Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

випускної кваліфікаційної роботи

бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: Удосконалення модулів автоматизованих пошукових комплексів засобів негласного отримання інформації

Виконавець: студент IV курсу, групи КБ-42

_____ **Кирило АВХИМЕНКО**
(підпис) (прізвище ім'я)

	Прізвище, ініціали	**Підпис**
Керівник	Олександр ЛАПТЄВ	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)
освітньої програми Кібербезпека
(назва освітньої програми)

студенту **КБ-42** **Авхименко Кирилу Миколайовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Удосконалення модулів автоматизованих пошукових комплексів засобів негласного отримання інформації

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол № 5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методики локалізації засобів негласного отримання інформації, виток інформації радіоканалом, існуючі загрози витоку інформації, захист інформації від витоку акустичними радіоканалами.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Поняття засобів негласного отримання інформації, характеристики каналів витоку інформації, метод тріангуляції, методика локалізації радіозакладних пристроїв, рекомендації. що до впровадження запропонованої методики локалізації.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Полягає в тому, що запропонований метод удосконалення

модулів може бути використаний для покращення пошуку виявлення витоку інформації**.**

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року.

Завдання видав _____ Олександр ЛАПТЄВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Кирило АВХИМЕНКО
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки завдання	29.10.2021 – 30.11.2021	*виконано*
2	Аналіз літератури	01.12.2021 – 31.01.2022	*виконано*
3	Обґрунтування вибору рішення	01.02.2022 – 24.02.2022	*виконано*
4	Збір даних	25.02.2022 – 01.03.2022	*виконано*
5	Виконати аналітичний огляд каналів витоку акустичної інформації	02.05.2022 – 08.05.2022	*виконано*
6	Проаналізувати принципи побудови, особливості роботи радіопристроїв прихованого знаття акустичної інформації	09.05.2022 – 29.05.2022	*виконано*
7	Удосконалення технічного модуля пошуку засобів негласного отримання інформації у мережі напруги 220 В	30.05.2022 – 04.06.2022	*виконано*
8	Розробити методику використання удосконаленого методу виявлення радіопристроїв прихованого знаття інформації.	30.05.2022 – 01.06.2022	*виконано*
9	Апробація роботи на науково-методичному семінарі	02.06.2022– 03.06.2022	*виконано*
10	Оформлення пояснювальної записки	04.06.2022– 07.06.2022	*виконано*
11	Підготовка до захисту	08.06.2022 – 13.06.2022	*виконано*

Термін подання дипломної роботи до ЕК 08.06.22.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Удосконалення модулів автоматизованих пошукових комплексів засобів негласного отримання інформації» складається зі вступу, основної частини, що містить 3 розділи, висновків і списку літератури та джерел. Загальний обсяг роботи – 50 сторінок. Робота містить 8 рисунка, 7 формули. Список використаних джерел включає 39 джерел.

Об'єкт дослідження: є технічні модулі пошуку сигналів засобів негласного отримання інформації апаратно програмних комплексів пошуку.

Мета роботи: є розробка рекомендацій щодо удосконалення технічних модулів автоматизованих програмно апаратних комплексів пошуку сигналів засобів негласного отримання інформації

Предмет дослідження: є удосконалення технічних модулів автоматизованих програмних комплексів пошуку сигналів засобів негласного отримання інформації у сеті електроживлення.

Перша глава розкриває всю сутність витоку інформації, що допомагає накреслити перші

У другому розділі проводиться класифікація закладних пристроїв негласного отримання інформації.

У третьому розділі представлено варіант удосконалення комплексу для виявлення закладних пристроїв та методи використання уже удосконаленого цього комплексу.

Результатом роботи є вироблені рекомендації щодо вдосконалення системи комплексу RS Turbo.

Ключові слова: RS Turbo, несанкціонований доступ, засоби негласного отримання інформації.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

НСД – Несанкціонований доступ

ТКВІ – Технічний каналу витоку інформації

ЛАСР – Лазерні мікрофони

ВТЗС – Допоміжні технічні засоби та системи

ТЗОІ – Технічний засіб обробки інформації

ПЕВ – Побочне електромагнітне випромінювання

ПЗ – Програмне забезпечення

ЗП – Закладний пристрій

ЗНОІ – Засоби негласного отримання інформації

ЗМІСТ

ВСТУП

Серед сьогодення інформація стала одним із найважливіших ресурсів. Її продають, купують, обмінюють, крадуть. «Хто володіє інформацією -володіє світом, а іноді інформація коштує більше ніж життя».-У. Черчіль

У вік інформатизації є фундаментальне питання на інформацію, вирубану невирішеним шляхом. Це є проблемою для організацій, обробляють інформацію у приміщеннях конторського типу. Отже, захист інформації через лиходіїв є одним із генеральних завдань. У цьому замітці оглянемо конкретніше систематизацію звукових каналів прибутку інформації.

Щоб отримати доступ до конфіденційної інформації не обмежуються діями інсайдерів та потайливим підключенням до телекомунікаційних каналів зв'язку. Непоодинокі випадки установки заставних пристроїв, що перехоплюють акустичні сигнали. Вони використовуються організаціями, що спеціалізуються на конкурентній розвідці, які пошук утруднений малодоступністю спеціального устаткування. Радіоканали витоку інформації продовжують залишатися актуальною проблемою інформаційної безпеки.

Враховуючи, що метою роботи було розробити рекомендацій щодо удосконалення технічних модулів автоматизованих програмно апаратних комплексів пошуку сигналів засобів негласного отримання інформації, для її досягнення було визначено такі завдання:

- Виконати аналітичний огляд каналів витоку акустичної інформації
- Проаналізувати принципи побудови, особливості роботи радіопристроїв прихованого знаття акустичної інформації
- Проаналізувати принципи захисту від пристроїв прихованого знаття акустичної інформації
- Удосконалення технічного модуля пошуку засобів негласного отримання інформації у сети напруги 220 В

- Розробити методику використання удосконаленого методу виявлення радіопристроїв прихованого знаття інформації.
- Надати додаткові методи захисту від пристроїв прихованого знаття акустичної інформації

РОЗДІЛ 1
АНАЛІЗ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

1.1 Класифікація каналів витоку інформації

Існують такі технічні канали витоку інформації як:

1. Акустичний канал
2. Акустоелектричний канал
3. Віброакустичний канал (телефонний)
4. Оптичний канал

У даній роботі ми детально будемо розглядати акустичний канал витоку інформації. Потрібно зазначити, що головне поширення акустичної інформації це повітря. За допогою світла відбувається ідентифікація каналу витоку інформації.

Під модуляцією видимого світла розуміється отримання акустичної інформації за допомогою обладнання, яке приймає модульований оптичний сигнал у видимому діапазоні. В модуляції видимого світла генерується мікроконтролером, який керує некогерентним світлодіодним джерелом видимого світла. Це дає можливість використовувати різні типи модуляції, наприклад аналогову амплітуду модуляція інтенсивності світла та види цифрової модуляції з точки зору тривалість та інтенсивність проходження світлових імпульсів. Технологічний перехід у створенні освітлення у приміщеннях від ламп розжарювання до високотехнологічних малоінерційних світлодіодних світильників містять контролери, створює передумови для формування новий канал витоку інформації [1,2].

Акустичний канал витоку інформації за допомогою модуляцією видимого світла розуміється як отримання акустичної інформації за допомогою обладнання, яке приймає модульований оптичний сигнал у видимому діапазоні. В модуляції видимого світла генерується мікроконтролером, який керує некогерентним світлодіодним джерелом видимого світла. Це можливо використовувати різні типи

модуляції, наприклад аналогову амплітуду модуляція інтенсивності світла та типи цифрової модуляції в термінах тривалості та інтенсивності світлових імпульсів, що проходять. Технологічний перехід у створенні освітлення в кімнатах від ламп розжарювання до високотехнологічних малоінерційних світлодіодних освітлювачів, що містить контролери створює передумови для формування новий канал витоку інформації.

1.2 Поняття технічного каналу витоку інформації

Грунтовне та повне поняття каналу витоку інформації дає закон України про розвідку. ТКВІ - являє собою сукупність об'єкта зняття інформації (вивчення, розвідки), це може бути як людина, так і комп'ютер, чи елемент архітектури комп'ютера, наприклад, клавіатури, акустичний або відеосигнал іншого походження, а також будь-якого технічного засобу, що застосовується для одержання даних, та фізичного середовища, яким поширюється інформаційний сигнал. ТКВІ подаються як спосіб одержання розвідувальної інформації. Стандарт роздивляється під цим терміном різні відомості про об'єкт, що інтересно, незалежить від того, в якому виді вони одержані та передані замовнику [3,4].

При аналізі радіоканалів витоку інформації об'єкт вбачається як акустичні дані у вигляді мови, телефонні розмови (в мобільному чи стаціонарному телефонному апараті дуже часто встановлюють прилад зняття даних) або відеозапис про діяльність людей, що цікавлять певного замовника, у визначеному помешканні чи приміщенні. Фізичним середовищем передачі сигналу є повітря. Використовуються різноманітні типи пристроїв для знімання з них даних [5].

Джерелом кожної акустичної інформації є (вхід сигналу інформації):

- людина, яка розмовляє, або звукоутворюючий пристрій, що озвучує мову людини;
- механічні вузли механізмів та машин, які створюють акустичні хвилі при своїй роботі.
- середовище поширене (перешкоди)

- повітря
- тверді тіл
- вода

Акустичний приймач (вихід сигналу інформації тобто, пристрій що приймає даний сигнал)

- гідрофон
- акселерометр
- стетоскоп
- мікрофон
- геофон

Витік будь-якої інформації за межі різних захищених структур будівель, приміщень, офісів, будинків і тд (рисунок 1.1):

1. за допомогою трансформації акустичних коливань в віброакустичні і назад.
2. за допомогою мембрамного ефекту
3. через отвори, тріщини і тд

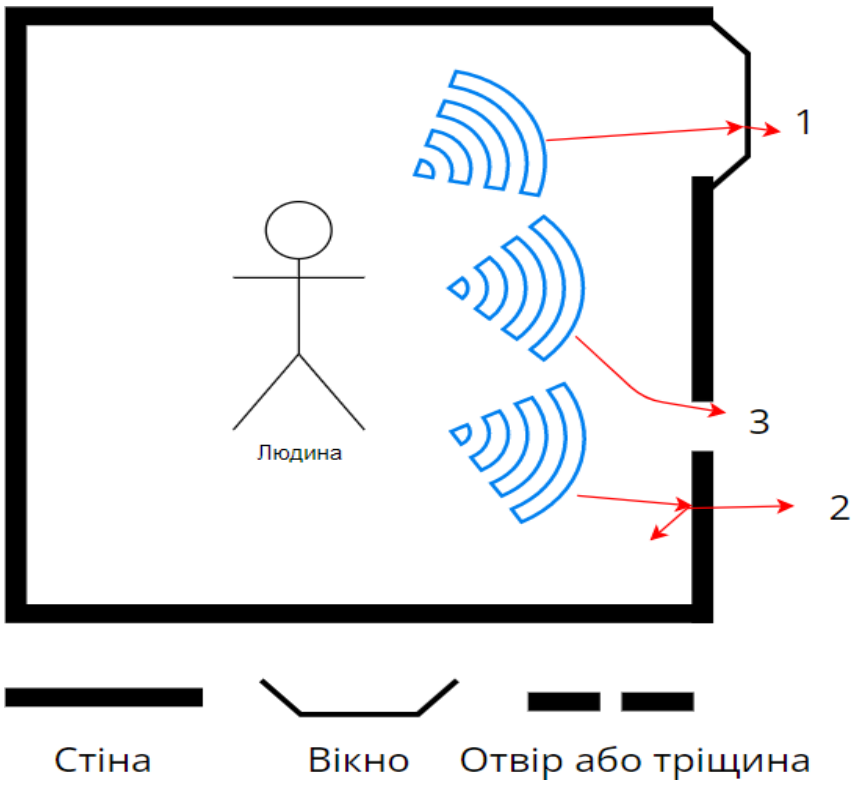

Рисунок 1.1 - Витік інформації.

Розглянемо всі перелічені канали витоку інформації з погляду на варіанти перехоплення.

У разі коли відбувається перехоплення інформації через будь-який повітряний канал витоку є можливість запису мовленнєвої інформації різними портативними приладами запису, які були таємно встановлені у певних приміщеннях. Заставні пристрої з датчиками мікрофонного типу існує можливість скрито встановити; за допомогою спрямованих мікрофонів відбувається прослуховування та запис розмов. У найближчих будівлях або транспортних засобах можуть бути встановлені спрямовані мікрофони. Основними елементами, які визначають весь вигляд та головні характеристики комплексів дистанційного перехоплення мовленнєвої інформації є саме акустичні антени. Їх основне призначення полягає саме у посиленні звуків, що приходять за основним напрямом, а також в істотному послабленні решти всіх інших акустичних сигналів. На даний час розроблено та досліджено кілька модифікацій даних антен, згідно до яких прийнято рішення класифікувати спрямовані мікрофони [6].

В разі перехоплення інформації по вібраційному каналу витоку залишається можливість прихованого прослуховування та відбувається запис розмови із прилеглих приміщень за допомогою використання електронних стетоскопів. А також можливе скрите встановлення інших заставних пристроїв з різними датчиками контактного типу, які по радіо або оптичним каналам можуть передавати інформацію.

При перехопленні важливої інформації по лазерному каналу витоку злочинники можуть використовувати опромінення шибок певного приміщення різними лазерними акустичними системами, які встановлені у найближчих будівлях або транспортних засобах. В разі необхідності перехоплення розмовної інформації з даного каналу можуть застосовуватися складні лазерні акустичні системи розвідки (ЛАСР),інша назва іх - лазерні мікрофони. Джерело когерентного випромінювання (лазера) та приймач оптичного випромінювання, що оснащений фокусуючою оптикою є складовими в ЛАСР. За для забезпечення високої механічної стійкості приймача та передавача, що є обов`язково необхідним для гарної роботи системи,

вони встановлюються на триніжних штативах. Зазвичай, у таких системах використовують лазери, що працюють у невидимому для ока ближньому інфрачервоному (ІЧ) діапазоні довжин хвиль (0,8...1,1 мкм). Принцип дії даної сис теми полягає ось у чому: вузьким лазерним променем передавач здійснює опромінення зовнішньої шибки; а приймач приймає відбите розсіяне випромінювання, яке згідно закону зміни акустичного (мовного) сигналу модулюване по амплітуді і фазі, що виникає в наслідок ведення розмов у певному, контрольованому приміщенні. Сигнал, який принятий посилюється, детектується та прослуховується на головних телефоних апаратах або записується на магнітофон. В приймачі використовують шумопригнічуючий спеціальний пристрій для покращення розбірливості мови.

Під час наведення лазерного променя на визначену ціль крім передавача і приймача застосовуються додаткові спеціальні пристрої – візири. Ці системи є найбільш ефективними під час прослуховування розмов у не великих приміщеннях, бо вони за своїми акустичними характеристиками дуже близькі до об'ємного резонатора, особливо коли всі двері та вікна приміщення досить гарно герметизовані.

В разі перехоплення інформації по акустоелектричному каналу витоку євірогідність підключення так званих спеціальних низькочастотних підсилювачів до з'єднувальних ліній ВТЗС, вони мають мікрофонний ефект, а також підключення до з'єднувальних ліній ВТЗС апаратури високочастотного нав'язування, що мають мікрофонний ефект.

Утворення будь-якого електроакустичного каналу витоку інформації пов'язане з наявністю в ТЗОІ випадкових електроакустичних перетворювачів, так звані випадкові мікрофони. Дані елементи можуть перетворювати акустичні коливання в електричні сигнали, не зважаючи на те, що не призначені для цієї мети. Елементи технічних засобів обробки інформації, що мають властивості випадкових електроакустичних перетворювачів, можуть піддаватися впливу акустичних полів з достатніми інтенсивністю і звуковим тиском [7]. Великий вплив мають акустичні

поля на елементи ТЗОІ, що може призвести до зміни положення, взаємної орієнтації або до їх деформації.

В результаті на виходах випадкових електроакустичних перетворювачів можуть, або виникнути електричні заряди, струми, або зміни параметрів напруг і струмів, що формуються в ланцюгах цих технічних засобів при їх функціонуванні, зумовлені небезпечними сигналами (скажімо, небажана модуляція). Мікрофонні особливості випадкових електроакустичних перетворювачів з'являються внаслідок різноманітних фізичних явищ, що спричиняють до появи струму або його деформації під дією акустичного поля. Індукційні (індуктивні) перетворювачі – велику групу складають випадкові електроакустичні перетворювачі. Приміром, якщо у магнітне поле, створюване постійним магнітом помістити рамку (котушку індуктивності), та змінювати її орієнтацію щодо напрямку вектора магнітної індукції поля, то на виході рамки з'явиться індукції. Під час ведення розмови в офісному приміщені, де розташовани технічний засіб повітряний поток змінної щільності може викликати переміщення рамки, що змінтьб її орієнтацію. До індуктивних випадкових електроакустичних перетворювачів належать гучномовці, електричні дзвінки, трансформатори, електромеханічні реле і т.д.

У разі перехоплення інформації на параметричному каналі витоку зловмисник використовує перехоплення ПЕВ на частоті високочастотного генератора, що входять до складу ВТСС, з мікрофонними ефектами, обладнанням, встановленим у прилеглих будівлях і транспортних засобах, а також високочастотним опроміненням ВТСС, з мікрофонним ефектом. Встановлюються в прилеглих будівлях або сусідніх приміщеннях.

Під технічним каналом витоку акустичної (голосової) інформації розуміють групи об'єктів розвідки (виділені приміщення), технічні засобу акустичної (голосової) розвідки, для перехоплення голосової інформації, та фізичне середовище, для поширення інформаційного сигналу. За фізичними властивостями інформаційног сигналу, середовищем розповсюдження та технічними каналами витоку акустичної (голосової) інформації його можна поділити на: пряму акустичну

(повітря), акустичну вібрацію (вібрація), акустооптичні (лазер), акустоелектрика та акустоелектромагнітна.

Реалізація каналу витоку акустичної інформації відбувається наступним чином:

• Підслуховування розмов на відкритих місцях і в приміщенні, поблизу або за допомогою спрямованих мікрофонів (іноді параболічних, трубчастих або плоских). Направленість 2-5 градусів, найпоширеніший середній діапазон – трубчастого – близько 100 метрів. За хороших погодних умов на відкритих місцях параболічні спрямовані мікрофони можуть працювати на відстані до 1 км;

• Приховати записи розмов на диктофонах або магнітофонах (включаючи цифрові диктофони, активовацією голоса);

• Підслуховування розмов за допомогою віддаленого мікрофона (діапазон радіомікрофонів 50-200 метрів без ретрансляторів).

Мікрофони, що використовуються в радіозакладках, можуть бути вбудованими або дистанційними і мають бути двох типів: акустичні (переважно чутливі до дії звукових вібрацій, призначені для перехоплення коливань повітря і призначені для перехоплення голосових повідомлень) і вібраційні (перетворюють вібрації, що виникають у різних жорстких конструкціях, у електричні сигнали).

1.3 Акустоелектричний канал

1. Акустоелектричний канал витоку інформації, його характеризується:
2. Підходячий у використанні (електромережа всюди);
3. Немає проблем з живленням мікрофона;

Перспектива отримання інформації через електромережі без підключення до неї (це можливо завдяки електромагнітному випромінюванню електромережі). Вся інформації, що надходить від так званих «жучків» надходить через спеціальні приймачі, підключені до електромережі в радіусі до 300 метрів від «жучків» по всій довжині проводки або до любого силового трансформаторного комплексу чи будівлі, що обслуговує будівлю [7].

При використанні електромережі для передачі інформації можливі перешкоди для роботи побутової техніки, а також при наявності великої кількості побутової техніки буде погана якість переданого сигналу.

Висновки до 1 розділу

Таким чином, відкривається дуже великий спектр різних заходів щодо захисту інформації при її обробці та захисту приміщень офісного типу для запобігання. Всі вище розглянуті канали витоку ми не можна залишати без уваги. Вся інформація передається переважно електормагнітним або звуковим полем. Тому для можливості забезпечення необхідного рівня захисту у приміщеннях офісного типу треба мати канали витоку інформації та розуміти наявні відомі вразливості [8,9].

РОЗДІЛ 2
ПРИНЦИПИ ПОБУДОВИ, ОСОБЛИВОСТІ РОБОТИ РАДІОПРИСТРОЇВ ПРИХОВАНОГО ЗНАТТЯ АКУСТИЧНОЇ ІНФОРМАЦІЇ

2.1 Загальні відомості про пристрої знімання інформації

Ринок спеціалізованих технічних засобів пропонує кілька видів пристроїв негласного перехоплення даних. Майже всі вони обмежені в обороті, законно купувати їх можуть організації, що мають ліцензію. Стаття 359 кримінального кодексу, що передбачає відповідальність за незаконний обіг технічних засобів, призначених для потайного отримання інформації. Закон розуміє під ними "комплекси, пристрої, спеціальні інструменти для проникнення в приміщення та ПЗ для доступу та отримання інформації, яким навмисно надано властивості для забезпечення функції прихованого отримання інформації або доступу до неї без відома її власника". До цього типу належать пристрої, призначені для зняття інформації з радіоканалів витоку. За купівлю, застосування чи продаж такого обладнання можна позбутися волі до 4 років [10,11].

Цікаво, що законодавець відносить до цієї категорії побутові диктофони, відеокамери, прилади геолокації, якщо їм шляхом доопрацювання надані властивості, що дозволяють негласно збирати інформацію. Те саме стосується ПЗ, що контролює поведінку користувача за комп'ютером. Якщо воно має індикацію, що дозволяє встановити його наявність та включення, використання дозволено. Якщо при доопрацюванні індикація знята і ПЗ працює потай для користувача — воно потрапить до категорії шпигунських програм [12].

При використанні радіоканалів застосовуються пристрої для зняття акустичної інформації різних типів. З погляду технічного виконання вони виробляються як окремий модуль у формі паралелепіпеда або камуфлюються під предмети побуту або офісну канцелярію: калькулятор, лампочку, вазу, годинник. У практиці зустрічалися випадки, коли радіозакладка вшивалася в обруч, який утримував на

голові арабську чоловічу хустку — арафатку. Розмір закладки може бути мінімальним — з горошину, але дальність передачі скоротиться до кількох десятків метрів, а працюватиме вона 3—4 години [13,14].

Акустичні закладки можна класифікувати за видом виконання, місцем установки, джерелом живлення, способом передачі інформації та її кодування, способом управління, на аналогові та електронні. Насамперед вони класифікуються за діапазоном радіохвиль [15]:

- HF (ВЧ) - декаметрові хвилі;
- VHF (ОВЧ) – метрові хвилі, у ньому зазвичай працюють нестабілізовані закладки;
- UHV (УВЧ) - дециметрові хвилі;
- SVF (GHz) – сантиметрові хвилі.

Від вибору діапазону залежить схованість роботи пристрою. Найчастіше використовуються пристрої, що працюють у діапазонах 88-108 МГц; 108-174 МГц; 400-512 МГц; 1100-1300 МГц.

Наступний тип класифікації – за потужністю випромінювання. Розрізняються пристрої малої потужності (до 10 мВт), середньої (10-100 мВт), високої (більше 100 мВт). Чим більша потужність, тим більшій відстані можна встановити пристрій прийому сигналу.

Класифікація по виду сигналів підрозділяє пристрої на моделі з простими сигналами (AM-, NFM-, WFM-модуляція), їх легко розшифрувати при перехопленні, і зі складними (шумоподібні, створювані за допомогою псевдовипадкової фазової модуляції, іноді використовуються аналогове скремблювання, що робить мова нерозбірливим. , перетворення на цифровий вигляд, кодування з псевдовипадковою перебудовою несучої частоти). При перетворенні акустичного сигналу на цифровий вигляд може проводитися його подальше шифрування.

По виду модуляції сигналу радіозакладки розрізняються ті, де модулюється основна, і ті, де модулюється проміжна частота. Для модульованого сигналу потрібні спеціальні приймачі. При спробі прослуховування його на звичайному мова сприйматиметься у вигляді нерозбірливого шуму. Широкосмугова модуляція

вимагає кварцової стабілізації частоти, такий сигнал може передаватися на далекі відстані.

За типом стабілізації частоти вони можуть працювати в м'якому каналі (нестабілізовані) і в жорсткому - зі схематичною або кварцовою стабілізацією частоти. Нестабілізовані змінюють частоту передачі довільно, залежно від переміщення всередині приміщення, але перевагою стає можливість виконання в міні-форматі. Приймачі для них повинні мати автоматичне підстроювання частоти або широку смугу фіксованих частот, що суттєво обмежує дальність передачі сигналу. Кварцова стабілізація дозволяє зберігати передавальну частоту, такі передавачі часто носять як годинників, гудзиків, інших аксесуарів.

Закладки можуть бути автономними, запитуватись електроенергією від батарей або акумуляторів, або прив'язаними до наявної у приміщенні мережі, які отримують енергію від телефонних мереж, мереж електроживлення, джерел живлення комп'ютерів та іншого обладнання, в яке вони монтуються. Автономний пристрій обмежений часом роботи: залежно від розміру та ємності акумулятора, він діятиме нетривалий час – від двох-трьох годин до кількох днів. Зовнішні джерела живлення забезпечують потужність ЗП до 100 мВт і вище, що гарантує передачу радіосигналу на відстань до кількох кілометрів.

Прості пристрої, що використовують передачі даних радіоканали витоку інформації, немає модуля управління, вони включаються автоматично, при підключенні до електроживлення. Це неефективно, оскільки час роботи може витрачатися на періоди мовчання, дороги, знаходження в приміщенні, що екранується. У складніші пристрої впроваджуються реле управління, вони включаються від голосу. У тиші вони працюють лише на прийом, при фіксації початку розмови пристрою розпочинають передачу сигналу. Такий алгоритм дій кілька разів збільшує час роботи автономного передавача.

У складніших моделях використовується дистанційне управління, оператор включає обладнання, перебуваючи на відстані від нього. Передача сигналу управління зазвичай відбувається в УКХ-діапазоні, щоб уникнути ризику фальш-спрацьовувань сигнал кодується. У межах дистанційного керування можлива зміна

режиму роботи та частоти передачі. Керовані ззовні радіопередавачі мають більші розміри, ніж нестабілізовані міні-пристрої, вони зазвичай ховаються у предметах інтер'єру.

Щоб знизити ризик виявлення демаскирующих сигналів, використовуються заставні пристрої, у яких етапи прийому та передачі інформації розділені за часом.

Пристрій складається з:

- цифрового накопичувача інформації;
- приймача сигналів керування;
- передавача, що дозволяє надсилати дані прискорено.

Приймачі для таких пристроїв мають спеціальний функціонал, накопичувачі для прийому інформації та відтворюють її в нормальному режимі.

Пристрої з функцією стиснення даних записують розмови протягом тривалого часу, для цього потрібен мінімальний струм, тому виявити їх зміни напруги в мережі електроживлення складно. Після заповнення накопичувача або сигналу дистанційного управління вони передають дані в стислому вигляді, і час передачі часто не перевищує декількох секунд, що також ускладнює їх виявлення. Виявити такі прилади можна лише у момент передачі. У своєму пристрої вони не мають напівпровідників, їх не можна знайти за допомогою нелінійних локаторів.

В окрему категорію виділяють ЗУ, що поєднують мікрофон та відеокамеру, вони одночасно передають звук та картинку. Зазвичай вони мають досить великі розміри, акустичний сигнал, що передається, модулюється.

Викривати закладні прилади можливо дякуючи особливим дослідженням (зоровий огляд без підтримки технічних механізмів) та особливим перевіркам (із застосуванням технічних механізмів) об'єктів ТЗПІ, а також відокремлених приміщень.

Задля маніфестації закладних пристроїв застосовують:

1) пасивні методи:

встановлення механізмів та систем маніфестації лазерного випромінювання (віконне підсвітлення скла);

встановлення постійних детекторів диктофонів;

пошук закладних приладів при використанні показчиків поля, інтерсепторів, частотомірів, а також сканувальних радіоприймачів і програмно-апаратних комплексів контролю;

влаштування радіоконтролю (безперебійно чи під час здійснення конфіденційних клопотів) другорядних електромагнітних випромінювань технічніх методів отримання, обробки, зберігання, а також передача інформації;

2) активні методи:

особливий контроль ізольованих приміщень під час застосування нелінійних локаторів;

особливий контроль ізольованих приміщень, технічні засоби приймання, обробки, а також зберігання і передачі інформації під час застосування рентгенівських структур.

2.2 Пристрої знімання інформації з телефонних мереж

Цей тип ЗП має особливості, джерелом витоку стає телефонна лінія, і канал має характер віброакустичного. Пристрої знімання інформації та її передачі автономні, територіально відокремлені друг від друга. Приймач знаходиться в телефонному апараті, передавач розміщується поза межами приміщення, це ускладнює пошуки. Якщо передавач розміщений у корпусі традиційного апарату, як мікрофон використовується телефонна трубка. Прийом і передача даних починаються в момент знімання трубки, але іноді зустрічаються ЗП з функцією запису та наступної трансляції, відносно великі розміри виключають їхнє часте використання. Передані дані кодуються з використанням різних алгоритмів [15].

Несанкціонований доступ (до інформації) НСД — доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

Закладний пристрій — елемент засобу (системи) негласного знімання інформації, що потайно впроваджується (закладається або вноситься) в місця можливого знімання інформації (в тому числі в огорожу, конструкцію, обладнання,

предмети інтер'єру, транспортні засоби, а також технічні засоби та системи обробки інформації).

Програмна закладка — потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері.

2.3 Мікрофони

Усі акустично інтелектуальні підходи для агентури в основному використовують різні типи та призначення мікрофонів та іншого допоміжного обладнання. Першочерговими параметрами для мікрофону є: частотна характеристика, чутливість, притаманний рівень шуму, а також характеристики спрямованості [16, 17].

При номінальному навантаженні чутливість визначається відношенням напруги U при виході мікрофону до звукового тиску p на вході під час номінального завантаження:

$$E = \frac{U}{p}, \tag{2.1}$$

Чутливість мікрофону характеризується частотою акустичного сигналу так як, від неї напряму залежить внутрішній опір. Для знаходження опосередкованої чутливості вноситься поняття середньоквадратичного значення в діапазоні номінальних частот.

Рівень чутливості – чутливість, яка виражена у децибелах відносно величини $1\frac{В}{Н/м}$.

Дистанційний фіксований рівень чутливості це є відображення Uн взаємозв`язок у номінальному навантаженні Rн та тиску, який завдається звуком кратному 1 Па=$1\frac{Н}{м}$ відносно напруги U, відповідному потужності p_0 =1мВт. Частотною характеристикою називається залежність рівня чутливості від частоти.

Характеристика напрямку полягає у тому, що чутливість мікрофону залежить від кута поміж працюючою віссю мікрофону (спрямованість найбільшої чутливості мікрофону) та спрямованістю джерела звуку. Дану характеристику розкривають задля частотної смуги. Нормовані характеристики ознаки, тобто, залежності співвідношення чутливості E_q, яка вимірюється під кутом q, відносно осьової чутливості E_0 розкривається виразом:

$$R_{(q)} = \frac{E_q}{E_0}, \tag{2.2}$$

Більша чисельність мікрофонів мають осьову симетрію. За допомогою характеристик спрямованості мікрофони, котрі застосовуються для акустичної розвідки діляться на такі групи: спрямовані (односпрямовані) та гостроспрямовані. Під діаграмою спрямованості розуміють графічне представлення характеристик спрямованості, які неодноразово відображають у полярних координатах.

Коефіцієнт спрямованості G – це співвідношення квадрату осьової чутливості мікрофону у вільному полі E_0 відносно середньоквадратичної чутливості за всіма радіальними напрямками E_{qs}:

$$G = \frac{E_0}{E_{qs}}, \tag{2.3}$$

Його спеціально визначають для смуги частот.

Особистий рівень шуму мікрофону L, приведений до акустичного входу визначається рівнем еквівалентного звукового тиску $P_{\text{ш}}$, за допомогою якого при впливі на конкретний мікрофон вийшла би вихідна напруга, яка дорівнює вихідній напрузі мікрофону $U_{\text{ш}}$, що зростає за відсутності звукових коливань:

$$L = 20\lg(P_{\text{Ш}}/P_0), \tag{2.4}$$

де $P_{\text{Ш}}$=$U_{\text{Ш}}/E_0$; E_0 – осьова чуттєвість;

P_0= 2*10^{-5} Па.

За принципом електромеханічного перетворення всі мікрофони поділяються на такі групи:

- електродинамічні;
- електростатичні;
- електромагнітні;
- релейні.

За конструкцією механічної системи електродинамічні мікрофони поділяються два види: котушкові (динамічні) і стрічкові [16]. Електростатичні мікрофони існують таких видів: конденсаторні (в тому числі електронні), п'єзо мікрофони. Електромагнітні поділяються на односторонні та диференціальні. А релейні в свою чергу поділяються на транзисторні та вугільні.

За акустичними характеристиками мікрофони поділяються на: приймачі тиску, приймачі градієнту тиску, групові і комбіновані.

Основною рисою приймача тиску є його «діафрагма», яка може знаходитись під впливом звукових тільки з одного боку.

Обидві сторони приймача градієнта тиску мають рухому механічну систему, відкриту для звукових хвиль, через це на неї впливає різниця тисків хвиль, що падають на передню частину поверхні діафрагми, яка огинає її задню сторону.

Для отримання різних форм характеристик спрямованості зазвичай комбінують приймачі тиску та градієнт тиску.

Динамічний мікрофон має котушку, яка знаходиться в магнітному полі кільцевого магніту, а також жорстко пов`язана з діафрагмою.

Конденсаторний мікрофон уявляє собою конденсатор, в середині якого є один із елементів наймасивніший, а другий – тонка натяжна мембрана. Під час коливання мембрани місткість конденсатору змінюється, а заряд q не змінюється (конденсатори в колі постійного струму з високим опором навантаження $R_{\text{н}}$ розряджатися не встигає). В результаті напруга на конденсаторі змінюється відповідно до виразу:

$$i = C\frac{du_c}{dt}, \quad (2.5)$$

З протидією навантаження знімається напруга.

В електронному мікрофоні поляризуюча напруга, утворена попередньою електризацією одного з електродів, які виготовляються з полімерів чи з керамічних поляризованих матеріалів. Даний електрод має металеву поверхню, яка є електродом конденсатору, електрет є джерелом поляризованої напруги. Через зниження поляризації електрета через деякий час необхідно або його замінити, або повторно його поляризувати за кілька років. За характеристиками даний мікрофон ідентичний конденсатному, але не потребує джерела напруги.

Для п`єзомікрофонів використовується явище п`єзоефекту. Під час деформації пластинки, виготовленої з кварцу або п`єзокераміків (барій, титан чи ін.) вони поляризуються, тобто концентрується заряд на площині. П`єзомікрофонам не потрібні джерела живлення оскільки вони відносяться до електростатичного типу мікрофонів. Дані мікрофони мають схожі властивості з електретними мікрофонами.

2.4 Спрямовані микрофони

Спрямовані мікрофони насамперед предназначені для акустичного контролю різних джерел звуків на відкритому просторі. Вирішальним фактором в таких випадках є відстань джерела звуку від спрямованого мікрофона, що призводить до значного ослаблення контрольованого звукового поля (крім того, на великій відстані звук стає значно менш когерентний через порушення простору внаслідок наявності природної атмосферної турбулентності, що утворюють перешкоди за наявності вітра) [17].

Тому, на відстані 100 м звуковий мінімум зменшується мінімум на 40 дБ (порівняно з дистанцією 1 м), в такому випадку гучностб звичайної розмови в 60 дБ не буде вищою 20 дБ в точці прийому. Даний тиск буде суттєво меншим не тільки за рівень фактичних навколишніх акустичних перешкод, але й меншим від порогової акустичної чутливості звичайних мікрофонів.

Спрямовані мікрофони на відміну від звичайних мають мати [17]:

Високу порогову акустичну чутливість, що дозволяє ослабленому звуковому сигналу перевищувати рівень власного (переважно теплового) шуму приймача. Це необхідно для контролю звуку на значній відстані від джерела, навіть коли відсутні навколишні акустичні перепони.

Типи спрямованих мікрофонів. Наразі виділяють чотири типи спрямованих мікрофонів [17]:

1) параболічні;

2) плоскі акустичні фазовані ґрати;

3) трубчасті, або мікрофони хвилі, що "біжить";

4) градієнтні.

Всі параболічні мікрофони складаються з відбивача звуку параболічної форми(увігнута параболічна тарілка), у фокусі якого розташований звичайний (ненаправлений) мікрофон. Відбивач може бути виготовлений з оптично прозорої та непрозорої сировини.

Розмір зовнішнього діаметра параболічного дзеркала коливається в межах від 200 до 500 мм. Принцип дії даного мікрофону трактується на рисунку 2.1:

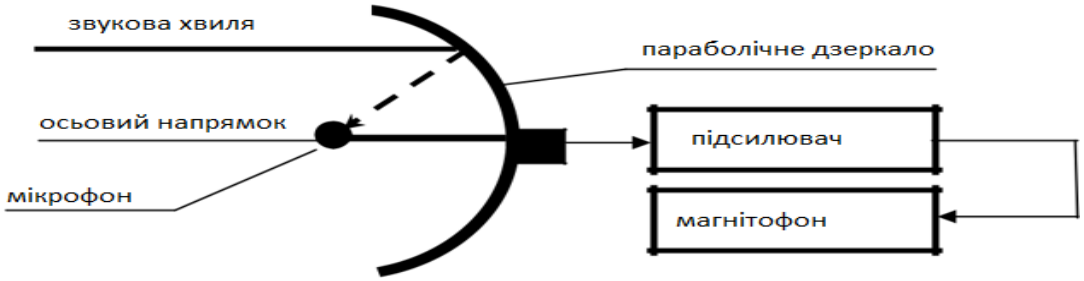

Рисунок 2.1 - Параболічний мікрофон.

Всі звукові хвилі, що надходять з осьового напрямку, відбиваються від параболічного дзеркала та в підсумку сумуються по фазі у фокусі . Завдяки цьому ефекту збільшується звукове поле. Більше посилення мікрофону характеризується більшим діаметром дзеркала. Посилення мікрофона буде зменшено тоді, коли направлення звукових хвиль буде не по осі, і тоді приплюсовування звукових хвиль,

котрі відбиваються від різних частин параболічного дзеркала в точці А, зміщуються по фазі. Чим більший кут звуку відносно осі, тим більше загасання. Зразком високочутливого мікрофону являється параболічний мікрофон, який є слабко спрямованим мікрофоном. Плоскі фазовані решітки надають можливість одночасного приймання звукового поля в перивистих точках у площині, яка перпендикулярна спрямованості джерела звуку (рисунок 2.2).

Трубчастий мікрофон має звуковід у вигляді шерехатої пустотілої трубки діаметром 10-30 мм із особливими щілинними порами, з коловою геометрією місцезнаходження окремо для всіх рядів, а також розташуванням їх упродовж всієї осі звуководу. З огляду на рівність темпів осьового розповсюдження звуку всередині та поза трубкою, вторгнення у звуковод крізь всі розщелини отворів відбуваються під час отримання звукової хвилі з осьового спрямування, в результаті чого здійснюється додача у фазі сигналів. Вразливість прийому спадає тоді, коли звук доходить під певним кутом до осі мікрофону, що зумовлене нерівномірністю тривалості шляхів розповсюдження звукових хвиль та фазового різнобою. Здебільшого довжина трубчастого мікрофона коливається від 15-230 мм до 1 м. З бокових та зворотніх шляхів сильніше придушується чутливість мікрофону, за умови його більшої довжини (рисунок 2.3).

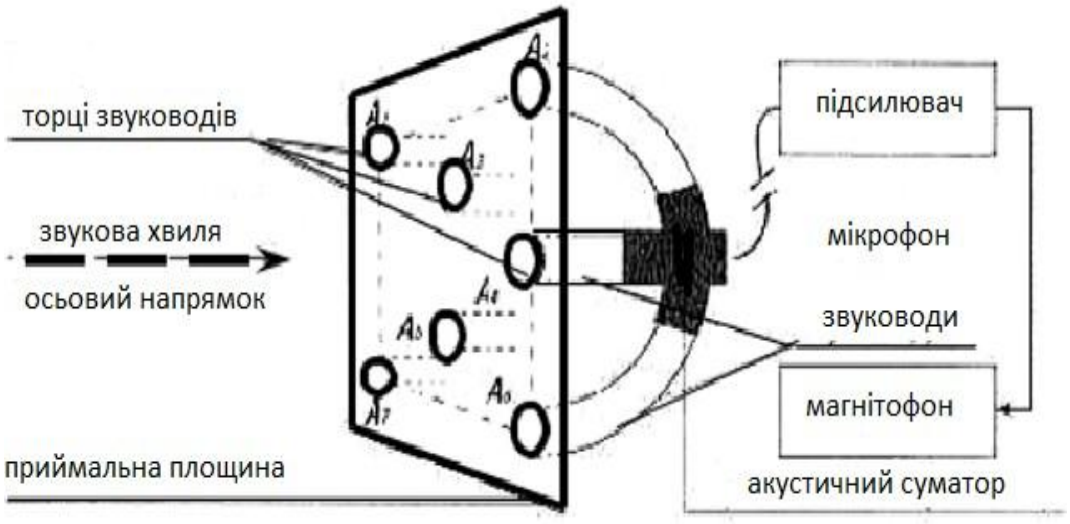

Рисунок 2.2 - Плоскі фазовані грати.

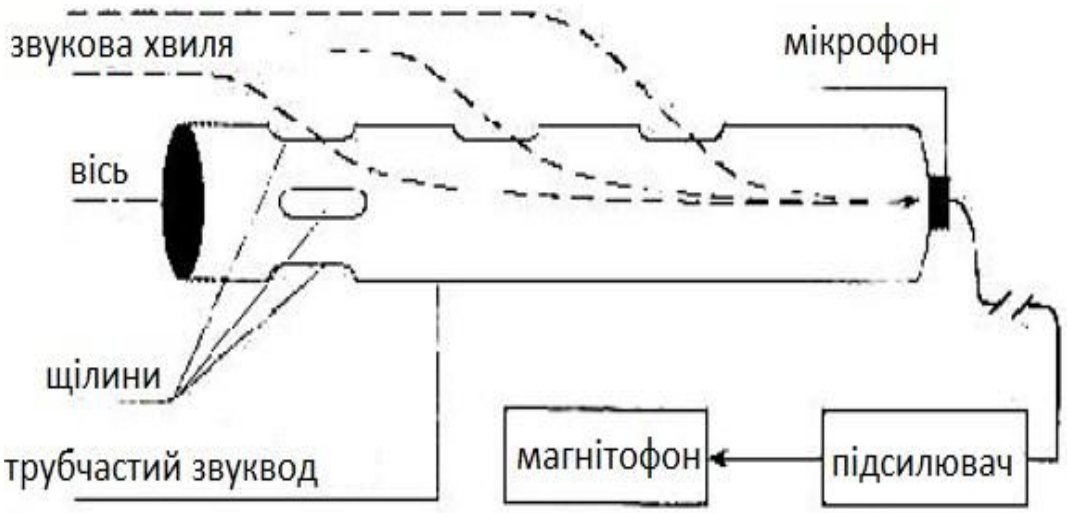

Рисунок 2.3 - Трубчастий мікрофон.

Спрямований мікрофон «СУПЕР ВУХО-100», який є частиною монокуляру, надає 8-кратне збільшення [18]. Створенню вузької діаграми спрямованості мікрофону слугує параболічний відбивач. За допомогою диктофону, який є вбудованим в сам мікрофон, може відбуватись запис вродовж 12 сек. Дія мікрофону розповсюджується на дистанцію до 100 м, а батарея зразку «Крона» надає йому живлення. Також разом з мікрофоном комплектуються навушники. Напрявлений мікрофон, який є професійним та над якісним приладом, який використовується за для прослуховування, а також для запису всіх сигналів звуку з віддалених об'єктів називається «Yukon» [19]. Встановлення мікрофону на усталений штатив відбувається за допомогою штативного гнізда ¼ дм.

В даному мікрофоні є витончену діаграму спрямованості, яка має назву супер-кардіоїд. Високочутливий конденсаторний мікрофон "Yukon" дає можливість вловити звуки на дистанції до 100 м, а також він зроблений за допомогою нової технології.

Даний пристрій може неперервно працювати впродовж 300 годин завдяки вбудованому автономному живленню. Від потоків повітря, які створюють непотрібний фон, захищає результативний вітрозахист. Впервину була прийнята до

реалізації ідея синхронного акустичного, а також візуального підконтролю при природній нічній ясності за об'єктами, які розміщені на великій дистанції відносно спостерігача та називається пристроєм нічного бачення зі спрямованим мікрофоном NVS 2,5×42 [20].

На основі електронно-оптичних перетворювачах стартового покоління в даному пристрої застосовується оптична схема. Досить висока якість зображення надається за допомогою світлосили і кратності (2,5), які є оптимально розрахованими. Вночі відео та фото зйомка відбувається завдяки вбудованому фотоадаптеру. Під час цілковитої темряви є змога проводити спостереження за допомогою потужного освітлювача ІЧ. Прослуховувати, а також записувати різноманітні звукові сигнали на дистанції до 100 м можна завдяки спрямованому мікрофону.

Ключові системи, портативні диктофони та електронні стетоскопи.

В залежності від потенційного доступу до підконтрольних місць обираються засоби акустичної розвідки.

Незалежно від типу усі мікрофони користуються діапазон чутливості в межах від 6 до 10 мВ/Па та дають можливість реєструвати на нормальній відстані у 10-15 м голос людини нормальної гучності, а деякі з них – аж до 20 м за частотного діапазону від 100 Гц до 20 кГц.

За можливості неперервного проникнення до підконтрольних приміщень, в них наперед є моливість встановлення мініатюрних мікрофонів, лінії транспортування сигналів котрих зводиться в спеціально для цього призначеномму приміщенні, в якому перебуває зловмисник та встановлена аппаратура, котра все реєструє. 5000 м може сягати протяжність лінії передачі сигналу. Дані системи називаються провідними [21].

Мікрофони маскуються під розбіжні предмети з метою гарантування їх прихованості, а також спеціально випускаються у надмініатюрному виконанні, їх діаметр може сягати менш ніж 2,5 м.

За допомогою забезпечення підключення мікрофонів підсилювачем можливе збільшення їх чутливості, а для поліпшення якості переловлених розмов мікрофони установлюються поблизу місць розмов.

Як апаратуру для реєстрування можуть застосовуватись диктофони і мікрофони, які мають досить тривалий час запису (16 годин). На даний час все з більшою частотою застосовуються магнітофони цифрового зразку тому, що вони дають можливість покращити якість запису та його прихованість.

Цифровий безкінематичний магнітофон U-7102

Кодер V-16 в апараті застосовується за для трансформації в цифровий потік мовного каналу [22]. В ускладених акустичних умовах певний алгоритм уможливлює одержувати велику якість мовної інформації, а також дає можливість досить тривалий час поза використанням програмного стиснення записувати всю інформацію.

В умовах встановлення незмінних акустичних препон, за умови роботи систем приглушення роботи диктофону, магнітофон має одну з пореваг в тому, що надає високий рівень запису інформації. А також його іншими перевагами є: програмне видалення отриманох інформації; змога програмного перетворення записаної інформації до стандартного WAV-файлу.

Можливість зв`язку з комп'ютером надає блок відображення певних мікрофонів.

Програмне забезпечення, яке використовується для керування відображенням, дає можливість для: в обраному прослуховуваному файлі одразу одержати доступ до всіх обраних в минулому отриманих та записаних частин розмови; розподілити записані розмови за певними особливостями, наприклад: час початку, тривалість, номер каналу із одним з мікрофонів для прослуховування; виділяти та копіювати в новий файл як цілком розмови, так і окремі фрагменти вибірково, а також в будь-якій послідовності; переписувати отримані фрагменти файлів на різноманітні носії. Еквалайзерами називають різноманітні пристрої особливого призначення з набором відмінних пристроїв таких, як: фільтрів верхніх і нижніх частот, смугових, основних і т.п.

Відповідно до характеру викривлень сигналу та перепон, дані фільтри вмикаються за певної програми і надають можливість усунути ці перешкоди.

Разом з спеціальнми програмно-апаратними комплексами застосовуються еквалайзери за для збільшення розбірливості мови. Найчастіше такі комплекси складаються з:

- Прилада введення/виведення мовних сигналів, які включають АЦП і ЦАП;
- Плати спеціалізованого сигнального процесора, функція якого полягає в здійснені процедури обробки різних мовних сигналів в реальному маштабі (наприклад шумоприглушення);
- Пульта керування;
- Персонального комп'ютера;
- Програмного забезпечення та прилади.

Електронні стетоскопи, які трасформують акустичні коливання в різних твердих тілах (стеля, підлога, стіни, труби) в електричні сигнали застосовують для накопичення збору мовної інформації в разі неможливості пробратися в контрольоване приміщення, але маючи спроможність проникнути в суміжне приміщення, Контактний мікрофон (в основному на базі п'єзоелементу) об'єднаний з підсилювачем являється однією з основних, чутливо. частиною в електорних стетоскопах.

Стетоскоп - це датчик вібрації, підсилювач і навушники. Наприклад розмір пристрою DTI становлять 2,2 × 8 см. Такими пристроями можливо прослуховувати діалоги через стіни товщиною до 1 м. Можливе оснащення стетоскопу радіо, дротовим чи інакшими видами каналів передачі інформації. Пріоритетом стетоскопа вважається проблематичність виявлення його при встановленні в суміжних кімнатах. Існують стетоскопи, до складу яких входять: підсилювач та чутливий елемент, а також радіопередавач і дані стетоскопи мають спільний корпус. Зразком даного пристрою є стетоскоп АТ-50. Даний стетоскоп надає можливість передавати інформацію через повітря, а також прослуховувати розмови крізь стіни, двері та вікна. Він задовольняє досить хорошу розбірливість, а також надвисокий рівень чутливості. Віддаленість його передачі може сягати до 100 м, а несуча частота є

встановленою на 470 МГц. Задля оцінки віброакустичного захисту конструкцій будівель застосовується так званий стереофонічний стетоскоп марки СС 021.

Датчики таких стетоскопів мають вразливість не менш ніж 10–5 г [23].

Через беттоні товщиною 50-100 см всі новітні електронні стетоскопи спроможні реєструвати слабкі звукові коливання (шуршання, тікання годинника) завдяки наявності коефіцієнта посилення 30 000 [16].

2.5 Радіомікрофони

Радіозакладки мікрофонного типу працюють на основі перетворення акустичного сигналу в електричний за допомогою мікрофона і передачі його по радіоканалу на приймальний пристрій. Цей пристрій для прослуховування став найпоширенішим завдяки своїй простоті та невисокій вартості. Автономні джерела живлення, електричні та телефонні мережі можуть використовуватися як джерела живлення.

Мікрофон, який може сприймати акустичні вібрації бесіди людей перетворює їх в електричні сигнали;

Радіопередавач, який отримує електричні сигнали від мікрофона та передає їх по радіоканалам на приймач, дозволяючи при цьому зловмиснику отримувати повний вміст розмови;

Осередок живлення радіопередавача, що обумовлює максимальний інтервал неспинної роботи радіозакладки.

Дальність дії будь-якого радіоканалу обумовлена радіопередавачем, межі ж акустичної чутливості (до 20-30 м) – мікрофоном. З огляду дальності дії передавача основними показниками явдяються стабільність несучої частоти, потужність, різні типи модуляції та діапазони частот.

За конструкцією радіозакладки бувають простими і працюють в основному із амплітудною або частотною модуляцією як прості передавачі. Водночас радіозакладки трапляються дуже складними (до складу яких входять прилади для дистанційного керування, а також для автоматичного включення за особливих умов,

комплекси накопичення інформації та передаванням її недовготривалими серіями на досить великих швидкостях тощо. В різноманітних ситуаціях необхідна постійна модель, яка забезпечується присутністю досить великої кількості варіацій моделей радіомікрофонів. Радіозакладка, приєднана до будь-якої телефонної лінії, використовує її як джерело живлення та як антену. Окремі з них допускають прослуховувати і телефонні розмови і навіть бесіди в кімнаті, де встановлений телефонний аппарат. Навіть коли трубка телефона вимкнена телефонний капсуль передає сигнал по мережі за рахунок впливу звукових хвиль під час розмови. В момемент коли хтось піднімає трубку включається режим запису та прослуховування телефонної бесіди.

Дані закладки практичні так, як надають можливість прослуховувати, як телефон, так і квартиру, навіть не потрапляючи в неї, за допомогою підключення закладки до телефонної лінії назовні будівлі. Вони під'єднуються за паралельною схемою до телефонної лінії. Час роботи закладного пристрою майже не є обмеженим так, як вона живиться від телефоної лінії.

2.6 Гідроакустичні датчики

Коли звукові хвилі проходять через воду вони майже не послаблюються. Даний принцип використовують для реєстрації їх, використовуючи рідину в системах водопостачання та каналізації. Всю цю інформацію можливо одержати всередині будівлі, але діапазон прослуховування буде значною мірою залежати від рівня шуму, особливо в системах водопостачання. Ефективніше використовувати гідролокатор, встановлений в батареї в кімнаті для прослуховування.

2.7 Іч-передавачі

Інфрачервоний канал використовується для підвищення конфіденційності передачі голосової інформації. Напівпровідникові лазери в основному застосовуються як передавачі звуку для мікрофонів.

Наприклад, прилад ТРМ-1830. Дальність діяння вдень – 150 м, а вночі – 400 м, час безперервної роботи до 20 годин. Розмір не повинен перевищувати 26×22×20 мм. Потреба прямої видимості від передавач до приймача та впливу перепон на якість передавання сигналів, являється недоліком даної системи. Можливість підвищення конфіденційності інформації, можливо за використання мікрохвильових каналів з діапазоном понад 10 ГГц.

Випромінювачі, виготовлені на діодах Ганна, можуть мати дуже невеликі розміри. До переваг такої системи відносяться: простота, брак перешкод та нестача ефективних серед сьогодення способів контролю. До недоліків можна віднести потребу в прямій видимості, хоча і в меншій мірі, оскільки мікрохвильові сигнали все ще можуть обходити невеликі перешкоди і проходити, незважаючи на тонке ослаблення, через тонкі діелектрики, такі як штори на вікнах.

Висновки до 2 розділу

Інформація є досить своєрідним продуктом. Згідно закону України «Про інформацію», усі задокументовані чи оголошені публічно відомості про явища та події, котрі трапляються у навколишньому середовищі або державі чи суспільстві трактуються поняттям «інформація». Встановлення та приведення в дію спільних для всіх норм, котрі скеровують взаємини стосовно реалізації дозволу на інформацію розбіжних суб`єктів та держави, порядок охорони інформації як предмету відносин недосяжно реалізувати за відсутності певних меж, котрі розкривають галузь інформації як об`єкта права та вимагають належним чином брати до уваги загрози для її існування [24].

Відомий науковець Гарвардського університету А. Еттінгер з початку XX століття, а саме 80-х років, підкреслив наступне: насувається час, за якого інформація виступає наперед серед усіх можливих ресурсів, доступних людству, таким чином відносно нього мають формулюватись такі самі складні та переломні питання, як: кому вона належить, хто має користь від цього (як в поганому, так і в

хорошому сенсі), її доступність для кожного, а також чи є можливим корисне та результативне її використання в будь якому часі [25,26].

На сьогоднішній день інформація є чи не найнеобхіднішим ресурсом для всього людства, за допомогою якого можливе з`єднання його всього в інформаційну систему, яка б була єдиною для всіх інших систем (соціальна, суспільна, технічна і т.д.).

Захист інформації в будь якій системи державної або приватної це нагальна потреба сучасного функціонування будь-якого підприємства. Вибір конкретних засобів захисту залежить від цінності інформації, але щоб зрозуміти як захистити свою інформацію потрібно знати як працює метод нападу. Тому при виборі засобів захисту слід оцінити реальні можлівисти закладних пристроїв. Звичайно викоростаня такого обладнення має уголвну кару. За Статтею 359. Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації [27,28].

Предмет злочину - це спеціальні технічні засоби негласного отримання інформації [29].

Караються такі дії штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк.

Ті самі дії, котрі були вчинені повторно або за попередньою змовою групи осіб, караються позбавленням волі на строк від чотирьох до семи років.

Тому, звичайно, зловмисник має подумати тричі, аніж застосувати дане обладненя. Також перешкодую стане ціна та час, котрий був витрачиний зловмисником на встановку закладки.

Маючи план атаки на інформацію ми можемо використовувати різні підходи та методи захисту до неї.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ МОДУЛІВ ПОШУКУ ЗАКЛАДНОГО ПРИСТРОЮ

3.1 Удосконалення технічного модуля пошуку засобів негласного отримання інформації у мережі напруги 220 В

Для вирішення поставленого технічного завдання – за основу обрано систему RS Turbo.

Дана система здійснює всі функції RS Turbo Mobile-L, але дає можливість сканувати радіодіапазон до 12 ГГц за допомогою додаткового конвертора. Використовуючи RS/L перетворювач, система знаходить сигнали, котрі передаються за допомогою живлення прослуховування чи будь-якому дроту в діапазоні від 0,6 кГц до 10 МГц, а також інфрачервону частину оптичного діапазону [30].

Приміром, перетворювачі RS/L застосовуються для аналізу дротових та оптичних каналів, а генератори RS/N (до 1800 МГц) – для нейтралізації виявленої бездротової потужності.

Загальна схема підключення обладнання системи RS turbo:

- Модуль локалізації антен,
- Скануючого приймача,
- Програмного засобу,
- Контролеру,
- Ноутбук
- Кейсу для транспортування обладнання.

Після одного періоду сканування програма складає таблицю, де кожне значення частоти налаштування відповідає спектру сигналу 8 МГц, виміряному послідовним аналізатором турбоконтролера RS, для сигналів вище заданого порогу з роздільною здатністю 12,5 кГц. Дана таблиця має назву - спектральна панорама.

Програмування даної системи RS turbo дозволяє виконувати спектральну панораму з урахуванням даних, здобутих в продовж поточного, а також будь-якої кількості попередніх циклів сканування. Дана таблиця спектральної панорами

зберігається в пам'яті комп'ютера вслід за ключовим циклом. Впродовж наступного циклу здійснюється створення нової таблиці, під час чого значення рівнів у ній видозмінюється відповідно до методу обробки, який обирається [31,32]:

- оновлення (записується нове значення, а старе стирається з таблиці);
- нагромадження (найбільший з двох рівнів записується в таблицю);
- усереднення (записуються середні значення двох рівнів).

Я пропоную удосконалення модуль локалізації антен.

Для локалізації комплекс буде використовувати принцип тріангуляції.

Метод тріангуляції. На основі приймання потужності сигналу з трьох чи більше точок доступу закладене формулювання положення елементу. Всі точки доступу, які "чує" сигнал, у відповідь сповіщує системі управління мережею значеннями рівня сигналу. Не відповідають такі точки доступу, які не мають можливості прийняти сигнал.

Кожна точка доступу, котра має можливість чути сигнали ЗНОІ, надає можливість проглянути інформацію, котра постачається після очікування певного часу мережевою системою управління.

Більш точно місце розташування ЗНОІ може бути визначеним тоді, коли свою інформацію надала більш чисельна кількість точок.

Потім система відображує навкруг всіх точок доступу, котрі відгукнулась, коло з радіусом, який вирізняється рівнем сигналу необхідного пристрою, котрий є прийнятим даною точкою. Коли рівень сигналу дорівнює 65 дБ, тоді коло з радіусом обирається дорівнюючим відстані, сигнал з котрого, зобов`язаний мати даний рівень. Коли рівень сигналу, котрий приймається інакшою точкою доступу становить 45 дБ, тоді радіус необхідного кола буде менше, тому як найвищий рівень сигналу означатиме, що сигнал надходить з найкоротшої відстані.

Крок розподілу території пошуку під час застосування методу тріангуляції являє собою приблизно 3 м, тож місцезнаходження ЗНОІ вдовольняється зоною розмірами приблизно 9 м2.

Недоліком є точність. В зв’язку з дуже малими розмірами закладних пристроїв та малим часом передачі накопиченої інформації треба зменшувати розміри

перетину кіл діаграм антен та часу виявлення. Схема принципу наведена на рисунку 3.1. Саме на перетини діаграм антен і знаходиться закладний пристрій.

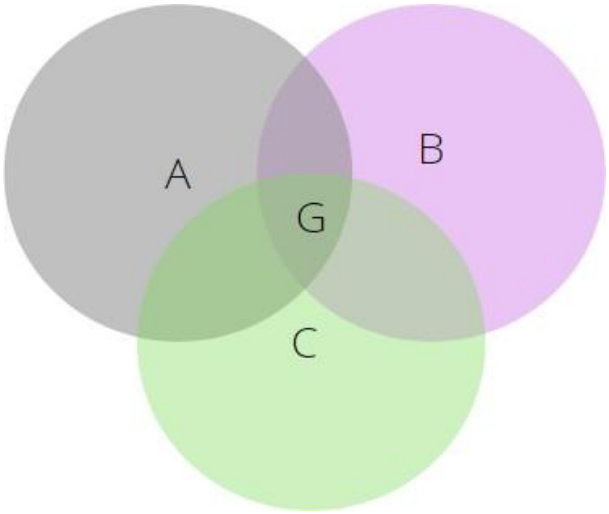

Рисунок 3.1 - Метод тріангуляції.

Багатопроменеве поширення. Існує декілька розбіжних шляхів за якими радіосигнал може йти до точки його прийому. Тому, якщо сигнал має рівень 65 дБ, то дане джерело повністю може бути на досить короткій відстані відносно точки прийому, аніж радіус кола, і це вказує для конкретного рівня чи сигнал пройшов шлях до точки прийому за не найкоротший шлях [33,34].

Математична частина методу тріангуляції зображена на рисунку 3.2:

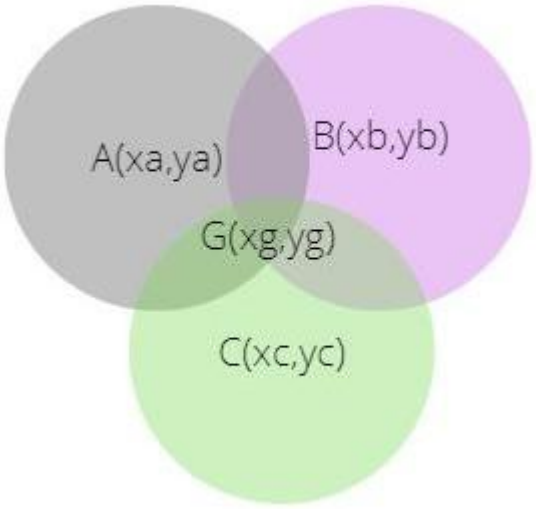

Рисунок 3.2 - Метод тріангуляції с координатами.

Нехай, A (xa, ya), B (xb, yb), C (xc, yc) - детектори сигналу із заданими координатами в якійсь прямокутній системі координат. G(xg, yg) – джерело сигналу.

Згадуємо зі шкільного підручника фізики, що амплітуда сигналу обернено пропорційна квадрату відстані до джерела. Таким чином, відстань Ra від джерела G до детектора A дорівнює

$$Ra = k_a/a_1^2, \tag{3.1}$$

де ka це деякий коефіцієнт, який ми можемо отримати при калібруванні пристроїв.

Формула для розрахунку відстані a1 беремо зі шкільного курсу геометрії.

$$a_1 = \sqrt[2]{(x_a - x_g)^2 + (y_a - y_g)^2}, \tag{3.2}$$

Гетерогенність середовища нехтуємо. Так, це дасть деяку похибку, але вирішення цієї проблеми виходить за межі завдання. Вважатимемо, що постійні чинники, що впливають поширення сигналу (наявність і матеріал стін, наприклад) — вже закладено коефіцієнт ka. Чинники тимчасові - інтерференція, перевідображення сигналу тощо. — впливатимуть на результат, але на практиці навіть у приміщенні заважають не дуже.

Таким чином, ми маємо формули залежності для відстані від усіх джерел.

Якщо вирішувати завдання — у нас є система квадратних рівнянь, розв'язання якої дасть нам точку з координатами xg, yg (див.рис.6.)

3.2 Розробка методу використання удосконаленого методу виявлення радіопристроїв прихованого знаття інформації.

Запропоновується 2 напрямки для застосування такого модернізування:

• Провідний: обладнати всі приміщення технічними модулями для виявлення закладних приладів і постійно користуватися комплексом протягом усього робочого часу. Оновіть програмне забезпечення, щоб воно могло працювати в режимі реального часу, автоматично виявляло нові радіосигнали та негайно відображало їх місцезнаходження. Зображено на рисунку 3.3.

• Можливий: кількість антен можна збільшити, щоб зменшити відстань позиціонування. Зображено на рисунку 3.4.

Рисунок 3.3 - Перший метод (Провідний).

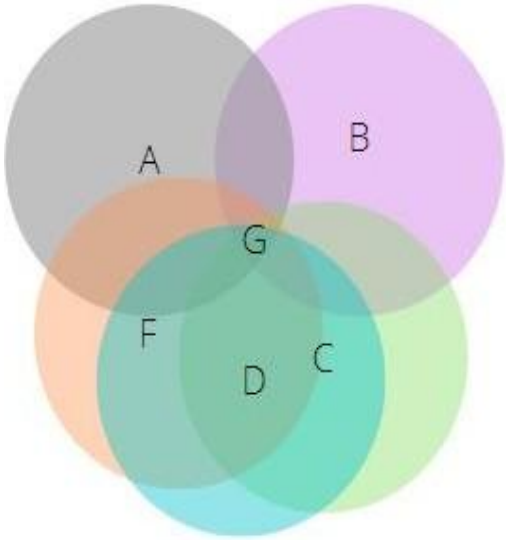

Рисунок 3.4 - Другий метод (Можливий).

Кожен з даних варіантів підвищить вартість системи, що стає мінусом цієї системи, але все це додає більш точних результатів пошуку для вбудованих пристроїв.

3.3 Додаткові рекомендації до захисту інформації від витоку через акустичні канали

Запобігання витоку інформації через акустичні канали – це комплекс заходів, що ліквідують або знижують спроможність витоку таємної інформації з контрольованої зони через звукове поле. Організаційно – технічні заходи являються основними типами такого захисту [35].

Режимні, просторово-архітектурні заходи відносяться до організаційних заходів, а от так звані пасивні (звукопоглинання, звукоізоляція) і активні (тиша) – до організаційно-технічних заходів. Технічні заходи також можуть бути реалізовані за допомогою спеціальних приладів безпеки таємних переговорів.

Будівельні та планувальні заходи -Забезпечте виконання певних вимог під час проектування чи під час реконструкції споруд для уникнення або зменшення неконтрольованого передачі звуку. Як приклад: наумисно розмістити чи спеціальне устаткування, чи приміщення з засобами звукового захисту (вікно чи двері до підконтрольної території) [36].

Режимні заходи - суворо контролювати перебування співробітників і відвідувачів на контрольованій території.

Організаційно-технічні заходи - застосування звукопоглинаючих засобів. Поглинаючими та звукоізолючими матеріалами являються -пористі і м’які матеріали (наприклад пінобетон, флісовий килим, пористий сухий гіпс, вата). Поміж твердими тілами та повітрям є велика кількість кордонів, які викликають незліченну кількість відображень і поглинань звукових коливань (передачі звука, відбиття, поглинання) [37].

Шумоміри використовуються для визначення звукоізоляції. Шумомір - це пристрій для вимірювання, який трасформує звукові коливання в числові значення. Вимірювання акустичної стійкості здійснюється за допомогою джерела зразка (скерованому рівні потужності і на скерованій частоті). Зразкові джерела звуку та шумоміри застосовуються для формулювання звукопоглинаючої здатності

приміщення. Рівні звукового тиску зразкових джерел звуку відомі. Міряйте шумоміром сигнал, отриманий з протилежного боку стіни. Різниця між коефіцієнтом поглинання та показником [38].

У випадках коли реактивні заходи не убезпечують необхідного рівня безпеки, використовуються активні заходи. Генератори шуму відносяться до технічних приладів, що генерують сигнали шумового типу. На вібраційні чи акустичні датчик надходять дані сигнали.

Акустичні датчики . Їх функція полягає в утворені вібраційного шуму для маскування шуму в огороджувальних приміщеннях, і акустичного шуму зовні та (або) всередині приміщення.

Датчик вібрації наклеють до захисної конструкції, , в якій генеруються акустичні вібрації. Інформацію від витоку зі стін, стелі, підлоги, вікон, дверей, труб, вентиляційних комунікацій та інших конструкцій можуть вивірено захистити генератори шуму.

Таким чином, через акустичний канал убезпечується захист від протікання.

• Застосування звукопоглинаючих матеріалів, спеціальних впускних і вихідних отворів, склопакетів.

• Застосування приглушення поверхневого акустичного шуму, а також гучності;

• Системи встановлення опалення, електропостачання, вентиляційні канали, телефонний та бездротовий зв'язок;

• ліквідація витоків інформації за допомогою спеціально сертифікованих засобів.

Висновки до 3 розділу

Віруючий розквіт модернізованих інформаційних технологій, а також технічних заходів слугує невпинному збільшенню діапазону вже існуючих каналів витоку інформації, з огляду на це аналіз каналів розповсюдження інформації все

більше виступає актуальною та більш недосяжною метою захисту інформації від зловмисників [38].

На сьогоднішній день в мережі Інтернет, можливо, відшукати багатто подібних комлексів як RS Turbo. Цей комплекс був обран за різніми показниками такі як ціна й якість та інші грунтовні показників [39]. Проте, за своїм функціоналом комплекс не поступається в дії як до того ж RS Turbo Mobile, між конкурентами він найкращий. За допомогою методу тріангуляції та удосконалення додатковами антенами. Комплекс RS Turbo стає одним із гарних варіантом для малобюджетних компаній [40].

ВИСНОВКИ

В ході проведення роботи була дана коротка характеристика пристрія для пошуку закладок, а саме RS TURBO. Було проведено аналіз цього комплексу. Було розроблено удосконалення пристрою та обраного методу пошуку закладних пристриїв. Запропоновано варіанти впровадження цього пристрою двума шляхами та запропонувани додаткові методи захисту від витоку акустичної інформації.

Результатом роботи є вироблені рекомендації щодо вдосконалення системи комплексу RS Turbo.

Поставлена задача була вирішена в повному обсязі, розроблене удосконалення та рекомендації, при дотриманні забезпечать необхідний рівень безпеки інформації на будь якому підприємстві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Швирєв Б. А. наукова статя OCCURRENCE CHANNEL OF LEAKAGE OF THE ACOUSTIC DUE TO THE MODULATION OF THE VISIBLE LIGHT / Б. А. Швирєв, А. В. Власенко // INTERNATIONAL SCIENTIFIC JOURNAL. – 2019.

2. Ananiev V.A. Balueva L.N. Murashko V.P. "Ventilation andair conditioning systems" theory and practice ed. Euroclimate,2008.

3. Громико І. О. Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації / І. О. Громико // Системи обробки інформації. — Х.: ХУПС, 2006. — Вип. 9 (58). — С. 3—9.

4. Шаповалов П. П. Поиск и оперативное пересечение негласного съема информации. – М.: ЗАО «Щит», 2000. – 83 с

5. Хорев А. А. «Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации» — Москва, 1997.

6. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.: ил. ISBN 5-93517-204-6.

7. Кравченко В. Б. Захист мовленнєвої інформації в каналах зв'язку // Спецтехніка. 1999. No 4. С. 2 - 9; 1999. No 5. С. 2 - 11.

8. Доценко С.М. Безопасность оптоволоконных кабельных систем // «Конфидент», №6, 1999.

9. Березанский Д.П. Металлодетекторы – устройства досмотра. Вопросы нормирования требований. «Специальная техника», №2, 1998 г.

10. [Електронний ресурс]:Стаття 359 уголвного кодексу України . – Режим доступу: https://protocol.ua/ru/kriminalniy_kodeks_ukraini_stattya_359

11. Незаконні придбання, збут або використання спеціальних технічних засобів негласного отримання інформації // Велика українська юридична енциклопедія. У 20 т. Т.

12. Кримінальне право / В. Я. Тацій (відп. ред.) та ін. — 2017. — С. 597. — ISBN 978-966-937-261-1.

13. Ананский Е.В. Что такое радиозакладки и как их обнаружить? (часть2)/журнал «Служба безопасности» [Электронный ресурс] режим доступ: http://www.kvirin.com/articles/267/

14. Закладние комплексы. [Электронный ресурс]:https://prom.ua/ua/Detektor-podslushivayuschih-ustrojstv.html

15. [Електронний ресурс]: Защита от утечек информации . – Режим доступу: https://searchinform.ru/analitika-v-oblasti-ib/utechki-

16. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.

17. Абалмазов Э.И. Направленные микрофоны: мифы и реальность // «Специальная техника» №4, 1996 г.

18. [Електронний ресурс]:Визр company . – Режим доступу: www.vizir-company.com

19. [Електронний ресурс]: . – Режим доступу: Svetainė neegzistuoja (yukonoptics.ru)

20. [Електронний ресурс]: Всебланки. – Режим доступу: www.vsebinokli.ru

21. Хорев А.А. Технические каналы утечки акустической (речевой) информации. «Специальная техника» №1, 1998 г.

22. [Електронний ресурс]:Перелік технічних засобів . – Режим доступу: www.bnti.ru

23. [Електронний ресурс]:Лабор комплкт . – Режим доступу: www.laborkomplekt.ru

24. Ярочкин В. И. Информационная безопасность. – М.: Международные отношения, 2000. – 400 с.

25. Лаврентьев А. В. Анализ технических каналов утечки информации и классификация технических средств разведки. - Безопасность информации. – 2000. - №4. – С. 32 – 38.

26. Калинцев Ю. Л. Конфиденциальность и защита информации: Учеб. пособие по курсу «Радиовещание и электроакустика». – М.:МТУСИ, 1997.- 60 с

27. Кошелєва О.В. Адміністративно-правове регулювання обороту спеціальних технічних засобів, призначених для негласного отримання інформації. - 27с

28. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Изд. Томского гос. ун-та систем управления и радиоэлектроники, 2004. – 197 с.

29. Пасєка О. Ф. Окремі проблемні аспекти кримінальної відповідальності за незаконне придбання, збут або використання спеціальних технічних засобів негласного отримання інформації за КК України // Науковий вісник ЛДУВС. – 2016. – No 2. – С. 301–310.

30. [Електронний ресурс]:Компанія Маском . – Режим доступу: https://www.mascom.ru/article255.asp.html

31. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. — М.: НЕЛК, 2001. — 138 с.

32. В.О.Хорошко, О.Д. Азаров, Г.О.Максименко, Ю.Є.Яремчук. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник.-Вінниця: ВНТУ, 2007.- 333 с.

33. [Електронний ресурс]:Тріангуляція . – Режим доступу: https://cyberleninka.ru/article/n/triangulyatsiya-kak-sposob-obespecheniya-validnosti-rezultatov-empiricheskogo-issledovaniya/viewer

34. С. Г. Судаков. 8. Кутові вимірювання / / Основні геодезичні мережі. - 368 с. НД ТЗІ 2.7-011-2012. Захист інформації на об’єктах інформаційної діяльності.Методичні вказівки з розробки методики виявлення закладних пристроїв.

35. Бузов Г.А. Защита от утечки информации по техническим каналам: учеб. пособ. / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия – Телеком, 2005. – 416 с.

36. Зайцев А.П. Технические средства и методы защиты информации: учебник для вузов / [А.П Зайцев., А.А. Шелупанов, Р.В. Мещеряков и др.]; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

37. Куренков Е. В., Лысов А. В., Остапенко А. Н. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за сет ПЭМИ. - Защита информации.—1998. –№ 4. – С. 48 – 50.

38. Поисковые комплексы. [Электронный ресурс]:https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php

39. Мультиагентна технологія пошуку цифрових радіозакладних пристроїв на основі кластеризації за методом бджолиної колонії. Савченко В. та ін. // Захист інформації, Том 21, No3, – 2019. – С. 194–202.