МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____В.В.Козловський

«____»_____2022

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ

«БАКАЛАВР»

Тема:«Захист персональних даних в телекомунікаційних мережах»

Автор: А.В. Ємець

Науковий керівник: Д. П. Чирва

Нормконтролер: М.О. Шутко

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітнього ступеня: «Бакалавр»

Спеціальність: 125 Кібербезпека

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗЗІ

_____ В.В. Козловський

«____»_____ 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
студентки Ємець Анастасії Вячеславівни

1. Тема: «Захист персональних даних у телекомунікаційних мережах» затверджена наказом ректора від 06.05.2022 р. № 483/ст.
2. Термін виконання: з 16 травня 2022р. по 19 червня 2022р.
3. Вихідні дані:
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):

1. Телекомунікаційні мережі та персональні дані, що у них циркулюють

2. Закладні пристрої для викрадення персональних даних у телекомунікаційній мережі

3. Захист персональних даних у телекомунікаційній мережі з використанням рангового коду та дотриманням анонімності

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі		Виконано
2.	Аналіз літературних джерел		Виконано
3.	Обґрунтування рішення		Виконано
4.	Збір інформації		Виконано
5.	Телекомунікаційні мережі та персональні дані, що у них циркулюють		Виконано
6.	Закладні пристрої для викрадення персональних даних у телекомунікаційній мережі		Виконано
7.	Захист персональних даних у телекомунікаційній мережі з використанням рангового коду та дотриманням анонімності		Виконано
8.	Дослідження сучасних програмних засобів для забезпечення відеонагляду		Виконано
9.	Оформлення і друк пояснювальної записки		Виконано
10.	Оформлення презентації		Виконано
11.	Отримання рецензій від опонентів		Виконано
12.	Захист в ЕК		

Дипломник А.В. Ємець
(підпис, дата)

Дипломний керівник Д. П. Чирва
(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 50 сторінок, має рисунків. Список використаних джерел містить 17 найменування і займає 2 сторінки.

Метою є дослідження сучасних методів захисту персональних даних у телекомунікаційних мережах

Ключові слова: ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, ПЕРСОНАЛЬНІ ДАНІ, ЗАКЛАДНІ ПРИСТРОЇ, ANOC.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПД – персональні дані;

ТМ – телекомунікаційна мережа;

ІБ – інформаційна безпека;

ТКВІ – технічний канал витоку інформації;

ЗП – закладні пристрої;

КВІ - канал витоку інформації;

РЗП – радіозакладні пристрої;

ВСТУП

Телекомунікаційні технології почали свій розвиток ще у 19 столітті. Першим відкриттям того часу стало винайдення Алессандро Вольтом електричної комірки. Даний винахід дав змогу Семюелю Морзе, у далекому 1835 році, розробити електромагнітний телеграф, та привів до розширення телефону у 1876 році Грехем Беллом. З моменту тих відкриттів вже минуло багато часу, тож прогрес у телекомунікаціях, як і у розвитку сучасного інформаційного суспільства, мав нестримний ріст, а також з'явилась потреба в створенні нових телекомунікаційних мереж.

Нині дуже важливо мати мережі та системи, які б могли забезпечити неперервний обіг інформації, причому такі, що не приносили дискомфорт в процесі інформаційного приймання та сприйняття. Не зважаючи на те, що з кожним днем таких систем та мереж з'являється більше, головною проблемою надалі залишається захист інформації, що циркулює у них.

За дослідженнями американських журналістів, персональні дані й надалі залишаються найвразливішою та незахищеною ланкою телекомунікаційних мереж.[1] В Україні контакти кожного п'ятого українця містяться в базах даних телекомунікаційних мереж без його згоди, навіть попри суттєву кількість законодавчих регуляторів, що ще раз підкреслює необхідність створення таких телекомунікаційних мереж, де б питання захисту персональних даних було вирішено. Розв'язання даної проблеми можливе тільки з захищеними новітніми надійними технічними засобами та закріпленням базових норм, які можуть гарантувати надійний захист персональних даних особи.

РОЗДІЛ 1

ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА ПЕРСОНАЛЬНІ ДАНІ У НИХ

В умовах існування різноманітних мережевих телекомунікаційних технологій, їх швидкого розвитку, а також зростання попиту населення до використання та передачі власних відомостей за допомогою цих новаційних методів, виникає необхідність забезпечення максимальної безпеки персональних даних користувачів від витоку. Одним із найголовніших факторів забезпечення захисту персональних даних у ТМ є дотримання класичних характеристик інформаційної безпеки: конфіденційності, цілісності та доступності. Аби віднайти найкращий спосіб, щоб це зробити, потрібно чітко розуміти що таке «телекомунікаційна мережа», «персональні дані», а також чітко визначити можливі варіанти витоку та способи захисту ПД у ТМ.

1.1 Загальні поняття

Загалом, під поняттям «телекомунікаційна мережа» слід розуміти сукупність різних засобів для забезпечення передачі інформації між двома кінцевими пристроями або абонентами.

У широкому розумінні телекомунікаційну мережу розглядають як комплекс технічних засобів телекомунікацій, а також споруд, призначення яких: комутація, маршрутизація, передавання та приймання сигналів, текстів, звуків тощо.

Як правило, до складу всіх ТМ входять:

- мережеве обладнання (кінцеві пристрої): персональний комп'ютер, сервери, зчитувачі, аудіо- та відеоапаратура тощо;
- комунікаційне обладнання: дротове, кабельне та бездротове середовище передачі даних;
- проміжні пристрої: модеми, мережеві адаптери, повторювачі, мости, комутатори;
- широкий арсенал програмного забезпечення;

- стеки комунікаційних протоколів для визначення правил взаємодії мережевих пристроїв ТМ.

Зазвичай структура ТМ (рис. 1.1.1.) є ієрархічною та показує інтенсивність трафіку між її окремими частинами – вузлами, що розташовані у різних локаціях (будівлі, населеному пункті, регіоні, країні тощо). .[4]

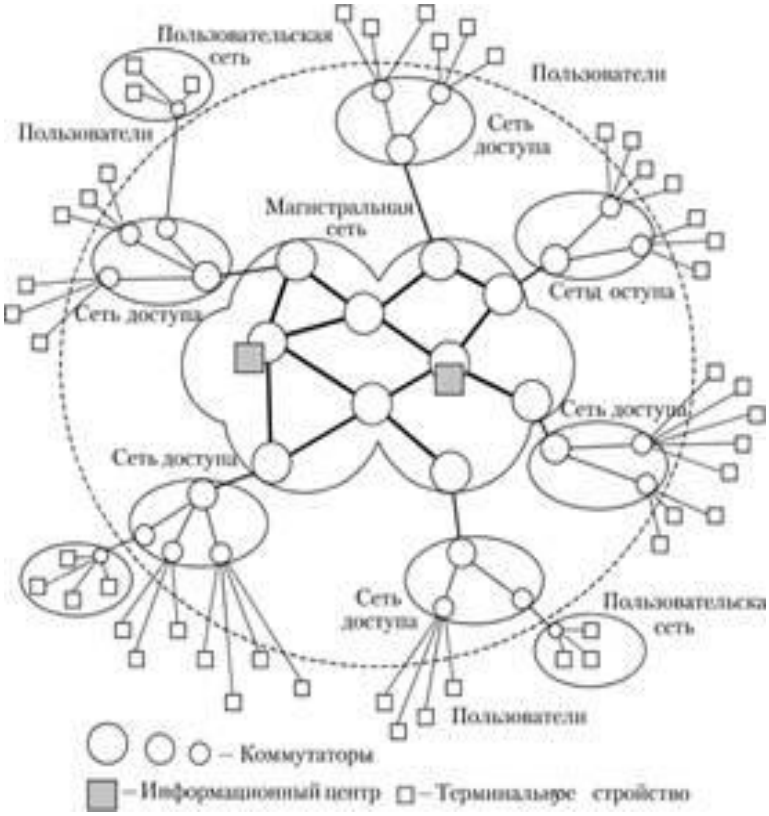


Рис. 1.1.1. Структура телекомунікаційної мережі

Звернемо увагу на окремі компоненти телекомунікаційної мережі:

- комутатори – мережеві вузли, багатопортові пристрої, до них підключають лінії зв'язку;
- термінальні пристрої – визначають назву мережі (у комп'ютерній мережі - комп'ютери, в телефонній - телефонні апарати, в телевізійній - телевізійні приймачі, в радіомовної мережі – радіоприймачі тощо);
- абонентський канал – канал, по якому циркулює уся інформація ТМ;

- мережа доступу – об'єднує інформаційні потоки, що надходять від численних користувальницьких пристроїв у загальний, а також приймає і ділить агрегований потік на окремі потоки аби користувач отримав тільки адресовану йому інформацію ;
- магістральна мережа – використовується для переміщення інформаційних потоків від відправника до одержувача
- інформаційний центр – призначений для управління сервісами по наданню інформаційних послуг усім абонентам та користувачам мережі.

Що стосується поняття «персональні дані», в більшості випадків його трактують як сукупність інформації про особу, що може її ідентифікувати. Слід також додати, що ПД розділяють на дві категорії: загальні та особливі (чутливі).

В свою чергу, до загальної категорії відносять: ім'я та прізвище; громадянство; сімейний стан; дату та місце народження; фінансове становище; дипломи про освіту; підпис тощо. А особлива категорія охоплює відомості про: етнічне та національне походження; віросповідання; політичні погляди; біометричні дані; генетичні дані; кримінальні провадження тощо.

У кожній ТМ відбувається процес обробки ПД – реєстрація, збирання, зберігання, заміна, поширення або видалення цієї інформації. Дуже важливо під час даного процесу враховувати категорії ПД та використовувати засоби запобігання їх витоку за допомогою встановлення рівнів безпеки доступу. Крім того, також потрібно мати згоду суб'єкта ПД аби мати можливість займатись обробкою отриманої інформації. .[5]

Отже, сфері електронної комерції згода суб’єкту персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційних системах суб’єкта електронної комерції шляхом позначення у спосіб, що дозволяє обробляти його персональні дані відповідно до цілей їх обробки, за умови, що такі системи до маркування не надають згоди на обробку їх персональних даних. [6]

1.2 Класифікація ТМ

Особливу увагу потрібно звернути саме на класифікацію ТМ, адже існує понад шість варіантів поділу їх за приналежністю, принципами побудови та призначенням. Маючи повне уявлення про види, типи та функціональність ТМ, можливо досконало виявити недоліки цих мереж та встановити необхідні вимоги й заходи щодо захисту ПД у них.

По-перше, визначають такі ТМ за функціональним призначенням:

1) транспортна мережа, друга назва «ядро мережі», транспортує та об'єднує окремі мережі, а також забезпечує транзит трафіку ними за допомогою високошвидкісних каналів. Зазвичай складається із транспортних вузлів, граничних вузлів, серверів сигналізації та шлюзів;
2) мережа доступу, є системно-мережною інфраструктурою, її головною функцією є концентрація інформаційних потоків. Її складовими є абонентські лінії, системі передачі та вузли доступу.

По-друге, за відомчою приналежністю виділяють наступні ТМ:

1) технологічні – для управління технологічними процесами та забезпечення виробничої діяльності;
2) виділенні – існують для надання послуг обраному колу користувачів;
3) загального користування – використовується для надання послуг кожному користувачеві;
4) спеціального призначення – забезпечують потреби оборони безпеки, державних управлінь тощо.

По-третє, за кількістю підтримувальних служб зв'язку відокремлюють такі ТМ:

1) моносервісні – надають підтримку тільки одну службу зв'язку;
2) мультисервісні – підтримують дві або більше служби зв'язку.

Також, важливо розуміти які існують ТМ за типом передавального середовища:

1) проводові;
2) безпроводові;
3) радіомережі;

4) змішані.

Що стосується розподілу за типом адміністративного розподілу, виділяють наступні ТМ:

1) магістральна – зв'язує усі телекомунікаційні вузли країни загалом;
2) зонова – знаходиться у певній зоні (регіоні) країни;
3) місцева – утворена на певній місцевості (міська або сільська);
4) міжнародна – пов'язана з мережами інших держав.

Необхідно підкреслити важливість класифікації ТМ за топологічним характером:

1) зірка – всі вузли підключені до хоста (центральний вузол); (рис. 1.2.1)
   Відзначається найбільшою швидкістю роботи та продуктивністю, адже передача усіх можливих даних відбувається через хост за відокремленою лінією, що використовується тільки окремою робочою станцією;

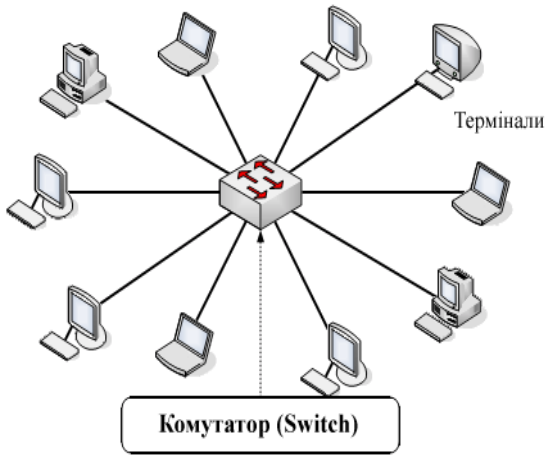


Рис. 1.2.1. Топологія мережі у вигляді зірки

2) кільцева – всі вузли підключені до замкнутого кільцевого каналу. (рис. 1.2.2).Уся інформація у даній мережі циркулює по колу. Найефективніша задача – пересилання повідомлень, адже воно відбувається за допомогою надсилання їх одне за іншим по кабелю з високою швидкістю. З недоліків, якщо одна із станцій виходить з ладу, вся мережа паралізується.

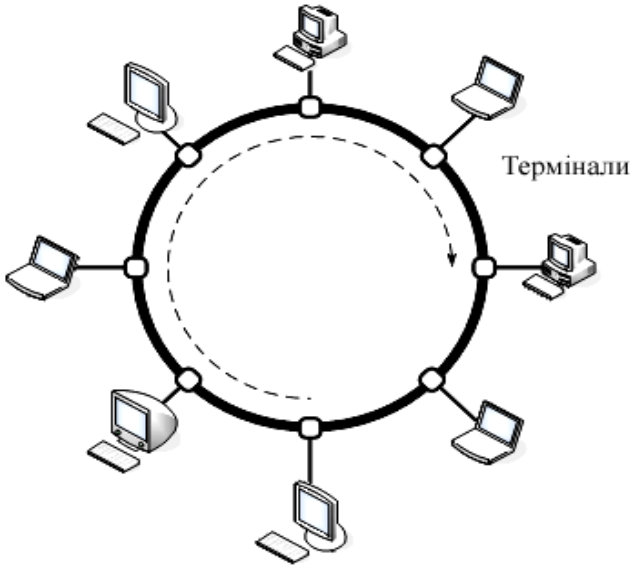


Рис. 1.2.2. Кільцева топологія мережі

3) шинна – всі вузли підключені до незамкнутого каналу (шини) (рис. 1.2.3). У даній мережі всі станції можуть вступати у безпосередній контакт, за умови що вони підключені до шини. У порівнянні з мережею кільцевої топології, дана мережа може функціонувати незалежно стану окремої робочої станції;

Рис. 1.2.3. Шинна топологія мережі

4) деревоподібна – ієрархічна структура побудови. (рис. 1.2.4). Загалом це комбінований тип, поєднання типологій «зірка», «шина» та «кільце».

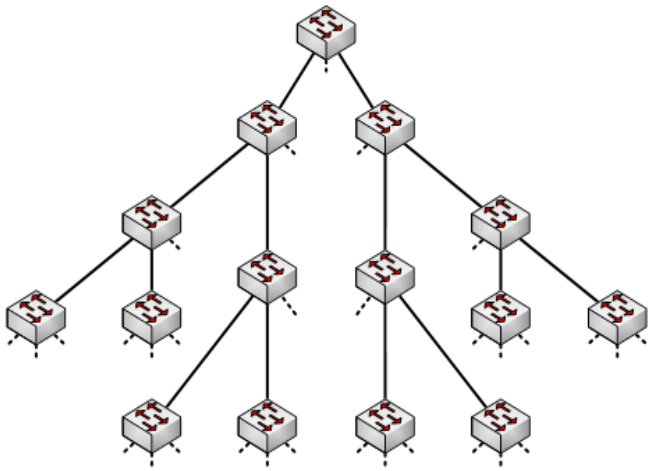


Рис. 1.2.4. Деревоподібна структура мережі

Ще існує розподіл ТМ за формами їх функціонування:

1) комерційна – користувач оплачує використання ресурсів та обладнання;
2) безплатна;
3) корпоративна – приватна, має певну кількість користувачів, що можуть використовувати її ресурс;
4) загального користування – доступ дозволений кожному абоненту.

Крім того, існує розподіл ТМ за територіальним принципом на:

1) глобальна мережа (Wide Area Network, WAN) – забезпечує роботу на великі відстані та забезпечує сервіси великій кількості кінцевих користувачів;
2) міська мережа (Metropolitan Area Network, MAN) – організовує роботу та взаємодію між абонентами у великому місті або економічному районі;
3) локальна мережа (Local Area Network, LAN) – забезпечує роботу для користувачів та абонентів у межах обмеженої території використовуючи високошвидкісні канали для передачі цифрової інформації;
4) корпоративна мережа – послуги надаються тільки для співробітників певного підприємства;
5) мережа відділів – використовується для окремого відділу підприємства;
6) мережа кампусів – призначена для використання у студентському містечку;

мережа масштабу підприємства - об’єднують велику кількість користувачів на всіх територіях окремого підприємства. Охоплювати можуть як місто, так і регіон ,країни, континенти тощо. [4]

1.3 Класифікація каналів витоку ПД із ТМ

Загалом, канал витоку ПД – неконтрольований шлях передачі інформації, в результаті якого зловмисник може отримати несанкціонований доступ до ПД, або викрасти конфіденційні дані особи. Також, це може привести до поширення чутливих відомостей про особу, що веде до її несанкціонованого отримання третіми особами та частого використання для шантажування та виманювання грошей за нерозголошення.

За загальноприйнятою класифікацією визначають такі канали витоку:

- прямий – коли при взаємодії, викрадач має доступ до обладнання та інформації, що циркулює в системі. Яскравим прикладом даного каналу є робота інсайдерів, адже загалом, самі працівники компанії стають засобом передачі інформації зловмиснику. Також, пряме копіювання інформації відносять до витоку через прямі канали;
- непрямий – коли зловмисник має прямий доступ до технічного середовища конкретної системи ІБ. Наприклад, втрата флеш-носія або його крадіжка; фотографування об'єктів інформаційної системи; прослуховування приміщень; зчитування електромагнітного випромінювання; дослідження сміття або викинутих документів.

За фізичною природою утворення каналів витоку інформації розрізняють:

- електричні;
- акустичні;
- візуально-оптичні;
- матеріально-речовинні;
- радіотехнічні.

Окрім того, джерелами небезпечних сигналів можуть бути елементи, провідники та вузли різних компонентів ТМ. Тож, існують таки природні канали витоку ПД із ТМ:

1) шляхом мікрофонних ефектів в елементах електронних схем ТМ;
2) внаслідок складових магнітного поля електронної схеми ТМ;
3) коштом електромагнітного випромінювання низьких та високих частот ТМ;
4) за колом живлення ТМ;
5) за колом заземлення ТМ;
6) завдяки взаємним впливам проводу та лінії зв'язку ТМ;

Також важливо врахувати усі технічні канали витоку, що передбачають використання крадіжки даних з використання фізичних властивостей ТМ, адже засоби, що використовує зломисник, зазвичай, технічні.

Загалом, технічний канал витоку інформації (ТКВІ) є середовищем поширення небезпечного сигналу різними технічними засобами зловмисника аби отримати бажані ПД з ТМ, тому важливо створювати завади для захисту даних від засобів технічної розвідки. (рис. 1.3.1)

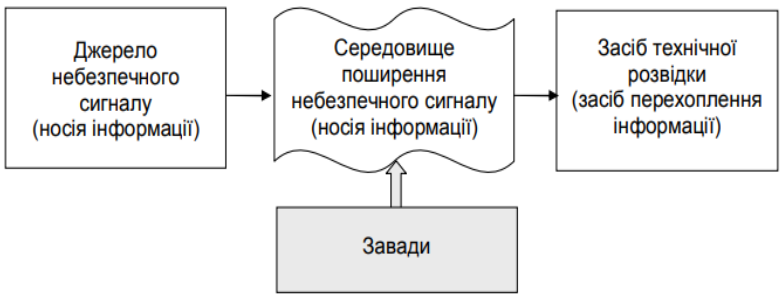


Рис. 1.3.1. Технічний канал витоку інформації

Виділяють такі типи технічних каналів витоку ПД у ТМ:

1) акустичний – несанкціоновано зчитується звук на об'єкті ТМ. Наприклад, прослуховуються телефонні розмови у реальному часі або записуються;
2) акустоелектричний – зчитування відбувається за допомогою звукових хвиль, а після передається по електромережі для перетворення в читабельну форму на стороні зловмисника;
3) оптичний – крадіжка даних за допомогою фотографій або тривалого візуального спостереження за ТМ;
4) віброакустичний – зчитуються коливання, що створені акустикою при впливі на стіни, вікна та архітектурні конструкції ТМ тощо;
5) електромагнітні – зловмисник видаляє бічне електромагнітне випромінювання ТМ та за допомогою спеціального обладнання перетворює в зрозумілу форму.

Крім того, головними ознаками відокремлення ТКВІ у ТМ є:

- вид інформаційної діяльності ;
- принцип формування носіїв ПД;
- середовище поширення ПД;
- способи перехоплення ПД засобами технічної розвідки;

За видом інформаційної діяльності відокремлюють такі ТКВІ у ТМ:

1) мовної інформації;
2) ПД що обробляються у мережі;
3) візуальної інформації;
4)матеріально-речовинні.

За цими ознаками ТКВІ за мовною інформацією у ТМ:

1) акустичний канал;
2) віброакустичний канал;
3) лазерний акустичний канал;
4) акустоелектричний канал;

5) відеоакустичний канал;
6) канали витоку мовної інформації на базі закладного пристрою.

За витоком візуальної інформації є такі ТКВІ у ТМ:

1) канали витоку візуальної інформації основних на закладних пристроях;
2) візуально-оптичний канал;
3) візуальний канал.

До матеріально-речовинних ТКВІ у ТМ відносять:

1) інформацію, що добута з магнітних та інших носіїв ПД, що виведені з ладу;
2) ПД, добуті з чернеток документів, видавництва, діловодства тощо;

Відокремлюють, також, такі ТКВІ за носіями ПД та формуванням небезпечного сигналу:

- електричний – побічний канал електромагнітних наведень на ПД, канали зняття ПД з ліній зв'язку;
- параметричний – канали модуляції ПД та високочастотного нав'язування;

За місцем витоку інформації у ТМ існують такі типи ТКВІ:

1) за межами ТМ;
2) за допомогою технічної розвідки встановленої безпосередньо у ТМ.

Найпоширенішими та найнебезпечнішим з точки зору зберігання конфіденційності ПД є канал акустичного витоку. Вже відомі тисячі випадків, коли зловмисники встановлювали пристрої прослуховування та звукозапису у ТМ, та отримували доступ до усіх ПД.

Також універсальним канаом витоку особистих даних є акустоелектричний канал, адже не потрібно використовувати додаткові пристрої для зчитування даних. Інформація збирається навіть без додаткового підключення до мережі, використовується випромінювання у вигляді електромагнітних хвиль.

Оптичний канал є доступним, тільки якщо робочий процесс ТМ можна візуально контролювати, робити фотографії або знімати їх на відео.

Крім технічних каналів, існує ще і фізичний спосіб крадіжки, що передбачає вилучення матеріальних носіїв ТМ із ПД.

1.4 Способи захисту ПД У ТМ

Усі телекомунікаційні мережі у яких циркулює інформація, а особливо така чутлива як ПД, потребує власних заходів системи безпеки, які були б перешкодою для зловмисника на всіх рівнях обробки даних у ній. Також, дані заходи мають бути створені з урахуванням всіх попередньо виявлених каналів витоку цих відомостей.

Перше, що може допомогти – обмеження передачі ПД. Часто, людський фактор є найслабшою ланкою в стратегії кібербезпеки. Незалежно від того, чи були вони скомпрометовані зловмисниками, чи ні, ПД знаходяться за один крок до витоку, а інсайдерські загрози є справжньою проблемою безпеки. Впроваджуючи рішення по запобіганні втраті даних (Data Loss Prevention чи DLP) можна обмежити шкоду, яку можуть завдати саме співробітники ТМ. Технологія DLP безпосередньо захищає конфіденційні дані. Телефонні компанії можуть вибирати заздалегідь визначені профілі для конфіденційної інформації, такої як PII та інформація про кредитні картки, а також профілі, орієнтовані на відповідність законам і стандартам, таким як GDPR і PCI DSS.

Після визначення конфіденційних даних рішення DLP можуть шукати їх у сотнях типів файлів за допомогою контекстного сканування та перевірки вмісту. Переміщення файлів, що містять ПД, можна відстежувати в режимі реального часу, а їх передачу можна обмежити або заблокувати. Таким чином, телекомунікаційні компанії можуть заборонити співробітникам ділитися ПД через програми для обміну повідомленнями, послуги обміну файлами, особисту електронну пошту тощо.

Друге рішення, контролювати знімальні пристрої, адже таким способом співробітники можуть вилучити ПД с ТМ. Інструменти DLP мають функції керування пристроєм, які дозволяють компаніям блокувати або обмежувати

використання USB-портів і периферійних портів, а також з’єднань Bluetooth. Не дозволяючи співробітникам підключати персональні знімні пристрої, які не відповідають стандартам безпеки компанії й можуть бути джерелом зараження мережі, телекомунікаційні компанії можуть допомогти зберегти ПД в безпеці.[11]

Можна також створити власну систему захисту інформаціїї для ТМ ,що являє собою усі можливі заходи, як програмно-технічні, так і організаційних, аби звести до мінімуму виток ПД із ТМ.

До технічних заходів від несанкціонованого доступу до ПД у ТМ можна віднести:

- резервування особливо важливих підсистем ТМ;
- організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок;
- встановлення обладнання для виявлення та гасіння пожежі;
- використання конструкційних заходів захисту від розкрадання, диверсій, вибухів;
- встановлення резервних систем електроживлення на ТМ;
- оснащення приміщень засобами виявлення та знищення підслуховуючих пристроїв або знімаючих електромагнітні випромінювання з ТМ;

До організаційних заходів щодо захисту можна віднести:

- охорону серверів,
- ретельний підбір персоналу,
- виключення випадків ведення особливо важливих робіт тільки однією людиною,
- наявність плану відновлення працездатності сервера після виходу його з ладу,
- універсальність засобів захисту від усіх користувачів (включаючи найвище керівництво). [9]

Щодо захисту від впливу на акустоелектричний канал, то він забезпечується так званим транспортним перехрестям, що здатне створювати перешкоди, так, що зловмисник не в змозі повністю прочитати інформацію.

Також, захист у випадку оптичного каналу, забезпечується обробкою ПД тільки в закритих приміщеннях без вікон та з міцною звукоізоляцією. [9]

Крім того, захист ПД можна забезпечити за допомогою використання традиційних методів захисту від несанкціонованого доступу до ТМ:

- ідентифікації – присвоєнню унікального ім'я або образу користувачу;
- аутентифікації – перевірка користувача на відповідність, з метою надання або заборони доступу до ТМ;
- захисту паролями – для захисту ПД та обмеження доступу до неї неавторизованим користувачам.

Заходи захисту ПД у ТМ від витоку каналами на основі закладних пристроїв:

1) Організаційні – аби унеможливити установку закладних пристроїв загалом:
   - встановлення режиму роботи ТМ;
   - контроль за доступом до ТМ;
   - перевірка приміщень ТМ на наявність закладних пристроїв;
   - аналізувати методи та способи установки закладних пристроїв, їх вигляду, конструкцій тощо.
2) З виявлення та протидії закладним пристроям:
   - аналіз можливих місць установки таких пристроїв;
   - організація роботи служби безпеки по контролю;
   - аналіз частотного діапазону ТМ.
3) Технічні:
   - створення системи керування доступом ;
   - використання технічних засобів, що виявляють закладні пристрої;
   - контроль радіовипромінювань;
   - контроль інфрачервоних випромінювань;
   - використання тепловізорів, металодетекторів;

- контроль сигналів у лініях живлення, вузлах ТМ;
- користуватись електромагнітними засобами зашумлення;
- мати акусто-вібраційне зашумлення;
- демонтувати, руйнувати та відключати закладні пристрої;
- мати у ТМ засоби візуального контролю;
- мати у використанні апаратуру нелінійної радіолокації та підповерхневої локації;
- користування апаратурою, що здатна протидіяти роботі закладних пристроїв та вивести їх з ладу.[10]

1.5 Висновки до першого розділу

В даному розділі було розглянуто важливість захисту ПД у ТМ. В даний час дуже багато варіантів і каналів витоку чутливих даних у ТМ, що приводить до необхідності вирішення питань захисту інформаціїї загалом. Тож, аби віднайти шляхи розв'язання цих проблем, були досліджені різні види ТМ, класифіковані ПД ,що передаються, проаналізовані потенційні загрози інформації , що в них циркулює та запропоновані методи задля захисту ПД від несанкціонованого доступу каналами витоку.

РОЗДІЛ 2

ЗАКЛАДНІ ПРИСТРОЇ ДЛЯ ВИКРАДЕННЯ ПД У ТМ

Як вже було розглянуто у попередньому розділі, ТМ як носій інформації складається із різних електронних та радіотехнічних засобів. Конструкції цих приладів складаються із передавальних і приймальних пристроїв, а також апаратури задля процесів реєстрації, зберігання та показу інформації. Такими пристроями є радіотехнічні й оптико-електронні, інфрачервоні й лазерні, акустичні й гідроакустичні прилади. Всі вони працюють на базі обчислювальної техніки й обслуговують ТМ пов'язані з циркуляцією чутливої інформації, а отже можуть бути джерелом витоку ПД. За допомогою ЗП в такому випадку буде дуже легко викрасти дані з ТМ, тому виникає проблема організації безпеки проти несанкціонованого зняття ПД за їх використання. [12]

2.1 Загальні поняття

У широкому розумінні, закладними пристроями є потай встановлені спеціальні електронні пристрої (зазвичай малогабаритні), що використовуються для несанкціонованого зняття інформації. Загалом, вигляд таких ЗП – предмети із повсякденного використання такі як електронні калькулятори, запальнички, годинники, ремінці, лампочки тощо.(рис. 2.1.1.)

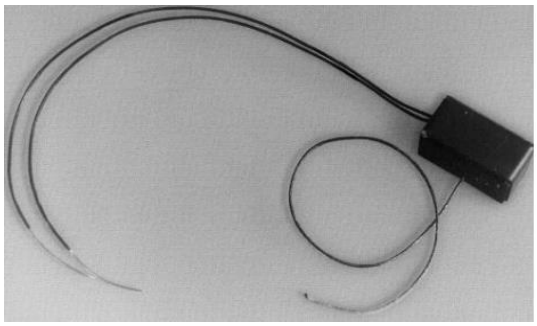


Рис. 2.1.1. РЗП у звичайному вигляді, для під’єднання до ТМ

Всі ЗП в залежності від типу інформації, що перехоплюють поділяють на акустичні, апаратні та відеосистеми тощо. (рис. 2.1.2.) [13]

Рис. 2.1.2. Класифікація пристроїв несанкціонованого зняття інформації

Щодо акустичних ЗП, то їх призначення – перехоплення мовної інформації у ТМ. ПД перехопленні за допомогою таких приладів можуть бути записані на звукозаписувальні пристрої або передані за допомогою радіоканалів, електромереж змінного струму, спеціально прокладених кабелях тощо. Їх класифікують по місцях встановлення, способах передачі інформації, кодуванню ПД, методах керування, джерелах живлення, типу виконання тощо.(рис. 2.1.3.) [13]

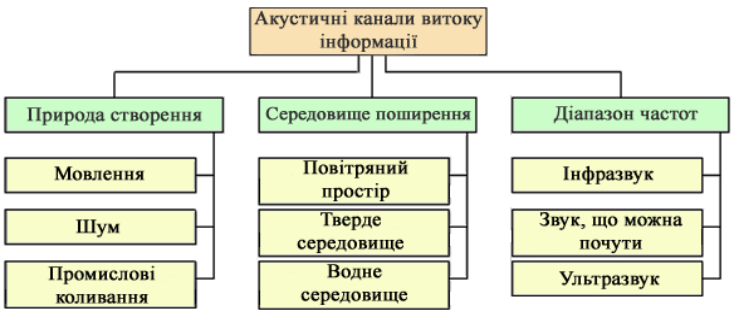


Рис. 2.1.3. Класифікація акустичних каналів

За середовищем поширення акустичних коливань, які перехоплюються ЗП виділяють:

- радіозакладки – зазвичай звичайні маленькі ЗП для перехоплення ПД у прямому повітряному КВІ.
- радіостетоскопи – перехоплюють сигнали по вібраційному КВІ за допомогою контактних, об'єднаних з мікропередавачами, мікрофонів. Часто чутливим елементом таких ЗП є електринний мікрофон або датчик акселерометричного типу. [13]

Акустичні ЗП живляться від різних акумуляторів, батарей, електромереж змінного струму, ТМ та від апаратури, у яку їх встановлюють. Тож, час роботи цих пристроїв може складати від декількох хвилин до декількох місяців, а за електроживлені від ТМ час роботи може бути не обмежений. Головною перевагою таких ЗП є висока скритність, адже виявити їх можна тільки коли відбувається передача ПД у ТМ. [13]

Також, за каналом передачі ПД у ТМ виділяють також наступні ЗП:

- інфрачервоні – використовують для викрадення інформації енергію електромагнітних хвиль у діапазоні інфрачервоного спектра. Головним недоліком є необхідність її знаходження у прямій видимості приймача, адже потрапляння будь-яких предметів погіршує якість передачі або унеможливлює її загалом;
- передають дані по провідниках – поширені для викрадення на досить велику відстань. Головними перевагами є гарне маскування передачі ПД, можливість використання напряму ТМ для живлення, простота встановлення тощо;
- записують дані на магнітофон – застосовують коли не важливе отримання інформації у конкретний реальний момент часу. Головний недолік – заміна касет.

Крім того, за способом отримання ПД у ТМ є такі типи ЗП:

- мікрофонний – перетворює акустичні коливання в електричний сигнал;

- вібраційний – перетворюють уловлені коливання із твердих поверхонь ТМ в електричний сигнал;
- підключений до лінії ТМ – перехоплює ПД безпосередньо у телефонних лініях, оптоволоконних лініях тощо.

Серед ЗП розрізняють ті, що вимагають фізичного проникнення у ТМ для встановлення та ті, що встановлюють без заходовим методом.

ЗП встановлені заходовим методом:

- радіозакладка;
- диктофон;
- «телефонне вухо»;
- провідний мікрофон;
- закладка що передає ПД за допомогою: ТМ, інфрачервоного діапазону; мережі 220В тощо.

Без заходовим методом встановлюють такі ЗП:

- апаратура, що працює за допомогою мікрофонного ефекту;
- лазерні та звичайні стетоскопи;
- спрямований мікрофон;
- високочастотні нав'язування тощо. [12]

Виділяють такі ЗП за наявністю пристрою управління:

- з неперервним випромінюванням – час роботи не перевищує 1-2 годин, споживає багато енергії, легкий до виявлення, адже безпосередньо випромінює енергію;
- з дистанційним керуванням – записує дані тільки коли це потрібно, енергоощадний пристрій, не легко виявити;
- з автоматичним включенням за умови появи сигналу. [14]

За використаним джерелом живлення ЗП поділяють на два види:

- з джерелом живлення від ТМ;
- з живленням від власного джерела.

2.2 Класифікація ЗП у ТМ

Існує дуже багато різних ЗП, проте дуже часто викрадення ПД у ТМ відбувається саме за допомогою:

- радіозакладок
- мікрофонів,
- акустичних антен,
- диктофонів,
- приладів високочастотного нав'язування,
- оптико-механічних приладів.

Радіозакладки широко застосовуються у викраденні ПД, бо перехоплюють інформацію саме із радіоканалу її передачі у ТМ.

Загалом можна виділити три групи за принципом формування сигналу у них:

- активні;
- напівактивні;
- пасивні.

Загалом, активні РЗП є найбільш поширені. В загальному випадку їх структурна схема виглядає так: (рис. 2.2.1.)

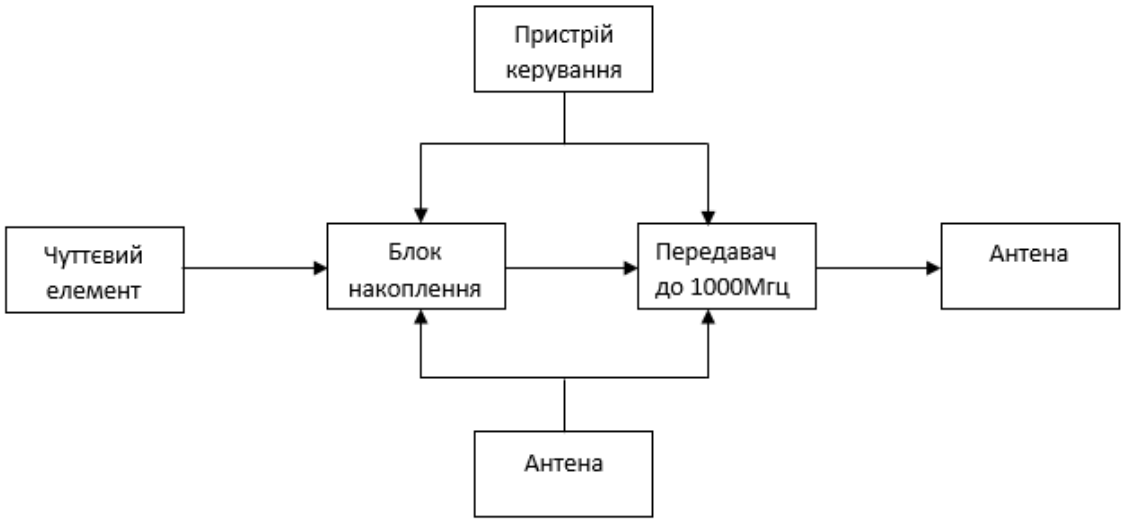


Рис. 2.2.1. Типова структурна схема активного РЗП

Приладом керування є акустомат або приймач сигналів від блоку дистанційного керування; чуттєвий елемент – мікрофон, вібродатчик або спеціальна антена для перехоплення; призначення блока накопичення та стиснення інформації – зменшення роботи чуттєвого елементу на випромінювання; передавач працює на частотах 100 - 1000Мгц; антена є елементом живлення. [14]

При кодуванні перехопленої інформації часто застосовується аналогове скремблювання, що змінює характеристики мовного сигналу таким чином, що він стає нерозбірливим. Так, у радіозакладанні РК-2010 S використовується проста інверсія спектра з точкою інверсії 1,862 кГц, а в радіозакладці "Брусок-ЛЗБ ДУ", РК-1380 SS - складна інверсія спектра. У ряді закладок використовується перетворення мовної інформації на цифровий вигляд (радіозакладки РК-1195-SS, РК-2050), а в радіозакладках SIM-PR-9000T і РК-1970 поряд з перетворенням інформації на цифровий вигляд використовується її шифрування [14]

До найбільш поширених активних РЗП у ТМ відносять:

1. «РК-935» - складається із шести мініатюрних електронних мікрофонів та міксеру для них. За його допомогою можна одразу напряму прослуховувати ПД у ТМ. Час роботи неперервно до дванадцяти годин. Загалом встановлюється у місцях, куди дуже складно дістатись для перевірки (наприклад, фундамент споруди ТМ). (рис 2.2.2)

Рис. 2.2.2. Комплект акустичної розвідки РК- 935

2. «Брусок – ЛЗБ ДУ» - використовує частотну модуляцію для передачі сигналу ТМ. Вихідна потужність – 300 мВт. Габарити – брусок. Тип антени живлення – штатна. Керується дистанційно. Кодування сигналу – складна інверсія спектру. (рис 2.2.3)

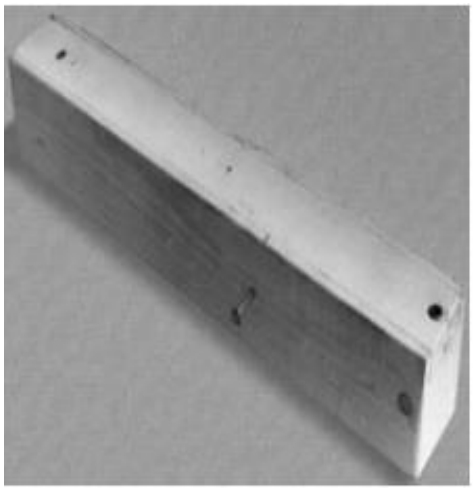


Рис. 2.2.3. «Брусок – ЛЗБ ДУ»

3. «Калькулятор-475» - використовує для роботи широку смугову частотну модуляцію. Вихідна потужність – 50 мВт. Антена живлення – штатна 3,2. Для роботи використовує стабілізацію частоти ТМ. Час роботи – 48 годин. (рис 2.2.4)

Рис. 2.2.4. «Калькулятор-475»

4. «Авторучка» - тип модуляції широко смуговий частотний. Дальність дії – 100 м. Габарити – 135*10.5мм. Тип живлення – кварцова стабілізація частоти. Час роботи – 6 годин. (рис 2.2.5)

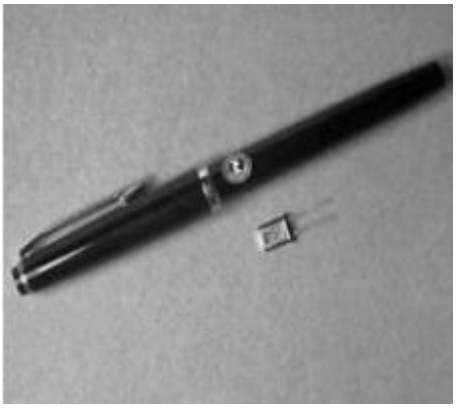


Рис. 2.2.5. «Авторучка»

Щодо напівактивних РЗП, то їх головною перевагою є функціонування до 4000 годин від автономного джерела живлення. Такі РЗП можуть працювати лише за наявності зовнішнього зондуючого електромагнітного поля через що, також, вони отримали назву «аудіо-транспондери». [14]

В загальному випадку їх структурна схема виглядає так: (рис. 2.2.6)

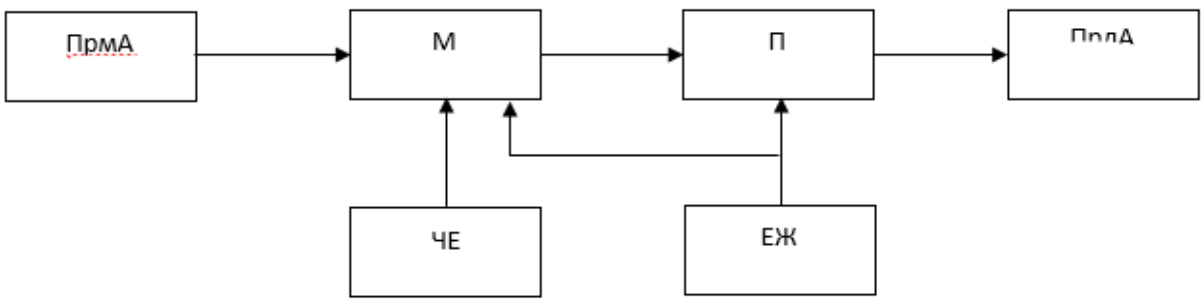


Рис. 2.2.6. Типова структурна схема напівактивного РЗП

де: ПрмА та ПрдА – приймаюча та передавальна антени;

М - модулятор ;

П – підсилювач;

ЧЕ – чуттєвий елемент РЗП;

ЕЖ – елемент живлення РЗП.

Найкращим представником із ряду аудіотрансопондерів є «РЗП SIM-АТР-16», що виглядає подібно дискеті та має розміри 90*90*4мм. Для роботи пристрій необхідно встановити біля генератора синусоїдального сигналу потужністю 10Вт та частотою випромінювання 160 МГц. Він здатен приймати із ТМ на відстані 500 м. Для прийому та вилученню сигналів використовується кільцева антена. [14]

Пасивні РЗП потребують досить потужне опромінення передавача ,яке дуже небезпечно для персоналу, через що вони не знайшли широке використання на практиці. Принцип дії пасивного РЗП зображений на рис. 2.2.7,

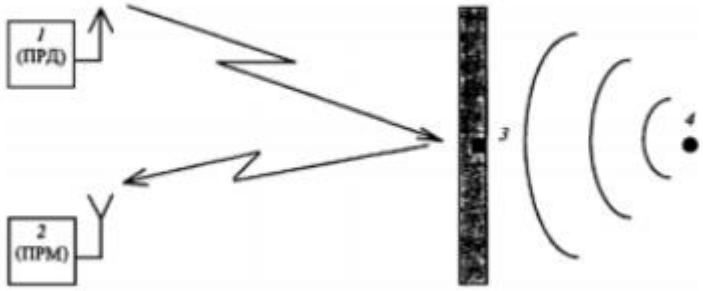


Рис. 2.2.7. Принцип дії пасивного РЗП

де: 1- передавач сигналу; 2 – приймач сигналу, що налаштований на робочі частоти РЗП; 3 – РЗП; 4 – Джерело акустичних коливань.

Прикладом пасивної закладки є «SIPE MM1» - розмірами 30*2.5см , виконана у вигляді стержня із дальністю дії 100 м. Поставляють її у комплекті із джерелом опромінення від ТМ та приймального пристрою.

Широкого поширення набули РЗП у ТМ, що використовують для живлення мережу 220В.Загалом такі пристрої встановлюють до силової мережі ТМ (трійники, подовжувачі, блоки живлення ТМ тощо). Схема прослуховування переговорів із задіянням енергомережі на рис. 2.2.8. [16]

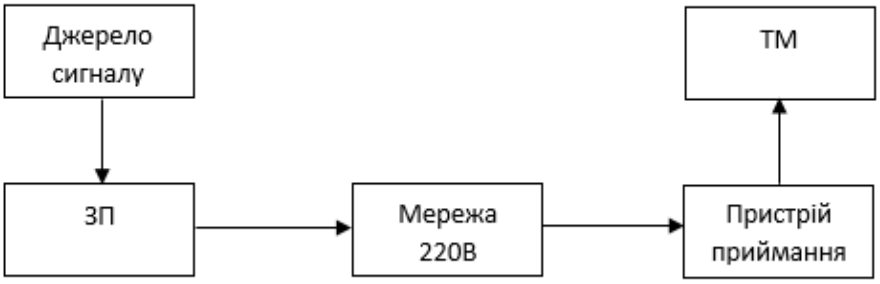


Рис. 2.2.8. Схема застосування закладного пристрою з передачею інформації по мережі 220 В

По-перше, робота можлива тільки в межах однієї фази електропровідної мережі. По-друге, на якість перехоплюваної інформації впливають різні мережеві перешкоди. По-третє, прилад, в який впроваджено ЗУ, може бути випадково відключений від мережі змінного струму. Тому застосування даної техніки зазвичай супроводжується ретельним вивченням схеми організації електропостачання, наявності та типів споживачів електроенергії, вибором камуфляжу. Прикладами серійно випускаються закладок з передачею інформації по ТМ можуть бути такі пристрої: UM104, IPS МСГ, РК170, Model SIM-ROTEL, SIM-ROTEL тощо. Варіант мережевих закладних пристроїв зображений на рис. 2.2.9 (а, б) [16]

а)  б) 

Рис. 2.2.9. Мікрофон закамуфльований :а) під електричний трійник; б) під електричну розетку.

Загалом, застосування таких мережевих ЗП має ряд переваг:

- майже не можливо віднайти пункт контролю таких ЗП;
- підвищена прихованість через відсутність радіовипромінювання;
- необмежений час роботи, через живлення від ТМ. [16]

Щодо акустичних антен, то вони є важливим елементом для мікрофонів та подальшого процесу обробки викраденої інформації із ТМ. Їх головне призначення це посилювати акустичні коливання із ПД та придушувати усі інші акустичні коливання. [16]

Часто, для перехоплення інформації з ТМ використовують саме направлений мікрофон з параболічним рефлектором. Його принцип роботи зображений на рис 2.2.10.

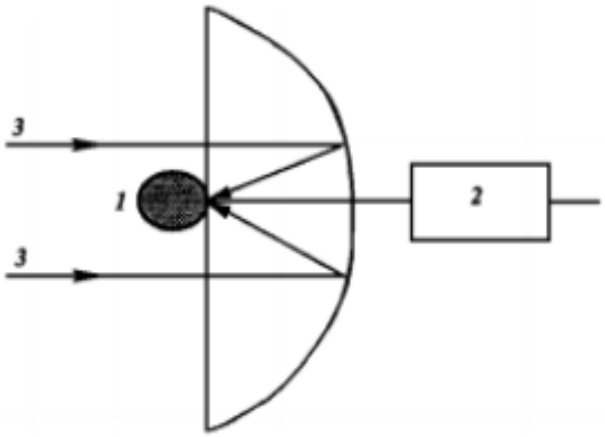


Рис. 2.2.10. Принцип роботи направленого мікрофону з параболічним рефлектором

Акустична хвиля (3) розповсюджуючись у просторі потрапляє на параболічний рефлектор (2). Хвилі, що відбиті від нього, складуються по фазі та потрапляють на мікрофон (1). В наслідок цих дій, посилюється акустична хвиля. Для більшого посилення використовують більші рефлектори.[16]

Найкращими приладами серед таких систем є:

1. «PRO-200» – параболічний приймач створений для дистанційного приймання акустичних хвиль, що має високу чутливість, оснащений регульованим фільтром котрий дозволяє робити частотну селекцію сигналу по ширині та положенню його спектра на осі частот. Дальність дії до 1 км. Має вихід під магнітофон. Елемент живлення від умонтованого акумулятора чи від зовнішньої мережі 220 В. Діаметр рефлектора – 60 см та 75 см . (рис 2.2.11.)

Рис. 2.2.11. Параболічний мікрофон з навушниками на тринозі «PRO-200»

2. «А-2» – параболічний приймач з діаметром 43 см. У комплектації із навушниками та підсилювачем. Дальність дії до 1 км. Коефіцієнт підсилення становить 80 дБ. Присутня автоматична система регулювання підсилення вхідного сигналу – 40 дБ. (рис 2.2.12.) [16]

Рис. 2.2.12. Ручний параболічний мікрофон «А-2»

Також, дуже поширені випадки викрадення ПД із ТМ за допомогою диктофонів, адже це найпростіший метод несанкціонованого викрадення інформації із будь-яких місць. Існує дуже багато факторів які впливають на якість звукозапису. Офісне приміщення ТМ це дуже складний в акустичному плані простір, там дуже багато відбитих хвиль, сторонніх голосів, шуми з вулиці тощо. Находження під одягом досить суттєво впливає на якість запису, наприклад: розмахування руками. Для якісного звукозапису користувачеві необхідно звертати на це увагу. Хоча сучасні диктофони ЗП досить компактні, але дуже складно їх замаскувати. Інша справа коли мікрофон можна «винести» з пристрою ТМ, це дуже суттєво покращить якість запису [16]

На рахунок оптико-акустичної апаратури для перехопення ПД із ТМ, то вони на сьогоднішній день дуже ефективні, та навіть використовуються американськими спецслужбами.

Ці пристрої отримали назву – лазерні системи акустичної розвідки. Їх принцип роботи полягає в наступному: лазерним передавачем генерується високочастотний сигнал, що проходить через атмосферу та поступає на скло. Потім цей сигнал модулюється з акустичною хвилею та відбивається до фото приймача, який за цей час встигає обробити та видати інформацію. Звукова хвиля потрапляючи на розділ «повітря-скло» викликає в останнього відхилення від свого положення. Ці відхилення створюють дифракцію світла, відбиваючись від цієї границі. (рис 2.2.13.) [16]

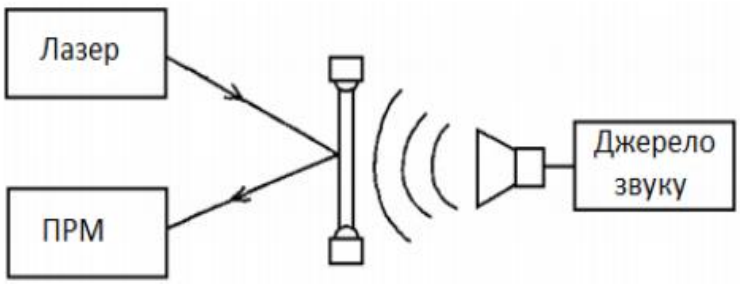


Рис. 2.2.13. Принцип роботи системи лазерної акустичної розвідки

2.3 Методи та їх пристрої для виявлення ЗП

Одним із найважливіших елементів систем захисту ПД у ТМ є виявлення вчасно ЗП. Цей пошук реалізують за допомогою двох груп методів.

У першій групі методів – пошук ЗП як фізичних об'єктів з масогабаритними характеристиками та певними властивостями.

До неї відносять:

- візуальний огляд ТМ та можливого місця встановлення ЗП, використовуючи дзеркала, засоби підсвічування тощо;
- контроль важкодоступних місць ТМ за допомогою встановлення відеоспостереження;
- застосування металодетекторів для пошуку ЗП. [16]

У другій групі методів – пошук ЗП як електронних систем.

Такими методами є:

- використання індикаторів поля, що мають реагувати на випромінювання ЗП у ТМ та знатні їх локалізувати;
- встановлення радіоприймальних пристроїв для пошуку сигналів та аналізу електромагнітної ситуації; [16]

Першим, та незамінним методом є візуальний огляд ТМ що спрямований на пошук у труднодоступних місцях ЗП як без камуфляжу, так і з ним. Особлива увага звертається на свіжі подряпини, зміни в інтер'єру, «випадкові» предмети тощо.Аби краще дослідити ТМ на ЗП використовують ліхтарі, дзеркала тощо.(рис. 2.3.1. (а, б))

а)  б) 

Рис. 2.3.1. Засоби для проведення візуального огляду: а) ліхтар; б) дзеркало.

Другий спосіб це використання спеціальних камер для проведення огляду ТМ. Такі пристрої поділяють на:

1. Ендоскопічне обладнання – фіброскопи, відеоскопи тощо. Для огляду прямих тонких щілин – бароскоп та для проходження складних просторових вигинів - фіброскоп. (рис. 2.3.2. (а, б))

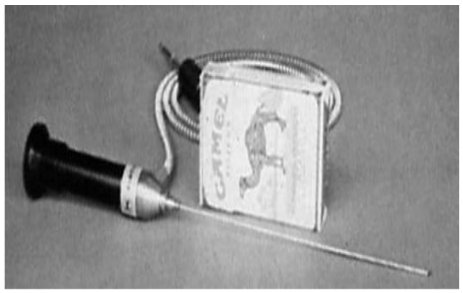
а)  б) 

Рис. 2.3.2.Ендоскопічне обладнання: а) бароскоп моделі PK 1700-S;
б) фіброскоп марки PK 1760.

2. Портативна оглядова відеосистема – загалом використовується тільки прикордонниками. Загалом пристрій зручно використовувати шляхом об'єднання телевізійної камери, відео монітору та регульованої штанги.

Третім кроком є пошук ЗП у ТМ за допомогою металодетекторів, адже не завжди можна знайти ЗП методом візуального огляду. Під дослідженням металодетектором розуміють контактне чи безконтактне використання апаратури, котре уловлює неоднорідності в просторі. При знайдені таких неоднорідностей з'являється звуковий чи світловий сигнал. Тим самим маємо можливість не тільки виявити ЗП, а і локалізувати його.

Найкращим прикладом є металодетектор призначений для пошуку кольорових й чорних металів у середовищах діелектриків та напівпровідників «АКА 7202М». При наближені до повних металів він подає звукові сигнали, що дає розуміння що саме знайдено. (рис. 2.3.3.)

Рис. 2.3.3. Металодетектор АКА-7202М

Його максимальна дальність дії 80 мм – гвинт М3х7; 100 мм – диск 15х1 мм. Елемент живлення – «крона» 9 В. [16]

Щодо другої групи методів та пристроїв – всі вони засновані на факті наявності радіовипромінювання із ЗП.

Основні ознаки радіовипромінювання ЗП:

- відносно високий рівень радіації, через необхідність передачі сигналу за межі контрольованого приміщення. Цей рівень тим вище, чим ближче до пам'яті знаходиться пошукове обладнання;
- наявність гармонік у випромінюванні радіозакладок;
- поява нового джерела на зазвичай вільній частоті діапазону;
- якщо закладка працює без маскування, то оператор шукає дані в її пам'яті, чує шум кімнати або тестовий сигнал, який він сам створив. У апаратній версії цей ефект відтворюють різного роду корелятори й так звана акустична ланка;
- не обладнані ланцюгами дистанційного запуску та VOX ЗП, деякий час працюватимуть безперервно. Закладки з VOX характеризуються переривчастою роботою протягом дня і майже повна тиша вночі.
- якщо одночасно з підняттям трубки виникає будь-яке випромінювання і зникає, коли слухавку кладуть, то це випромінювання прямо чи опосередковано пов'язане з витоком інформації.

Наведений вище перелік функцій не є вичерпним і його можна значно розширити. [16]

Першим представником притроїв що виявляють ЗП як електронний пристрій є індикатор поля.(рис. 2.3.4.)

Рис. 2.3.4. Індикатор поля «ПИТОН»

Індикатор – приймач з малою чутливістю, здатний виявити ЗП на відстані до 40 см. Чим і проводиться селекція несанкціонованих сигналів на фоні «дозволених». Головною перевагою таких пристроїв, окрім простоти, є віднаходження РЗП в незалежності від їх модуляції. Принцип роботи – знайти абсолютний максимум випромінювання. Польові індикатори також використовуються в так званому «режимі очікування», це коли в приміщенні було проведено пошукову операцію з виявлення РЗП, а потім вимірюють рівень поля в кімнаті, і прилад переводять в режим очікування змін (підвищення рівня) в електромагнітному полі, і коли воно буде зафіксоване, подасть сигнал. Однак ця функція не зовсім надійна: по-перше, індикатор може бути досить далеко від РЗП, по-друге, в РЗП може бути малий рівень випромінювання, що детектор не зловить. [16]

Найкращим представником класу індикаторів поля є «ПИТОН» - це приймач-детектор, призначений для виявлення і демодуляція частотно-модульованих сигналів, що використовуються в радіопередавачах мовлення, а також пошук несанкціонованих радіопередавачів за допомогою акустичного блокування та індикатора рівня отриманого сигналу. Технічні характеристики приладу: діапазон частот - від 30 до 1000 МГц; час сканування діапазону не більше 2 с; затримка пошуку після втрати сигналу – не більше 3 с; живиться від 6 елементів по 1,5 В. [16]

Другим приладом є панорамний приймач – пристрій який можна налаштувати на роботу РЗП на певній частоті, виділяє певний сигнал серед існуючих завад та може демодулювати різноманітні типи сигналів. Спеціальні приймачі мають проводити одразу пошук по всім частотам та робити це послідовно за відносно малий час. Тому такі приймачі і отримали назву – панорамні. Головна їх задача відділити необхідну частоту зі всього спектру, та подавити інші. Якість цієї роботи характеризують, як вибірковість. [16]

Існують панорамні приймачі з послідовним (рис. 2.3.5.) та паралельним аналізом спектра.(рис. 2.3.6.).

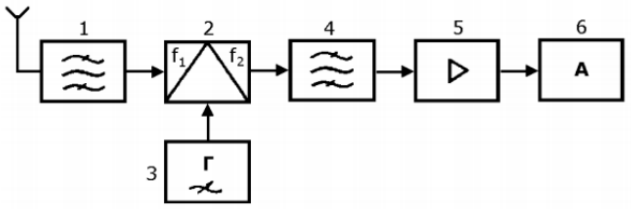


Рис. 2.3.5. Структурна схема з послідовним аналізом в приймачі

У структурній схемі : 1 – фільтр високих частот; 2 – змішувач; 3 – гетеродин (призводить налаштування приймача у заданій полосі); 4 – смуговий фільтр; 5 – вихідний підсилювач; 6 – прилад для аналізу. При режимі автоматичного налаштування сканує весь частотний діапазон у ТМ та отримав назву сканер. [16]

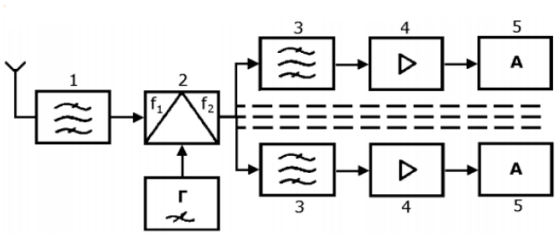


Рис. 2.3.6. Структурна схема з паралельним аналізом в приймачі

У структурній схемі : 1 – фільтр високих частот; 2 – змішувач; 3 – смуговий фільтр (для розділення частот); 4 – вихідний підсилювач; 7 – прилад для аналізу інформації. При режимі автоматичного налаштування сканує весь частотний діапазон у ТМ, також отримав назву сканер. Ця структура дає можливість практично за найменший час проаналізувати увесь спектр пошуку, якщо сигнал буде перевищувати порогову чутливість пристрою. [16]

2.4 Висновки до другого розділу

У даному розділі були досліджені усі ЗП, що можуть бути встановлені у ТМ задля несанкціонованого доступу до ПД. Проаналізувавши доступні методи та пристрої захисту телекомунікаційних мереж від ЗП стає зрозумілим, що кожен має як свої переваги, так і свої недоліки. Тож доцільним є використання методів захисту які надають значно вищий рівень безпеки ПД у ТМ та є вигіднішими у використанні. На основі порівняльного аналізу були обрані методи захисту ПД в ТМ та подальшої розробки алгоритму протекції.

РОЗДІЛ 3

ЗАХИСТ ПД У ТМ З ВИКОРИСТАННЯМ РАНГОВОГО КОДУ ТА ДОТРИМАННЯМ АНОНІМНОСТІ

Мережа зв'язку схильна до втручання у її функціонування зловмисників. Деякі з них можуть спостерігати та аналізувати трафік, інші можуть включати свої повідомлення та використовувати різні закладні пристрої, щоб затруднити правильний прийом ПД. Серед різних методів усунення викрадення ПД у ТМ, центральне місце посідає метод шифрування. Особливий інтерес має передача, коли передавальна та приймальна сторона бажають залишитись невідомими для зловмисника. У цьому виді передачі є досить багато цікавих методів забезпечення анонімності. До огляду включено дослідження двох методів захисту ПД у ТМ: з використанням рангового кода та дотриманням анонімності. [17]

3.1 Захист ПД у ТМ за допомогою рангових кодів

У даному випадку розглядається одноадресна передача ПД у ТМ та застосовується випадкове мережеве кодування на базі рангових кодів.

Модель зловмисника така: він має можливість додавати та вставляти в передачу свої повідомлення. На приймальній стороні треба витягувати інформацію, що передається від джерела, ігноруючи помилкові повідомлення.

Для вирішення цього питання пропоную метод, який ґрунтується на підпросторовій метриці, адже проблеми кодування у підпросторовій метриці можуть бути зведені до побудови кодів із заданою метрикою. Рангові коди достатньо ефективно працюють у схемі ліфтингової конструкції кодової матриці бо вони мають добре розроблені алгоритми виправлення помилок та стирань.

Щодо концепції надійного зв'язку та захисту ПД в когерентному мережевому кодуванні, коли відомі коефіцієнти лінійних комбінацій пакетів повідомлень, то модель зловмисника така: у мережі діє зловмисник, що має доступ до певної кількості ліній зв'язку для підслуховування переданих повідомлень. Крім того, зловмисник у

кожний фіксованний часовий інтервал включає передачу t своїх пакетів. Схема рангового кодування може виправляти рангові t помилок за умови, що відповідна умовна ентропія дорівнює нулю; схема передачі абсолютно секретна, якщо взаємна інформація між реальним повідомленням та повідомленням, підслуханим зловмисником, дорівнює нулю. У цій схемі передачі оптимальні показники досягаються при використанні рангових кодів.

Також можна піти далі існує універсальна схема багатоадресної передачі по мережі довільної конфігурації. Завдання поставлено в такий спосіб. Джерело S за один такт передачі формує n пакетів повідомлень, кожен з яких представляє послідовність довжини m і є елементом поля $GF(q)$. З цих пакетів складається матриця X, яка передається через мережу. На проміжних вузлах мережі складаються лінійні комбінації пакетів. Є два варіанти мережевого кодування: матриця перетворення A відома чи невідома. У першому випадку мережеве кодування називається когерентним, у другому у разі – некогерентним. Здебільшого розглянуто когерентний варіант. У мережі є зловмисник, який має доступ до μ лініях зв'язку і записує передані за цими лініях повідомлення, а також є інший зловмисник, який вносить у мережу t своїх, помилкових для одержувача повідомлень. Поставлено завдання забезпечити безпомилковий зв'язок із досконалою секретністю за типом, визначеним Шенноном [6]. Для забезпечення секретності використаний метод Озарова-Вайнера, в якому переданим повідомленням є синдром для випадково вибраного елемента суміжного класу. Розглянуто два типи атак зловмисників: один включає в мережевий потік свої повідомлення, а інший записує (або підслуховує) повідомлення із основного потоку. Проти атак обох зловмисників використано криптосистему з відкритим ключем ГПТ [12], назва якої утворена з початкових букв прізвищ трьох авторів – Габідулін, Парамонов, Третьяков. Як випадкове мережеве кодування, так і криптосистема ГПТ засновані на рангових кодах. Це дало можливість поєднати в одну процедуру завдання розшифрування та декодування, доповнивши їх проміжним перетворенням. Показано, що за певного вибору параметрів рангового коду система забезпечує захист інформації в мережі: випадкові мережеві коди у

визначеній ступені протистоять включенню помилкових повідомлень зловмисником, а криптосистема ГПТ захищає повідомлення від дешифрування їх криптоаналітиком зловмисником. Застосована тут гібридна схема СКК-ГПТ захищає інформацію, що передається по мережі, від обох типів зловмисників – пасивного (підслуховуючого) та активного. [17]

3.2 Заддання забезпечення анонімності ПД користувачів ТМ

Існують такі ситуації, коли відправник або одержувач ТМ не бажають виявляти свої імена, хочуть зберегти анонімність ПД та приховати факт своєї співпраці. Тут розглянемо методи забезпечення анонімності у ТМ із мережним типом кодуванням.

Треба поділити на три рівні умови забезпечення анонімності: передача повинна бути організована таким чином, щоб приховати сам факт передачі ПД, таку ситуацію визначають як неспостережливість; треба забезпечити анонімність відправника або одержувача повідомлення, тобто встановити , що йде процес передачі повідомлення, але неможливо визначити, хто відправник та одержувач; треба забезпечити анонімність сеансу зв'язку, тобто неможливо встановити зв'язок відправника з отримувачем. [17]

Умови забезпечення анонімної передачі можна задати так: інформація про маршрут доступна лише вузлам мережі, що беруть участь у передачі; передача повідомлення ПД має відбуватися так щоб зловмисник не зміг простежити його маршрут. При маршрутизації повідомлення кожному проміжному вузлу відомі ідентифікатори відправителя та одержувача цього повідомлення. Для анонімної передачі повідомлення кожному вузлу має бути відведено мінімальну кількість маршрутної інформації, тобто тільки адреси попереднього та наступного вузлів маршруту. [17]

Щоб зловмисник міг визначити зв'язок відправник-одержувач, він аналізує трафік: прослуховує з'єднання і використовує кореляцію повідомлень, що входять і виходять з вузла, взаємозв'язок їх розмірів та тимчасових характеристик. При використанні мережевого кодування всі проміжні вузли виробляють лінійні комбінації пакетів, тобто їх «перемішують». Це приховує кореляцію вхідних та

вихідних повідомлень. До того ж закодовані повідомлення мають вигляд пакетів однакового розміру, вони можуть бути затримані на якийсь час на проміжних вузлах. Все це перешкоджає зловмиснику робити аналіз повідомлень за їх розмірами та часом проходження та ускладнює аналіз трафіку[17]

Відомі два підходи забезпечення анонімності передачі ПД у ТМ з мережевим кодуванням: поділ повідомлень на частини; перетворення кодуючого вектора. У першому випадку частини вихідного повідомлення передаються різними маршрутами, кінцевою точкою яких є одержувач повідомлення. Цей підхід цікавий тим, що можна забезпечити анонімність без шифрування. У другому випадку враховують, що при використанні мережевого кодування найуразливішою частиною повідомлення, що передається, є кодуючий вектор, тобто вектор, що визначає правила перетворення повідомлень на проміжних вузлах. Можна вирішити задачу забезпечення анонімності в мережах з мережевим кодуванням, пристосувавши до цих мереж методи забезпечення анонімності, які добре показали себе на мережах з традиційним способом ретрансляції на вузлах. Гарним підходом у нашому випадку є метод ANOC який забезпечує анонімність сеансу зв'язку. [17]

Основу методу ANOC становить лукова маршрутизація. Луковою маршрутизацією називається метод забезпечення анонімності, у якому повідомлення передачі послідовно шифрують за допомогою відкритих ключів всіх вузлів, що входять до маршруту, починаючи з останнього. Маршрут встановлюється наперед. Проміжні вузли виконують над повідомленнями, що надійшли операцію складання по модулю два. Це не дозволяє коректно здійснювати шифрування/розшифрування, властиве луковій маршрутизації. Для вирішення цього конфлікту в ANOC вводяться додаткові операції розподілу сесійних ключів для симетричної системи шифрування та додаткове розшифрування. Розглянемо приклад схеми передачі, поданий на рис. 3.2.1. Кожен вузол має відкритий ключ pk, наприклад pkC - відкритий ключ, що належить вузлу C. [17]

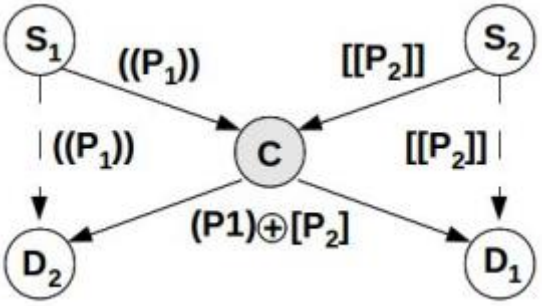


Рис. 3.2.1. Схема роботи методу ANOC

Етап 1: Вузлу $S1$ необхідно передати секретні сесійні ключі k_C^1 та k_D^1 вузлам C і $D1$ відповідно. Для цього $S1$ відправляє C повідомлення $E_{pkc1}(E_{pkD1}(\mathrm{k}_D^1), \mathrm{k}_C^1, I_{D1})$, де $E_{(.)}^{(.)}$ – функція асиметричного шифрування. Розшифрувавши це повідомлення, вузол C витягає свій секретний ключ k_C^1. Ідентифікатор I_{D1} вказує вузлу C на те, що наступним вузлом у маршруті буде $D1$. Узел C відправить повідомлення $E_{pkD1}(\mathrm{k}_D^1)$, вузлу $D1$, який витягне свій секретний ключ k_D^1. Аналогічним чином $S2$ встановить секретні сесійні ключі k_C^2 та k_{D2}^2 з вузлами C та $D2$ відповідно.

Етап 2: Тепер якщо вузол $S1$ хоче передати повідомлення $m1$ вузлу $D1$, то він передає повідомлення $\big((P1)\big) = E_{\mathrm{k}_C^1}(E_{\mathrm{k}_{D1}^1}(m1))$, яке буде отримано вузлом C, а також вузлом $D2$, який прослуховує ефір. Щоб передати повідомлення $m2$ вузлу $D2$, вузол $S2$ відправить повідомлення $[[P2]] = E_{\mathrm{k}_C^2}(E_{\mathrm{k}_{D2}^2}(m2))$, яке отримають вузли C та $D1$.

Етап 3: Вузол C знімає один рівень шифрування з отриманих повідомлень $((P1))$, $[[P2]]$ та відправляє вузлам $D1$ та $D2$ повідомлення виду $(P1) + [P2]$. Вузол $D1$, маючи повідомлення $[[P2]]$ та $(P1)\bigoplus[P2]$, не зможе отримати $m1$. Аналогічно $D2$ з повідомлень $((P1))$ та $(P1)\bigoplus[P2]$ не отримає $m2$.

Етап 4: Вузол C широкомовно відправляє свої секретні ключі k_C^1 та k_C^2 сусіднім вузлам. Вузол $D1$ за допомогою ключа k_C^2 із повідомлення $[[P2]]$ витягує $[P2]$. Склавши по модулю два повідомлення $(P1)\bigoplus[P2]$ з повідомленням $[P2]$, він отримає

($P1$). Розшифрування цього повідомлення на сайті $D1$ дасть повідомлення $m1$. Аналогічно вузол $D2$ отримує повідомлення $m2$. [17]

Завдання зловмисника полягає в тому, щоб визначити, хто кому надсилає повідомлення. Пасивному зловмиснику доступне лише прослуховування трафіку. Зловмисник, здатний прослуховувати вхідні та вихідні повідомлення деякого вузла, не зможе скомпрометувати кореспондентів завдяки властивостям мережевого кодування та шифрування, що ускладнюють аналіз трафіку. Внутрішній зловмисник повністю контролює деякий вузол мережі: йому відомо, як кодуються повідомлення, що проходять через цей вузол. Зловмисник може контролювати проміжні вузли, йому відома інформація тільки про попередній і наступний сайт. Наявність додаткової операції розподілу секретних ключів може дозволити зловмисник визначити деяку кількість вузлів маршруту на додаток до попереднього та наступного.

3.3 Висновки до третього розділу

У даному розділі запропоновані методи для захисту ПД у ТМ, а саме метод анонімності ANOC та метод кодування ПД у ТМ за допомогою рангових кодів. Зазначено, що рангове кодування дозволяє оптимізувати схему передачі і максимізувати швидкість передачі. Показано, що гібридна схема випадкового мережевого кодування і шифрування захищають ПД , що передаються по мережі, від обох типів зловмисників – пасивного та активного. Всі розглянуті та проаналізовані методи захисту інформації в телекомунікаційних мережах дозволяють зробити загальний висновок про те, що найбільш перспективною і найменш доступною для зловмисника схемою передачі є мережне кодування, суміщене з шифруванням повідомлень, що передаються.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи були виконані наступні задачі:

- Телекомунікаційні мережі та персональні дані, що у них циркулюють.
- Закладні пристрої для викрадення персональних даних у телекомунікаційній мережі.
- Захист персональних даних у телекомунікаційній мережі з використанням рангового коду та дотриманням анонімності.

У першому розділі було розглянуто важливість захисту ПД у ТМ. В даний час дуже багато варіантів і каналів витоку чутливих даних у ТМ, що приводить до необхідності вирішення питань захисту інформаціїї загалом. Тож, аби віднайти шляхи розв'язання цих проблем, були досліджені різні види ТМ, класифіковані ПД ,що передаються, проаналізовані потенційні загрози інформації , що в них циркулює та запропоновані методи задля захисту ПД від несанкціонованого доступу каналами витоку.

У другому розділі були досліджені усі ЗП, що можуть бути встановлені у ТМ задля несанкціонованого доступу до ПД. Проаналізувавши доступні методи та пристрої захисту телекомунікаційних мереж від ЗП стає зрозумілим, що кожен має як свої переваги, так і свої недоліки. Тож доцільним є використання методів захисту які надають значно вищий рівень безпеки ПД у ТМ та є вигіднішими у використанні. На основі порівняльного аналізу були обрані методи захисту ПД в ТМ та подальшої розробки методики протекції.

У третьому розділі запропоновані методи для захисту ПД у ТМ, а саме метод анонімності ANOC та метод кодування ПД у ТМ за допомогою рангових кодів. Зазначено, що рангове кодування дозволяє оптимізувати схему передачі і максимізувати швидкість передачі. Показано, що гібридна схема випадкового мережевого кодування і шифрування захищають ПД , що передаються по мережі, від обох типів зловмисників – пасивного та активного. Всі розглянуті та проаналізовані методи захисту інформації в телекомунікаційних мережах дозволяють зробити

загальний висновок про те, що найбільш перспективною і найменш доступною для зловмисника схемою передачі є мережне кодування, суміщене з шифруванням повідомлень, що передаються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. About privacy and the vulnerability of their personal data[Електронний ресурс] https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/
2. Захищеність персональних даних в Україні[Електронний ресурс] https://zib.com.ua/ua/pda/145437.html
3. ЗУ Про телекомунікації[Електронний ресурс] https://kodeksy.com.ua/dictionary/t/telekomunikatsijna_merezha.htm
4. Телекомунікаційна мережа і її складові частини[Електронний ресурс] https://stud.com.ua/94307/informatika/telekomunikatsiyna_merezha_skladovi_chastini
5. Сфера захисту персональних даних[Електронний ресурс] https://ecpl.com.ua/news/top-10-pytan-u-sferi-zakhystu-personal-nykh-danykh/
6. Закон Україні «Про захист персональних даних» [Електронний ресурс] https://zakon.rada.gov.ua/laws/show/2297-17#Text
7. Класифікація телекомунікаційних мереж[Електронний ресурс] https://www.znanius.com/3561.html
8. Main channels of information leakage [Електронний ресурс] https://searchinform.com/challenges/information-security/information-security-analytics/information-leaks/information-leakage-causes/main-channels-of-information-leakage/
9. Захист інформації в телекомунікаційних мережах [Електронний ресурс] http://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf

10. Tekhnichni_kanaly_vytku [Електронний ресурс] https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

11. How to reduce data security risks in the telecom industry[Електронний ресурс] https://www.endpointprotector.com/blog/reducing-data-security-risks-in-the-telecom-industry/

12. Технічний захист інформації [Електронний ресурс] https://www.znanius.com/3853.html

13. Характеристика електронних пристроїв перехоплення інформації [Електронний ресурс] https://radio.bobrodobro.ru/4496

14. Системы и устройства информационной безопасности. Учебное пособие /под ред. проф. В.А. Хорошко/ Соавторы: А.П. Провозин, О.В., Рыбальский, В.А.Хорошко, Д.В. Чирков/- К.ДУИКТ, 2007

15. Радіозакладки [Електронний ресурс] https://cyberpedia.su/17x1373c.html

16. Захист інформації технічними способами [Електронний ресурс] https://books.ifmo.ru/file/pdf/975.pdf

17. Захист інформації у ТМ [Електронний ресурс] https://cyberleninka.ru/article/n/zaschita-informatsii-v-telekommunikatsionnyh-setyah/viewer

ДОДАТОК А

Оформлення слайдів та роздаткового матеріалу