:

1. Збільшення затримки передачі мовної інформації.
2. Зниження якості передачі на лініях зв’язку мовної інформації.
3. Можлива обмежена адаптивність до змінюючогося вмісту, що може спричинювати неправильне фільтрування.

Дані засоби є корисні у захисту мовної інформації при передачі лініями зв’язку, але вони не гарантують повного захисту інформації. Для забезпечення повної передачі вони також потребують додаткових заходів захисту через можливість зняття зашифрованої інформації за допомогою спеціальних технологій.

2.13 Засоби високочастотного шуму

В якості використовуваного приладу високочастотного шуму є затверджений дерспецзв’язком прилад “PIAC-1C”. Даний засіб є стаціонарним пристроєм, який призначений для генерації широкосмугового шуму у високочастотному діапазоні. Він працює в діапазоні від 20 кГц до 100 кГц і використовується в комплексах технічного захисту інформації для захисту від акустичних каналів витоку інформації.

Основна функція PIAC-1C полягає в створенні шумового фону, який маскує акустичні сигнали, що можуть містити конфіденційну інформацію. Він генерує широкосмуговий шум, який заповнює весь високочастотний діапазон, унеможливлюючи аналіз та перехоплення акустичних сигналів.

Рисунок 2.8 - Вигляд “PIAC-1C”

Оцінювання ефективності можна здійснити згідно з такими показниками:

—Діапазон підавлення передатчиків: Від 180 Гц до 2 ГГц і вище. Широкий діапазон підавлення показує, що прилад здатний приглушувати сигнали від маломощних передатчиків в цих частотних діапазонах.

—Коєфіцієнт якості шумового сигналу: Мінімальний рівень 0,8 свідчить про наявність достатньо якісного шумового сигналу.

—Коєфіцієнт міжспектральних кореляційних зв'язків: Значення не більше 6 дБ вказує на відсутність суттєвих зв'язків між різними частотними компонентами шумового сигналу.

—Регулювання рівня шумового сигналу: Можливість регулювання рівня шуму на величину не менше 20 дБ дозволяє адаптувати сигнал до конкретних умов і потреб.

—Максимальне інтегральне значення вихідної потужності: Значення не менше 10 Вт свідчить про наявність достатньої потужності для створення шумового фону.

—Вбудована система автоматичного контролю та звукова індикація цілісності антен.

—Час технічної готовності: Не більше 5 секунд вказує на швидкість і готовність пристрою до роботи.

—Споживана потужність: Не більше 20 Вт забезпечує економічну ефективність використання.

Загалом, з урахуванням наведених характеристик, можна припустити, що PIAC-1C є ефективним засобом для захисту від акустичних каналів витоку інформації,

оскільки він здатний генерувати широкосмуговий шум у високочастотному діапазоні з заданими параметрами підавлення та контролю рівня шуму. Проте, окремі технічні показники можуть варіюватись в залежності від конкретної реалізації пристрою та умов експлуатації.

2.14 Високочастотні фільтри

Лінійні фільтри захисту (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв'язку, як правило застосовується для забезпечення надійності сигналів від спотворення та шумів, які можуть виникнути на лінії зв’язку. Вигляд лінійного фільтру захисту наведено на рисунку 2.5.

Рисунок 2.9 - Вигляд високочастотного електромагнітного фільтру.

Важливим етапом роботи з високочастотними фільтрами є встановлення на ОІД даних фільтрів, які можуть бути розміщені, як на лінійних дротах, так і на елементах обладнання телекодового зв’язку особливо корисним є застосування даних засобів захисту, при наявних електричних перешкодах та в умовах шумів.

Високочастотні фільтри мають наступні основні функції, а саме:

1. Захист обладнання від перенапруг та впливу природних електромагнітних випромінювань.
2. Захист обладнання від створення перешкод, які можуть виникнути, якщо на лінії зв’язку трапиться інтерференція від електромагнітного поля чи пристрою.

3. Зменшення наявних шумів та спотворень, які утворюються внаслідок дії зовнішних джерел на лінії зв’язку.

4. Забезпечення більш стабільної роботи обладнання.

5. Зменшення ризику пошкодження внаслідок впливу електромагнітних випромінювань.

Окрім, основних функції в високочастотних фільтрах є також важливим і їх частотна характеристика та рівень підсилення. Частотна характеристика відповідає за рівень перешкоджання різним частотам сигналів, а рівень підсилення в свою чергу відповідає за показ того, як добре передається корисний сигнал.

Загалом використання високочастотних фільтрів є важливим, якщо на ОІД буде здійснюватись експлуатація телекодового зв’яку чи для зниження рівня електромагнітного випромінювання та шумів.

Висновки за розділом 2

В даному розділі було виконано два завдання встановлених до кваліфікаційної роботи. Згідно другого завдання було проаналізовано вимоги керівних документів, які використовуються в процесі створення комплексу технічного захисту інформації.

В ході виконання завдання було досліджено загальні вимоги щодо комплексів засобів захисту та стандарти на які слід посилатись створюючи комплекси технічного захисту інформації. Також розглянуто вимоги до створення режимних приміщень та сигналізацій, які мають бути встановлення на об’єкті інформаційної діяльності.

Для виконання третього завдання було виконано аналіз технічних засобів, які використовуються в процесі створення комплексу технічного захисту. Виконано аналіз засобів, які використовуються для захисту від несанкціонованого доступу до інформації технічними каналами витоку. Наведено, які пристрої можливо використовувати, для чого конкретно вони призначаються та наведено їх переваги та недоліки.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ЩОДО УДОСКОНАЛЕННЯ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Рекомендації щодо використання засобів захисту від електромагнітних каналів витоку

Отже, проаналізувавши багато інформації про технічні канали витоку інформації, засоби, які застосовуються та про наявні стандарти для комплексів технічного захисту інформації, я можу надати певні рекомендації по засобами захисту, які можливо використовувати додатково в КТЗІ для побудови дійсно надійного захисту. Розпочнемо ми з розгляду засобів захисту, які можливо застосувати для удосконалення комплексу технічного захисту інформації від електромагнітних каналів витоку інформації.

Для здійснення ефективного захисту від витоку інформації електромагнітними каналами необхідно застосувувати в комплексах технічного захисту інформації різноманітні засоби технічного захисту. В даному розділі буде розглянуто засоби, які можуть безпосередньо покращити захист від електромагнітних каналів витоку інформації.

Для удосконалення комплекссу технічного захисту інформації від електромагнітних каналів витоку інформації, можливо використосувати наступні засоби захисту:

1. Фільтри захисні протизавадні

Мною до використання рекомендується до використання “ФЗП-110-2”, який використовуються для збільшення рівню захисту від витоку інформації через електромагнітні канали. Вигляд даного фільтру наведений на рисунку 3.1.

Основною фукнцією даних засобів є фільтрація та здійснення поглинання небажних електромагнітних сигналів та забезпечення високого рівня

електромагнітної сумістності. Вони здатні здійснювати фільтрацію електромагнітних сигнаілв різного діапазону частот та підвищити захист наявних комплексів ТЗІ.

Рисунок 3.1 - Фільтри захисні протизавадні “ФЗП-110-2”

Переваги даного фільтру:

—Ефективність захисту: Фільтр забезпечує високий рівень захисту від витоку інформації в широкому діапазоні частот (10 кГц...18 ГГц) і здатний поглинати значні амплітуди імпульсних перешкод.

—Надійність: Фільтр витримує перегрузки по току впродовж певного часу, що сприяє його надійному функціонуванню в умовах високого навантаження.

—Компактність: Фільтр має невеликі габарити і масу, що спрощує його установку та застосування у різних умовах.

Недоліки «ФЗП-110-2»:

—Обмежений діапазон напруги: Фільтр працює з номінальною напругою 220 В, що може бути недостатньо для деяких специфічних вимог або систем з високими напруговими параметрами.

—Обмеженість захищених каналів: Фільтр спрямований на захист від витоку інформації через акустичний канал, але може не бути ефективним проти інших потенційних каналів, таких як електромагнітний чи оптичний.

«ФЗП-110-2» виявляється ефективним захисним протизавадним фільтром. Він пропонує номінальну робочу напругу та струм, здатність витримувати перегрузки,

широкий захищений діапазон частот та здатність поглинати великі амплітуди імпульсних перешкод. Крім того, він має малий розмір і вагу, що сприяє його зручності в установці та використанні. Також даний фільтру пройшов перевірку Держспецзв'язку і є рекомендованим засобом захисту. З урахуванням цих факторів, можна стверджувати, що «ФЗП-110-2» є надійним і ефективним захисним фільтром для захисту від витоку інформації.

2. Фільтри обмежувачі

Використання обмежувальний фільтрів полягає в здійсненні контролювання частотного діапазону електромагнітних сигналів та обмежувати прийом або передачу безпосередньо до самих пристроїв. Допомагають знизити рівень електромагнітних перешкод і можуть або збільшити захист разом з електромагнітним екрануванням або бути заміною екрануванню хоча і більш слабкою. Одним з видів даних фільтрів є феритові фільтри наведений на рисунку 3.2.

Рисунок 3.2 - Вигляд феритового фільтру

Цей засіб допомагає поглинати високочастотні шуми та електромагнітні перешкоди, що можуть впливати на провідні лінії та кабелі. Він знижує рівень шумів та електромагнітних інтерференцій, що переносяться по провідникам, тим самим зменшуючи можливість витоку інформації через ці канали. Їх можливо використовувати, як додатковий засіб захисту від спотворення сигналу чи наведень на дроти пристроїв. Встановлюються вони в 2-3 см від виходу дроту з пристроя та є бюджетним засобом, який допомагає знизити рівень впливу на пристроїв електромагнітними сигналами.

3. Кофіденційні зони.

Створення кофіденційних зон являє собою ефективний засіб захисту від електромагнітних каналів витоку інформації. Створена КЗ має бути не меншою за Зону 2 та необхідно здійснити організацію режиму доступу до КЗ на ОІД. Також при створенні треба розраховувати на паразитну модуляцію небезпечним сигналом коливань. Дані зони представляються захищену від електромагнітного сигналу та фізично відокремлену зону, яка надає обмеження доступності для несанкціонованого доступу. Можуть використовуватись затухання електромагнітних сигналів та певні властивості екранування.

4. Електромагнітний аналіз.

Даний вид засобу захисту використовується для безпосереднього аналізу наявних елетромагнітних активностей з метою виявлення незвичнної діяльності, що вказує на потенційний канал витоку інформації.

Мною рекомендується використання Keysight N9020A MXA Signal Analyzer (рисунок 3.3), який є потужним засобом для аналізу електромагнітних сигналів.

Рисунок 3.3 - Вигляд сигнального аналізатора “Keysight N9020A MXA”

Оцінити його можливо за наступними характеристиками:

—Частотний діапазон: Має широкий діапазон робочих частот, що дозволяє аналізувати сигнали в широкому спектрі від низьких до високих частот (10 Гц до 26,5 ГГц із смугою аналізу до 160 МГц).

—Чутливість: Даний аналізатор має високу чутливість, що дозволяє виявляти навіть слабкі електромагнітні сигнали.

—Роздільна здатність та точність: Забезпечує високу роздільну здатність і точність вимірювань, що дозволяє детально аналізувати характеристики сигналів та виявляти недоліки або аномалії.

—Функціональність: Має розширені можливості аналізу, які включають спектральний аналіз, вимірювання параметрів сигналу, пошук сигналів та ідентифікацію модуляцій.

—Інтеграція: Keysight N9020A MXA може бути інтегрований з іншими засобами технічного захисту та автоматизованими системами, що сприяє комплексному захисту інформації.

Оглядаючи ці характеристики, Keysight N9020A MXA Signal Analyzer є потужним засобом захисту від електромагнітних каналів витоку інформації. Проте, перед використанням слід врахувати специфічні вимоги та потреби системи, а також врахувати фактори бюджету та доступності.

5. Організація фізичного контролю: Фізичний контроль за доступом до електронних пристроїв та інфраструктури є важливим аспектом комплексу технічного захисту. Це може включати контроль доступу до серверних кімнат, використання системи ідентифікації та контролю доступу (наприклад, картки доступу або біометричні системи) та встановлення систем відеоспостереження. Організація фізичного контролю здійснюється в залежності від бюджету та від розміру ОІД.

Перечислені засоби можливо використовувати для удосконалення та підвищення ефективності захисту комплексу технічного захисту інформації від електромагнітних каналів витоку інформації, але слід регулярно проводити аудит безпеки для виявлення потенційних загроз.

3.2 Рекомендації щодо використання засобів захисту від акустичних каналів витоку

Забезпечення ефективного захисту від акустичних каналів інформації є важливою задачею в комплексі технічного захисту інформації. В даному розділі буде розглянуто засоби, які можуть безпосередньо покращити захист від акустичних

каналів витоку інформації. Засоби захисту можуть включати в собі технології шифрування, акустичну ізоляцію, контроль акустичного середовища та інші методи. Для удосконалення комплексу ТЗІ, пропонується використання наступних засобів:

1. Акустична ізоляція.

Даний вид захисту підрозуміває застосування екранування для зменшення можливості перехоплення акустичних сигналів та використання акустичних бар’рів та звукопоглинаючих матеріалів для запобігання витоку акустичних сигналів. Є ефективним засобом захисту, але може бути надто дорогим особливо коли проводиться екранування великих приміщень.

2. Контроль акустичного середовища.

Застосування акустичних датчиків та мікрофонів, які здатні виявляти несанкціонований запис акустичних сигналів чи наявність засобів шпигунства.

Мною рекомендується застосування цього засобу захисту - Louroe Electronics ASK4-300, який є пристроєм акустичної детекції, який використовується для спостереження та контролю акустичного середовища в автоматизованих системах. Основна функція ASK4-300 - виявлення звукових подій та реагування на них. Вигляд даного пристрою акустичної детекції наведено на рисунку 3.4.

Рисунок 3.4 - Вигляд Louroe Electronics ASK4-300

На основі його характеристик, можна зробити наступну оцінку ефективності захисту засобу Louroe Electronics ASK4-300 проти акустичних каналів витоку інформації:

— Засіб може сприймати звук на відстані до 5 метрів або в межах круга діаметром 10 метрів.

—Засіб має адаптер звукового інтерфейсу IF-1, який дозволяє підключати мікрофон до різних пристроїв, таких як камери або записувачі, за допомогою RCA або стерео з'єднання.

—В ньому є функція регулювання підсилення, яка допомагає уникнути перевантаження сигналу до записувачів або мережевих камер, що забезпечує якійсний та безперебійний запис звуку.

—Наявно 2 типи аудіовиходів, які сумісні з більшістю пристроїв запису, що приймають лінійний аудіовхід в режимі реального часу.

Загалом, засіб Louroe Electronics ASK4-300 має деякі важливі характеристики, які надають можливість збільшити ефективність комплексу ТЗІ в захисті від акустичних каналів витоку інформації. Однак, оцінка його повної ефективності варіюватиметься в залежності від конкретних вимог і умов експлуатації автоматизованої системи класу 2.

3. Фізичний контроль доступу.

Застосування контролю доступу до приміщень в яких перебувають генератори просторового та лінійного зашумлення та в приміщення до обробляється конфіденційна інформація. Проте варто проводити навчання персоналу з приводу безпеки для запобігання реалізації слабкого місця у вигляді соціальної інженерії.

4. Шифрування акустичних сигналів.

Полягає в застосування методу аутентифікації для підтвердження вірності між вхідними акустичними сигналами і сигналами відправника. Ефективність буде залежати від обраного методу шифрування.

5. Вібраційні датчики

Використання вібраційних датчиків є корисними для виявлення вібраційних сигналів, які випромінюються об’єктами. Дані об’єкти можуть бути розташовані в місцях з конфіденційною інформацією тому є корисними для виявлення віброакустичних каналів витоку інформації. Проте вібраційні датчики не можуть попередити заздалегідь про витік лише знаходять вже наявні.

Серед вібраційних датчиків мною рекомендується застосування Dytran 3035B наведений на рисунку 3.5. Даний датчик є високочутливим вібраційним датчиком, який можливо використовувати для захисту проти акустичних каналів витоку інформації. Він здатний вимірювати навіть незначні коливання, що можуть бути пов'язані з акустичними сигналами.

Рисунок 3.5 - Вібраційний датчикDytran 3035B

Для захисту від акустичних каналів витоку інформації, Dytran 3035B може бути використаний для:

Виявлення недоречних акустичних звуків: Датчик може реєструвати навіть незначні коливання, які виникають внаслідок акустичних сигналів. Це дозволяє виявити присутність акустичного потоку та потенційних каналів витоку інформації.

Моніторинг вібрацій: Dytran 3035B може вимірювати характеристики акустичних коливань, такі як амплітуда, частота та спектральний склад. Це дозволяє аналізувати акустичні сигнали та виявляти потенційні канали витоку інформації.

Виявлення несанкціонованого звукового запису: Датчик може допомогти виявити наявність несанкціонованого запису звуку в приміщенні або навколо автоматизованої системи. Він може реагувати на звукові сигнали та сприяти виявленню можливих загроз безпеці інформації.

Враховуючи ці фактори, ефективність Dytran 3035B може бути високою, особливо якщо він відповідає вимогам та специфікації системи технічного захисту.

Також для захисту від акустичних каналів витоку інформації використовується раніше згадані генератори просторового та лінійного зашумлення. Їх використання є корисним для створення та налаштування керованих параметрів шуму, що сприяє

збільшенню захисту проти акустичних каналів витоку інформації проте вони мають свої недоліки. Для перекреття недоліків даних засобів захисту необхідно:

1. Акустичні фільтри.

Для більшої боротьби проти звукових сигналів можливе використання адаптивних акустичних фільтрів, які адаптуються для ідентифікації та нейтралізації небажаних звукових сигналів. Їх налаштовують для виявлення та блокування небажаних шумів.

Загалом адаптивні акустичні фільтри можуть забезпечити високий рівень захисту від акустичних каналів витоку інформації за наступними причинами:

—Адаптивні акустичні фільтри можуть нейтралізувати небажані звуки, адаптуючись до змінних умов та шумових характеристик.

—Адаптивні акустичні фільтри використовують складні алгоритми розпізнавання звуку, що дозволяє точно ідентифікувати небажані сигнали та розрізняти їх від бажаних.

—Мають гнучкість в налаштуваннях тому можуть бути налаштовані для конкретних потреб та вимог захисту.

—Можуть ефективно ідентифікувати небажані шуми та блокувати їх передачу, забезпечуючи ефективний захист від акустичних каналів витоку інформації.

Однак, ефективність захисту від акустичних каналів витоку інформації залежить від багатьох факторів, таких як якість самого фільтра, сила та характеристики небажаних звуків, шумове середовище та можливість обхідних шляхів передачі інформації. Тому остаточна оцінка рівня захисту потребує детального аналізу конкретного адаптивного акустичного фільтра в контексті його використання та умов експлуатації.

2. Аналіз та усунення слабких місць.

Спрямоване на проведення детального аналузі приміщення з метою ідентифікацією слабких місць через наявність, яких може бути значно зменшена ефективність генераторів.

Наведені засоби збільшують надійність та ефективність комплексу технічного захисту інформації проти акустичних каналів витоку інформації і можуть працювати комбіновано з іншими засобами без перешкод.

3.3 Рекомендації щодо використання засобів захисту від візуально-оптичних каналів витоку

В ході виконання кваліфікаційної роботи було з’ясовано що існує два види забезпечення захисту від даних каналів витоку інформації, а саме пасивний та активний вид захисту. Було також досліджено, що загалом вимоги до ВОК ставляться лише в організації базового пасивного захисту, а саме застосування жалюзів чи штор на вікнах застосування бар’єрів між робочими екранами та правильне розташування моніторів так, щоб їх не можливо було побачити з вікна чи з дверного пройому для несанкціонованого доступу.

Через те, що базові засоби захисту є досить слабкими від витоку візуально-оптичними каналами мною було рекомендавно наступні засоби, які зможуть перекрити недоліки та нададуть збільшений захист та зменшений ризик витоку.Загалом існує кілька засобів, які можуть зменшити ймовірність несанкціонованого доступу до інформації, а саме:

1. Застосування екрану конфіденційності на робочих моніторах де обробляється конфіденційна інформація. Дані екрани обмежують можливість перехоплення інформації знаходячись зі сторони монітору або з далекої відстані.

Рекомендую застосування 3M™ Privacy Filters, які є спеціально розробленими прозорими плівками, які накладаються на екрани різних пристроїв. Вони призначені для захисту конфіденційної інформації шляхом обмеження кута огляду, з якого можна бачити екран.

Основні характеристики 3M™ Privacy Filters включають:

—Технологія мікроламелей: Ця технологія дозволяє забезпечує зменшення кута огляду і ускладнює перегляд екрана з боків.

—Захист від відблисків: Наявне антиблікове покриття, яке допомагає зменшити відблиски і блиск на екрані, що полегшує комфортний перегляд і забезпечує більшу конфіденційність.

3M™ Privacy Filters є ефективним засобом захисту від візуально-оптичних каналів витоку інформації. Завдяки своїм технологіям і спеціальній конструкції, вони дозволяють обмежити кут огляду і зберігати конфіденційні дані приватними для осіб, які не перебувають в прямому полі зору екрана. Однак, варто зазначити, що ефективність захисту може залежати від кута огляду, освітлення та якихось інших факторів.

2. Затемнення вікон. Для більш надійного захисту від оптичного спостереження можна використати спеціальні полімерні плівки, які наносяться на вікна чи двері в основі яких є скло. Застосування даних плівок дозволить забезпечити низький конфіцієнт пропускання видимого світла, що в свою чергу робить візуально-оптичну розвідку майже не можливою.

3. Фізичні бар’єри. Застосування перегородок чи шторок, які зможуть обмежити прямий огляд в приміщенні, де обробляється ІзОД.

Наведені засоби дозволяють збільшити рівень захисту інформації зберігаючи її від несанкціонованого доступу і спостереження. Зменшуються ризик витоку даних та є легкими в установленні і використанні.

4. Інфрачервоні ба’єри. Засоби захисту, які підрозумівають встановлення спеціальних бар’єрів, які будуть реагувати на інфрачервоне випромінювання. Використовують в своїй структури створення невидимої стіни, яка буде здійснювати виявлення вторгнень шляхом прийому та передачі світлових променів. Коли відбувається “розрив” всередині променя, то система вмикає тривогу, аби вказати на наявне вторгнення.

Серед можливих варіантів інфрачервоного бар’єрів мною рекомендується застосування OPTEX SL-350QN. Даний бар’єр складається з передавача і приймача, розташованих на протилежних сторонах об'єкта, його робота засновується на принципі відслідковування перешкод в зоні між передавачем і приймачем. Коли об'єкт перекриває промінь між передавачем і приймачем, спрацьовує сигнал тривоги,

вказуючи на виявлення руху. Вигляд інфрачервоного бар’єру “OPTEX SL-350QN” наведено на рисунку 3.5.

Рисунок 3.5 - Зображення інфрачервоного бар’єра “OPTEX SL-350QN”

Цей інфрачервоний бар’єр має наступні характеристики:

—Максимальна відстань між приймачем і передавачем складає 100 метрів, що дозволяє охопити широку зону і виявляти перешкоди на великій відстані.

—Час преривання роботи луча становить 50-500 м/с тому він має досить високу швидкість виявлення перешкод, що дозволяє реагувати на швидкі рухи та швидкі перешкоди.

—Має ступінь захисту корпуса IP65, що захищає бар'єр від пилу та струменів води та сприяє його надійності і тривалому.

—Наявність тамперного контакту та захисту від розрядів дозволяє виявляти незаконне втручання та забезпечує безпеку пристрою.

—Можливість регулювати кут нахилу променя дозволяє налаштовувати бар'єр під різні умови і розміри об'єктів.

Загалом, 4-променевий інфрачервоний бар'єр має досить великий потенціал для ефективного захисту від витоку інформації через акустичні канали, забезпечуючи надійну інфраструктуру детекції руху та захисту об'єкта.

Недоліками можуть бути:

1. Вартість.Збільшена вартість на організацію технічного захисту інформації

2. Ефективність. Хоча наведені засоби і удосконалюють комплекс технічного захисту інформації проте вони все ще не гарантують абсолютної безпеки.

3. Потенційне обмеження на проникнення світла. Використання спеціальних полімерних плівок або екранів конфіденціності можуть впливати на проникнення світла або на яскравість зображення.

Застосування таких додаткових засобів захисту значно збільшують захищеність від візуально-оптичних каналів та є достатньо доступними для їх застосування. Проте важливо постійно проводити аудити безпеки для оцінки потенційних загроз та адаптувати заходи безпеки.

3.4 Рекомендації щодо використання засобів захисту від матеріально-речових каналів витоку

Матеріально-речові канали витоку охоплюють в собі фізичні засоби та методи, які використовуються для захисту від несанкціонованого доступу до іфнормації чи її витоку. В даному розділі будуть наведені засоби захисту, які здатні підвищити рівень захисту та усунути недоліки базового захисту. Наведені засоби можливо використовувати окремо або в комбінації, залежно від фінансових можливостей та контректних потреб. Для збільшення захисту від даних каналів витоку інформації, пропонується додати до КТЗІ наступні засоби:

1. Біометрична ідентифікація.

Використання засобів захисту, які містять своїй основі ідентифікацію людини по відбитку пальця чи через розпізнавання обличчя значно підвищує рівень захисту проти матеріально-речових каналів витоку інформації. Ефективний засіб захисту, але вартісний.

Даний засіб захисту можливо використовувати, як основний спосіб авторизації або можливо реалізувати двофакторну аутентифікацію з застосуванням паролю та біометрії.

2. Облік обладнання та фізичний контроль.

Дані засоби захисту підрозумівають під собою використання міток RFID, систем інвентаризації та моніторингу руху обладння. Дозволяє виявляти незвичайні рухи чи втрату обладнання.

Для обліку даних рекомендую використання Impinj Speedway Revolution R220 UHF RFID Reader (рисунок 3.6), який є потужним засобом ідентифікації на основі RFID-технології. Він має два порти зчитування, що дозволяє одночасно зчитувати дані з двох RFID-тегів або об'єктів.

Рисунок 3.6 - Вигляд Impinj Speedway Revolution R220

Основні характеристики Impinj Speedway Revolution R220:

—Air Interface Protocol: GS1/EPCglobal UHF Class 1 Gen 2 (ISO 18000-6C): Цей протокол забезпечує стандартизований доступ та комунікацію з RFID-тегами, що підвищує ефективність ідентифікації та контролю об'єктів.

—Робоча частота UHF(860-960 MHz), дозволяє зчитувати теги на великій відстані, що покращує ефективність системи.

—Змінний діапазон потужності передачі дозволяє пристосувати зчитувач до різних умов і вимог, що підвищує його гнучкість та ефективність.

—Може зчитувати до 200 зчитувань на секунду.

—Рейтинг IP 52 забезпечує певний рівень захисту від пилу та вологи, що робить зчитувач відповідним для використання в різних умовах.

Оцінка ефективності проти матеріально-речових каналів витоку інформації залежить від конкретних вимог і умов використання. Загалом Impinj Speedway Revolution R220 є високоякісним RFID-считувачем, який забезпечує швидку та точну ідентифікацію об'єктів, проте ефективність проти витоку інформації залежатиме від додаткових заходів безпеки, які вживаються в рамках системи, таких як шифрування даних, фізичний контроль доступу та інші заходи безпеки, що встановлюються окремо.

3. Шифрування даних.

Застосування сильних видів шифрування на ІзОД збільшує рівень захисту у випадках коли носій з інформацією було викрадено. Залежить від обраного методу шифрування.

Перераховані засоби можуть удосконалити наявний комплекс технічного захисту інформації проти несанкціонованого доступу через матеріально-речовий канал витоку інформації. Вони працюють у поєднанні з базовим захистом, який здійснюється згідно вимог до КТЗІ та усувають їх недоліки тим сами збільшуючи рівень захисту комплексу ТЗІ і зменшуючи можливість реалізації несанкціонованого доступу.

Окрім, захисту від несанкціонованого доступу важливою проблемою є правильне знищення застарілих носіїв інформації. Через те, що добування інформації з магнітних носіїв є великою загрозою в матеріально-речових каналах витоку інформації. Для максимізації захисту від даної загрози потрібно не лише використовувати базові засоби по стиранню та перезапису файлів з носія, адже інформацію все ще можна буде відновити хоча все і не штатними засобами. Досягнути зменшення ризкику витоку інформації можливо лише при перезаписі даних декілька разів на носії та подальшому повному знищенню структури магнітного середовища.

Для знищення з носія мною рекомендується використання наступного засобу захисту Garner HD-2XT Degausser (рисунок 3.7), який є високоефективним засобом для безпечного знищення магнітної інформації з різних типів носіїв даних, таких як жорсткі диски (HDD), магнітні стрічки і картриджі, флеш-пам'ять і т.д.

Рисунок 3.7 Вигляд Garner HD-2XT Degausser

Даний засіб має наступні властивості:

1. Має потужні електромагніти, які забезпечують достатньо сильне магнітне поле для повного вимагнічування даних з носіїв.
2. Цей дегаусер може швидко та ефективно вимагнічувати дані з носіїв.
3. HD-2XT має вбудовані захисні функції, що запобігають випадковому вмиканню і забезпечують безпеку під час використання
4. Цей засіб забезпечує високу ефективність у захисті від матеріально-речових каналів витоку інформації, оскільки він повністю вимагнічує дані з носіїв, роблячи їх практично незчитуваними.

Загалом, Garner HD-2XT Degausse є надійним та ефективним засобом для безпечного знищення магнітної інформації. Його висока потужність, швидкість та безпечність роботи роблять його ефективним у захисті від матеріально-речових каналів витоку інформації.Проте навіть після застосування цього засобу рекомендується подальше роздрібнювання, застосування вибухівки чи застосування високих температур на використані магнітні носії.

Висновки за розділом 3

В даному розділі було розглянуто останнє завдання кваліфікаційної роботи, а саме розробка рекомандації для удосконалення захисту інформації на об’єктах інформаційної діяльності. В ході виконання даного завдання було наведено різні

засоби захисту проти кожного каналу витоку інформації окремо, які працюють в комплексі без перешкод один одному.

Комбінація розглянутих засобів захисту забезпечить більший рівень захисту від технічних каналів витоку інформаї, але все ще не гарантує абсолютного захисту, адже не можливо цілком повністю захиститись від усього. Тому враховуючи постійний розвитоку технологій і зростання загроз, важливо постійно оцінювати потенційні загрози та адаптувати заходи безпеки відповідно до змінюючогося оточення.

ВИСНОВКИ

Інформація, яка обробляється на об’єктах інформаціної діяльності, яка має статус інформації з обмеженим доступом потребує захисту. Одним з видів захисту є організація технічного захисту інформації, для цього створюються комплекси ТЗІ, які можуть захистити інформацію від несанкціонованого доступу технічними каналами витоку інформації.

В кваліфікаційній роботі було проаналізовано різні види технічних каналів витоку інформації, а саме: акустичні, електромагнітні, матеріально-речові, візуально-оптичні. Їх було детально досліджено для з’ясування, що це саме за канали так, як саме здійснюється витік інформації в кожному виді.

Також в ході роботи було досліджено керівні документи відносно створення комплексу технічного захисту та вимоги відносно режимних приміщень в яких обробляється ІзОД. Розглянуто, які саме засоби виокристовуються в комплексах ТЗІ для протидії витоку інформації та наведено їх недоліки та переваги.

В результаті проведених досліджень, було наведено та досліджено засоби, якими можливо удосконалити комплекс технічного захисту інформації для максимізації захисту та зменшення ризику втрати інформації.

Комбінація розглянутих засобів захисту забезпечить більший рівень захисту від технічних каналів витоку інформаї, але все ще не гарантує абсолютного захисту, адже не можливо цілком повністю захиститись від усього. Тому враховуючи постійний розвитоку технологій і зростання загроз, важливо постійно оцінювати потенційні загрози та адаптувати заходи безпеки відповідно до змінюючогося оточення.

В результаті виконання кваліфікаційної роботи були виконані завдання, наведені в меті роботи:

- Провести дослідження технічних каналів витоку інформації на об’єктах інформаційної діяльності
- Проаналізувати вимоги керівних документів щодо створення комплексу технічного захисту інформації

- Провести аналіз технічних засобів, які використовуються в процесі створення комплексу технічного захисту
- Розробити рекомендації для удосконалення захисту інформації на об’єктах інформаційної діяльності

Всі поставлені задачі було виконано в повному обсязі. Мету роботи було досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію [Електронний ресурс] : Закон України від 01.01.2022 № 2657-XII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 01.01.2022 № 80/94-ВР. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#n99.

3. Про Положення про технічний захист інформації в Україні [Електронний ресурс]: Указ Президента від 11.04.2008 № 333/2008 (– Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text.

4. Технічні канали витоку інформації. Порядок створення комплексу технічного захисту інформації [Електронний ресурс]: Навчальний посібник - Режим доступу:https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

5. Електромагнітні канали витоку інформації [Електронний ресурс]. - Режим доступу:http://ni.biz.ua/8/8_4/8_40380_elektromagnitnie-kanali-utechki-informatsii.html

6. Технічні канали витоку інформації [Електронний ресурс]. - Режим доступу до ресурсу: https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html

7. Візуально-оптичні канали витоку інформації [Електронний ресурс]. - Режим доступу: http://ni.biz.ua/9/9_8/9_84215_vizualno-opticheskie-kanali-utechki-

8. Матеріально-речові канали витоку інформації [Електронний ресурс]. - Режим доступу: https://ssbb.ua/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/materialno-veshestvennye-kanaly-utechki-informacii/

9. ДСТУ 3396.0-96 Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення [Електронний ресурс]: ДСТУ 3396.0-96. – Режим доступу: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf

10. Про затвердження Концепції технічного захисту інформації в Україні [Електронний ресурс]: ПОСТАНОВА від 8 жовтня 1997 р. № 1126 - Режим доступу:http://www.ukrbook.net/zakony/Sfera_inform/Pos_1126.pdf

11. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс]: - Режим доступу до ресурсу:http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi

12. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення [Електронний ресурс]: НД ТЗІ 2.1-001-2001.- Режим доступу до ресурсу: https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-2.1-001-2001.pdf.

13. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи [Електронний ресурс]: НД ТЗІ 3.1-001-07.- Режим доступу: https://tzi.com.ua/downloads/3.1-001-07.pdf

14. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 1.1-002-99 - Режим Доступу до ресурсу: https://tzi.ua/assets/files/НД%20ТЗИ%201.1-002-99.pdf.

15. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації [Електронний ресурс]: НД ТЗІ 3.3-001-07. .- Режим доступу: https://tzi.com.ua/downloads/3.3-001-07.pdf

16. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації [Електронний ресурс]: НД ТЗІ 1.1-005-07 – Режим доступу :https://usts.kiev.ua/wp-content/uploads/2020/07/nd-tzi-1.1-005-07.pdf

17. Про нормативні документи [Електронний ресурс]: Наказ №25 від 09.06.95. - Режим доступу:https://zakon.rada.gov.ua/rada/show/v0025267-95#Text

18. White Noise Generator [Електронний ресурс]. - Режим доступу: https://www.workplacetesting.com/definition/4627/white-noise-generator

19. Генератор шумових сигналів «МАРС-ТЗО-4-2» [Електронний ресурс]. - Режим доступу: http://www.mapc.com.ua/img/files/3GenN.pdf

20. Розроблення класифікації електромагнітних екранів будівель і приміщень [Електронний ресурс]: - Режим доступу:http://science.lp.edu.ua/sites/default/files/Papers/pohrebennyk_v.d._pihur_n.v.pdf

21. Для чого потрібен мережевий фільтр і де його розміщувати? [Електронний ресурс]: - Режим доступу: https://www.soselectronic.com/pl/articles/schurter/do-czego-potrzebny-jest-filtr-sieciowy-i-gdzie-nalezy-go-umiescic-2261

22. МЕТОДИ І ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА АБОНЕНТСЬКИХ ТЕЛЕФОННИХ ЛІНІЯХ [Електронний ресурс]. - Режим доступу: https://vlp.com.ua/files/12_4.pdf