МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____В.В. Козловський

«___»_____ 2022

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ
«БАКАЛАВР»

Тема: Система захисту інформації від витоку акустичними каналами

Виконавець: Я.Р. Францева

Науковий керівник: старший викладач Д.П. Чирва

Нормконтролер: д.т.н., професор М.О. Шутко

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітньо-кваліфікаційного рівня: «Бакалавр»

Напрям: 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____В.В. Козловський

«___»_____2022

ЗАВДАННЯ

на виконання дипломного проекту

Францевої Яни Романівни

1. Тема роботи: «Система захисту інформації від витоку акустичними каналами» затверджена наказом ректора від «06» травня 2022 №483/ст.

2. Термін виконання: з 16.05.2022р. по 19.06.2022р.

3. Вихідні дані: Система захисту інформації від витоку акустичними каналами

4. Зміст пояснювальної записки:

У 1 розділі було розглянуто основні відомості канали витоку інформації, їх види, та основне про захист інформації під підслуховування.

У 2 розділі були розглянуті засоби захисту інформації від витоку акустичними каналами.

У 3 розділі було розглянуто приміщення, де буде розроблятись система захисту від витоку акустичними каналами, а також основні канали витоку у цьому приміщенні.

У 4 розділі була розроблена система захисту інформації від витоку акустичними каналами.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Зміст	16.05.2022	Виконано
2.	Вступ	20.05.2022	Виконано
3.	1. Канали витоку інформації як одна з причин захисту об’єктів інформаційної діяльності	23.05.2022	Виконано
4.	2. Засоби захисту мовної інфомації від витоку акустичними каналами	27.05.2022	Виконано
5.	3. Опис приміщення	30.05.2022	Виконано
6.	4. Створення системи захисту інформації від витоку акустичними каналами	05.06.2022	Виконано
7.	Висновки	10.06.2022	Виконано
8.	Оформлення пояснювальної записки	15.06.2022	Виконано

6. Дата видачі завдання: «16» травня 2022 р.

Керівник дипломної роботи (проекту) _____ Чирва Д.П.

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Францева Я.Р.

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота складається із: вступу, чотирьох розділів, висновків та переліку використаних джерел. Обсяг роботи складає 74 сторінки. Список використаних джерел містить 44 джерела.

Метою роботи є побудова системи захисту інформації від витоку акустичними каналами.

В дипломній роботі розглянуто приміщення з обмеженим доступом, приведено його точний план, досліджено місця каналів витоку інформації та описано методи для закриття доступу до конфіденційної акустичної інформації яка циркулює на об’єкті.

В результаті розроблена система захисту інформації від витоку акустичними каналами.

ЗМІСТ

Скорочення

ОТЗС – Основні технічні засоби і системи

ДТЗС – Допоміжні технічні засоби і системи

ТЗІ – Технічний захист інформації

КЗ – Контрольована зона

ОІД – Об’єкт інформаційної діяльності

ІзОД – інформація з обмеженим доступом

ТКВІ – Технічний канал витоку інформації

ЗТР – Засоби технічної розвідки

ЗКТ – Засоби комп’ютерної техніки

ТЗВР – Технічні засоби ведення розвідки

ДЦВ ТЗІ – Державний центр випробувань засобів технічного захисту інформації

АЧХ – амплітудно-частотна характеристика

ОК – огороджувальні конструкції

ГКЛ – гіпсокартонні листи

ВСТУП

Через стрімкий розвиток суспільства, інформація є найціннішим ресурсом, який наразі є у людства. А людська мова є одним з фундаментальних способів обміну інформацією.

Кожен власник інформації намагається зберегти її в секреті, створюючи систему, яка запобігає несанкціонованому доступу зловмисників. Зловмисниками, у свою чергу, можуть бути особи чи організації, зацікавлені в несанкціонованому доступі до конфіденційної інформації, які намагалися або здійснили такий доступ.

Одним із джерел важливої інформації для організації є нарада, на якій подається матеріал про наявні результати та плани роботи. Наявність великої кількості покупців і великої кількості великих майданчиків створює проблеми для цих організацій зі збереженням комерційної таємниці.

Головне завдання інформаційної безпеки — виявити та вчасно виявити технічні канали, через які може витікати акустична інформація. Канал витоку акустичної (мовної) інформації вважається одним з найнебезпечніших, оскільки його легко реалізувати.

Таким чином, захист від прослуховування інформації включає методи та засоби блокування будь-якого каналу, через який протікає голосова інформація.

РОЗДІЛ 1. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ ЯК ОДНА З ПРИЧИН ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1. Витік інформації

Витік інформації – це розповсюдження даних, яке не піддається контролю, як наслідок виникає несанкціоноване отримання інформації зловмисником.[1, с. 17]

Витік інформації в загалом розглядають як неналежне розголошення конфіденційних даних поза границями організації або обмеженого середовища осіб, котрим ці повідомлення були довірені.

Витік інформації за своєю суттю постійно означає незаконне (секретне чи видиме, свідоме чи не передбачене) володіння прихованими даними, і як це було досягнуто не є важливим.

Відтік захищеної інформації може відбуватися в різних ситуаціях. Якщо зловмисник цікавиться такою інформацією і витрачає певні зусилля та ресурси на її отримання. А також якщо за певних умов він може розраховувати на привласнення інформації що цікавить його (з меншими зусиллями, що витрачаються на це, ніж на те, щоб витягти її самостійно).

Причинами, зазвичай, є недосконалість норм зберігання конфіденційної інформації, а ще порушення їх (зокрема недосконалість), і на додачу відхилення від приписань ставлення до супутніх документів, технічних засобів, зразків продукції та іншими матеріалами, що мають у собі конфіденційні дані.

До умов належать різні фактори і ситуації, які утворюються підприємствами (організаціями) у процесі рекламної, наукової, звітної, виробничої, видавничої, інформаційної та інших практик, що роблять умови для витоку інформації. Такі фактори та випадки мають змогу включати, скажімо:

– працівники компанії недостатньо розуміють правила захисту інформації, а також присутнє нерозуміння (або непорозуміння) потреби уважного дотримання правил;

– обробка конфіденційної інформації з використанням неперевірених технічних засобів;
– поганий контроль за додержанням норм захисту інформації організаційними, правовими й інженерно-технічними доповненнями;
– непостійність кадрів, у тому числі володільців секретними відомостями.

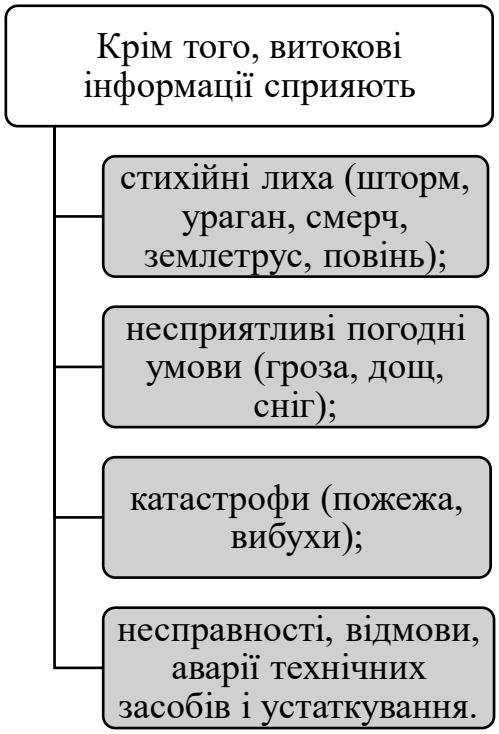

Рис. 1.1. Що сприяє витоку інформації

Видно, що більшість причин і умов, які утворюють передумови та можливості привласнення конфіденційної інформації випливає з недостатності компетенцій у керівників і працівників підприємств і організацій.

Які засади витоку інформації? Як ми всі знаємо, інформація зазвичай передається або переноситься за допомогою енергії або матерії. Але ні передана енергія, ні сама передана матерія не мають значення, вони лише слугують носієм інформації.

Виходячи з цього, ми можемо стверджувати що за фізичним походженням існуть такі шляхи передачі інформації:

– матеріали і речовини;
– світлові промені;

– електромагнітні хвилі;
– звукові хвилі.

Інших способів для переносу інформації в природі не існує.[2]

1.2. Канали передачі інформації: інформаційні характеристики, класифікація.

Основні інформаційні характеристики каналу передачі включають:

– тип каналу (телеграфний, телефонний, телевізійний тощо);
– місця розміщення початку і кінця каналу;
– пропускаюча здатність каналу;
– структура каналу передачі (кодери, декодери, модулятори, демодулятори, датчики, лінії, блокувальні пристрої тощо);
– швидкість передачі та кількість переданої інформації;
– прийоми трансформації даних у вузлах каналу передачі (засоби кодування, модуляції і т.д.);
– ємність каналу;
– форма інформації (безперервна чи дискретна), що передається у ланці каналів.

Крім того, канали передачі можна класифікувати за такими пунктами: [2]

по виду сигналів і засобові передачі:	по виконанню:	за принципом дії:
• телефонні, • телеграфні, • передача даних, • телеметричні, • радіосигнали, • телевізійні, • спеціальні;	• провідні, • кабельні, • світловодні, • радіо та ін.;	• електромагнітні, • оптичні, • акустичні

Рис. 1.2. Класифікація каналів передачі

1.3. Канали витоку інформації

Канали витоку інформації – способи і засоби витоку даних з інформаційних систем; паразитарна (небажана) низка інформаційних носіїв, один або кілька з яких є

(можливо) порушником правил або їх спеціальним обладнанням. Як фактор інформаційної безпеки вони виконують ключове призначення у захисті інформації.

Усі канали витоку відомостей поділяють на такі види як непрямі та прямі. Непрямі канали не зобов'язують мати прямої наявності технічних засобів інформаційних систем. Для прямих необхідно мати доступ до апаратних засобів та змісту інформаційної системи.

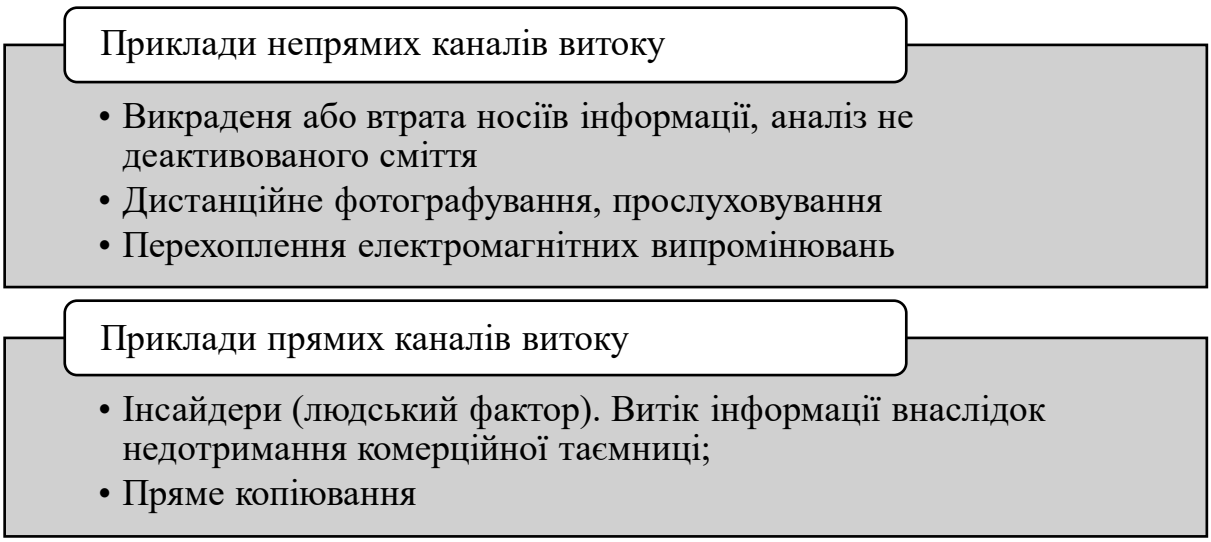

Рис. 1.3. Прямі та непрямі канали витоку

Канали витоку інформації теж розділяють за фізичними характеристиками і принципами роботи:

- акустичні — записування звуку, підслуховування і прослуховування;
- електромагнітні — копіювання полів шляхом усунення індуктивних наводок;
- акустоелектричні — інформація приймається шляхом звукових хвиль, а потім передаються шляхом мережі живлення;
- електричні сигнали чи радіовипромінювання від запроваджених у технічних засобах і приміщеннях професійних електронних приладів запису мовленнєвої інформації «закладних пристроїв», які модулюються інформативними сигналами;

- віброакустичні — це такі сигнали, що утворюються за рахунок конверсії акустичного сигналу, що містить інформацію, при дії його на структури будівель і інженерно-технічні споруди об’єктів, які потрібно захистити;
- матеріальні — інформація, яка знаходиться на паперових або будь-яких інших фізичних носіях;
- оптичні — візуальні шляхи, спостереження, фотографування, відеозйомка.[3]

Особливий інтерес привертають короткі характеристики перших двох категорій, оскільки вони є найчастіше порушуваними об’єктами злочинності у сфері інформаційної злочинності.[2]

1.3.1. Технічні канали витоку

Відповідними каналами витоку відбувається витік інформації.

Через те, що розвідувальні способи порушника зазвичай технічні, тому й канали витоку теж кличуть технічними.

Технічний канал витоку інформації (ТКВІ) - комплекс початкової точки секретного сигналу, середовища, де він поширюється, а також засобів технічного розвідування (рис. 1.4.).

До того потрібно враховувати завади, що діють на вході засобу технічної розвідки.

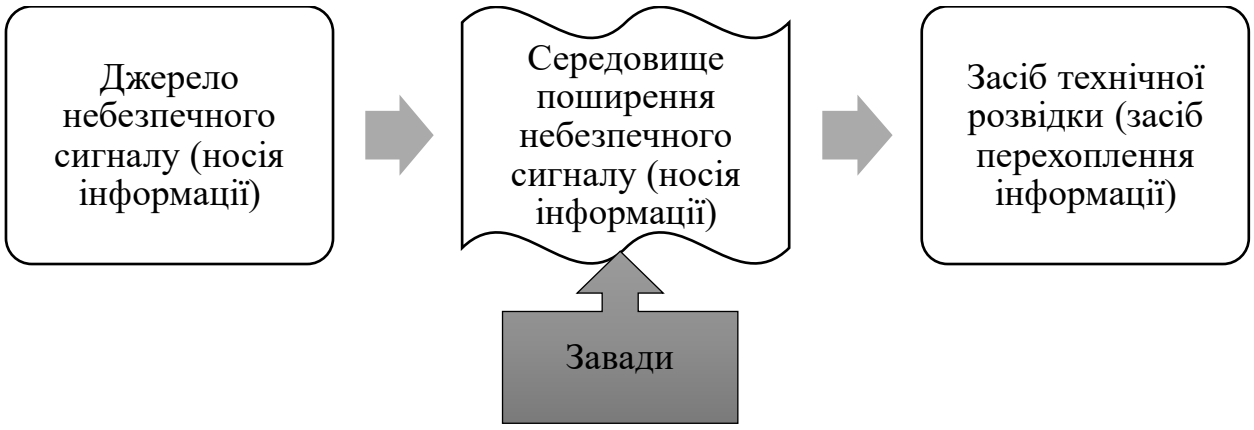

Рис. 1.4. Технічний канал витоку інформації

Інакше кажучи, ТКВІ – матеріальний маршрут небезпечного сигналу (даних що знаходяться на носії) від точки початку небезпечного сигналу до злодія.

Небезпечний сигнал - сигнал, у тому числі сторонній, чи будь-який його компонент (фрагмент) усілякого речового походження, що містить інформацію, доступ до якої обмежений і може бути знятий (перехоплений) технічними розвідками.

Носій інформації - небезпечний сигнал або хімічна речовина, що містить дані з лімітованим доступом.

Носіями інформації можуть бути:

- електричний струм;
- електромагнітне поле;
- світло (електромагнітне поле в світловому діапазоні частот);
- лазерний промінь (електромагнітне поле в оптоелектронному діапазоні частот);
- акустичне поле;
- вібраційне поле;
- хімічні матеріали, речовини тощо;
- інші носії.

Середовище поширення небезпечного сигналу (носія інформації) - матеріальні середовища, такі як повітря, вода, тощо; хімічні речовини; пружні і струмопровідні матеріали, (лінії заземлення, електроживлення, управління, зв'язку, сигналізації, моніторингу та інше; кінцеве та сполучне обладнання; інженерні комунікації, споруди, огороджувальні будівельні конструкції, світлопроникні частини будівель і споруд, ґрунт, поверхня землі та інше), якими має змогу поширюватися небезпечний сигнал (носій інформації).

Засоби технічної розвідки (ЗТР) - технічні прийоми, призначені для зйому (здобування, перехоплення) інформації без авторизації.[1]

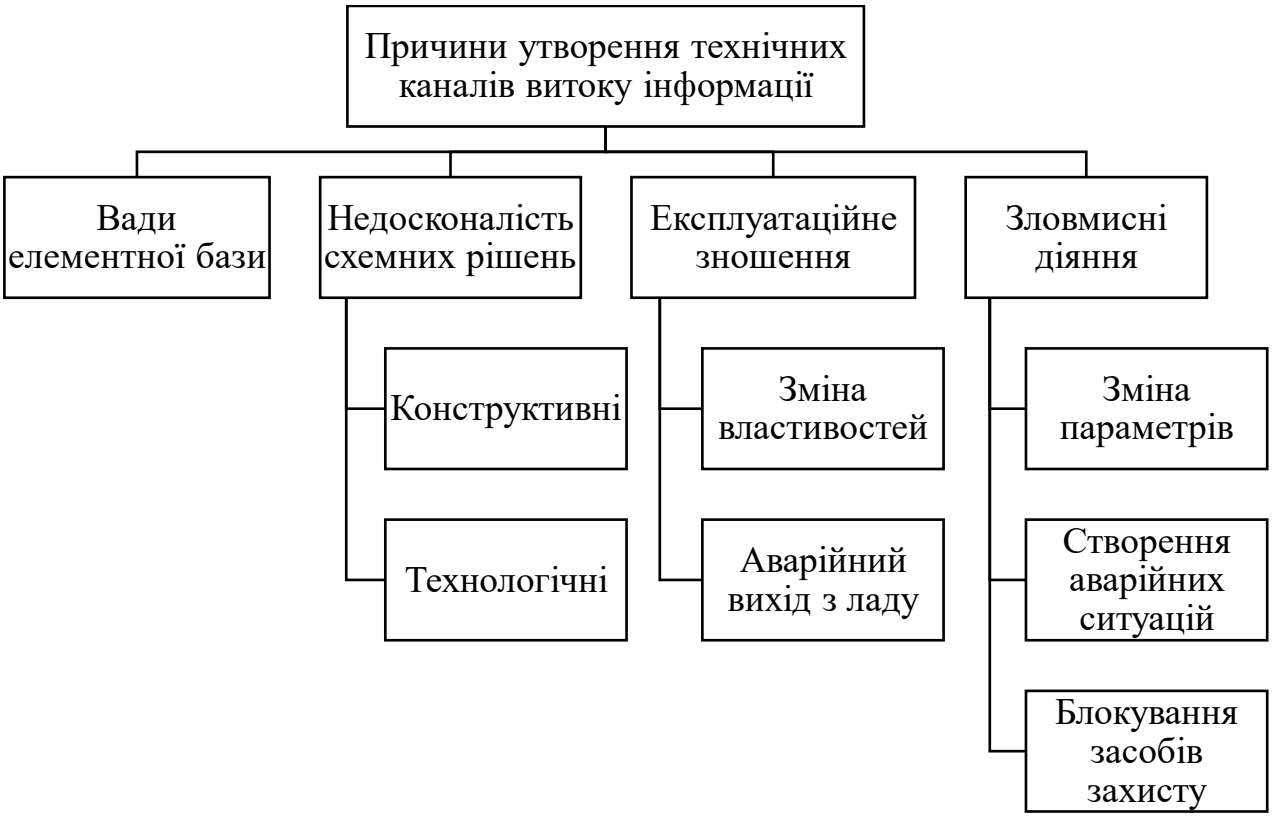

Рис. 1.5. Причини утворення ТКВІ

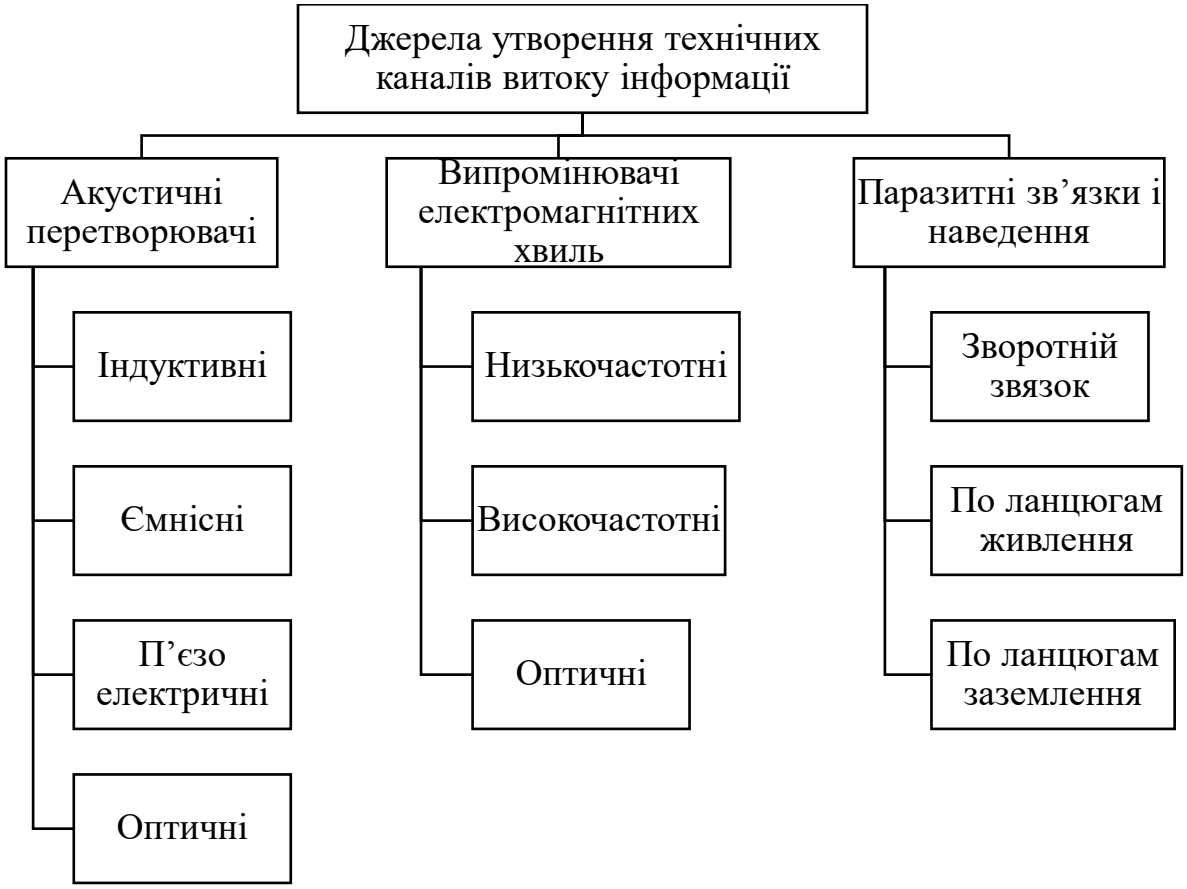

Рис. 1.6. Джерела утворення ТКВІ [4]

1.3.2. Класифікація технічних каналів витоку інформації

Класифікація технічних каналів каналами здійснена за певними ознаками для визначення вимог та організації захисту інформації. Типи ТКВІ виокремлюють за такими ознаками:

- за типом інформаційної діяльності на ОІД,

- за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації),

- за середовищем поширення небезпечного сигналу,

- за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

На ОІД виділяються такі типи ТКВІ за типами інформаційної діяльності:

1) технічні канали витоку мовної інформації,

2) ТКВІ, що обробляється в ОТЗС,

3) технічні канали витоку візуальної інформації,

4) матеріально-речовинні канали витоку інформації.

Розглянемо систематизацію ТКВІ за засадами формування небезпечного сигналу, колом поширення небезпечного сигналу та способами перехоплення (зняття) небезпечного сигналу засобами технічної розвідки зловмисника.[1]

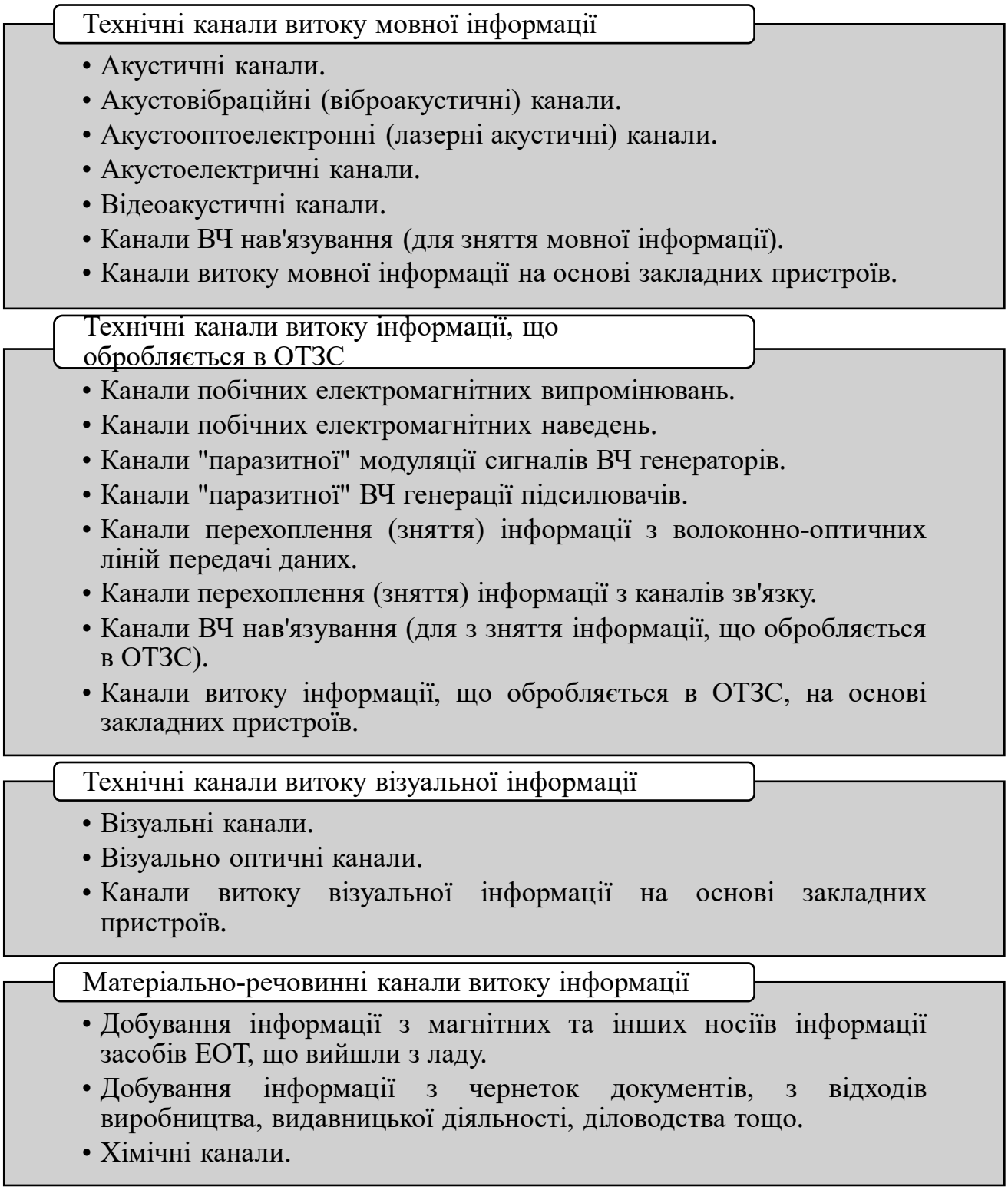

Рис. 1.7. Види ТКВІ

Також можна виділити способи витоку аудіо- та відеоінформації, які традиційно використовують порушники:

- Підключення до електронного обладнання контактно або безконтактно. Вмонтування мікрофонів, відео- і радіозакладок в меблі, предмети, стіни.

- Використання лазерних пристроїв для викрадення акустичної інформації з відображаючих поверхонь.
- Дистанційне знімання відеоінформації за допомогою оптичних приладів.
- Застосування вузькоспрямованих диктофонів та мікрофонів.
- Знімання інформації що витікає по заземлювальних ланцюгах, мереж гучномовного зв'язку, систем пожежної та охоронної сигналізації, мереж електропостачання і ліній зв’язку.
- Використання високочастотних каналів інформаційного витоку різної побутової техніки.
- Погано звукоізольовані перекриття і стіни також є об’єктом для знімання інформації.
- Проводження противником дослідів з промисловими і технологічними відходами.
- Витік інформації через телефонні і факсимільні апарати.
- Витік даних через створення віброканалів через мережі опалення газо- і водопостачання.
- Не компетентний персонал, через який стається витік інформації.

Не так давно зловмисники почали використовувати канали витоку інформації з ЗКТ та технічні пристрої знімання цієї інформації.
Для отримання інформації з вищезгаданих традиційних каналів витоку використовуються спеціалізовані ТЗВР, які в основному поділяються на такі категорії:

- мікрофони та радіомікрофони;
- пристрої для перехоплення повідомлень з телефонів;
- оптичні системи;
- відеосистеми запису і спостереження;
- пристрої прийому, запису, контролю;
- системи визначення місцезнаходження об'єктів, що контролюються;

- системи контролю та впливу на комп'ютери і їх мережі.[5]

1.4. Акустичний канал витоку

Рис. 1.8. Передумови появи акустичних каналів витоку

Канал витоку акустичної інформації реалізується в наступному:

- підслуховування мови на вулиці та в приміщенні, будучи поблизу чи за допомогою спрямованих мікрофонів (наприклад параболічних, трубчастих чи плоских). Спрямованість досягає 2-5 градусів. У найпоширеніших трубчастих мікрофонів середня дальність дії - близько 100 метрів. За комфортних погодних умов на вулиці спрямований параболічний мікрофон працює на відстані до 0,9-1 км;
- таємне записування розмов на магнітофони чи диктофони (в т.ч. цифрові диктофони, що активізуються голосом);
- підслуховування діалогів з застосуванням переносних мікрофонів (без наявних ретрансляторів дальність дії 50-200 метрів).[7]

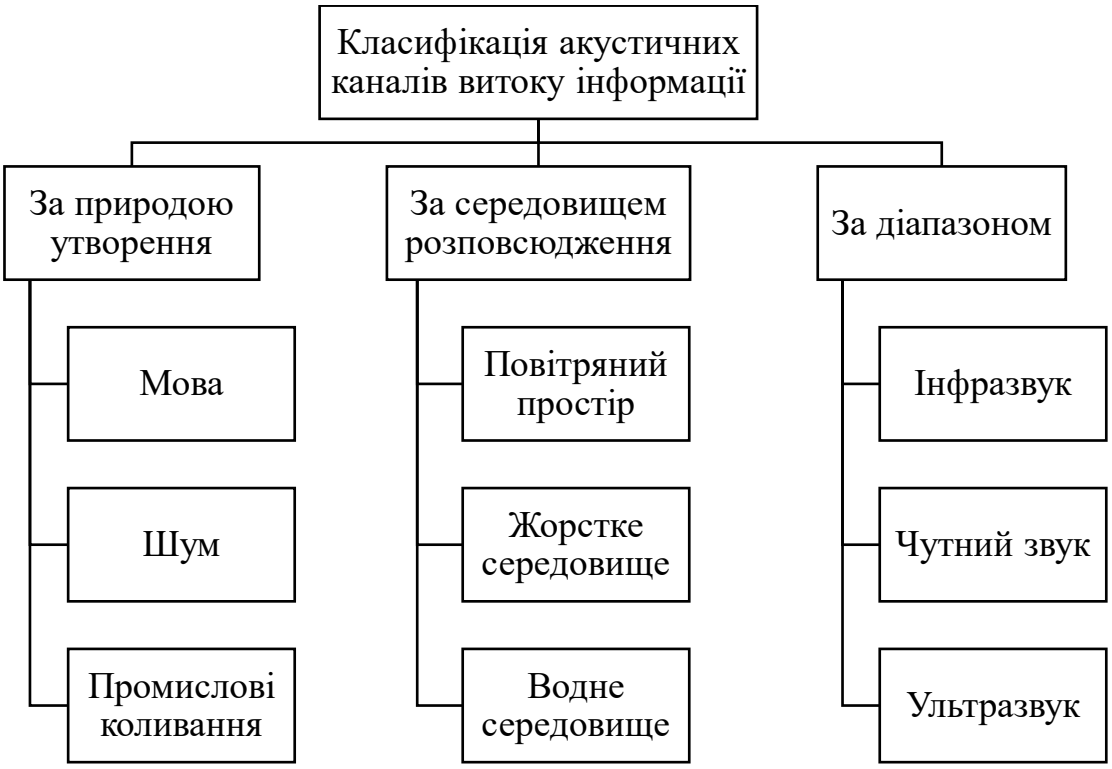

Рис. 1.9. Класифікація акустичних каналів витоку інформації

Як вже було зазначено раніше, канали витоку акустичної інформації формуються через викрадення мовленнєвих сигналів (полів акустики) з ОІД. Перехоплення може здійснюватись беззаходовими (без фізичного проникнення зловмисника на об’єкт) способами чи заходовими (фізичне проникнення).

Засоби, що встановлюються заходовими методами:
• радіозакладки; • закладки з передачею акустичної інформації в інфрачервоному діапазоні; • закладки з передачею інформації за допомогою мережі 220 В; • закладки з передачею акустичної інформації за допомогою телефонної лінії; • диктофони; • провідні мікрофони; • «телефонне вухо».

Засоби, що встановлюються беззаходовими методами:
• апаратура, що використовує мікрофонний ефект; • високочастотне нав’язування; • стетоскопи; • лазерні стетоскопи; • спрямовані мікрофони.[6]

Кожен з цих способів визначає використання специфічних технічних приладів. Щоб створити рекомендації щодо побудови ефективної системи захисту, подивимось чому з‘являються такі канали витоку інформації.

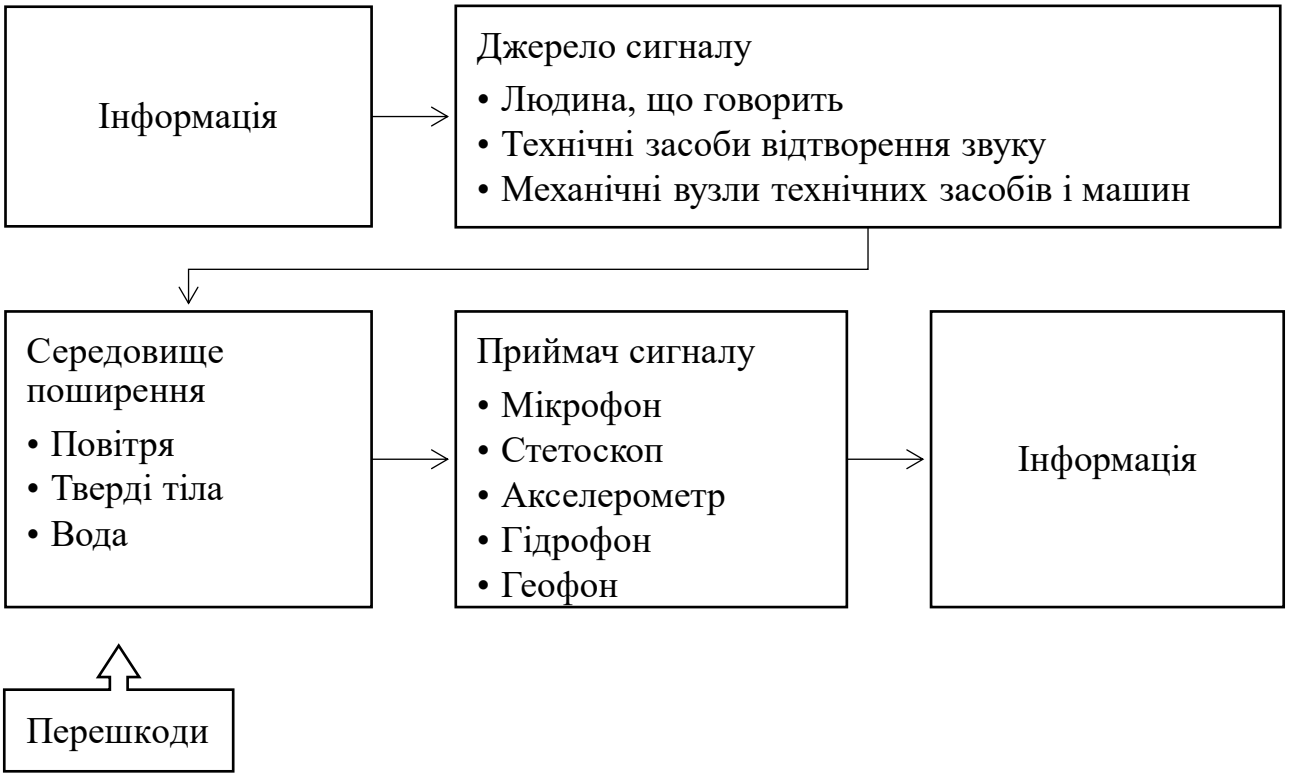

Рис. 1.10. Структура каналу витоку інформації

Канал витоку акустичної інформації має структуру, що проілюстрована на рис. 1.10. [8]

Витік інформації акустичним каналом за межі перегородок можливий через три шляхи:

- через дію «мембранного ефекту», що зумовлений коливаннями тонких (відносно довжини) і, зазвичай відносно легких, елементів ОК (пластикових, фанерних, гіпсокартонних, перегородок, скла з вікон тощо), здатних вигинатись під впливом звуку;
- прямим розповсюдженням акустичних коливань через отвори, щілини, тріщини та інші акустичні отвори;
- внаслідок перетворення акустичних коливань в віброакустичні, а потім знов в акустичні. Як це відбувається? Частина енергії акустичних коливань відбивається,

а частина падає на поверхню перегородки, внаслідок чого перетворюється у віброакустичну енергію, тобто в коливання твердих частинок матеріалу. Далі частина енергії віброакустичних коливань знову відбивається, а частина перетворюється на акустичну енергію і виділяється у вигляді акустичних коливань.

Захоплення акустичної інформації реально і без застосування прийомів технічної розвідки при непередбаченому прослуховуванні (без навмисних дій, спрямованих на отримання цих відомостей), а також з використанням приладів технічної розвідки.

Перехоплені голосові повідомлення можуть бути записані на портативний магнітофон (магнітофон) або передані по радіоканалах, мережах електропостачання, оптичних каналах, що з'єднують лінії, сторонніх провідниках, комунальних мережах тощо.

Також варто зазначити, що інформація, яку перехоплюють, може бути записана на портативні звукозаписуючі пристрої (диктофон) та/або можуть передаватися по радіоканалах, стороннім провідникам, оптичних каналах з'єднувальних ліній, інженерним комунікаціям, мережах електропостачання і таке інше.[9]

1.5. Захист інформації від підслуховування

1.5.1. Інформаційне закриття акустичних сигналів та мовної інформації: способи

Інформаційне закриття акустичних сигналів та мовної інформації передбачає:

- технічне закриття та шифрування семантичної мовної інформації у функціональних каналах зв'язку;

- дезінформування.

Інформаційне приховування мовленнєвої інформації забезпечується технічним закриттям (аналоговим скремблюванням) та шифруванням сигналів мовленнєвої інформації, що передаються по кабелях та радіоканалах.[10]

1.5.2. Сутність способів технічного закриття

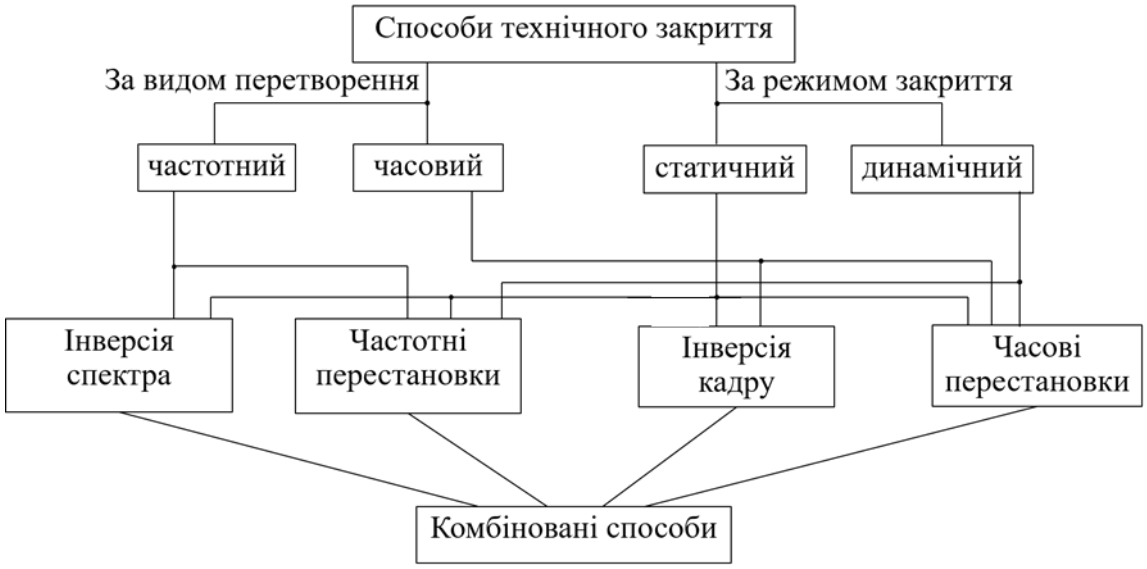

Рис. 1.11. Класифікація способів технічного закриття [10]

Закривання мовленнєвого сигналу у вузькосмуговому телефонному каналі реалізується способами **технічного** чи **аналогового закриття**. По назві технічних способів, що постачають технічне закриття, такі види дії називають ще скремблюванням (перемішування).

При технічному закритті реалізується у такий спосіб: змінюються ознаки (характеристики) вихідного мовного сигналу в таким чином, що він схожий шум, але знаходиться у тій ж частотній смузі. Це дає можливість без проблем передавати його по тих же каналах зв’язку, що і звичайну мову.

Перевага методів технічного закриття - простота (по відношенню до шифрування) технічної реалізації скремблеров і, як наслідок, менша їх вартість і малі габарити, а також можливість експлуатації скремблеров практично на будь-яких каналах зв'язку, призначених для передачі мовних повідомлень.	Недолік методів технічного закриття - низька стійкість закриття інформації. Скремблери спотворюють відновлений мовний сигнал, за винятком найпростішого (з частотної інверсії). Їх поява викликана тим, що при зворотному перетворенні сигналу у одержувача, спотворюються межі частотних смуг і тимчасових сегментів, що призводить до деякого спотворення спектра відновленого мовного сигналу. Групова затримка компонента мовного сигналу також має несприятливий вплив. Спотворення, внесені технікою, призводить до (3-5)% зменшення надмірності мовного сигналу.

Незважаючи на недоліки, методи часового і частотного скремблювання, та їх різноманітні комбінації дозволяють забезпечити захист інформації на тактичному і на наближення до стратегічного рівнях захисту. [11]

1.5.3. Типи і параметри скремблерів.

Залежно від того, як перетворюється сигнал розрізняють частотні та часові методи технічного закриття, а, від того який режим закриття - статичні та динамічні.

Частотні методи скремблювання, що реалізуються на аналогових елементах, з'явилися раніше ніж часові методи, які виконуються набагато простіше на дискретних елементах. У скремблері, який виконує інверсію спектра і називається маскіратором, спектр мовного сигналу здійснює поворот навколо деякої центральної частоти f_0. (Рис. 1.12)[11]

В такому випадку здобувається ефект трансформації низьких частот у вищі та інакше. Цей спосіб забезпечує невисокий рівень закриття, так як при перехопленні досить легко визначається значення частоти f_0 інверсії спектра мовного сигналу.

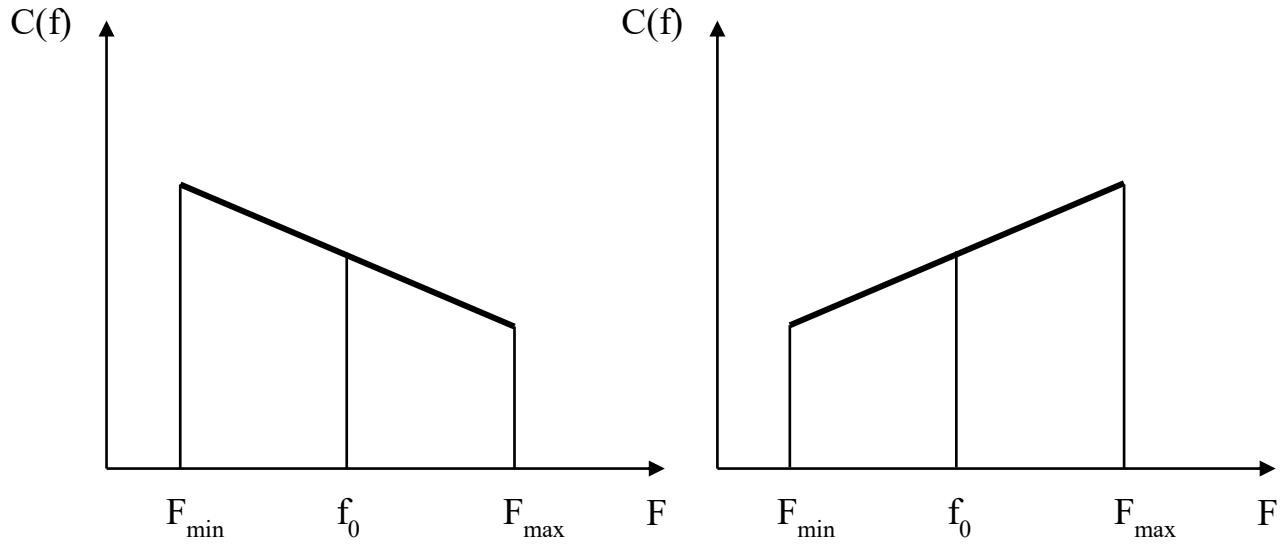

Рис. 1.12. Принципи інверсії частотного спектра мовного сигналу [12]

У скремблері, що виконує частотні перестановки (рис. 1.13), спектр вихідного мовного сигналу розбивається на кілька частотних смуг рівної або нерівної ширини. У у теперішніх екземплярах кількість смуг може бути 10 – 15. Зміна ключа в ході сеансу зв'язку в скремблері з динамічним закриттям дозволяє підвищити ступінь закриття, але вимагає передачі сигналу синхронізації на приймаючу сторону, що відповідає моментам зміни ключа.

Інші види перетворення носіїв мовної інформації реалізують часові методи технічного закриття з вищим рівнем захисту. Інверсія кадру забезпечується попереднім запам'ятовуванням передавального скремблера інтервалу мовного повідомлення (також називають кадром) тривалістю $T_к$ і зчитування його (з передачею в телефонну лінію) з кінця кадру – інверсно. При прийомі кадр повідомлення зберігається і зчитується з пам'яті у зворотному порядку, відновлюючи вихідне повідомлення.

У процесі технічного закриття з часовою перестановкою (Рис. 1.14) кадр мовного повідомлення розбивається на сегменти, де кожен тривалістю τ_c. Порядок передачі в лінію сегментів визначається (правилом) ключем, який має бути відомий одержувачу.[11]

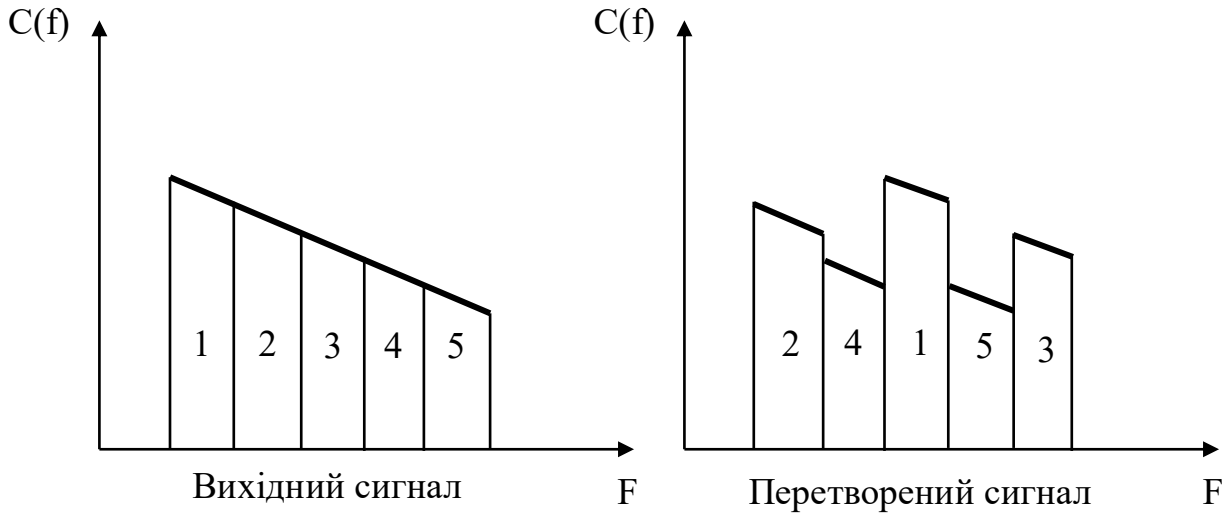

Рис. 1.13. Принципи частотної перестановки

Щоб досягти незрозумілості мови, тривалість кадру повинна бути не менше 250 мс. У цьому випадку загальна тривалість пам’яті та зворотної передачі кадру становить близько 500 мс, що може створити помітну затримку телефонного сигналу.

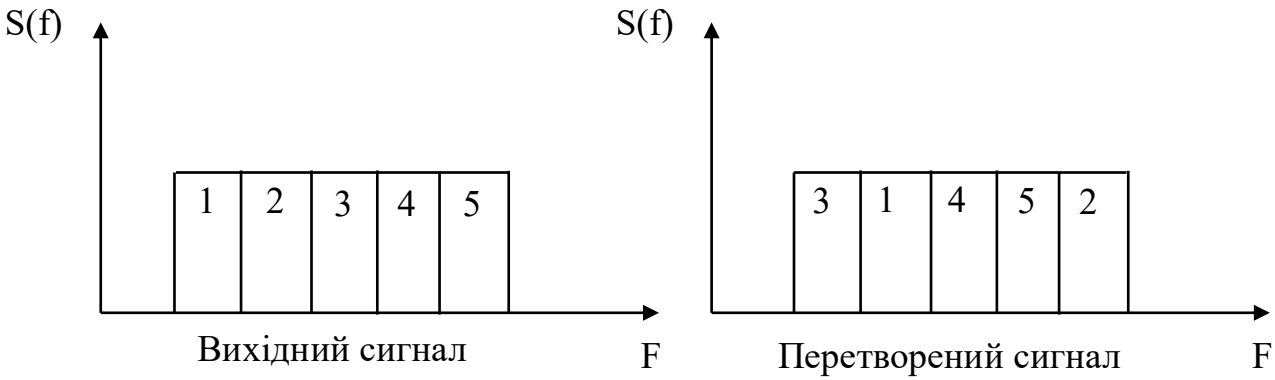

Рис. 1.14. Принципи часової перестановки

Через накопичення інформації в блоці тимчасового перетворення виникає затримка між надходженням вихідного мовного сигналу передавач і відновленням його в приймачі. Якщо затримка перевищує 1-2 с, може неприємно сприймається на слух. Тому Т до вибирають рівною (4-16) t_c.[12]

Найвищий рівень стабільності за аналогового кодування досягається шляхом об’єднання часового та частотного скремблювання. При цьому вони доповнюють один одного: часові перестановки плутають сенс повідомлення, а частотні перетворення змішують дзвінкі звуки. Кількість частотних смуг зазвичай береться не більше 5 ... 6. [13, с. 4]

У комбінованому (частотно-часовому) скремблері вихідне повідомлення поділяється на кадри та сегменти, що зберігаються у пам'яті скремблера. При формуванні повідомлення, що передається, проводяться часові перестановки сегментів кадру і перестановки смуг спектра мовного сигналу кожного сегмента. Якщо ще додати динамічну зміну ключа у часовій і частотній перестановці, то рівень захищеності такого закриття може не поступатися цифровому шифруванню. Однак складність реалізації цього методу і вимога до якості передачі синхроімпульсів між скремблерами телефонних користувачів також дуже високі. [12]

У простих скремблерах, які застосовують тільки від знімання розмови дилетантами, використовують виключно частотні перестановки і інверсії, тому кількість каналів не перевищує 4, а інтервали комутації - постійна величина.

Скремблери середнього рівня, гарантують стійкість протягом декількох годин, і в таких приладах використовують частотно-часові перестановки з кількістю частотних каналів від 5 до 10.

У складних скремблерах, які забезпечують стійкість протягом декількох днів, інтервали комутації повинні бути змінними, використовуватися частотно-часові перестановки з великою (більше 10) кількістю частотних каналів і переставляються часовими інтервалами. Кількість можливих ключових комбінацій має бути не менше 1015.

Також варто звернути увагу на те, який тип зв’язку підтримує скремблер:

- симплексний (передача інформації тільки в одному напрямку);
- напівдуплексний (почерговий обмін інформацією між двома абонентами);
- двобічний (одночасний двосторонній обмін).

В поєднанні з «людським фактором» цей файт іноді може мати значний вплив на захист інформації.

Практика показала, що для ділових розмов потрібно використовувати ті скремблери, що працюють в дуплексному режимі з максимально спрощеною системою управління (в кращому випадку перемикання повинно бути натисненням однієї кнопки).[13, с. 6]

1.5.4. Способи, засоби і методи енергетичного приховання акустичних сигналів. Звукоізоляція та звукопоглинання.

Рис. 1.15. Способи енергетичного приховання

Енергетичне приховання акустичних мовленнєвих сигналів є методом захисту від підслуховування і включає звукоізоляцію акустичних сигналів за рахунок поглинання акустичної хвилі в звуко поглинаючих матеріалах (пасивні засоби) і зашумлення в певних зонах приміщення і твердих середовищах поширення мови спеціальними шумами, перешкодами, а також прилади, що забезпечують маскування мови (активні засоби.)

Енергетичне приховування акустичних сигналів відтворюється шляхом використання засобів, що примножують енергію перешкод чи зменшують енергію носія.

При використанні першого способу використовується звукоізоляція, звукопоглинання і заглушення звуку. Другий спосіб завбачає використання активного пристрою – генератора акустичної перешкоди.

Метою звукоізоляції є локалізація джерела акустичного сигналу в закритому просторі в межах контрольованої зони. Головна вимога до нього - поза цієї зони

відношення сигнал/шум не повинно перевищувати максимально допустимого значення, що виключає вилучення інформації. [14]

Рівень гучності мовлення за межами ОК (контрольованої зони) зменшують за рахунок поліпшення звукоізоляції приміщення, що захищається: звуковідображення від внутрішніх стін і звукопоглинання конструкціями, що захищають. Тільки поєднання цих двох різних за своєю природою взаємодій матеріалів зі звуком створює надійну перешкоду для звуку (шуму).

Звукопоглинання досягається шляхом трансформації кінетичної енергії акустичних хвиль в звукопоглинальних матеріалів в теплову енергію. Коефіцієнтом звукопоглинання оцінюються звукопоглинальні властивості матеріалів. Цей коефіцієнт визначається ставленням енергії, що поглинається в матеріалі до звукової енергії, що падає на поверхню матеріалу.

До погіршення сигналу в різних кутках приміщення може призводити надмірне звукопоглинання, а до погіршення розбірливості через накладення різних звуків – великий час реверберації.[15]

Матеріали за конструктивними характеристиками поділяють на пухкі акустичні, плитні, звукопоглинальні штукатурки та резонансні поглинальні матеріали у вигляді щитів і панелей з дерева та іншого.

Методи звукопоглинання в приміщеннях, які застосовують для акустичної обробки, поділяють на:

- звукопоглинаючі облицювання у вигляді акустичних плит дрібної зернистої або осередкової структури (плити мінераловатні «Акмігран», «Акмант», «Сілакпор», «Вініпор», ПА/С, ПА/О, ПП-80, ППМ, ПММ);

- поглинання звуку обкладеннями з шару пористого і волокнистого матеріалу (мінеральної вати, базальтового чи скляного волокна,) в захисній оболонці із плівки з перфорованим покриттям типа гіпсу, металу та інше, або тканини. У якості захисних обшивок підбирають: тканини типу ЕЗ-100, А-1, ТСД, лап, ЛАК, листи сталеві

перфоровані, плівки типу ПЕТФ, азбоцементні перфоровані листи, листи гіпсові типу АП1, АГШБ і ін, алюмінієві перфоровані панелі типу ПА.

Глушення звуку робиться шляхом інтенсивного поглинання енергії акустичних хвиль при поширенні у спеціальних конструкціях, які мають назву глушник. За різними методами глушення звуку глушники поділяються на реактивні, абсорбційні та комбіновані. В абсорбційних глушниках відбувається звукопоглинання у конструкціях та матеріалах, у реактивних – за рахунок відбиття звуку назад до джерела. Комбіновані глушники об'єднують обидва ці способи. [16]

Якщо акустичний генератор знаходиться ближче до акустичного приймача противника, ніж джерело звукової інформації, то акустичне зашумлення кімнати створює ефективний захист інформації. Наприклад, акустичний генератор добре буде розташувати біля дверей або на підвіконні вікна, коли підслуховування можна здійснити через відкрите вікно або двері.[17]

Вібраційне зашумлення є корисним та активним узагальненим засобом захисту інформації. Оскільки рівень структурного шуму, створюваного генератором, вище за рівень мовного сигналу в твердих тілах, але нижче за рівень чутності, то вібраційне зашумлення слід використовувати у всіх ситуаціях, де присутня ймовірність витоку за допомогою структурного звуку. Шум у звуковому діапазоні в твердих тілах створюють п'єзокерамічні вібратори акустичного генератора, що прикріплюються (приклеюються) до поверхні огорожі (вікна, стелі, стіни тощо) або твердого звукопроводу (труби)

1.5.5. Звукоізоляція огороджень, кабін, акустичних екранів, вікон та дверей.

До звукоізолюючих матеріалів відносяться щільні, масивні матеріали: бетон, гіпсокартон, цегла. Також сюди можна додати плити ДДФ (дрібно-дисперсійна фракція - деревоволокнисті плити середньої щільності - (англ.) Medium Density Fibreboard) - панелі, виготовлені методом сухого пресування деревної стружки високим тиском. До звукоізолюючих огороджень відносять стіни, перегородки, перекриття, вікна, двері. [18]

Звукоізоляція забезпечується за допомогою архітектурних та інженерних конструкцій: огорож, екранів, кабін, кожухів, що зображено на рис. Вікна та двері є одним із найслабших звукоізоляційних елементів у закритій конструкції вибраного приміщення.

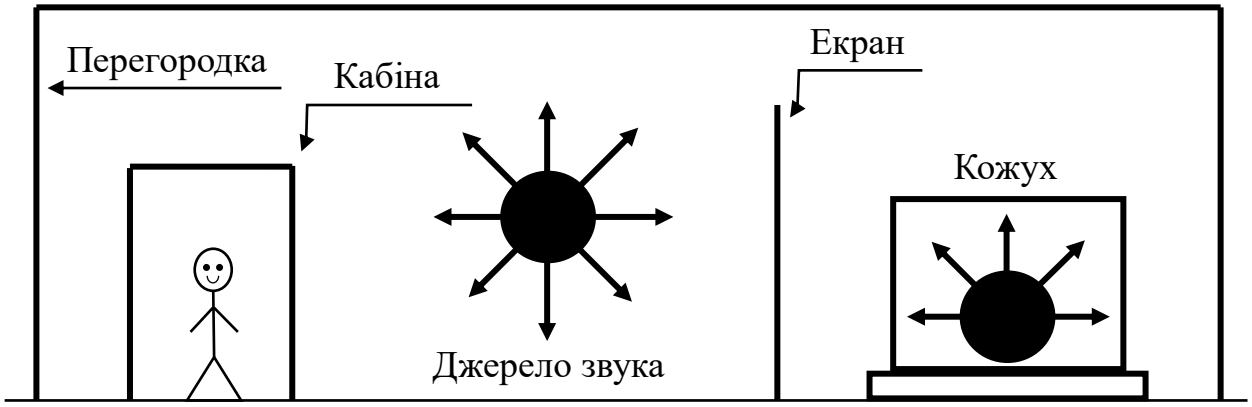

Рис. 1.16. Основні засоби звукоізоляції

Для збільшення звукоізоляційних дверей застосовуються ущільнюючі прокладки по периметру дверей. При використанні тамбурів внутрішня поверхня тамбуру облицьовується звукопоглинаючими покриттями.

Для звукоізоляції вікон застосовують роздільні перельоти, шириною повітряного проміжку понад 200 мм, або з потрійним склом.

Також застосовують склопакети з герметизацією повітряних проміжків, заповненням проміжків газами або створення вакуумів.

В будівлях застосовують акустичні екрани, які розміщують на маршрутах розповсюдження звуку для зниження небезпечного акустичного сигналу. Акустичні бар'єри ставлять між точкою найслабшого звукопоглинання ОК та розрахунковими точками, в яких мовленнєвий сигнал повинен бути незрозумілим. Акустичні екрани діють через відображення звукових хвиль.

Звукоізолюючі огородження будівель і приміщень - це перекриття, стіни, двері, перегородки, вікна, що створюють контакти з подібними огородженнями. Величина звукоізоляції одношарової перегородки описується складною нелінійною залежністю і від частоти коливання акустичних хвиль, таке від групи характеристик перегородок.

У загальному випадку цю залежність можна як наступної функції:

$$R = F(f_{ЗВ}, m, h/f_{or}, p, v),$$

де m - поверхнева маса (маса 1 м$_2$) огорожі; h - коефіцієнт втрат енергії у матеріалі; f_{or} - власна частота коливань огорожі; p - питома щільність матеріалу огорожі; v — швидкість звуку у матеріалі огорожі.

Звукоізоляція конструкції огорожі, що містить декілька елементів, необхідно щоб оцінювалась за звукоізоляцією елемента який втрачає свою здатність швидше. Такими елементами найчастіше бувають одношарові плоскі огорожі. Для підвищення величини ослаблення на плоску огорожу наносять шар звукопоглинального матеріалу, яке збільшує звукоізоляцію R за рахунок додаткового послаблення звуку в матеріалі звукопоглинального і підвищення загальної маси складового огородження.

Також для збільшення звукоізоляції використовують багатошарові огорожі, як правило, подвійні. Вони будуються з двох поверхонь з одного шару, розділених у найпримітивнішому випадку шаром повітря. Між поверхнями, з'єднаними ребрами жорсткості, розташовують різні звукопоглинальні матеріали. [16]

1.5.6. Типи та способи застосування генераторів акустичного та вібраційного зашумлення.

Акустичні генератори шуму використовуються для зашумлення акустичного діапазону в приміщеннях і в лініях зв'язку. Загалом шум розуміється як завада, що є сумішшю короткочасних і випадкових періодичних сигналів. Якщо розглядати вужче, то шум це так званий білий шум, що розкривається розподіленим за нормальним законом амплітудним спектр, а спектральна щільність потужності являється постійною для всіх частот.

Головними перевагами генераторів білого шуму є їх просте виконання і невелика вартість. Але недоліків більше. Найголовніший з них виходить з самого принципу дії приладу. Насправді, багато матеріалів і будівельних споруд мають різний акустичний опір на різноманітних частотах. Для надійного захисту необхідно встановлювати значну інтенсивність шумових завад, що може доставляти

незручності тим, хто веде переговори. Враховуючи ще те, що генератори білого шуму постійно виконують свою роботу, і зупиняються якщо їх вимкнути.[16]

Віброакустичне маскування застосовують для захисту мовленнєвих даних від знімання через віброакустичні та акустооптичні (оптико-електронні) канали і має на увазі створення вібраційних шумів в елементах будівель та в інженерних мережах. Віброакустичне маскування добре діє для пригнічення таких засобів викрадення інформації, таких як електронні та радіостетоскопи, а також лазерні акустичні системи розвідки.

Процес сприйняття акустичної інформації в шумі супроводжується втратою складових елементів повідомлення. Як покажчик оцінки ефективності систем віброакустичного маскування вживається словесна зрозумілість мови, що характеризується числом вірно розібраних слів і показує якісну область зрозумілості, яка виражається в категоріях подробицями довідки про вкрадене за сприянням технічних засобів розвідки діалогу. Стандарти ефективності захисту мовної інформації значною мірою залежать від цілей, що переслідують при влаштуванні захисту, наприклад: приховати зміст розмови, приховати тематику розмови, що ведеться і т.д.

При складовій розбірливості 25-40% розуміння мови з перепопитами, повтореннями й більшою напругою уваги. При складовій розбірливості менш 25% присутня нерозбірливість тексту протягом довгих інтервалів часу.

Враховуючи, що взаємозв'язок словесної й складової розбірливості, можна розрахувати очікування зриву зв'язок при словесній розбірливості менш 71%. Не є можливим скласти детальну довідку про зміст перехопленої розмови при розбірливості слів менше 60-70%, а маленької довідки-анотації - при розбірливості менше ніж 40-50%.

При словесній розбірливості менше чим 20-30% дуже важко встановити предмет розмови, а при словесній розбірливості менш 10% це практично неможливо і якщо використовувати сучасну техніку фільтрування завад.[19]

До складу типової системи віброакустичного маскування входять: генератор шуму, комплект вібровипромінювачів, комплект акустичних випромінювачів (звукових колонок), а також обладнання, необхідне регулювання та налаштування системи.

На практиці широке застосування знайшли аналогові, цифрові та комбіновані генератори шуму.

Велику групу генераторів аналогового шуму становлять пристрої, принцип дії яких заснований на посиленні коливань первинних джерел шумів, в якості останніх використовуються електровакуумні, газорозрядні, напівпровідникові та інші електронні прилади та елементи.

Ще використовується тимчасовий випадковий процес, подібний за своїми характеристиками до шумових коливань, який можна отримати і за допомогою цифрових генераторів шуму. Ті в свою чергу формують псевдовипадкові послідовності двійкових символів, що переходить у послідовності хаотичних імпульсів.

Акустичні та віброакустичні системи маскування, зазвича, користуються шумовими перешкодами таких типів:

1. "білий" шум (шум з постійною спектральною щільністю в мовному діапазоні частот);
2. "рожевий" шум (шум з тенденцією спаду спектральної щільності 3 дБ на октаву у бік високих частот);
3. шум із тенденцією спаду спектральної щільності 6 дБ на октаву у бік високих частот;
4. шумова "мовоподібна" перешкода (шум з огинаючою амплітудного спектра подібної до мовного сигналу).

Виділяють два види вібровипромінювачів: магнітодинамічні та п'єзоелектричні.

Магнітодинамічні вібровипромінювачі. По структурі вони схожі на звукові динаміки, але елементи, що коливаються, більш масивні (для підвищення ефективності передачі вібрації в конструкцію, до якої вони кріпляться). Втім, наявність механічно рухливих частин призводить до швидкого зношування таких випромінювачів.

П'єзокристалічні вібровипромінювачі. Вони складаються з металевого корпусу у формі циліндра із закріпленим усередині п'єзокристалом. При подачі напруги на кристал відбувається його стиснення. Таким чином, при подачі на кристал шумового сигналу він передає коливання корпусу датчика, а той, у свою чергу, через кріплення в конструкцію, до якої він кріпиться.

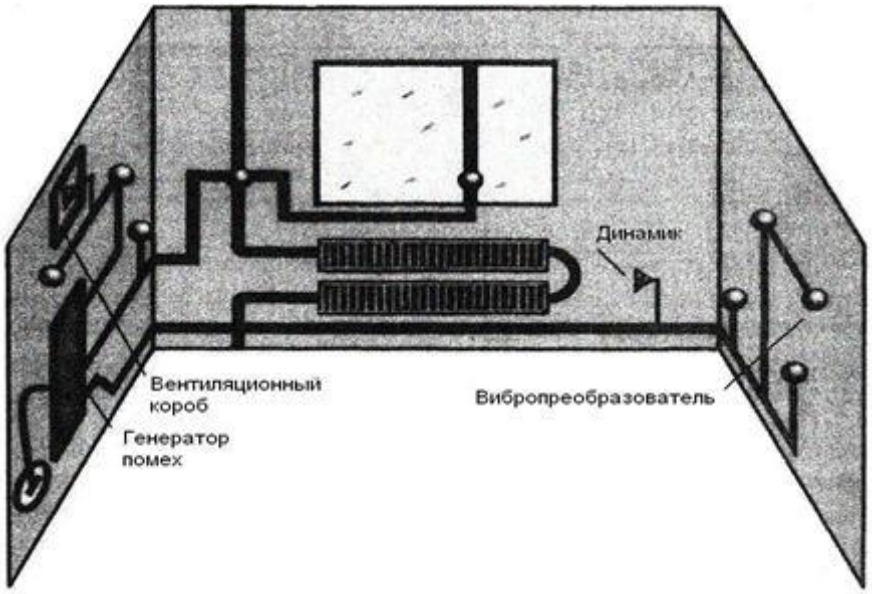

Рис. 1.17. Приклад схеми розміщення випромінювачів системи віброакустичного захисту

Найбільш ефективним активним засобом захисту є пристрої віброакустичного захисту. Дані пристрої дозволяють захиститись від прослуховування за допомогою дротових мікрофонів, радіомікрофонів, електронних стетоскопів тощо. Захисний принцип полягає у створенні віброакустичних шумових коливань у елементах конструкцій приміщень. Типова система віброакустичного захисту складається з генератора шуму та 6-25 вібраційних випромінювачів. Додатково до складу системи можуть включатись звукові колонки (спікери).

Працює все так. Генератор формує шум у діапазоні звукових частот. Коливання шуму передаються на частини конструкції за допомогою електромагнітних і п'єзоелектричних випромінювачів з елементами кріплення. Оскільки рівень шуму, створюваного генератором, вище за рівень мовного сигналу в твердих тілах, але нижче за рівень чутності, цей тип шуму краще вставляти у всіх ситуаціях, коли можливий витік структурного звуку.

З розгляду узагальненої схеми каналів витоку Загалом можна зробити цікаві висновки, які є першочерговими для покращення приладів формування акустичних та вібраційних завад, розглядаючи схеми каналів витоку:

- В комплект апаратури повинні входити випромінювачі як вібраційного, так і акустичного типів, розраховані на установку в типових умовах;

- Загальна кількість випромінювачів обох типів має бути достатнім для оптимального рішення деякої типової задачі захисту з урахуванням конструктивних елементів приміщення (трубопроводів, вікон, дверей, перекриттів і ін.);

- Перешкоджаючі сигнали в каналах випромінювання повинні бути незалежні для виключення можливості зниження захисних властивостей при використанні корельованості перешкод в системах негласного контролю інформації;

- Канали випромінювання повинні дозволяти регулювати рівні потужності випромінювання і спектри завадових сигналів роздільно по різних каналах випромінювання, що дозволяє мінімізувати енергетичні витрати;

- Апаратура повинна допускати установку та контроль за основним параметром захисту;

- Апаратура повинна дозволяти встановлювати рівень захищеності з урахуванням вимог на допустимий рівень залишкових акустичних шумів;

- Розробник повинен пропонувати комплекс заходів пасивного захисту, який можна застосувати до різних ситуацій з урахуванням особливостей розробленої апаратури. [17]

РОЗДІЛ 2. ЗАСОБИ ЗАХИСТУ МОВЛЕННЄВОЇ ІНФОМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМИ КАНАЛАМИ

2.1. Несанкціоноване зняття інформації

У закритих будівельних конструкціях і інженерних мережах в приміщенні, де знаходиться джерело звукового сигналу, під впливом акустичних коливань виникають вібрації.

Рис. 2.1. Вторинні джерела

Рис. 2.2. Методи перехоплення

Мовний сигнал у приміщенні існує у вигляді акустики та вібрації у своєму первісному вигляді. Різні акустичні та вібраційні перетворювачі є вторинними джерелами.

Щоб захистити акустичну інформацію від каналів витоку на інформаційні об’єкти з обмеженим доступом до інформаційного обігу створено комплекс технічного захисту інформації (абревіатура – КТЗІ або комплекс ТЗІ), який являє собою комплекс організаційних, інженерно-технічних заходів.

Акустична розвідка реалізується шляхом перехоплення шуму, що створюється об'єктом, і перехоплення голосової інформації. [20]

Класифікація пристроїв несанкціонованого зняття інформації наведена на рис. 2.3.

Розглянемо пасивні та активні засоби захисту мовної інформації.

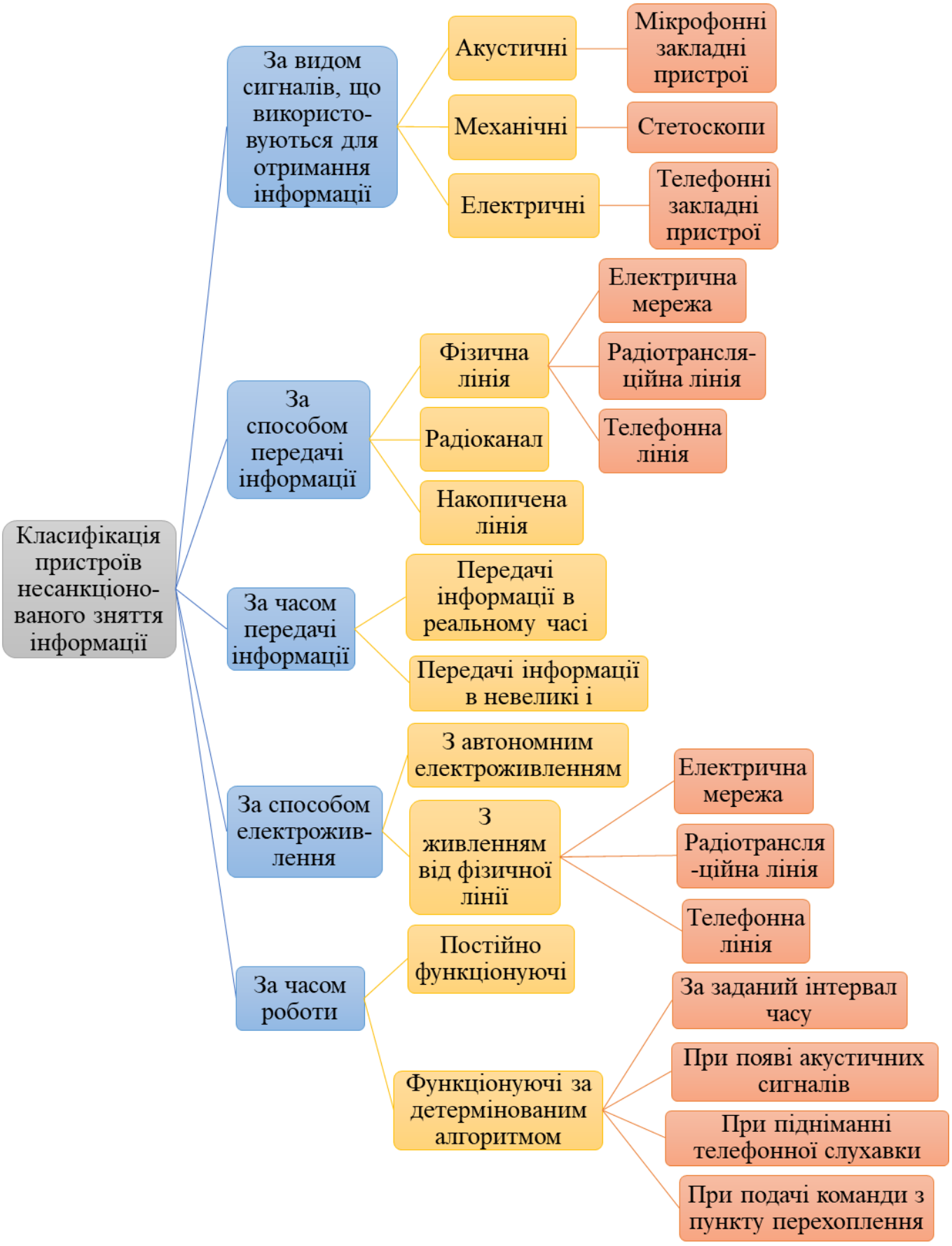

Рис. 2.3. Класифікація пристроїв несанкціонованого зняття інформації[6]

2.2. Пасивні засоби захисту

Пасивний захист інформації облаштовують для підвищення звукоізоляції огороджувальних конструкцій або ОК ОІД (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючих підлог», встановлення звукоізоляційних фільтрів у повітроводах тощо).[21]

Головні цілі пасивного методу захисту акустичної (мовної) інформації:

- применшити акустичний (мовний) сигнал на межі контрольованої зони до значення, яке гарантує, що його неможливо вирізнити за допомогою розвідувальних пристроїв на тлі природних шумів;
- ослаблення інформаційних електричних сигналів у з'єднувальних лініях, у тому числі в електроакустичних перетворювачах (з мікрофонним ефектом), для забезпечення значень, які неможливо розділити розвідкою на фоні природного шуму;
- Винятки (ослаблення) для проходження високочастотних накладених сигналів у допоміжних технічних засобах, у тому числі в електроакустичних перетворювачах (з мікрофонним ефектом);
- знаходження акустичних закладок, побічного електромагнітного випромінювання в режимі запису;
- виявлення несанкціонованих підключень телефонної лінії.[22]

2.2.1. «ФТЦЛ-Т» – телефонний фільтр

Рис. 2.4. «ФТЦЛ-Т»

Фільтр телефонний «ФТЦЛ-Т», призначений для захисту від прослуховування голосової та іншої акустичної інформації, що циркулює в приміщеннях, акустоелектричним каналом аналогових двопровідних телефонних мереж, що виходять за межі контрольованої зони.

«ФТЦЛ-Т» запобігає витоку інформативних сигналів при телефонній трубці, що лежить на важелі, і запобігає навмисному зніманню інформації за допомогою високочастотного накладення.

Технічні характеристики

Послаблення сигналу в телефонній лінії при мікротелефонній трубці, що лежить на важелі, на частоті 20 кГц, не менше……20

Послаблення сигналу в телефонній лінії при мікротелефонній трубці, що лежить на важелі, на частоті 100 кГц, не менше……40

Ослаблення малоамплітудного сигналу в телефонній лінії при мікротелефонній трубці, що лежить на важелі, в смузі 0,3...3,4 кГц, не менше……..40

Ослаблення сигналу в телефонній лінії при піднятій з важеля мікротелефонної трубки в смузі 0,3...3,4 кГц, трохи більше……0,2

Країна виробник……Казахстан [23]

2.2.2. GSM SAFE 3 – акустичний сейф (9648 грн)

Рис. 2.5. GSM SAFE 3

GSM SAFE 3 – акустичний сейф для мобільних телефонів. Цей пристрій використовується для запобігання прослуховування мобільного телефону користувача. GSM SAFE 3 оснащений радіочастотним детектором і генератором шуму. Не потрібно вимикати телефон, коли він знаходиться в звуконепроникному сейфі. Це дозволяє залишатися на зв’язку. При виявленні активності телефону в сейфі пристрій або сигналізує лише світловою індикацією, або починає видавати спеціальний шум, який відключає мікрофон.

Технічні характеристики

Розмір……102x84x74 мм

Виявлені комунікації…… Wi-Fi/Bluetooth, GSM 900/1800, WCDMA 2100 (3G, UMTS), CDMA 850

Живлення виробу……3 В, 2xAA

Частотний діапазон акустичного шуму……300—5000 Гц

Тип захисту……Акустичний сейф [24]

2.2.3. LockerBox – екрануюча скринька фарадея для телефонів (17250 грн)

Рис. 2.6. Екрануюча скринька LockerBox

Радіопоглинаюча скриня LockerBox призначена для блокування широкого діапазону сигналів і відноситься до категорії виробів пасивного захисту інформації. На відміну від глушників, він не впливає на роботу всієї мережі, а тільки на поміщений в скриню смартфон.

Властивості екранування скрині дозволяють відхиляти сигнали в діапазоні від 1 МГц до 10 ГГц і зменшувати рівень сигналу на 120 dBi. Діапазон включає канали, наприклад GPS, GSM, CDMA, 3G, WiFi, Bluetooth та інші базові протоколи даних.

Коробка LockerBox призначена для миттєвого блокування сигналу смартфона, не відключаючись і не втручаючись в роботу мережі. Цей спосіб захисту інформації підходить для ситуацій, таких як розміщення у кабінеті керівника, проведення конфіденційних зустрічей тощо, де необхідно забезпечити переговори та запобігти витоку інформації через стільниковий зв'язок.

Технічні характеристики

Матеріал виготовлення……Деревина, мідь 2мм

Призначення……Для смартфона

Тип захисту……Екрануюча скринька

Рівень зниження сигналу……120 dBm[25]

2.3. Активні засоби захисту

Активні заходи застосовуються у випадках, якщо пасивні заходи не забезпечують необхідного рівня безпеки. До активних пристроїв належать генератори шуму — технічні пристрої, які генерують шумоподібні сигнали. Ці сигнали подаються на акустичні або вібраційні перетворювачі.

Акустичні датчики призначені для створення акустичного шуму і вібрації в приміщенні або на вулиці - для маскування шуму в конструкціях.

Датчики вібрації приклеюються до захищеної конструкції, де вони генерують звукові коливання.

Генератори шуму з великою надійністю захищають інформацію від витоку через стіни, стелю, підлогу, вікна, двері, канали, вентиляцію та інші конструкції з високим ступенем надійності. [26]

Заходи активного захисту інформації існують для зниження відношення сигнал/шум шляхом розповсюдження акустичного/віброакустичного шуму на границях ОК ОІД.[21]

Метою активних методів захисту акустичної інформації є:

- створити маскуючі акустичні та вібраційні бар'єри, щоб зменшити відношення сигнал/шум на кордонах контрольованої зони, щоб гарантувати, що інформаційні акустичні сигнали не можуть бути виділені шляхом розвідки;
- створення маскуючих електромагнітних завад у з’єднувальних лініях ДТЗС, що мають у своєму складі електроакустичні перетворювачі, які мають мікрофонний ефект, щоб зменшити відношення сигнал/завада до величин, що роблять неможливість;

- у режимі запису електромагнітне придушення диктофонів;
- у режимі запису ультразвукове придушення диктофонів;
- створення маскуючих електромагнітних перешкод у лініях електроживлення ДТЗС, що мають мікрофонний ефект, з метою зменшення відношення сигнал/шум до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки;
- створювати цільові радіоперешкоди для голосових і телефонних радіозакладок, щоб зменшити відношення сигнал/шум до значення, яке гарантує, що неможливо ізолювати інформаційний сигнал інтелектуальними засобами;
- пригнічення (порушення функціонування) засобів несанкціонованого підключення до телефонних ліній;
- ліквідація (виведення з ладу) засобів несанкціонованого з'єднання з телефонною лінією.[27]

Технічні заходи із застосуванням активних методів захисту інформації.

Просторовий шум використовується для запобігання перехоплення побічного електромагнітного випромінювання через електромагнітний канал, а лінійний шум використовується для виключення зйому інформаційних сигналів на зовнішніх провідниках і з'єднувальних лініях.

Застосовуються такі вимоги до систем просторового шуму, які використовуються з метою утворення екранованих електромагнітних завад:

- система повинна генерувати електромагнітні завади в діапазоні частот можливого розсіяного електромагнітного випромінювання;
- створювані бар'єри не повинні мати регулярну структуру;
- рівень створюваних перешкод (електромагнітні перешкоди, що становлять поле) повинен забезпечувати, щоб співвідношення завада/шум на межі контрольованої зони було меншим за допустиме значення у всьому діапазоні частот можливого розсіяного електромагнітного випромінювання;

- система повинна перешкоджати як горизонтальній, так і вертикальній поляризації (тому особливу увагу слід приділити вибору антени генератора перешкод);
- на межах контрольованої зони рівень завад від систем просторового шуму не має переважати необхідних стандартів.

Просторове зашумлення вважається досягнутим, якщо відношення небезпечний сигнал/шум на межі контрольної зони не перевищує певного допустимого значення, розрахованого спеціальним методом для кожної частоти інформаційного (небезпечного) побічного електромагнітного випромінювання.

Системи просторового зашумлення переважно використовують «білий шум» або «синфазні завади».[22]

В підсумку, таким чином досягається захист від витоку акустичним каналом:

- використання звукопоглинаючого облицювання, спеціальних додаткових тамбурів, подвійних віконних рам;

- використання засобів акустичного зашумлення об'ємів і поверхонь;

- закриття вентиляційних каналів, систем опалення, електроенергії, телефонних та радіозв'язків;

- використання спеціальних атестованих приміщень, що виключають виникнення каналів витоку інформації.[8]

2.3.1. NG-303 - пристрій захисту від витоку інформації

Рис. 2. 7. NG-303

Виконує функції захисту телефонних ліній від прослуховування та захисту мереж змінного струму 220 В 50 Гц від несанкціонованого використання для передачі голосової інформації за допомогою різних методів прихованого запису інформації (аналогічно продукту NG-401).

На відміну від попередніх аналогічних моделей, пристрій здатний сигналізувати про «піратське» підключення до телефонної лінії та блокувати несанкціоновані паралельні з'єднання ТА. Ще однією перевагою є простота налаштування продукту.

Фактично це комплекс, що складається з генератора, що захищає мережу, і кількох незалежних генераторів, які використовуються для «зашумлення» телефонних ліній. У ньому використовуються такі види випромінювання:

- синфазні перешкоди у вигляді складних шумоподібних сигналів у цифровій формі (М-послідовність) в звуковому діапазоні частот (100 Гц ... 10 кГц);
- парафазні перешкода цифрових формувань (М-послідовність), що забезпечує пригнічення радіозаставних пристроїв в діапазоні частот що складає 30 кГц ... 650 МГц.
- спеціального сигналу, що обнуляє ланцюги живлення паралельно підключених пристроїв знімання інформації в місцях їх підключення.

Пристрій підтримує роздільні ефективні заходи проти таких засобів негласного записування інформації:

- мікрофони для передачі інформації по електромережу 220 В;

- радіопередавачі для прямого (послідовного та паралельного) та індуктивного підключення до телефонних ліній;

- пристрої магнітного запису, підключені до телефонних ліній контактними або індуктивними датчиками;

- телефони, факси, модеми, таємно підключені до телефонних ліній.

Технічні характеристики

Гарантована захисна смуга сигналу ..... 80 ... 5000 кГц

Потужність сигналу захисту ..... 5 Вт

Відношення сигнал/шум в пристрої прослуховування телефонного каналу, не менше……20 дБ

Відношення сигнал / шум в телефонному апараті, не менше……14 дБ

Габарити…..205х60х155 мм; живлення……220 В.[13, лек № 8, с. 5]

2.3.2. Shark - модуль захисту телефонної лінії

Рис. 2.8. Shark

Призначений для запобігання несанкціонованого зніманню інформації під час дзвінків і під час покладення трубки.

Технічні характеристики:

Регулювання струму в лінії в режимі розмови ... 7 ... 30 мА

Шумова перешкода у вигляді псевдовипадкової послідовності з обмеженням спектра в смузі .. 8 ... 25кГц

Напруга шумових перешкод……до 25 В

Споживана потужність…....10Вт

Напруга живлення…..220.

Активація та налаштування захисних функцій.....ручні.[13, лек № 8, с. 6]

2.3.3. Скремблер для смартфону iProTech FSM-U1 (20640 грн)

Рис. 2.9. iProTech FSM-U1

FSM-U1 – це новий кодер дзвінків для мобільних телефонів або смартфонів. Скремблер втілює новий сильний алгоритм «закриття» діалогу за допомогою технології «багатодинамічної фазової обробки». При використанні FSM-U1 підслуховування розмови стає повністю неможливим, незалежно від використовуваної технології перехоплення. Маються на увазі будь-які методи, включаючи такі речі, як контроль «у оператора», пасивне перехоплення

телефонної зони, активне перехоплення з перемиканням телефону на «помилкову» базу і т.д.

Відносно низька вартість скремблера дозволяє будувати «мережу» між постійними партнерами або «зверху» всередині компанії, де ведуться повністю «закриті» переговори.

Коли скремблер підключений, розмова йде через нього або гарнітуру.

FSM-U1 має вбудований динамік і мікрофон.

Пристрій живиться від акумулятора 3,7 В ємністю 290 мАг.

Час роботи батареї - до 2,5 годин розмови в зашифрованому режимі.

Час зарядки - 2 години через USB (комп'ютер, мережа або автомобільний роз'єм).[28]

2.3.4. iProTech PIAC-4 – пристрій телефонного захисту (16104 грн)

Рис. 2.10. iProTech PIAC-4

PIAC-4 виключає можливість використання обладнання, що передає інформацію по мережі 220 В, і обладнання, яке знімає інформацію з телефонних ліній. В мережі 220 В розмір частот шумових перешкод - 180 Гц - 5000 кГц. В телефонній мережі розмір частот шумових перешкод - 180 Гц - 10 кГц

Специфікація

- Діапазон частот шумового сигналу в електромережі: 180 Гц - 5 МГц
- Діапазон частот шумового сигналу в телефонній мережі: 180 Гц - 10 кГц
- Амплітуда шумового сигналу у мережі: чи не менше 0,2 В (у визначеному діапазоні частот) з навантаженням близько 1 кВА
- Амплітуда шумового сигналу в телефонній мережі: не більше 10 мВ в режимі розмови, не менше 100 мВ в режимі очікування

- Час технічної готовності приладу: не більше 1 с
- Живлення від електромережі: 220 (± 22) В, 50 (± 1) Гц
- Маса: не більше 1,5 кг[29]

2.3.5. DNG-KIT1 – комплект віброакустичного захисту 62080 грн

Рис. 2.11. DNG-KIT1

Оснащений такими приладами зі своєї лінійки як: вібровипромінювачі (перетворювачі) та акустичні випромінювачі (динаміки). DNG-KIT1 діє проти методів прослуховування, за допомогою того що створює потужні перешкоди, які не можливо відфільтрувати для архітектурних конструкцій та порожнеч.

Особливості DNG-KIT1

• Забезпечує надійний захист від викрадення для багатьох типів віброакустики, передаючи нефільтрований шум на довколишні конструкції та пустоти.

• Є важливою частиною системи захисту, що теж має у собі підключені до дротів вібраційні та акустичні передавачі

• Створення білого шуму – вихідні шуми рівномірно розташовуються по спектру людського голосу

• Має 3 незалежних вихідних канали: 2 для вібровипромінювачів, 1 для акустичних випромінювачів

• Усі 3 канали можна індивідуально налаштувати за рівнем

• Канали акустичних випромінювачів живить до 12 динаміків [30]

2.3.6. iProTech DNG-2300 - генератор шуму (28480 грн)

Рис. 2.12. iProTech DNG-2300

3-х канальний генератор «білого» шуму (2 «вібро» каналу + 1 «акусто» канал). Його функції зроблені для протекції периметра приміщення знімання даних стетоскопами, контактними мікрофонами. Добре застосовувати у парі з вібровипромінювачем TRN-2000. При використанні акустичного випромінювача OMS-2000 може створювати перешкоди для диктофонів і закладних пристроїв у кімнаті. Смуга частот 250-5000 Гц. Сертифікований ДЦВ ТЗІ України.

DNG-2300 розроблено для захисту важливої інформації від знімання вбудованими пристроями, які не можуть бути виявлені традиційними шукаючими системами. І захистити обладнання, встановлене навколо захищених об'єктів або взагалі поза межами приміщення – провідні мікрофони, контактні мікрофони, передавачі, що передають інформацію за допомогою мережі 220 В і також віконних систем, дія яких сформована на відбиванні лазерних/інфрачервоних/мікрохвильових променів.

Присутність всіх складових гармонік вимови людини допускає дієво боротися з різними методами фільтрування мовленнєвої інформації. DNG-2300 включає 3 незалежних цифрових канали генератору «білих» шумів. «Білий» оскільки він вміщає усі частотні гармоніки, присутні у даному спектрі.

Як завжди пристрої містять вузький розмах частот (від 300 до 3 кГц) через обмежену схему та обмежований час роботи від акумулятора. DNG-2300 працює в діапазоні 250-5000 Гц, що є найкращим вибором для пригнічення найпоширеніших видів пристроїв для прослуховування. [31]

2.3.7. iProTech MNG-300 Rabbler – мобільний генератор шуму (11680 грн)

Рис. 2.13. iProTech MNG-300 Rabbler

3-х канальний генератор «білого» шуму (2 «вібро» каналу + 1 «акусто» канал). Його функції зроблені для протекції периметра приміщення знімання даних стетоскопами, контактними мікрофонами. Добре застосовувати у парі з вібровипромінювачем TRN-2000.

Новий спосіб захисту від диктофонів і прослуховування. Пристрій створює мовні перешкоди, які ефективно перешкоджають запису. Добре розташовується у кишені або сумочці.

Технічні характеристики:

Частотний діапазон……300 - 3600 Гц

Споживаний струм……до 120 мА

Живлення……9В

Органи управління……живлення, індикатор рівня, регулятор рівня

Габарити……85 × 53 × 21 мм[32]

2.3.8. DRUID D-06 – пристрій забезпечення конфіденційних переговорів

Рис. 2.14. DRUID D-06

Обладнання для конфіденційних переговорів на 6 осіб. Запобігає прослуховуванню будь-яких пристроїв, враховуючи всі типи радіомікрофонів, стетоскопів, диктофонів, пасивних резонаторів, дротяних мікрофонів тощо. Працює базуючись на синхронізованих звукових перешкодах. Живиться від вмонтованого акумулятора чи блоку живлення 220 В, з 4 навушниками Plantronics Audio 355 в наборі.

Принцип роботи DRUID D-06 заснований на генерації звукових перешкод, які відтворюються синхронно з людською мовою. Гучність перешкоди вище гучності розмови, тому ні «жучок», ні диктофон не чують мови.

Утворені перешкоди неможливо відфільтрувати методами видалення шумів. Водночас відтворені перешкоди не доставляють незручностей членам переговорів через спеціальну гарнітуру. Навушники дають чітку передачу звуку.

Технічні характеристики

Тип шуму……спотворення + реверберація

Кількість каналів……6

Джерело живлення……мережа 220 В, акумулятор

Тривалість роботи від акумулятора……3-6 годин

Розмір……23×6,5×17 см [33]

2.3.9. «SAPSAN+» – портативний подавлювач сигналів (15348 грн)

Генератор завад «SAPSAN+» - портативний пристрій з вмонтованим акумулятором, який є найбільш популярним, оскільки здатний придушувати не лише мобільний сигнал GSM/DCS, мобільний інтернет 3G/4G та Wi-Fi, а й частоти супутникової навігації GPS. Вони вільно застосовуються для відстеження GPS, тому «SAPSAN+» надійно вбереже від стеження та приховає місцезнаходження від зловмисників.

Рис. 2.15. «SAPSAN+»

Ще однією характерною перевагою «SAPSAN +» є підвищений радіус дії - його потужність дозволяє обсягти площу від 5 до 30 кв. м, і цього цілком достатньо, аби безпечно закрити радіус в офісі переговорів чи всередині автомобіля, на який без відома власника можуть почепити трекер або жучок.

Технічні характеристики:

Живлення……AC100-240V-DC12V

Загальна потужність……8 Вт

Антени …….. – 8 шт

Маса……1,3 кг

Радіус дії……від 3 до 30 м (залежить від розміщення базових станцій)

Розміри……150x80x40 мм (без антен)

Час автономної роботи……..від 120 до 180 хв [34]

2.3.10. Генератор акустичного шуму ANG-2200

Рис. 2.16. ANG-2200

Генератор шуму ANG-2200 використовується для захисту приміщень від можливого прослуховування дротовими мікрофонами, радіомікрофонами та стетоскопами. Пристрій також може видаляти акустичну інформацію з вікон шляхом лазерного блокування та створювати акустичні перешкоди для записуючого обладнання.

Пристрій має два вихідні канали. ANG-2200 може підключати кілька випромінювачів, а також можливе регулювання АЧХ та шуму.

Технічні характеристики:

Діапазон частот шуму…250...5000Гц.

При навантаженні в 6 Ом можлива вихідна напруга……0 ... 14 В.

Мінімальний опір навантаження……1 Ом

Опір одного випромінювача……6 Ом

Від постійного струму можливе живлення 12…18 В. Для підключення в мережу з 220 В потрібно використовувати адаптер.

Розміри блоку……43х152х254 мм

Маса блоку……1,36 кг.

На один блок можливо підключити до вісімнадцяти випромінювачів.[35]

2.3.11. Стаціонарний подавлювач телефонів "Піранія X20-5G" 59000 грн

Стаціонарний подавлювач захищає власника від прослуховуючих пристроїв, у тому числі через телефонні дзвінки, витоку інформації, відстеження руху. З цієї причини у важливих місцях зустрічей зазвичай встановлюють приглушувачі сигналу. Подавлювач можна встановити в залах театрів, музеїв, бібліотек тощо, щоб дзвінки на мобільний телефон не відволікали відвідувачів чи гостей.

Рис. 2.17. "Піранія X20-5G"

Технічні характеристики

Живлення……AC100-240V-DC12V

Загальна потужність……58 Вт

Антени ……20 шт

Маса……7,5 кг

Радіус дії……від 20 до 50 м (на це впливає розміщення базових станцій)

Розміри……430 х 240 х 90 мм (без антен)

Час автономної роботи……Безперервно.[36]

2.3.12. Захисний пристрій «Базальт-4ГА»

Рис. 2.18. «Базальт-4ГА»

Пристрій націлений для протекції об'єктів від витоку мовленнєвої інформації з акустичного, віброакустичного та акустоелектричного каналів. Захист забезпечується придушенням потенційних акустоелектричних перехідних сигналів у слабострумових колах, інформативних акустичних і вібраційних сигналах, відповідних шумових сигналах.

Це є двоканальним генератором електричних шумових сигналів, з октавним регулюванням частотної характеристики двох каналів. Пристрій можна обладнувати акустичними та віброакустичними передавачами наприклад «Базальт-4ДА», «Базальт-4ДВМ», «TRN-2000», «OMS-2000» тощо.

Технічні характеристики:

Напруга живлення 50Гц, В……198 — 240

Струм, А……не біль-ше 0,3

Максимальна дієва напруга вихідних сигналів шуму у смузі частот (170 — 5700) Гц:

на мінімальному опорі навантаження 1 Ом, В……не менше 2;

на мінімальному опорі навантаження 50 Ом, В……не менше 15

Діапазон регулювання напруги вихідних шумових сигналів на обох виходах, дБ……не менше 20

Глибина регулювання напруги вихідних сигналів шуму у октавних смугах з центральними частотами 250, 500, 1000, 2000, 4000 Гц на обох виходах, дБ……не менше 25

Габаритні розміри, мм……не більше 200х145х75

Маса, кг……не більше 3.[37]

РОЗДІЛ 3. ОПИС ПРИМІЩЕННЯ, У ЯКОМУ МОЖЕ БУТИ ВИТІК ІНФОРМАЦІЇ АКУСТИЧНИМИ КАНАЛАМИ

3.1. Обстеження приміщення

Об’єкт інформаційної діяльності для якого розробляється система захисту інформації від витоку по акустичному каналу знаходиться в будівлі бізнес-центру за адресою – м. Зарічне, район Радужний, вулиця Шевченка, 17-А. Назва компанії ТОВ «BetaCall». ТОВ «BetaCall» є оператором зв’язку для бізнесу. Компанія надає послуги на дому, малому та великому бізнесу, провайдерам та операторам. Завдяки великій клієнтській базі, ця компанія стає цікавою для зловмисників.

Компанія працює 5 днів на тиждень, з понеділка по п’ятницю. Є декілька змін, через це компанія працює з 07:00 до 23:00. Прибирання приміщення проводиться кожного буднього дня з 6:30 до 7:00.

Територія будинку охороняється цілодобово. При вході у бізнес центр є охоронець. Також при вході до приміщення офісу компанії є охоронець, зі штату працівників цього філіалу. Об’єкт інформаційної діяльності знаходиться на території, яка обнесена парканом. Вхід на ОІД здійснюється за допомогою ключ-карти та має два входи:

- 1 основний;
- 1 запасний.

В ТОВ «BetaCall» працює 48 осіб. Нижче представлені посади та їх обов’язки.

Керівник – 1 людина. Координує роботу всіх ділянок.

Секретар – 1 людина. Займається організацією зустрічей, ведення документів.

Рекрутер – 1 людина. Займається пошуком та наймом нових співробітників.

Team-лідер – 2 людини. Займаються підготовкою нових співробітників до роботи.

Оператор – 41 людина.

Охоронець – 1 людина. Охороняє підприємство.

Прибиральниця – 1 людина.

Об’єкт інформаційною діяльності розташований в будівлі бізнес центру на третьому поверсі за адресою – м. Зарічне, район Радужний, вулиця Шевченка, 17-А. Вікна ОІД виходять на усі 4 сторони.

Рис. 3.1. Схема загального розташування будівлі бізнес-центру

Архітектурно-будівельні особливості приміщення:

Товщина стін – 300мм.

Висота перекриття – 3500 мм.

Склад зовнішніх стін – залізобетон.

Склад внутрішніх стін – скло та цегла.

Стеля – залізобетонна монолітна заливна товщиною 250мм.

Підлога – залізобетонна монолітна заливна товщинною 250мм.

Покриття підлоги – лінолеум 5мм.

Вікна (11 шт. Розміром 1000Х2000мм; 4шт. Розміром 750Х1000мм) – металопластикові з двокамерним склопакетом. Товщина скла 3мм. Жалюзі відсутні.

Зовнішні двері (1шт. Розміром 900X2100мм;) – дерев’яна одностулкова шириною 40мм

(1шт. Розміром 1800X2100мм;) – скляна двостулкова шириною 25мм

Внутрішні двері (2шт. Розміром 1800X2100мм;) – броньовані двері з магнітом шириною 50мм розділені тамбуром. (2шт. Розміром 1800X2100мм;) – броньовані двері з магнітом шириною 50мм (5шт Розміром 900X2100мм;) – дерев’яні одностулкові шириною 40мм

Контрольована зона обмежена територією ОІД. ОІД обладнано системою пожежної сигналізації, контролю доступу та камерами спостереження. Далі наведено плани приміщень, та умовні позначення (Таблиця)

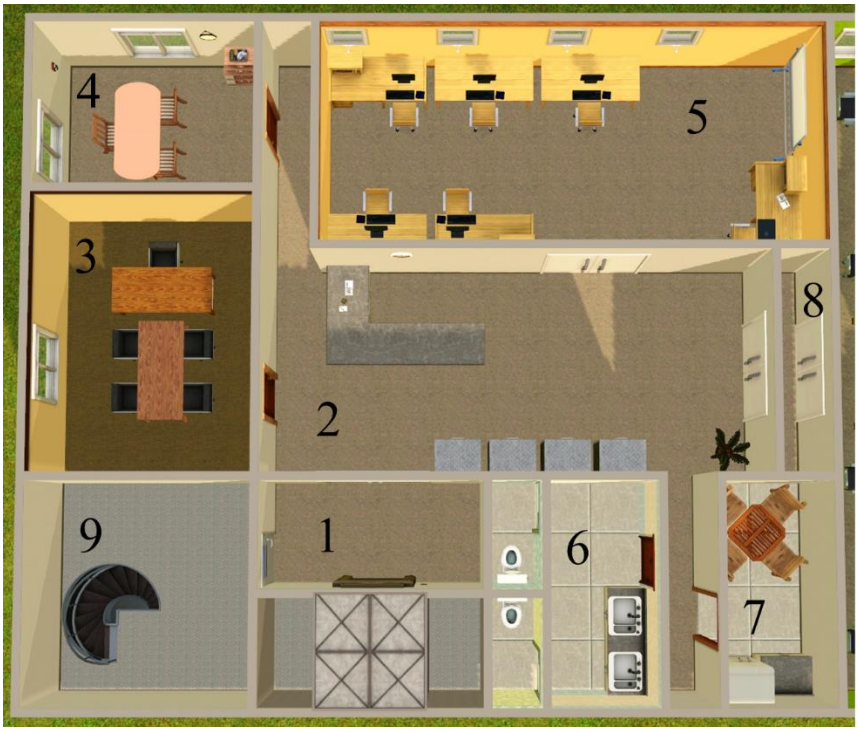

Рис. 3.2. План приміщень ОІД (права частина)

Рис. 3.3. План приміщень ОІД (ліва частина)

Таблиця 3.1. Умовні позначення

Номер	Назва приміщення
1	Тамбур між ліфтом та коворкінгом
2	Приймальня - коворкінг
3	Кабінет переговорів на нарад
4	Кабінет рекрутера
5	Відділ навчання
6	Санвузол
7	Кухня
8	Тамбур
9	Запасний вихід зі сходами
10	Операторська зала
11	Кабінет керівника

12	Приймальня керівника
13	Санвузол

Рис. 3.4. Загальний вигляд плану ОІД

На території ОІД знаходяться декілька видів систем комунікацій (Таблиця).

Таблиця 3.2. Системи комунікацій компанії

Комунікації	Підключення
Електроживлення	підключено до підстанції № 1321, для обслуговування споживачів, знаходиться в межах КЗ
Заземлення	всі електроприлади є заземленими на спільний контур заземлення, він замкнений і знаходиться за межами КЗ
Телефонна лінія	підключена до АТС «Vodafon». На офіс виділено 3 номера (Номера для ресепшену, рекрутера, team-лідера, консультації телефоном, приймальні керівника, керівника). Виходить за межі КЗ.
Система каналізації	підключена до міської центральної каналізаційної мережі, яка розташована за межами КЗ
Система водопостачання	підключена до міського водоканалу, котрий виходить за межі КЗ (пластикові труби, однотрубна вертикальна система водопостачання)

Система вентиляції	припливно-витяжна, штучна

Мережеве обладнання заземлено. Стрижні заземлення вкопані у внутрішньому дворі. Заземлені на загальний контур заземлення, який являється замкнутим та розташовується у межах КЗ.

3.2 Можливі місця витоку інформації

Проаналізувавши територію, характеристики та властивості ОІД, вже можна зробити висновок, що є місця, де ризик витоку інформації найбільший, і навпаки. Щоб краще зрозуміти, нам потрібно навести кілька прикладів.

1) Так як, у керівника можуть відбуватись ділові зустрічі з сторонніми особами, то в них є можливість підслухати розмову, або записати її на звукопереносні пристрої. Також зловмисники можуть застосувати до кабінету керівника заходові засоби, такі як «телефонне вухо», диктофон, провідний мікрофон тощо.
2) Зловмисники можуть отримувати інформацію за допомогою спрямованих мікрофонів – спеціальних пристроїв, які дають змогу прослуховувати слова з відстані десятків метрів. Оскільки ОІД знаходиться в місці під охороною та двері і вікна щільно закриті, то цей варіант є малоймовірним.
3) Зловмисники можуть збирати інформацію використовуючи стетоскопи – прилади, що знімають вібрації будівельних споруд, які виникають через розмову в приміщенні, та перетворюють їх в електричні сигнали звуку, які потім можна прослуховувати. Оскільки ОІД межує з вулицею ймовірність прослуховування таким чином дуже висока.
4) На підприємстві працівники мають доступ до конфіденційної інформації клієнтів, тому зловмисники можуть влаштуватися на роботу та взяти необхідну інформацію.
5) Перехоплення за допомогою віконного скла з лазерним або інфрачервоним детектором. Цей метод не вимагає близького наближення до об’єкта розвідки, його можна виконувати на відстані. Наприклад, під час розмови в приміщенні спостерігається дуже незначна вібрація віконного скла, викликана повітряними

звуковими хвилями, і віконне скло модулюється цією розмовою. Якщо з протилежного будинку чи іншої будівлі на ці окуляри направляється лазерний промінь і отримує відображення від цих окулярів, усі розмови можна почути та записати. Оскільки ОІД межує з вулицею і має віконних прорізи, ризик отримання інформації таким способом досить високий.

РОЗДІЛ 4. СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМИ КАНАЛАМИ

Щоб розробити систему захисту від витоку акустичними каналами необхідно визначити місця, де буде озвучуватись найбільше важливої інформації. У нашому випадку це: кабінет керівника, кабінет для конференцій та зустрічей, а також операторська зала.

4.1. Засоби захисту для кабінету конференцій та зустрічей.

Оскільки ця кімната знаходиться неподалік від коворкінгу, де можуть знаходитись інші співробітники, для яких не призначена інформація, яка може озвучуватись у кабінеті переговорів, тому потрібно зважати на звукоізоляцію дверей. Для цього можна застосувати двері, які складаються зі сталевих листів. Сталеві двері набувають звукоізоляційних якостей, якщо між листами сталі прокладено ізолятор (буде добре якщо це мінеральна вата або матеріал Tecsound 2FT 80). За відсутності ізолятора сталевий лист може, навпаки, посилювати шум. [38]

Рис. 4.1. Матеріал Tecsound 2FT 80

Ціна такого матеріалу 2047 грн за квадратний метр. Двері з таким ізолятором будуть коштувати приблизно 14919 грн.

Звукоізоляція підлоги має важливе значення. Для цього доцільно використовувати ковролін. 1 квадратний метр ковроліну коштує приблизно 339 грн. Площа ділянки офісу, де потрібне ковролінове покриття приблизно 270 кв. м. Тоді 339 грн * 270 кв. м. = 91 530 грн. [39]

Також необхідно подбати про звукоізоляцію внутрішніх та зовнішніх стін.

У внутрішніх стін щоб збільшити звукоізоляцію каркасних перегородок

рекомендовано використовувати конструкції з двома облицюваннями, натомість одинарних каркасів використовувати подвійні, застосовувати не менше двох чи трьох шарів ГКЛ, заповнювати каркаси професійним звукопоглинальним матеріалом, застосовувати пружні прокладення між будівельними конструкціями ф напрямними профілями.

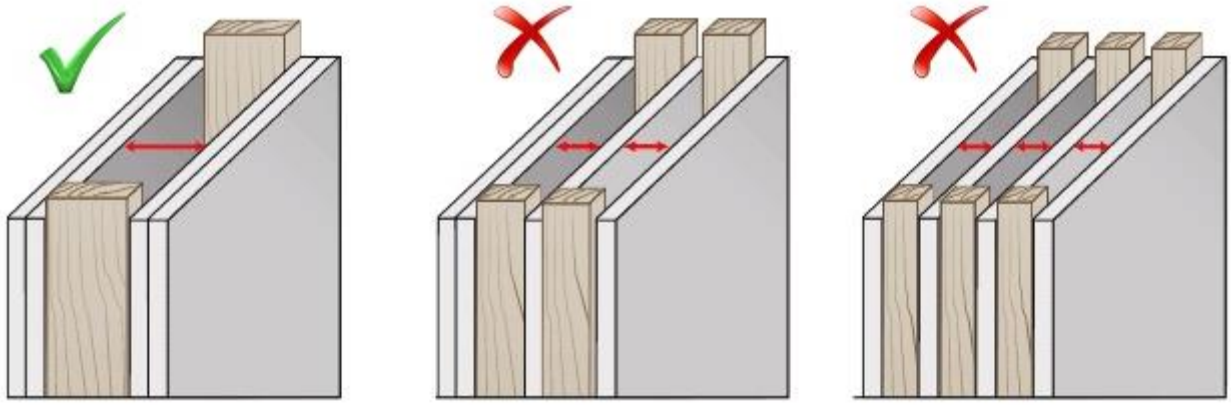

Рис. 4.2. Звукоізоляція перегородок

Для зовнішніх стін необхідно підбирати звукоізоляційні матеріали для обшивки. Можна використати акустичну панель з поролону Ecosound Mini з коефіцієнтом звукового поглинання 0,85. Розмір однієї панелі 50х50 см. [40]

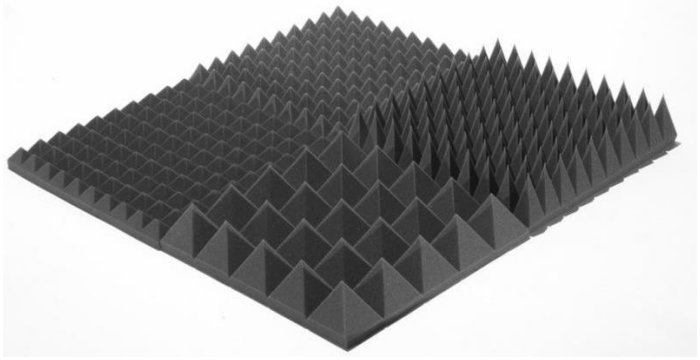

Рис. 4.3. Панель з акустичного поролону Ecosound Mini

Для повного облицювання зовнішніх стін кабінету директора та кабінету нарад необхідно приблизно 56 таких панелей загальною вартістю 15 344 грн.

Для підвищення звукоізоляції вікон порадою буде використовувати склопакет з максимально можливою шириною, який складається з 2-х масивних стекол, непогано би різної товщини (до прикладу 6 та 8 мм) і найбільшої планки. Якщо все таки використовуються двокамерні склопакети, рекомендується різна товщина скла і повітряні проміжки різної ширини. Профільна система мусить забезпечувати трьох

контурне ущільнення стулок по периметру віконної рами.

Найефективнішою конструкцією з точки зору звукоізоляції є комбіноване вікно з двох стулок, одна з яких - склопакет з двома шарами скла 6-8 мм, а інша - склопакет товщиною 8-10 мм. [41]

Ціна одного великого вікна буде приблизно 2 912 грн. * 11 шт = 32 032 грн. Ціна малого вікна буде приблизно 1 954 грн * 4 шт = 7 816 грн.

Як вже було вказано раніше, у керівника можуть проходити ділові зустрічі з партнерами, тому необхідно забезпечити захист від потенціально пронесених в кімнату різних звукозаписуючих пристроїв та жучків. Для цього добре підходить iProTech MNG-300 Rabbler.

Рис. 4.4. iProTech MNG-300 Rabbler

Технічні характеристики

Вид……..Генератори шуму

Живлення……"Крона"

Протоколи/частоти……300 — 3600 Гц

Споживаний струм……До 120 мА

Розміри……85 х 53 х 21 мм[42]

Види підслуховуючих пристроїв, від яких захищає цей пристрій:

- що носяться на тілі відеокамери, годинники, краватки і т. д. (придушення акустики)
- GSM і 3G жучки
- диктофони
- радіомікрофони
- провідні мікрофони
- інші види «жучків»

Ціна цього пристрою 11 680 грн.

Також необхідно забезпечити захист від знімання інформації з вікон за допомогою лазерних або інфрачервоних пристроїв . Для цього можна обрати генератор акустичного шуму ANG-2200.

Для даної ситуації добре вписується генератор шуму ANG-2200, який окрім забезпечення необхідного захисту для лазерних і мікрохвильових систем, він також створює перешкоди, які заважають використовувати дротові мікрофони, радіомікрофони та стетоскопи для запису інформації.

Рис. 4.5. Генератор шуму ANG-2200, у комплекті йдуть вібровипромінювачі TRN-2000, та акустовипромінювачі OMS-2000

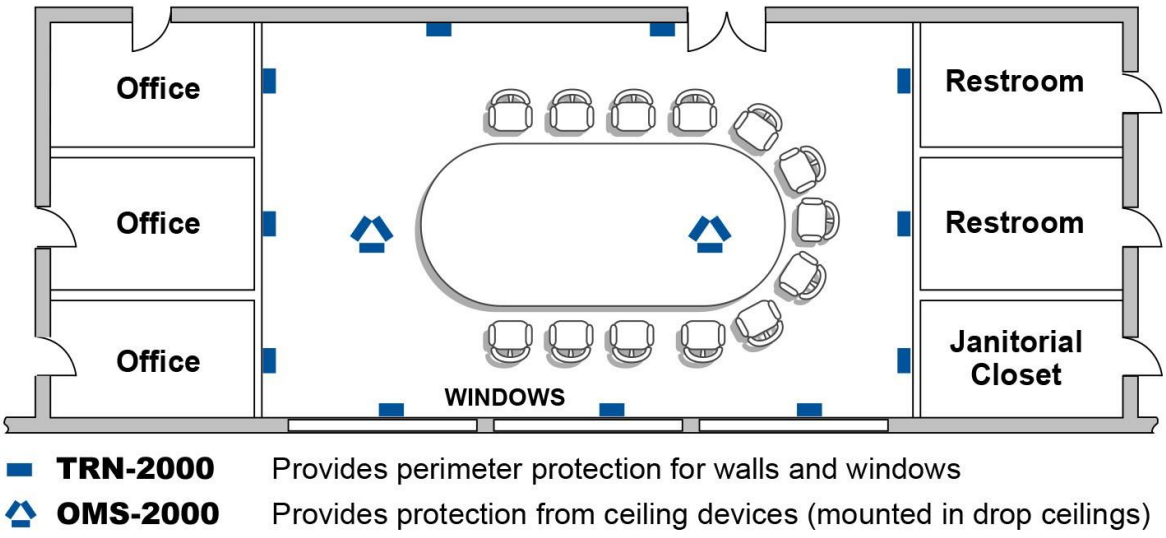

Рис. 4.6. Приклад розміщення всіх складових комплекту віброакустичного захисту ANG-2200

Технічні характеристики

Вихідна напруга……..10 Vp-p при 6 Ω

Діапазон частот…….від 125 Гц до 4 кГц

Регулювання частотної характеристики…….НЧ 180 Гц ± 12 дБ; ВЧ 3 кГц ± 12 дБ

Живлення генератора білого шуму……12 В постійного струму на 1 А (адаптер змінного струму в комплекті) [43, 44]

Ціна цього комплекту 33429 грн

4.2. Засоби для захисту операторської зали та відділу навчання нових працівників.

Операторська зала і навчальний відділ так само як і кабінет переговорів знаходяться через стіну з коворкінгом, тобто необхідно зайнятися звукоізоляцією дверей, стін, та вікон. Зробити це можна аналогічно з заходами для кабінету переговорів.

Оскільки працівники мають доступ до конфіденційно інформації, то необхідно забезпечити умови для того щоб ця інформація не виходила за межі контрольованої зони. Для цього при прийомі на роботу необхідно укладати договір про нерозголошення конфіденційної інформації. А перед початком роботи на своїй зміні необхідно щоб кожен робітник залишав свої пристрої у спеціально відведених комірках, які відведені для цього, і знаходяться під охороною. Це важлива умова для допущення співробітника до свого робочого місця.

Також коворкінг та операторську залу розділяють двоє броньованих двостулкових дверей з тамбуром, що відчиняються магнітною ключ-картою, яка видається співробітникам охоронцем після огляду співробітника. А відділ навчання та коворкінг розділяють одні такі ж двері.

При будуванні тамбурів дверей звукоізоляцію покращує зменшення щілин над підлогою при відсутності порогу, і до того ж доцільне оббивання внутрішніх поверхонь тамбура звукопоглинальними покриттями.

Облицювання тамбура згаданими вище панелями звукоізоляції буде коштувати приблизно 9864 грн.

Троє дверей будуть коштувати 14919 грн * 3 шт = 44 757 грн.

Для операторської зали та відділу навчання (можна використовувати одразу для двох приміщень) в якості захисту вікон та стін від знімання акустичної інформації підійде комплект віброакустичного захисту DNG-KIT1. У комплектації знаходиться генератор шуму iProTech DNG-2300 акустичні випромінювачі SP2300, та вібровипромінювачі TD2300

Рис. 4.7. Комплект віброакустичного захисту DNG-KIT1

Цей комплект забезпечує пригнічення стінних контактних мікрофонів, віконних лазерних систем та провідних мікрофонів у стінах, порожнинах та вентиляційних шахтах.

Технічні характеристики

Вихід акустичних випромінювачів:

АЧХ……180-7000 Гц

Максимальна вихідна потужність……1 х 8 Вт

Максимальна кількість динаміків……12

Мінімальний імпеданс навантаження……8 Ом

Вихід вібровипромінювачів:

АЧХ……180-5600 Гц

Максимальна вихідна потужність……2 х 10 Вт

Максимальна кількість перетворювачів на канал……24 (легкі конструкції), 12 (тяжкі конструкції)

Мінімальний імпеданс навантаження……3 Ом

Характеристики техніки захисту:

Канали виходів……2 для вібровипромінювачів, 1 для акустичних випромінювачів

Максимальна вихідна напруга……12 В

Живлення……110-220В, 50-60 Гц[30]

Вартість такого комплекту 62 080 грн.

4.3. Засоби захисту для кабінету керівника.

Оскільки кабінет керівника знаходиться за операторською залою, до якої можна потрапити лише за допомогою магнітної ключ-картки, то сторонні люди не мають змоги потрапити до його кабінету. Отже немає необхідності створювати додаткову звукоізоляцію у внутрішніх стінах. Але керівник може проводити ділові розмови зі співробітниками, або по стаціонарному телефону. В усьому офісі стаціонарних телефоній усього 5: у керівника, секретаря, рекрутера, team-лідера, охоронця.

Для захисту стаціонарних телефонів можна використовувати iProTech PIAC-4.

Рис. 4.8. Пристрій для телефонного захисту iProTech PIAC-4

Технічні характеристики

Частотний діапазон шумового сигналу в електромережі……180 Гц - 5 МГц

Частотний діапазон шумового сигналу в телефонній мережі……180 Гц - 10 кГц

Амплітуда шумового сигналу в електромережі……чи не менше 0,2 В (в зазначеному діапазоні частот) під навантаженням 1 кВА

Амплітуда шумового сигналу в телефонній мережі……в режимі розмови не більше 10 мВ, в режимі очікування не менше 100 мВ

Час технічної готовності приладу……не більше 1 с

Живлення від електромережі……220 (± 22) В, 50 (± 1) Гц[29]

Ціна такого приладу 16 104 грн.

Також керівник може проводити телефонні розмови по своєму смартфону. Під час розмов можна використовувати скремблер для смартфону iProTech FSM-U1.

Рис. 4.9. iProTech FSM-U1

Ціна такого виробу 20 640 грн.

Коли ж керівник не використовує свій смартфон, можливе використання спеціальних боксів для виключення ситуацій прослуховування мобільного телефону. Можна використовувати акустичний сейф GSM SAFE 3.

Рис. 4.10. Акустичний сейф GSM SAFE 3

Ціна такого приладу 9 648 грн.

4.4. Загальна вартість системи захисту інформації від витоку акустичними каналами

Акустичні панелі з поролону Ecosound Mini: 15 344 грн.

Облицювання тамбуру панелями з поролону Ecosound Mini: 9 864 грн.

Ковролінове покриття: 91 530

Вікна двостулкові двокамерні: 32 032 грн. + 7 816 грн.

Генератор акустичного «білого» шуму iProTech MNG-300 Rabbler: 11 680 грн.

Комплект віброакустичного захисту з генератором ANG-2200: 33 429 грн.

4 шт звукоізолюючих дверей: 4 шт * 14 919 грн. = 59 676 грн.

Комплект віброакустичного захисту DNG-KIT1: 62 080 грн.

Пристрій для телефонного захисту iProTech PIAC-4: 16 104 грн.

Скремблер для смартфону iProTech FSM-U1: 20 640 грн.

Акустичний сейф GSM SAFE 3: 9 648 грн.

Сума: 369 843 грн.

Так як «BetaCall» є оператором зв’язку, вона надає послуги для багатьох компаній, та працює з великими об’ємами інформації та великими клієнтськими базами, є одним з кращих надавачів послуг у своїй сфері по всій країні, така система захисту з легкістю окупиться за 1-1,5 роки.

ВИСНОВКИ

В дипломному проекті була наголошена важливість даної теми, визначено завдання проекту, окреслено основні поняття та визначено які бувають канали витоку інформації, на що вони впливають, чому важливо захищати інформацію, яким чином це робиться для кожного з видів каналів витоку.

Відповідно до вищезгаданої теми видно, що основним предметом, який був точніше описаний в проекті це саме акустичний канал витоку інформації. Було описано звідки береться цей канал, на чому базується, його фізичний зміст, та структура, та реалізація.

Також розглянуто основні визначення, які характеризують захист інформації від витоку саме цим каналом, наведена класифікація, сутність та способи закриття інформації від викрадення. Описано основні способи енергетичного приховання та їх втілення.

Були проаналізовані пасивні та активні засоби для захисту інформації від витоку акустичним каналом. Наведений перелік найдієвіших на думку автора засобів із зазначенням основних технічних характеристик до кожного.

Було досліджене та докладно описане приміщення, у якому циркулює конфіденційна інформація, а також зазначені потенціальні місцерозташування каналів витоку.

Згідно умов, які диктує приміщення, було розроблено систему захисту інформації від витоку акустичними каналами, шляхом підбору найефективніших засобів захисту.

Проаналізувавши все описане можна дійти до висновку, що завдання проекту було розкрито у повній мірі.

СПИСОК ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf
2. https://ukr.detective-ua.com/vitik-inform/
3. https://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8_%D0%B2%D0%B8%D1%82%D0%BE%D0%BA%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97
4. https://learn.ztu.edu.ua/mod/resource/view.php?id=98533&lang=ru
5. https://ua-referat.com/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8_%D0%B2%D0%B8%D1%82%D0%BE%D0%BA%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97
6. https://www.znanius.com/3853.html
7. https://studfile.net/preview/9650062/page:2/
8. http://journals.dut.edu.ua/index.php/dataprotect/article/view/2458/2358
9. https://tzi.com.ua/akustichn-kanali-vitoku-nformacz.html
10. https://lektsii.com/2-9480.html
11. http://ni.biz.ua/18/18_7/18_70372_strukturnoe-skritie-rechevoy-informatsii-v-kanalah-svyazi.html
12. https://ru.bmstu.wiki/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8_%D0%BE%D1%82_%D1%83%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%BF%D0%BE_%D0%B0%D0%BA%D1%83%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%BC_%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%B0%D0%BC
13. Курс лекцій з дисципліни «Методи та засоби технічного захисту інформації», лекції №8 і №9
14. https://uadoc.zavantag.com/text/34684/index-31.html
15. https://studfile.net/preview/9649855/page:5/
16. http://um.co.ua/6/6-6/6-65546.html
17. http://um.co.ua/2/2-15/2-150879.html
18. http://fanplit.com.ua/produktsiya/derevovoloknisti-pliti-dvp-mdf/

19. https://knowledge.allbest.ru/radio/2c0b65625a3bc78a4d43b88521306c27_1.html
20. https://tzi.com.ua/zaxist-movno-nformacz.html
21. https://tzi.com.ua/zaxist-nformacz-vd-vitoku-texnchnimi-kanalami.html
22. https://studfile.net/preview/9650062/page:4/
23. https://topol.kz/catalog/katalog-produkcii/oborudovanie-zashity-sredstv-informacii/fil-tr-telefonnyj-cifrovyh-linij-ftcl-t
24. https://yug.com.ua/uk/akusticheskij-sejf-iprotech-gsm-safe3.html
25. https://yug.com.ua/uk/locker-box.html
26. http://um.co.ua/9/9-2/9-26964.html
27. https://helpiks.org/8-76372.html
28. https://lockers.com.ua/skrembler-iprotech-fsm-u1/
29. https://lockers.com.ua/ustrojstvo-telefonnoj-zashhiti-rias-4/
30. https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/komplekt-vibroakustichnogo-zaxistu-dng-kit1/
31. https://lockers.com.ua/generator-shuma-dng-2300/
32. https://lockers.com.ua/mobilnij-generator-shuma-mng-300-rabbler/
33. https://yug.com.ua/uk/druid-d-06.html
34. https://lockers.com.ua/6470-15-an-102/
35. https://www.savehome.ru/product_3756.html
36. https://lockers.com.ua/piranja-h20-5g-universalnaja-glushilka-telefonov-20-chastot-58vt-do-50-m/
37. https://webcache.googleusercontent.com/search?q=cache:l8GC7i0lY-AJ:https://usts.kiev.ua/prystrij-zakhysnyj-bazalt-4ha/+&cd=1&hl=ru&ct=clnk&gl=ua
38. https://www.tecsound.com.ua/ru/as/akusticheskie-sistemyi-16/
39. https://polmall.com.ua/kovrolin-timzo-rubin-2113/
40. https://epicentrk.ua/shop/mplc-akustichna-panel-ecosound-mini-piramida-90-mm-50kh50-sm-chornii-grafit-1eba68e9-81d5-60b4-a683- 5739f3b70872.html
41. https://acoustic.ua/recommendations/438
42. https://rozetka.com.ua/iprotech_mng_300_rabber/p234881/characteristics/
43. https://reiusa.net/audio-security/ang-2200-acoustic-noise-generator/
44. https://www.detective-store.com/white-noise-generator-ang-2200--188.html