Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)

Кафедра _____Автоматизації проектування обчислювальної техніки_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
(рівень вищої освіти)

_____Система забезпечення конфіденційності передачі інформації у _____ прихованому каналі _____
_____
(тема)

Виконав: студент 2 курсу, групи СКСм18-1
_____Левочко Т.Г._____
(прізвище, ініціали)

Спеціальність _123 Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми__освітньо-професійна_____
_____
(освітньо-професійна або освітньо-наукова)

Освітня програма___Спеціалізовані_____
_____комп'ютерні системи_____
(повна назва освітньої програми)

Керівник __ст.викл. Рожнова Т.Г._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ __Чумаченко С.В.___
(підпис) (прізвище, ініціали)

20_19 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
Кафедра Автоматизації проектування обчислювальної техніки
Рівень вищої освіти другий (магістерський)
Спеціальність 123 – Комп'ютерна інженерія
Тип програми Освітньо-професійна
Освітня програма Спеціалізовані комп'ютерні системи
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Левочко Тетяні Геннадіївні
(прізвище, ім'я, по батькові)

1. Тема роботи Система забезпечення конфіденційності передачі інформації у прихованому каналі
затверджена наказом по університету від 04 11 20 19 р. № 1624 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 24.12. 20 19 р.
3. Вихідні дані до роботи параметри аудіо контейнеру: частота дискретизації 44100Гц, кількість біт представлення – 32 біт пакет MATLAB2014A, бібліотеку Audio System, завантаження аудіо контейнеру на основі функціоналу wavread

4. Перелік питань, що потрібно опрацювати в роботі 1) аналіз існуючих підходів забезпечення обміну інформації в комп'ютерних системах ;
2) аналіз джерел та існуючих вітчизняних та закордонних зразків обладнання обміну інформацією ;
3) аналіз криптографічних алгоритмів гарантованого захисту інформації;
4) розробка методу прихованої передачі повідомлень в системі забезпечення конфіденційності передачі інформації у прихованому каналі;
5) Розробка програмного коду для тестування системи забезпечення захисту конфіденційності передачі інформації у прихованому каналі

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 24 слайди

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Спец.розділ	Ст. викл. Каф. АПОТ Рожнова Т.Г.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	10.09.2019	
2	Аналіз предметної області	20.09.2019	
3	Аналіз джерел та існуючих вітчизняних та закордонних зразків обладнання обміну інформацією	10.10.2019	
4	Аналіз криптографічних алгоритмів гарантованого захисту	15.10.2019	

5	Формулювання вимог до методу прихованої передачіданих	25.10.2019	
6	Розробка методу прихованої передачі повідомлень в системі забезпечення конфіденційності	20.11.2019	
7	Розробка програмного коду	01.12.2019	
8	Оформлення пояснювальної записки	10.12.2019	
9	Перевірка виконаного проекту керівником	15.12.2019	
10	Захист атестаційної роботи	24.12.2019	

Дата видачі завдання 10.09.2019

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить : 71 листів, 18 рисунків, 20 джерел за переліком посилань.

МАСКУВАННЯ, ДЕМАСКУВАННЯ, АУДІО КОНТЕЙНЕР, МОВНЕ ПОВІДОМЛЕННЯ, ПРОГРАМНИЙ КОД

Метою роботи є створення системи забезпечення конфіденційності передачі інформації за рахунок методу прихованої передачі інформації в аудіо контейнері.

Після аналізу підходів до забезпечення інформаційної захищеності обміну даними виділено два методи: 1) криптографічний метод; 2) метод маскування інформації. Сформульовано вимоги щодо методу приховуваної передачі даних у контейнері.

Розроблено метод прямого маскування інформації в мовному повідомленні та демаскування із забезпеченням виконання вимог до розробленого методу Розроблено програму для проведеня аналізу ефективності розробленого методу.

Система забезпечення конфіденційності передачі інформації у прихованому каналі, що розроблено у роботі та запропонований метод особливо актуальні для використання в корпоративних комп’ютерних системах, що базуються на засобах телекомунікаційного зв’язку і комп’ютерних мереж передачі даних, де необхідно забезпечити рівень безпеки спеціальних інформаційних ресурсів.

Технології, що використано в роботі, засновано на непрямій модифікації компонент фазового спектру аудіоконтейнеру за сформульованим правилом.

ABSTRACT

Explanatory note contains : 71 pages, 18 drawingsfig, 20 sources by reference list

MASKING, UNMASKING, AUDIO CONTAINER, VOICE MESSAGES., PROGRAM CODE

The aim of the work is to create a system for ensuring the confidentiality of information transfer on the basis of the method for embedding data in an audio container by indirectly modifying the components of the phase spectrum.

After analyzing approaches to ensuring information security of data exchange, two methods are distinguished: 1) the cryptographic method, 2) the method of information masking. Formulated requirements for the method of hidden data transfer in the container.

A method has been developed for direct masking of information in a voice message and unmasking to ensure the requirements for the developed method. A program has been developed for analyzing the effectiveness of the developed method.

A system for ensuring the confidentiality of information transmission in a hidden channel is developed and the method proposed is especially relevant for use in corporate computer systems based on telecommunication facilities and computer data transfer networks where it is necessary to ensure the level of security of special information resources.

The technologies used in the work are based on an indirect modification of the phase spectrum components of the audio container, taking into account the formulated rule.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

DES – Data Encryption Standard, алгоритм для симетричного шифрування;

RSA – Rivest, Shamir and Aldeman, асиметричне шифрування на основі відкритого ключа;

КМ – комп’ютерна мережа;

КС – комп’ютерна система ;

ПКЗД – Пристрої криптографічного захисту даних;

РЕБ – радіоелектронна боротьба ;

СІР – спеціальні інформаційні ресурси;

СК – системний комп’ютер ; КС

– комп’ютерна система.

ВСТУП

Стрімкий розвиток інформаційних технологій та їх поширення практично в усіх сферах діяльності людини диктує вимоги щодо інформаційного забезпечення комп'ютерної системи безпекою. З метою приведення усіх компонентів системи до стандартів безпеки, у тому числі, систем управління та обміну інформацією, до сучасного рівня та з метою підвищення ефективності системи управління та інформаційної підтримки комп'ютерних мереж (КМ) в цілому, а також на компонентному рівні використовують принцип єдиного інформаційного простору.

Розвиток сучасних інформаційних технологій супроводжується збільшенням ролі телекомунікаційних систем різного призначення та комп'ютерних мереж. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі й управлінської, для якої важливе значення мають оперативність її доставки до користувачів.

Особливе місце в цих завданнях займають сучасні технології комп'ютерних мереж, серед яких слід виділити локальні та глобальні мережі. Це пояснюється необхідністю використання корпоративної інформації, що міститься в корпоративних базах даних, які можуть розташовуватися як в окремих підрозділах підприємства, так й за його межами. Отже сучасні технології обробки документації різного призначення повинні базуватися на засобах телекомунікаційного зв'язку й стандартів комп'ютерних мереж, які виступають як транспортні системи передачі даних, де і виникає потреба необхідного рівня безпеки спеціальних інформаційних ресурсів.

Питання забезпечення інформаційної захищеності в таких системах найбільш актуально стоїть для державних силових структур та відомств, не виключно і для Збройних Сил України, а взагалі для любої корпоративної системи де є загроза порушення конфіденційності та цілісності інформації.

Аналіз основних тенденцій розвитку корпоративних систем, а також досвід конфліктів останнього часу показує, що одним з пріоритетних напрямків в забезпеченні ефективного управління є удосконалення засобів зв'язку та передачі даних як у самій системі, так і за її межами. Важливість надійного, якісного, завадозахищеного зв'язку наочно продиктована необхідністю захисту інформації. В першу чергу це вимагає приведення існуючих засобів зв'язку до сучасних вимог та стандартів, існує необхідність використання нових підходів до вирішення задачі захисту інформації в комп'ютерних системах та мережах.

Тому підвищення безпеки в інфокомунікаційних комп'ютерних системах є актуальним напрямом для науково-прикладних досліджень. Одним з таких напрямів забезпечення безпеки інформаційного ресурсу є використання стенографічних та криптографічних методів вбудовування інформації у контейнері.

Базою для реалізації такого підходу є системи відеоконференції, що дозволяють використовувати мультимедійні засоби зв'язку, застосовувати контейнер-зображення і звуковий-контейнер для передавання конфіденційної інформації у перетвореному вигляді.

Тому створення прихованого каналу передачі даних, про який не дізнається опонент (супротивник по бізнесу, та інші), а знають лише відправник інформації та її одержувач, тобто приховані повідомлення кодуються всередині голосового повідомлення таким чином, що змін не помітити, є актуальним.

Кваліфікаційна робота за темою: «Система забезпечення конфіденційності передачі інформації у прихованому каналі», що присвячено цій проблемі є також своєчасною та актуальною.

Об’єктом дослідження є методи забезпечення конфіденційності інформації .

Метою кваліфікаційної роботи є створення системи забезпечення конфіденційної передачі інформації за рахунок методу прихованої передачі інформації в аудіоконтейнері.

Для досягнення поставленої мети необхідно розв’язати такі задачі**:**

– провести аналіз існуючих підходів забезпечення обміну інформацією в комп’ютерних інформаційних системах;

– проаналізувати існуючи підходи до забезпечення інформаційної захищеності обміну даними ;

– розробити метод прихованої передачі інформаційних повідомлень.

1 АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ЗАБЕЗПЕЧЕННЯ ОБМІНУ ІНФОРМАЦІЄЮ В КОМПЮТЕРНИХ СИСТЕМАХ

1.1 Аналіз стану інформаційного забезпечення

Сучасні тенденції щодо розвитку інформаційних технологій та їх поширення практично у всіх сферах діяльності людини диктує вимоги щодо інформаційного забезпечення. В першу чергу це обумовлено необхідністю швидкого обміну оперативною інформацією для прийняття рішень уповноваженими особами. В той же час функціонування сучасних систем управління неможливе без відповідного інформаційного забезпечення.

На теперішній час виділяються два підходи до проблеми забезпечення безпеки комп'ютерних систем та мереж : – фрагментарний, або частковий підхід; – комплексний підхід.

Фрагментарний, або частковий підхід спрямовано на протидію загрозам у заданих умовах, що чітко визначені.

В якості прикладів реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми та інше.

Переваги підходу: висока вибірковість до конкретної загрози.

Недолік: відсутність єдиного захищеного середовища обробки інформації.

Отже фрагментарні заходи захисту інформації забезпечують лише захист конкретних об'єктів КС тільки від конкретної загрози, а незначна видозміна загрози призведе до втрати ефективного захисту.

Комплексний підхід орієнтовано на створення захищеного середовища обробки інформації в КС. Така система об'єднує в єдиний комплекс різнорідні заходи протидії загрозам.

Створення захищеного середовища обробки інформації дозволяє забезпечити певний рівень безпеки КС, це і є достоїнством комплексного підходу.

Недоліками цього підходу є обмеження на свободу дій користувачів у комп'ютерній системі, складність управління та необхідність налаштування засобів захисту. Комплексний підхід застосовують для захисту КС великих організацій також систем, що обробляють особливо важливу інформацію.

Порушення безпеки інформації в КС організацій може нанести величезний матеріальний збиток як самим організаціям, так і їх клієнтам, тому треба приділяти особливу увагу гарантіям безпеки та використовувати комплексний захист.

Комплексний підхід захисту інформації притаманно для більшості державних і комерційних підприємств. Цей підхід знайшов своє відображення в різних стандартах. Комплексний підхід до проблеми забезпечення безпеки засновано на розробленні для конкретної КС політики безпеки [1].

Політика безпеки охоплює всі особливості процесу обробки інформації в комп'ютерній системі, вона диктує поведінку системи в різних ситуаціях та створює надійну систему безпеки мережі .

Інформаційні системи (ІС) компаній зачастую побудовано на основі програмних і апаратних продуктів різних виробників. Поки немає жодної компанії-розробника, яка надала б споживачеві повний перелік засобів, від апаратних до програмних, для побудови сучасної КІС.

Щоб забезпечити в різнородній ІС надійний захист інформації потрібні фахівці високої кваліфікації, які повинні відповідати за безпеку кожного

компонента ІС: правильно їх налаштовувати, постійно відслідковувати зміни, контролювати роботу користувачів, чим різноманітнішою є КІС, тим складніше забезпечити її безпеку.

В корпоративних мережах і системах достатньо пристроїв захисту, міжмережевих екранів (МЕ), шлюзів і VPN і таке інше. Але попит на доступ до корпоративних даних з боку співробітників, партнерів і замовників призводять до створення складного середовища захисту.

Таке середовище є важким для управління, а іноді стає вибір – або захист даних, або швидкий доступ для користувачів. Вирішення безпеки має гарантувати захист інформації на всіх платформах в рамках організації КС. Тому виникає потреба в застосуванні єдиного набору стандартів засобів захисту для систем безпеки. Стандарти є необхідною основою, що забезпечує сумісність продуктів різних виробників, на якій будуються всі роботи щодо забезпечення інформаційної безпеки. Стандарти визначають критерії, яким має слідувати управління безпекою – це той фундамент, на якому будується вся система захисту корпоративних мереж [1,2].

1.2 Заходи і засоби програмно-технічного рівня.

На сьогоднішній день на етапі стрімкого розвитку усіх компонентів систем управління та обміну інформацією, та приведення їх до сучасного рівня, найактуальнішими питаннями щодо інформаційного забезпечення, особливо важливі заходи програмно-технічного рівня, оскільки основна загроза комп'ютерних систем виходить безпосередньо від них самих:

- збої обладнання;
- помилки програмного забезпечення;

– промахи користувачів і адміністраторів і т.п.

В сучасних інформаційних системах повинно бути впровадження наступних механізмів безпеки для обміну та захисту інформації, таких як :

– сучасні технології обміну оперативною інформацією;

– ідентифікація та перевірка справжності користувачів (аутентифікація та авторизація);

– захищені комунікаційні протоколи;

– засоби криптографії;

– антивірусні комплекси;

– програми виявлення атак ;

–засоби централізованого управління контролем доступу користувачів, а також безпечного обміну пакетами даних і повідомленнями у відкритих IPмережах;

– системи захисту інформації від несанкціонованого доступу, управління доступом;

– нові методи та алгоритми обробки інформації;

– системи моніторингу та оцінки;

– інтелектуальні технології прийняття рішень на основі штучного інтелекту.

Для сучасних систем характерною рисою є функціонування різних елементів КС у єдиному інформаційному просторі, основні компоненти, з яких складається така система, представлено на рисунку 1.1.

На теперешній день з метою підвищення ефективності системи управління та інформаційної підтримки КС та КМ в цілому, визначають такі основні

напрямки подальшого розвитку з використанням принципу єдиного інформаційного простору :

– доступ усіх учасників до незалежної інформації про об'єкти взаємодії в реальному масштабі часу;

– обмежена залежність інформаційної підтримки від рівнів ієрархії органів управління;

– розроблення нового підходу до планування – об'єднання етапів загального та безпосереднього планування та здійснення планування у єдиному органі;

– розвиток глобальних комунікаційних зв'язків між територіально розосередженими, але об’єднаними в єдину мережу ПК, забезпечення можливості для всіх складових системи та її частин обмінюватися інформаційними потоками безперешкоджено.

СПК – спеціалізований ПК

ПК– персональний комп’ютер

Засоби РЕБ – засоби радіоелектронної безпеки

Рисунок 1.1 – Концепція взаємодії компонентів КС в єдиному інформаційному просторі

Інформаційна підтримка обміну даними в комп'ютерній системі показано на рисунку1.2.

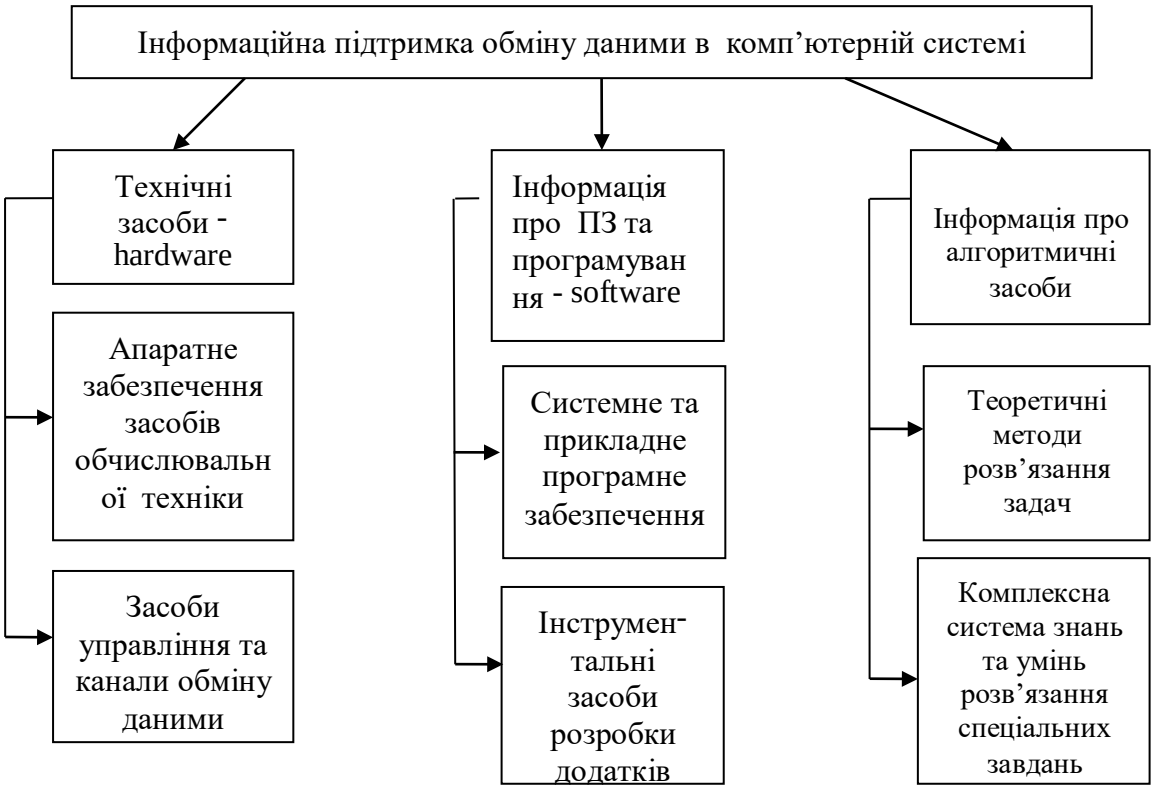

Рисунок 1.2 – Підтримка обміну між компонентами системи

Під час функціонування КС виникають загрози інформаційної безпеки, які можна розподілити на три умовні групи [2,3] :

– загрози конфіденційності інформаційного ресурсу, тобто доступ до конкретної інформації обмеженому кругу осіб;

– загрози цілісності інформаційного ресурсу під час передавання та обробки інформації за необережністю або навмисно;

– загрози доступності до інформаційного ресурсу, тобто порушення доступності до інформації за інтервал часу, необхідний для своєчасного обміну даними.

Види загроз для обміну даними між компонентами системи та джерела виникненнях таких загроз представлено на рисунку 1.3.

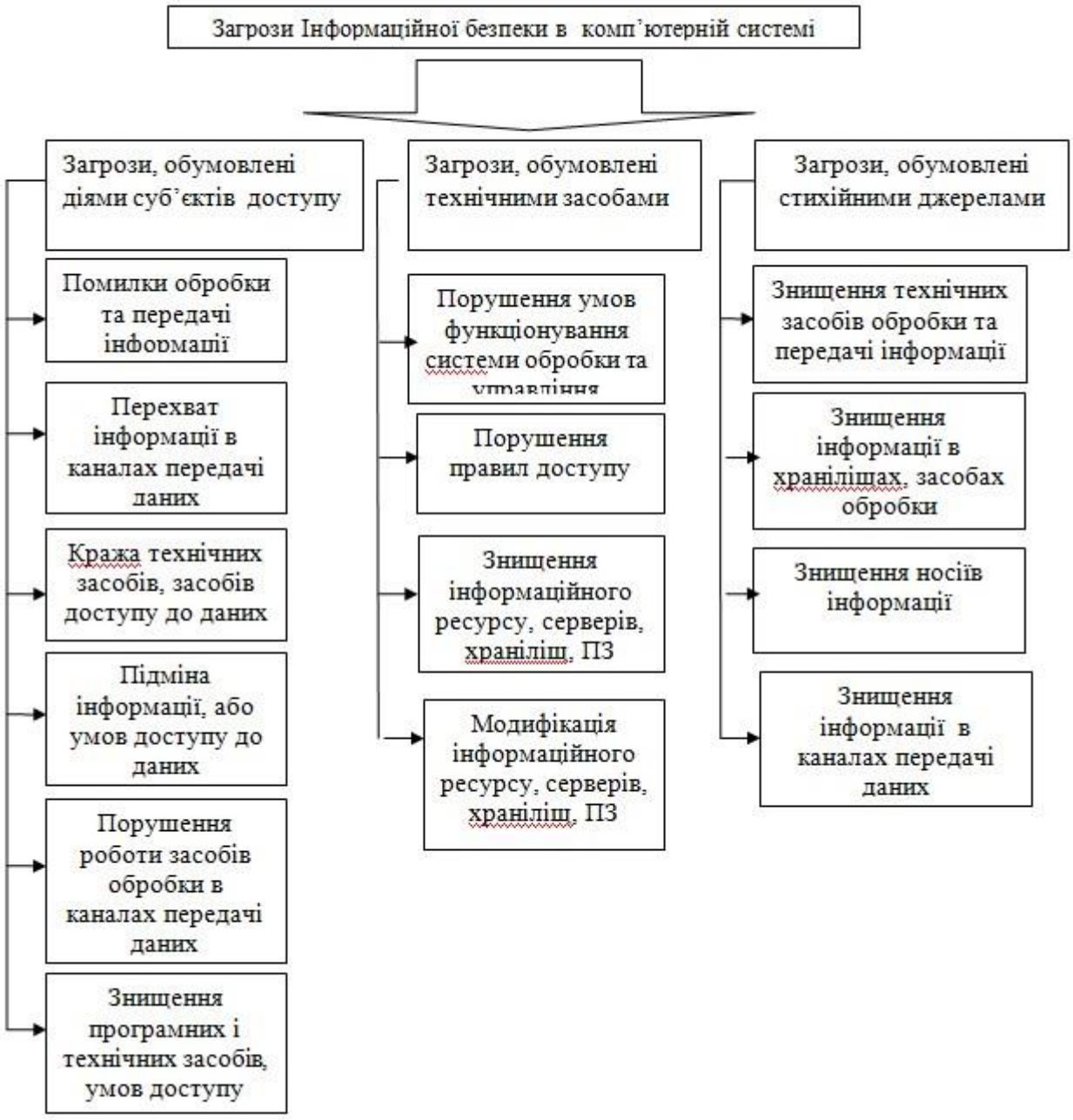

Рисунок 1.3 – Види загроз для обміну даними між компонентами системи та джерела виникненнях загроз

Для найбільш ефективної роботи системи є своєчасний та достовірний обмін зазначеною інформацією, така робота системи вимагає використання сучасної каналоутворюючої апаратури з достатньою пропускною здатністю.

1.2 Аналіз існуючих вітчизняних та закордонних зразків обладнання обміну інформацією

Серед сучасних засобів забезпечення обміну інформацією у режимі частотної телеграфії з використання допоміжного обладнання найбільш поширеною є радіостанція Р-862. Забезпечення обміну інформацією відбувається при наявності блоку частотної телеграфії, який перетворює вхідну інформацію на сигнал звукового діапазону з двома частотами. При цьому логічному нулю відповідає значення низької частоти, а логічній одиниці відповідає значення високої частоти [3,4]. Технічні характеристики радіостанції Р-862 наведено в таблиці 1.1.

Таблиця 1.1 – Технічні характеристики радіостанції Р-862

Діапазон робочих частот	100-149,975 МГц 220-399,975 МГц
Рознос частот	25 кГц
Кількість фіксованих частот зв’язку	в МХ діапазоні 2000 в ДМХ діапазоні 200
Потужність передавача	В МХ діапазоні 10 Вт В ДЦХ діапазоні 8 Вт
Чутливість приймача	3 мкВ
Вид модуляції	АМ, ЧМ, ЧТ
Частота настройки аварійного приймача	в МХ діапазоні 121,5 МГц в ДМХ діапазоні 243 МГц
Час готовності до роботи	5 хв.
Час переходу з каналу на канал	Не більше 1,5 с

Час безперервної роботи на ПЕРЕДАЧУ	Не більше 20 хв.
Маса комплекту	13,83 кг
Напруга живлення	27 В

Радіостанція Р-862 є аналоговим засобом передачі інформації. В умовах передачі даних за допомогою Р-862 при роботі в єдиному інформаційному просторі виникають наступні системні недоліки:

1) обмежена пропускна здатність каналу передачі даних;

2) відсутність можливості одночасного ведення переговорів та забезпечення обміну інформацією;

3) обмежений рівень інформаційної скритості обміну повідомлень.

У порівняні з аналоговими радіостанціями цифрові бортові засоби передачі інформації мають ряд переваг.

Функціонування бортових цифрових засобів розглянемо на прикладі бортової авіаційної багатофункціональної УКХ радіостанції RF-7850A-MR виробництва Сполучених Штатів Америки. Технічні характеристики радіостанції RF-7850A-MR наведено в таблиці 1.2.

Таблиця 1.2 –Технічні характеристики радіостанції RF-7850A-MR

Діапазон робочих частот	30-512 МГц 225-512 МГц
Рознос частот	8.33, 12.5, 25, 75 кГц и 1,2 МГц
Кількість каналів	2
Потужність передавача	по 5 Вт на канал

Режими зв’язку	Аналоговий мовний зв’язок AM/FM, Мовний зв’язок FSK/ASK MELP, Мовний зв’язок FSK/ASK CVSD, Обмін даними ASK, FSK/TCM Широкосмуговий обмін даними
Напруга живлення	28 В

Радіостанція RF-7850A-MR забезпечує обмін повідомленнями відповідно до загальноприйнятих протоколів передачі даних (ASK DTE Data, ECCM IP Data, WBFSK/TCM DTE Data, WBFSK/TCM IP Data, ANW2Ce IP Data). При цьому можливо використання криптографічних алгоритмів забезпечення гарантованої захищеності повідомлень AES 256 та AES 126.

На рисунку 1.4. представлено схему функціонування радіостанції в єдиному інформаційному просторі управління силами та засобами.

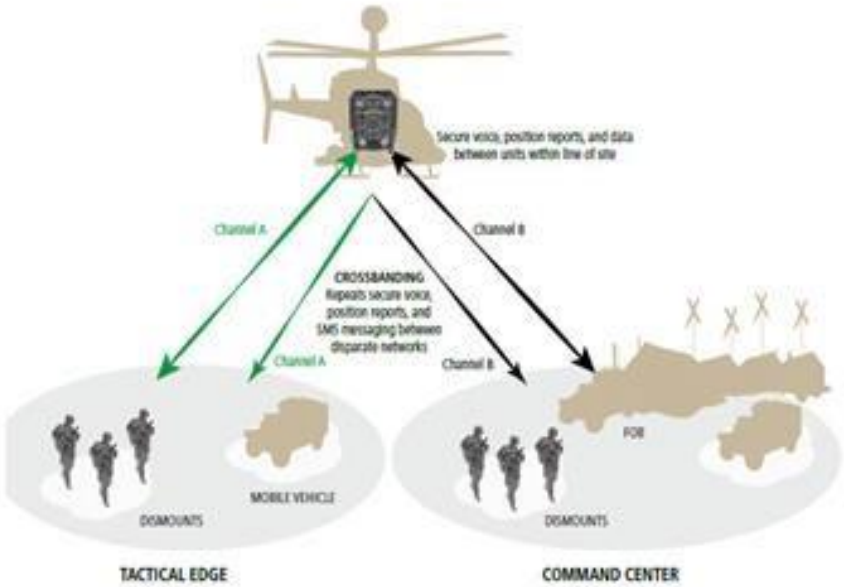

Рисунок 1.4 – Функціонування радіостанції RF-7850A-MR в єдиному інформаційному просторі управління силами та засобами

Аналіз закордонних зразків обладнання обміну інформацією дає можливість зробити висновок, що у випадку впровадження технології обміну інформацією між користувачами в системі при роботі цифрових та аналогових засобів зв'язку у рамках єдиного інформаційного простору виникають проблемні обмеження [3,4]., які представлено на рисунку 1.5.

Рисунок 1.5 – Проблемні моменти (недоліки) роботи обладнання

Для усунення виявлених недоліків необхідно розробити метод передачі інформації для обміну голосовим повідомленням одночасно з можливістю обміну додаткових даних.

1.3 Аналіз стану захищеності інформації під час роботи каналів передачі даних

При створені каналів передачі даних актуальним питанням є забезпечення заданого рівня інформаційної захищеності, що в свою чергу впливає на своєчасний та якісний обмін інформаційними повідомленнями. Але для самого каналу передачі даних існують загрози порушення складових інформаційної безпеки. Розглянемо існуючі різновиди загроз [4]:

1) загрози доступності до інформаційних повідомлень. Порушення доступності являє собою створення таких умов, при яких доступ до інформації або неможливий, або можливий за інтервал часу, який не забезпечить абоненту виконання своїх цілей (своєчасного обміну даними);

2) загрози цілісності інформаційних повідомлень. Загрози порушення цілісності даних – це загрози, пов'язані з ймовірністю навмисної або пасивної модифікації повідомлень, що оброблюються, зберігаються або передаються в інформаційній системі. Порушення цілісності може бути викликано різними чинниками – від умисних дій до виходу з ладу обладнання для передачі інформації;

3) загрози конфіденційності обміну даними. Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Тобто інформаційна складова обміну даними може стати відомою противнику, конкуренту по бізнесу та іншим.

Можна виділити наступні фактори, що впливають на загрозу інформаційної безпеки обміну даними:

– відсутність механізмів гарантованого забезпечення конфіденційності обміну даними у середині комп’ютерної системи.

– знищення каналу передачі даних.

Аналіз сьогоднішнього досвіду ведення бойових дій в зоні АТО , наприклад, показав, що супротивник може застосовував засоби РЕБ, такі як: «Ртуть-БМ», «Житель», та інші, які знищують канал передачі даних між підрозділами, не даючи таким чином змоги ефективного управління в мережі. Це означає, що для забезпечення обміну повідомленнями між користувачами в мережі при роботі в єдиному інформаційному просторі в умовах складної радіотехнічної обстановки необхідно одночасно з розробкою методу передачі інформації забезпечити належний рівень інформаційної захищеності даних.

Для виконання такого роду задач далі буде проведено аналіз існуючих методів захисту інформації.

У розділі розглянуто актуальність питання удосконалення засобів зв’язку та передачі даних КС. Визначено, що функціонування сучасних комп’ютерних систем, в першу чергу таких як системи озброєння, комерційні системи неможливе без відповідного інформаційного забезпечення.

2. АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОБМІНУ ДАНИМИ.

2.1 Кріптографія технологія безпеки КС

Конфіденційність інформації або повідомлень в КС може використовуватися, коли необхідно забезпечити будь-який ступінь таємності інформації. Як перший ступінь захисту використовується контроль входу в систему, розмежування доступу до ресурсів, але для забезпечення таємниці деяких документів використовують шифрування інформації. Таке перетворення інформації в незрозумілу форму, зветься шифротекстом [5].

Інформація може зашифровуватись апаратним методом, для зберігання на певних носіях; кодуватися програмними методами, що ускладнює розшифровку, якщо зловмисник або опонент не знає принципу кодування. Інформацію можна кодувати із застосуванням розділених ключів, для обмеження доступу, тільки фіксованому списку осіб. Більш трудомісткою по швидкості дешифрування є методика розміщення даних в графічні зображення.

Інформаційна безпека в комп'ютерних системах, а точніше в інформаційних комп'ютерних система спирається на криптографічні методи. Контроль входу в систему, розмежування доступу до ресурсів, та безпечне зберігання даних в КС спираються на використання криптографічних алгоритмів.

Само шифрування представляє собою процесс перетворення повідомлення з відкритого тексту в шифротекст таким чином щоб:

– прочитати повідомлення змогли тільки ті кому воно адресовано ;

– можна перевірити подлинність відправника, аутентифікувати; – можливість первірки що відправник перслав це повідомлення.

Наявність ключа в алгоритмах шифрування – це основа методу. Ключ – це якийсь параметр, що не залежить від відкритого тексту. У криптографії прийнято правило Кірхгоффа: "Стійкість шифру повинна визначатися тільки секретністю ключа".

Використання методу шифрування з секретним або симетричним ключем, де є один ключ, що використовують для шифрування, так і для розшифровування повідомлення. Це ускладнює використання системи шифрування, такий ключ потрібно зберігати в секреті та постійно змінювати, та секретно передавати . Популярні алгоритми шифрування з секретним ключем DES, TripleDES та інші.

Частіше використовується шифрування за допомогою односторонньої функції, також хеш- функцією, або дайджест-функцією. Використання цієї функції до зашифрованих даних дозволяє сформувати невеликий дайджест з декількох байтів, за яким неможливо відновити вихідний текст. Одержувач повідомлення перевіряє цілісність даних, порівнюючи отриманий разом з повідомленням дайджест за обчисленнгям знову за допомогою тієї ж односторонньої функції. Цей спосіб використовують для контролю входу в систему.

Найбільш поширеними є системи шифрування з public / assymmetric key – відкритим або асиметричним ключем. В таких системах використовується два ключі, один з ключів, так званий відкритий, не є секретним, використовується

для шифрування повідомлень, які можуть бути розшифровані тільки за допомогою секретного ключа, що є у одержувача, для якого призначено повідомлення. Іноді для шифрування повідомлення використовується секретний ключ, і якщо повідомлення можна розшифрувати за допомогою відкритого ключа, справжність відправника буде гарантовано (наприклад, система електронного підпису). Цей принцип винайдено Уітфілдом Діффі та Мартіном Хеллманом.

На даний час асиметричне шифрування на основі відкритого ключа RSA використовує більшість продуктів на ринку інформаційної безпеки. Його криптостійкість грунтується на складності розкладання на множники великих чисел, а саме – на винятковій складності завдання визначити секретний ключ на підставі відкритого, так як для цього буде потрібно вирішити задачу про існування дільників цілого числа. Найбільш криптостійкі системи використовують 1024-бітові і великі числа.

2.1.1 Криптографічна система з відкритим ключем

Асиметричне шифрування – це система шифрування або електронного цифрового підпису (ЕЦП), при якій відкритий ключ передається по незахищеному від стороннього спостереження каналу, і використовується для перевірки ЕЦП і шифрування повідомлення. Ключі можна використовувати парами – ключ шифрування і ключ дешифрування, завдяки чому отримати один ключ із іншого не представляється можливим. На рисунку 2.1 показано схему передавання інформації відправником А отримувачу В через систему асиметричного шифрування.

Велику частину безпечних алгоритмів засновано на, так званих, необоротних функціях. У криптографії під необоротними функціями мають на

увазі, таки що за ними неможливо отримання зворотного значення за допомогою сучасної техніки за доступний інтервал часу.

Всі, відомі на даний момент, системи з відкритим ключем базуються на одному з трьох типів необоротних перетворень:

– розклад великих чисел на прості множники, RSA;

– обчислення логарифма в кінцевому полі, криптосистема Ель-Гамаля;

– обчислення коренів алгебраїчних рівнянь, на базі еліптичних рівнянь.

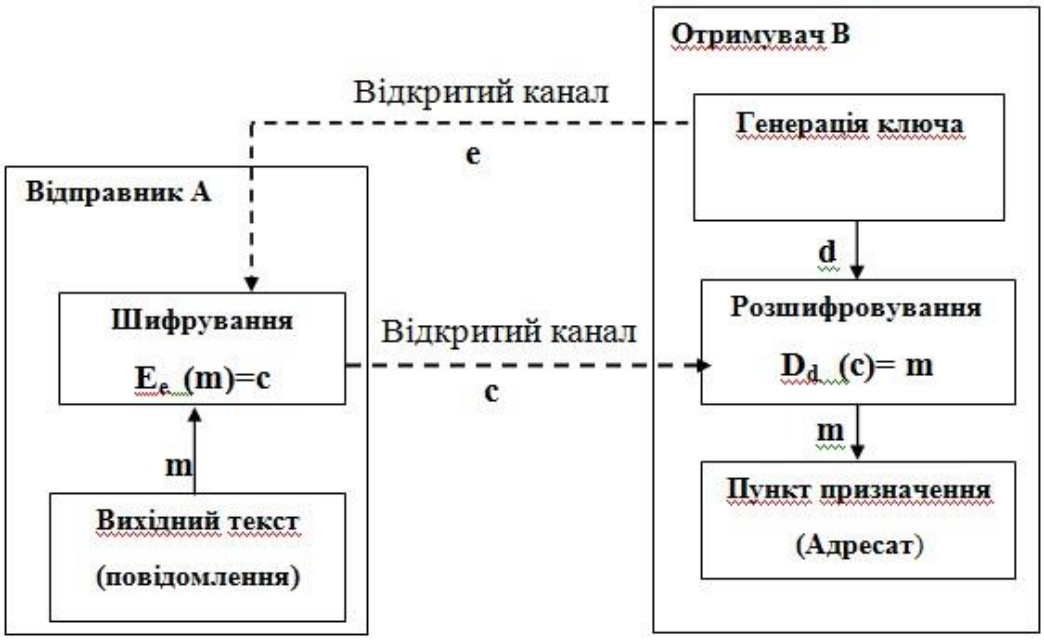

Рисунок 2.1 – Схема передавання повідомлення відправником A отримувачу B

Криптосистеми з відкритим ключем останнім часом широко застосовуються в якості самостійних засобів захисту переданих і збережених даних, як засіб для розподілу ключів і засоби аутентифікації користувачів [6,7]..

Всі сучасні криптосистеми з відкритим ключем дуже повільні і практично жодна з них не може зрівнятися за швидкодією з симетричними криптосистемами.

Швидкодія RSA в тисячі разів нижче, ніж у DES Тому ефективніше використовувати гібридні криптосистеми.

2.1.2 Атаки на криптосистему

Прикладом того як працюють методи криптографії з відкритим ключем є зберігання паролів в комп'ютері. У кожного користувач в мережі є свій секретний пароль. При вході в мережу, користувач вказує своє ім'я і вводить пароль. для вирішення завдання використовується одностороння або необоротна функція. У процесі створення секретного пароля в комп'ютері зберігається деякий час сам пароль, а потім результат обчислення функції від цього пароля та імя користувача, тому зміна даже однієї літери в паролі або імені дасть зовсім інший результат обчислення значення функції.

На рисунку 2.2 показано як може захватити систему без зламування системи шифрування перехоплювач під час роботи каналів передавання даних.

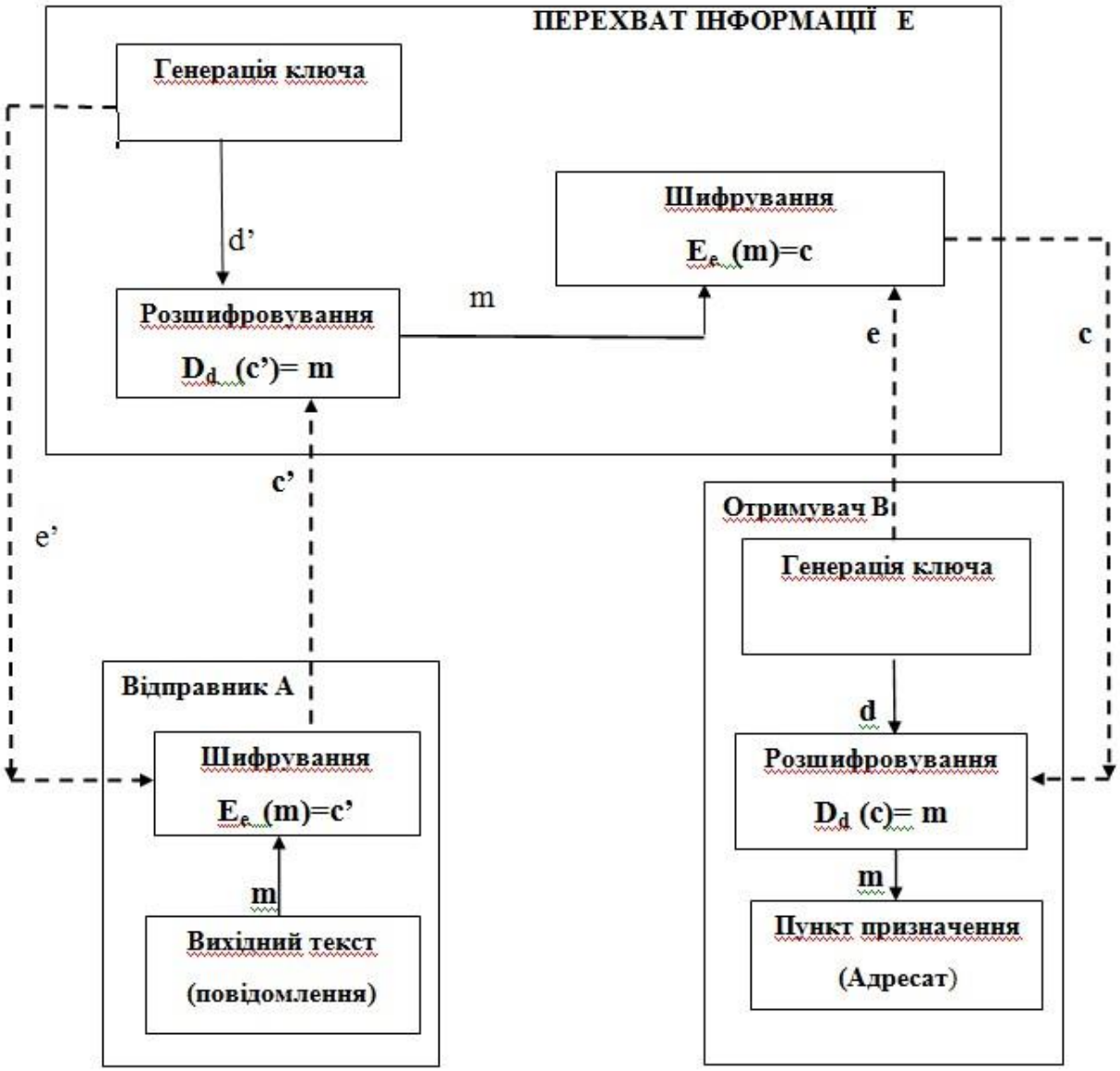

Рисунок 2.2 – Демонстрація, того як може захватити систему без зламування системи шифрування перехоплювач

На рисунку 2.3 показано атаку обчислення закритого ключа, коли відомо відкритий.

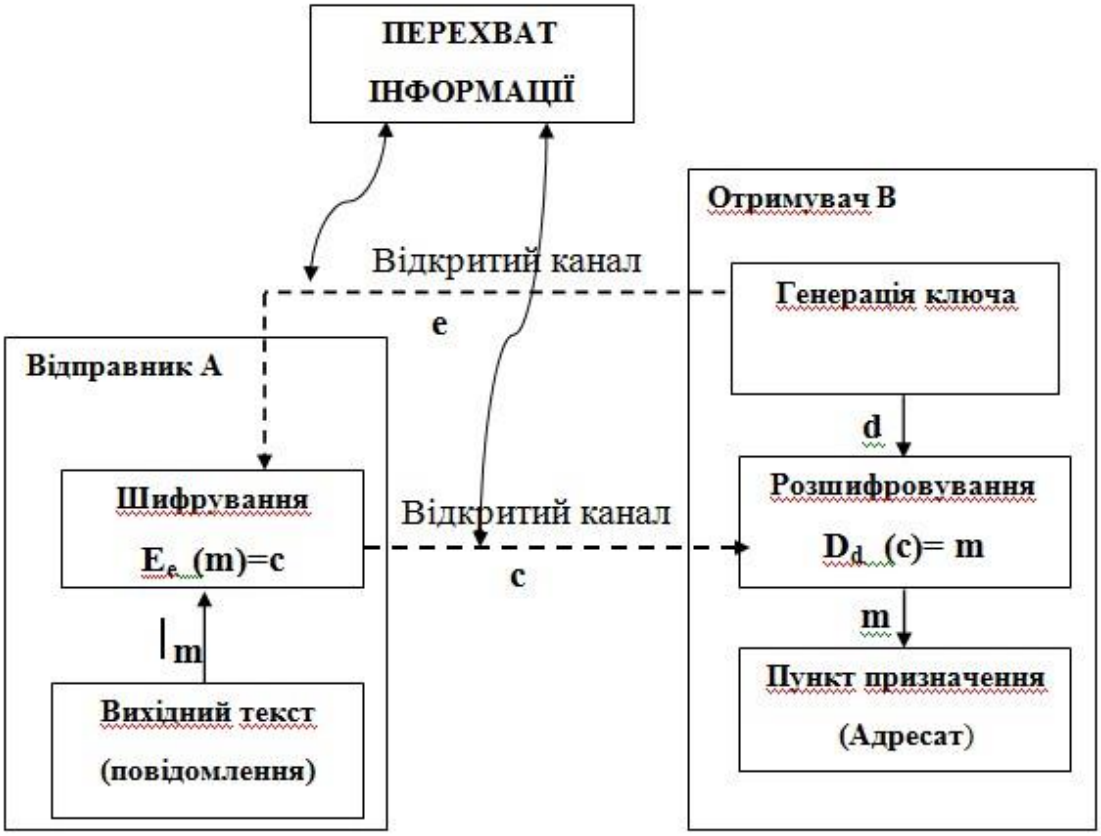

Рисунок 2.3 – Форма атаки – обчислення закритого ключа по відкритому

Існує пять основних принципів побудови криптосистем з відкритим ключем:

– початковий етап – вирішення складного завдання P. Складність цього завдання полягає в відсутність алгоритму, за допомогою якого можна підібрати всі можливі варіанти вирішення задачі P за поліноміальний час щодо розміру завдання;

– рішення легкої підзадачі P 'з P, яке повинно бути здійснено за лінійний час;

– «перетасовуючи і збовтуючи » P '. Для того, щоб отримати завдання P ", абсолютно відмінне від початкового, необхідна задача P " у вигляді оригінальної важко розвязаної задачі P;

– використання завдання P " з описом в ролі ключа шифрування. Процес отримання P 'з P' 'тримається в тайні ;

– результат – система криптосистема організована таким чином, що алгоритми розшифрування для легального користувача і криптоаналитика істотно різні. У той час як перший вирішує P " завдання, другий використовує секретну частину і так вирішує P ' завдання [6,5].

Для дешифрування тексту необхідно мати довідник, складений по зростанню номерів. Він допомагає отримати вихідний текст тільки легальним користувачам. Відсутність такого довідника значно збільшить час на розшифровку тексту.

До головних достоїнств асиметричних шифрів відносять:

– відсутність необхідності попередньої передачі секретного ключа по надійному каналу;

– для асиметричної криптосистеми тільки один ключ тримається в секреті; – в асиметричних криптосистемах пару секретних ключів можна не міняти на протязі тривалого періоду;

– та кількість ключів в асиметричної криптосистемі значно менше, ніж в симетричній.

Але, як завжди, є недоліки:

– складність внесення змін до асиметричного алгоритму шифрування;

– даже за достатньою надійностю шифрування, одержувач і відправник самим фактом пересилання шифрованого повідомлення ставлять під загрозу безпеку секретної інформації;

– використання великих за розміром ключів в асиметричних алгоритмах;

– швидкість процесу шифрування та розшифрування з використанням пари ключів не є високою;

– необхідно значно більше обчислювальних ресурсів для асиметричної криптосистеми [7].

2.1.3 Захист інформації на основі методу криптографічний сіль

Для захисту паролів і цифрових підписів від підробки створено кілька методів, які працюють навіть в тому випадку, якщо криптоаналітику відомі способи побудови колізій для використовуваної хеш-функції.

Одним з таких методів є додавання до вхідних даних так званої криптографічної «солі» – рядки випадкових даних; іноді «сіль» додається і до хеш-коду. Додавання випадкових даних значно ускладнює аналіз підсумкових хеш-таблиць. Даний метод, наприклад, використовується при збереженні паролів в UNIX-подібних операційних системах.

Хеш-функції широко використовуються в криптографії. Хеш використовується як ключ у багатьох структурах даних – хеш-табліцах, фільтрах Блума і декартових деревах.

Криптографічні хеш-функції. Серед хеш-функцій, що існують , прийнято виділяти криптографічно стійкі, що застосовуються в криптографії, так як на них накладаються додаткові вимоги.

Для того, щоб хеш-функція H вважалася криптографично стійкою, вона повинна задовольняти трьом основним вимогам, на яких засновано більшість застосувань хеш-функцій в криптографії:

1) незворотність – для заданого значення хеш-функції m повинно бути обчислювально нездійсненно знайти блок даних;

2) стійкість до колізій першого роду: для заданого повідомлення M має бути обчислювально нездійсненно підібрати інше повідомлення N, для якого виконується (N)=H (M);

3) стійкість до колізій другого роду має бути такою, що обчислювально нездійсненно підібрати пару повідомлень (M, M'), що мають однаковий хеш H(M)=H(M, M').

Дані вимоги не є незалежними:

– оборотна функція нестійка до колізій першого і другого роду;

– функція, нестійка до колізій першого роду, нестійка до колізій другого роду, зворотне невірно.

Не доведено існування незворотніх хеш-функцій, для яких обчислення будь-якого прообразу заданого значення хеш-функції теоретично неможливо. Зазвичай знаходження зворотного значення є лише обчислювально складним завданням.

Атака «днів народження» дозволяє знаходити колізії для хеш-функції з довжиною значень n бітів в середньому за приблизно 2!(n/2) обчислень хешфункції.

Тому n-бітова хеш-функція вважається крипостійкість, якщо обчислювальна складність знаходження колізій для неї близька до 2!(n/2).

Для криптографічних хеш-функцій важливо, щоб при щонайменшій зміні аргументу значення функції сильно змінювалося (лавинний ефект). Зокрема, значення хешу не повинно давати витоку інформації навіть про окремі біти аргументу. Ця вимога є запорукою кріптостійкості алгоритмів хешування, що хешують пароль користувача для отримання ключа [8].

Хешування часто використовується в алгоритмах електронно-цифрового підпису, де шифрується не саме повідомлення, а його хеш-код, що зменшує час обчислення, а також підвищує криптостойкость. Також в більшості випадків замість паролів зберігаються значення їх хеш-кодів.

2.1.4 Алгоритм обчислення контрольних сум

Алгоритми обчислення контрольних сум – нескладні, швидкі і легко реалізовані апаратно алгоритми, використовувані для захисту даних від ненавмисних спотворень, в тому числі – від помилок апаратури.

З точки зору математики такі алгоритми є хеш-функціями, що обчислюють контрольний код. Контрольний код застосовується для виявлення помилок, які можуть виникнути при передачі і зберіганні інформації.

Алгоритми обчислення контрольних сум за швидкістю обчислення в десятки і сотні разів швидше, ніж криптографічні хеш-функції, і значно простіше в апаратному виконанні.

Платою за таку високу швидкість є відсутність криптостійкості – можливість легко «підігнати» повідомлення під заздалегідь відому контрольну суму.

Також зазвичай розрядність контрольних сум (типове число: 32 біта) нижче, ніж розрядність криптографічних хеш-кодувань (типові числа: 128 і 256 біт), що означає можливість виникнення ненавмисних колізій.

Найпростішим алгоритмом обчислення контрольної суми є розподіл повідомлення (вхідних даних) на 32 або 16-бітові слова з наступним підсумовуванням слів. Такий алгоритм застосовується, наприклад, в протоколах TCP/IP.

Як правило, алгоритми обчислення контрольних сум повинні виявляти типові апаратні помилки, наприклад, повинні виявляти кілька поспіль помилкових біт до заданої довжини. Сімейство алгоритмів так званих «циклічних надлишкових кодів» задовольняє цим вимогам. До них відноситься, наприклад, алгоритм CRC32, застосовуваний в пристроях Ethernet і в форматі стиснення даних ZIP [8].

Контрольна сума, наприклад, може бути передана по каналу зв'язку разом з основним текстом (даними). На приймальному кінці, контрольна сума може бути розрахована заново і може порівнюватися з переданим значенням. Якщо буде виявлено розбіжність, то при передачі виникли спотворення, і можна запросити повторну передачу.

Приклад застосування хешування в побуті – підрахунок кількості валіз, що перевозяться в багажі літака. Для перевірки збереження валіз не потрібно перевіряти збереження кожної валізи, досить порахувати кількість валіз під час завантаження і розвантаження. Збіг чисел означатиме, що жодну з валіз не втрачено. Тобто, число валіз є хеш-кодом.

Даний метод можна доповнити для захисту переданої інформації від фальсифікації (метод MAC). В цьому випадку змішування проводиться крипостійкою функцією над повідомленням, об'єднаним з секретним ключем, відомим тільки відправнику і одержувачу повідомлення. Криптоаналітик, що перехопив повідомлення і значення хеш-функції, не зможе відновити код, тобто не зможе підробити повідомлення.

2.1.5 Геометричне хешування

Geometric hashing – метод, широко застосовуваний в комп'ютерній графіці і обчислювальної геометрії для вирішення завдань на площині або в

тривимірному просторі, наприклад для знаходження найближчих пар точок серед безлічі точок або для пошуку однакових зображень. Хеш-функція в даному методі зазвичай отримує на вхід будь-яке метричний простір і розділяє його, створюючи сітку з клітин. Хеш-таблиця в даному випадку є масивом з двома або більше індексами і називається «файлом сітки», grid file.

Геометричне хешування застосовується в телекомунікаціях при роботі з багатовимірними сигналами [9].

2.1.6 Прискорення пошуку даннях

Прискорення пошуку даннях Хеш-таблиці називається структура даних, що дозволяє зберігати пари виду «ключ» - «хеш-код» і підтримує операції пошуку, вставки і видалення елемента. Хеш-таблиці застосовуються з метою прискорення пошуку, наприклад, під час запису текстових полів в базі даних може розраховуватися їх хеш-код, і дані можуть міститися в розділ, що відповідає цьому хеш-коду. Тоді при пошуку даних треба буде спочатку обчислити хеш-код тексту, і відразу стане відомо, в якому розділі їх треба шукати. Тобто шукати треба буде не по всій базі, а тільки по одному її розділу, а це прискорює пошук.

Побутовим аналогом хешування в даному випадку може бути розміщення слів у словнику в алфавітному порядку. Перша літера слова є його хеш-кодом, і при пошуку проглядається не весь словник, а тільки слова, що починаються на потрібну букву [9].

2.2 Аналіз криптографічних алгоритмів гарантованого захисту

На сучасному етапі розвитку технічних засобів та компонентів інформаційних комп’ютерних систем можливе використання різних методів для

забезпечення захисту інформаційного ресурсу. Рішення завдання по забезпеченню інформаційної безпеки даних, що передаються між компонентами системи базується на основі таких методів:

1) криптографічний метод;

2) метод маскування інформації.

Криптографічні методи захисту інформації є спеціальними методами шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. У криптографічному методі захисту охороняється безпосередньо сама інформація, а не доступ до неї. Процес зміни вихідного повідомлення в форму називають шифруванням, а зворотній процес відновлення вихідного повідомлення по криптотексту – дешифруванням (рис. 2.4).

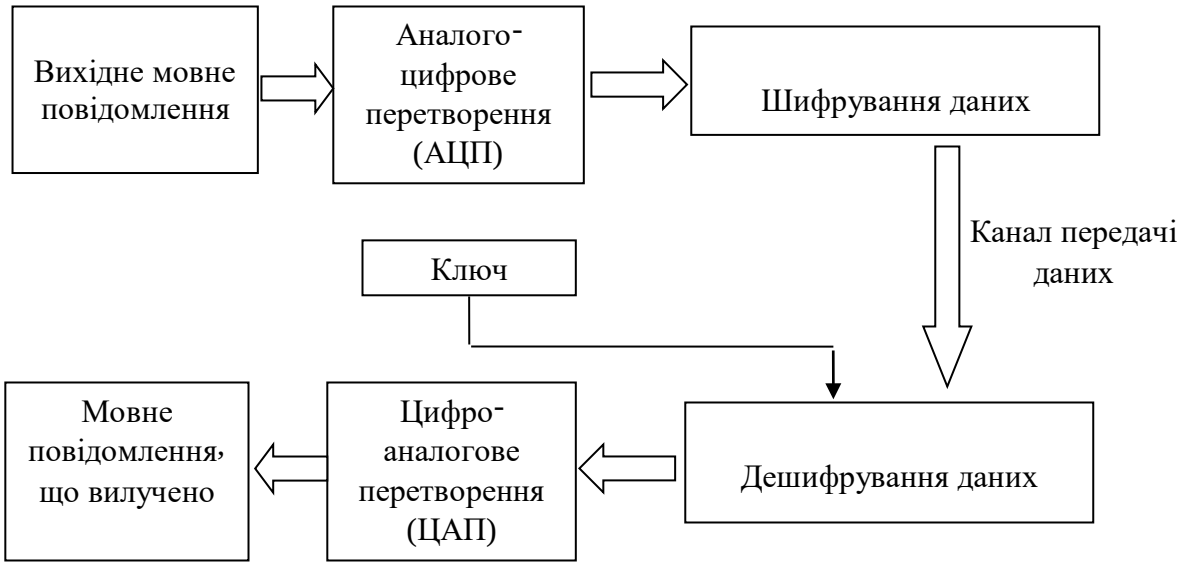

Рисунок 2.4 – Структурна схема функціонування криптографічного алгоритму

Для сучасних криптографічних систем захисту інформації сформульовані наступні вимоги, що загальноприйняті:

1) зашифроване повідомлення повинно піддаватися дешифруванню тільки при наявності ключа;

2) знання алгоритму шифрування не повинно впливати на надійність захисту;

3) незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

4) структурні елементи алгоритму шифрування повинні бути незмінними;

5) додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

6) довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

7) не повинно бути простих і легко встановлюваних залежностей між ключами, що послідовно використовуються в процесі шифрування;

8) будь-який ключ, що складається з безлічі можливих повинен забезпечувати надійний захист інформації.

Криптографічні методи можуть бути реалізовано або програмним, або апаратним способом. Можливість програмної реалізації обумовлюється тим, що всі методи криптографічного перетворення формальні і можуть бути представлені у вигляді кінцевої алгоритмічної процедури.

При апаратній реалізації всі процедури шифрування і дешифрування виконуються спеціальними електронними схемами. Найбільшого поширення

набули модулі, що реалізують комбіновані методи. Більшість зарубіжних серійних засобів шифрування засновано на американському стандарті DES.

Алгоритм DES (Data Encryption Standard) – алгоритм для симетричного шифрування, який було прийнято урядом США в 1977, як офіційний стандарт, що призначений для захисту від несанкціонованого доступу до важливої інформації.

DES являє собою блоковий шифр, який забезпечує шифрування даних 64бітовими блоками. Іншими словами у якості вихідного повідомлення використовується 64-бітовий блок відкритого тексту, а у якості перетвореного повідомлення 64-бітовий блок шифротексту. Довжина ключа дорівнює 56 біт. Ключ, який може бути одним з 56-бітових чисел, можна змінити в будь-який момент часу [10,14].

Російські розробки, такі як, наприклад, пристрій КРИПТОН (рис. 2.5), використовує власний стандарт шифрування. Пристрої криптографічного захисту даних (ПКЗД) серії КРИПТОН – це апаратні шифратори. Пристрої застосовуються у складі засобів і систем криптографічного захисту даних для забезпечення інформаційної безпеки (у тому числі захисту з високим рівнем секретності в державних і комерційних структурах).

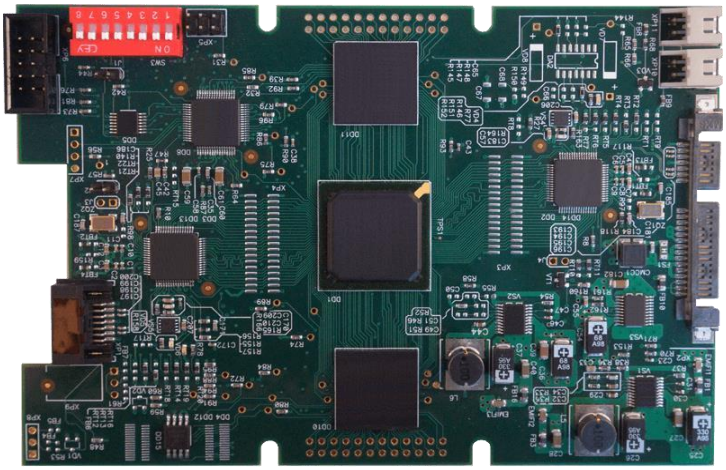

Рисунок 2.5 – Пристрій шифрування КРИПТОН

До недоліків криптографічних алгоритмів слід віднести:

1) значні витрати обчислювального ресурсу (часу, потужності процесорів) на виконання криптографічних перетворень інформації;

2) труднощі спільного використання інформації, яку перетворено криптографічно;

3) високі вимоги що до зберігання секретних ключів та захисту відкритих ключів від підміни.

Одним з головних обмежень криптографічних методів, з точки зору забезпечення захищеності інформації, є створення закритого каналу передачі даних, який відомо конкуренту. Іншими словами, конкуренту відомо факт передачі інформації.

2.3 Захист інформації на основі маскування інформаційних повідомлень.

Альтернативним методом захисту інформації від несанкціонованого доступу є маскування інформаційних повідомлень в контейнерах.

На відміну від криптографічного захисту, коли у конкурента існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, метод маскування дозволяє приховати інформаційні повідомлення у контейнері (рис. 2.6).

Приховування даних в мовне повідомлення можливо при використанні наступних методів[13,17]:

1) кодування найменш значущих біт (просторово-часова область) відбувається шляхом використання голосового сигналу із заміною НЗБ кожної точки здійснення вибірки, представленої двійковою послідовністю;

2) фазового кодування (частотна область) полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає собою дані, які необхідно приховати;

3) розширення спектру (просторово-часова область) використовує технологію PC, що розширює сигнал даних (повідомлення), помножуючи його на сигнал несучої та псевдовипадкову шумову послідовність, що характеризується широким частотним спектром;

4) приховування даних з використанням ехо-сигналу полягає у вбудовуванні даних в голосовий сигнал контейнер шляхом введення в нього ехо-сигналу. Дані приховуються зміною трьох параметрів ехо-сигналу: початкової амплітуди, швидкості загасання та зсуву в часі [12,14].

Серед додаткових вимог до методів маскування інформаційних повідомлень можна віднести такі:

1) властивості контейнера повинно бути модифіковано таким чином, щоб зміни неможливо було виявити при пасивному аналізі, що характеризує якість приховування повідомлення;

2) повідомлення повинно бути стійким до спотворень, в тому числі і до зловмисних;

3) для збереження цілісності вбудованого повідомлення необхідно використовувати коди з виправленням помилок;

4) для підвищення надійності повідомлення, що вбудовано має повторюватись декілька разів.

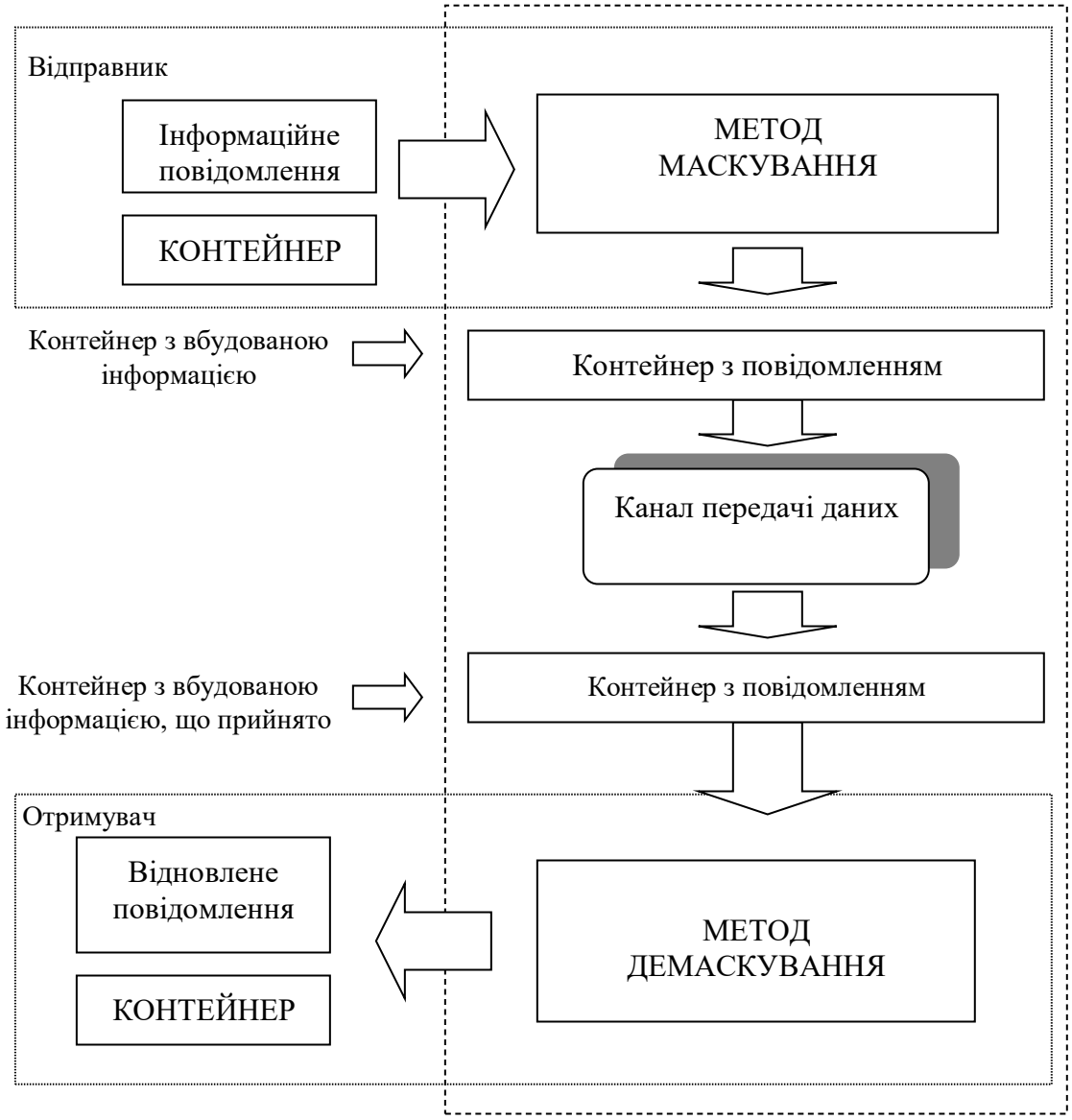

Рисунок 2.6 – Структурна схема методу маскування інформаційних повідомлень

Одночасно з реалізацією конфіденційності повідомлень, метод маскування додатково враховує питання забезпечення таких аспектів, як :

– цілісність інформації, що має на увазі гарантію того, що дані буде збережено у вихідному вигляді без спотворень;

– доступність інформації, під якою розуміється здатність забезпечення своєчасного безперешкодного доступу і обміну інформацією.

У порівнянні з криптографічними алгоритмами маскування інформації дозволяє приховати сам факт наявності вбудованого інформаційного повідомлення [9,15].

Таким чином, можна зробити висновок, що маскування інформації в мовних повідомленнях може використовуватись для забезпечення захищеності даних під час передавання їх каналами в системі між користувачами.

2.4 Формулювання вимог до методу прихованої передачі даних

Для задовільнення вимог, щодо забезпечення захисту інформації висуваються наступні вимоги щодо методу маскування даних:

1) вимоги мінімізації спотворень голосового контейнера A.

Дана вимога характеризується тим, що величина □(A; A□), яка показує ступінь відмінності вихідного голосового контейнера A від перетвореного повідомлення A□ повинна приймати мінімальне значення, а саме:

$$\eta(A; A\square) \square \min .$$

В цьому випадку буде забезпечуватись приховування інформаційного повідомлення одночасно з забезпеченням заданої якості голосових повідомлень;

2) вимоги максимальної схожості корисного повідомлення В. Для оцінки ступеня схожості вихідного інформаційного повідомлення В відносно повідомлення В після вилучення з контейнеру вводиться величина (В; В), яка характеризує метод с позиції спотворень, які вносяться в результаті передачі. У цьому випадку для забезпечення мінімальної відмінності між повідомленням В та В величина (В; В) повинна приймати мінімальне значення, а саме:

$$(B; B') \to \min ;$$

3) ймовірність $P_в$ виявлення противником наявності додаткової інформації в голосовому повідомленні повинна бути мінімальною:

$$P_в \to \min ;$$

4) пропускна здатність Q прихованого каналу передачі інформації повинна бути максимальною:

$$Q \to \max;$$

5) час $t_{вбуд}$ вбудовування інформації в голосове повідомлення повинно бути мінімальним:

$$t_{вбуд} \to \min .$$

Проведено аналіз методів криптографічного захисту. Це спеціальний метод шифрування в результаті якого зміст повідомлення стає недоступним без пред'явлення ключа криптограми та зворотнього перетворення. У криптографічному методі захисту приховується безпосередньо зміст інформації одночасно з забезпеченням вільного доступу до неї.

Було проаналізовано метод маскування інформаційних повідомлень. На відміну від криптографічного захисту, коли у супротивника існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, метод маскування дозволяє приховати інформаційні повідомлення в контейнери, таким чином, щоб приховати сам факт передачі інформації, що приховано.

Для забезпечення захищеності даних пропонується використовувати метод маскування інформації в мовних повідомленнях. Сформульовано систему вимог щодо методу маскування інформації в голосових повідомлення, який розробляється.

3 РОЗРОБКА МЕТОДУ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЙНІХ ПОВІДОМЛЕНЬ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПЕРЕДАЧИ ІНФОРМАЦІЇ

3.1. Розробка методу прямого маскування інформації в мовному повідомленні

Нехай A – вихідне голосове повідомлення, яке розбивається на фрагменти A□ (рис. 3.1).

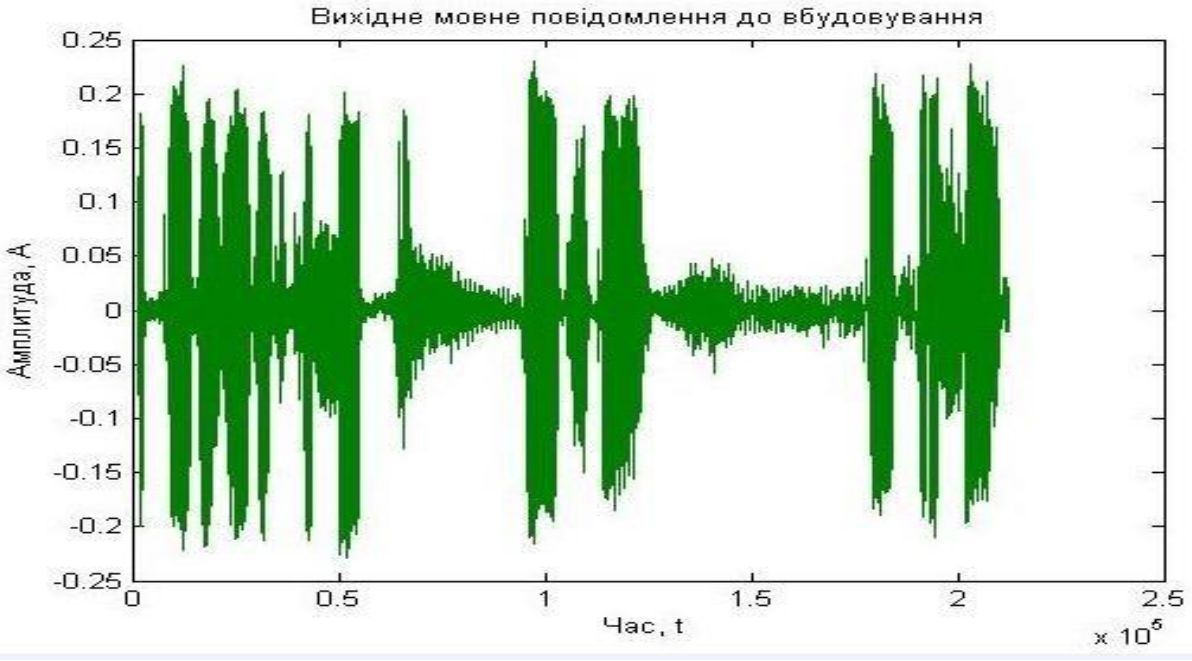

Рисунок 3.1 – Вихідне мовне повідомлення

Кількість фрагментів для голосового повідомлення A дорівнює G, яке обчислюється на основі наступного виразу:

T

$$G = \frac{T}{t},$$

де T– довжина голосового повідомлення A, секунд;

t – довжина фрагмента A_γ, секунд.

Голосове повідомлення підлягає дискретизації. При цьому необхідно забезпечити виконання критерію Найквіста-Шенона. Враховуючи, що максимальне значення частоти f_{max} фрагменту голосового повідомлення A_γ дорівнює 20 кГц, розрахуємо значення частоти дискретизації $f_д$ та часовий інтервал між дискретами Δt :

$$f_Д = 2 \cdot f_{max} = 40(кГц),$$

$$\Delta t = \frac{1}{2 \cdot f_{max}} = 0{,}000025 = 2{,}5 \cdot 10^{-5}(c).$$

Операція дискретизації задається наступним виразом:

$$I_\gamma = \varphi_Д(A_\gamma),$$

де $I\gamma$ – фрагмент голосового повідомлення A_γ, $\gamma = \overline{1,G}$;

$\varphi_д$ – функціонал, який описує операцію дискретизації.

Після операції дискретизації фрагмент голосового повідомлення $I_{\square}$ буде мати наступний вигляд:

$$I_{\gamma} \square \square i_1;i_2;...;i_i;...;i_N \square,$$

де i_i – i- та складова фрагмента $I_{\square}$ голосового повідомлення, i $\square$1, N.

Для розрахунку кількості складових для фрагменту після дискретизації використовується наступна формула:

$$N \square \frac{t}{\square t}.$$

Сам фрагмент мовного повідомлення $I_{\square}$ має наступний вигляд (рис. 3.2):

Рисунок 3.2 – Фрагмент мовного повідомлення після дискретизації

Наступний етап обробки фрагменту передбачає виконання фільтрації. Враховуючи, що в існуючих засобах радіозв'язку голосові повідомлення підлягають фільтрації з метою виділення сигналу на частотах мовних повідомлень від $f_{c\,min} = 300$ Гц до $f_{c\,max} = 3400$ Гц, то в процесі передачі повідомлень можливо знищення частини інформації, яка передається. Звідси, необхідно провести попередню обробку шляхом цифрової фільтрації фрагмента I_{Φ}.

Значить необхідно отримати спектр голосового повідомлення дискретного перетворення Фур'є за допомогою формули:

$$y_k = \sum_{i=1}^{N} i_i \cdot e^{\frac{i 2 \Pi k i}{N}},$$

де y_k – комплексна амплітуда, яка відповідає значенню сигналу на частоті k, $k = \overline{1, K}$.

i_i – i- та складова фрагмента I_{Φ} голосового повідомлення, $i = \overline{1, N}$.

Враховуючи що ДПФ може виконуватись для різного значення $K = \overline{1,20000}$ компонент розкладу сигналу, то для відповідності позиції спектральної компоненти реальному значенню частоти сигналу необхідно виконати наступний розрахунок:

$$k_c = \frac{K \cdot f^c}{20000},$$

де K– кількість компонент спектрального розкладу ДПФ; f_c– необхідне значення частоти сигналу; k_c– компонента спектрального представлення, яка відповідає частоті f_c.

Спектральне представлення Y_y фрагменту $I_{\square}$ голосового повідомлення буде мати вигляд (рис. 3.3):

$$Y_\gamma = (y_1; y_2; ...; y_k; ...; y_K).$$

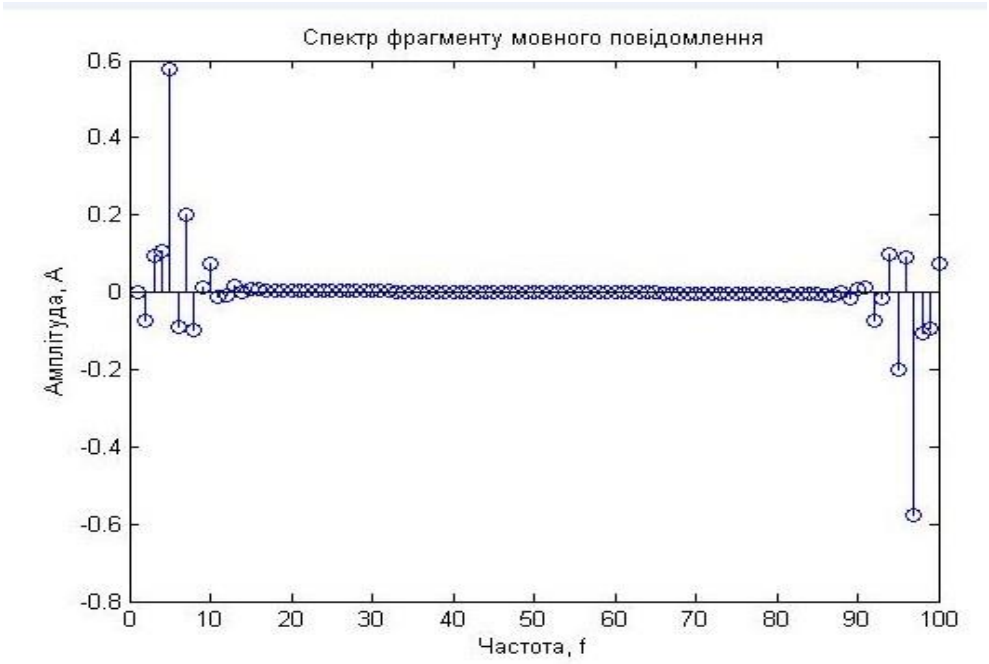

Рисунок 3.3 – Спектр фрагменту мовного повідомлення після фільтрації.

Тоді операція цифрової фільтрації буде виконуватись на основі системи рівнянь:

$$\begin{cases} y_i = 0, & i = 1 \ldots k_{c\min} - 1; \\ y_i = y_i, & i = k_{c\min} \ldots k_{c\max}; \\ y_i = 0, & i = k_{c\max} \ldots f_{\max}. \end{cases}$$

Тут y' – і-та спектральна компонента голосового фрагменту I_Φ після операції фільтрації; λ – коефіцієнт фільтрації.

Для забезпечення виконання вимог до розробленого методу щодо зменшення спотворень вихідного повідомлення пропонується вбудовування інформаційного повідомлення виконувати шляхом модифікації фази. На відміну від амплітуди та частоти мовного повідомлення, фаза звукового сигналу не містить семантичної інформації та її модифікація не впливатиме на слухове сприйняття людиною. Іншими словами фаза мовного повідомлення представляє собою надлишковість. Звідси пропонується використовувати таку надлишковість для вбудовування інформації.

Для виділення фазових складових $\{\varphi_k\}$ фрагменту мовного повідомлення I_Φ зі значення частотного спектру Y_y після фільтрації використовується наступний вираз:

$$\varphi_k = \operatorname{arctg}\left(y_{kI} / y_{kR} \right),$$

де y_{kI} – k-та компонента уявної частини спектральної складової y_k, $k = \overline{1, K}$. y_{kR} – k-та компонента реальної частини спектральної складової y_k, $k = \overline{1, K}$.

У цьому випадку отримаємо фазовий спектр φ, який буде мати вигляд :

$$\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_k, \ldots, \varphi_K),$$

де φ_k – k-та компонента фазового спектру, $k = \overline{1, K}$.

На рисунку 3.4 представлено фазовий спектр фрагменту мовного повідомлення після виділення фазових складових зі значення частотного спектру.

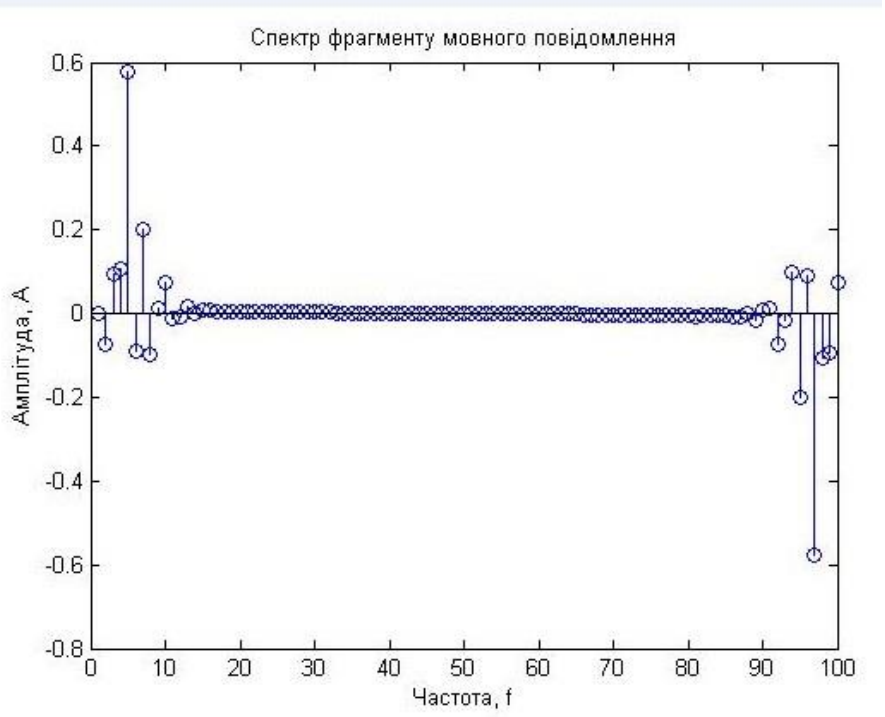

Рисунок 3.4 – Фазовий спектр фрагменту мовного повідомлення .

На наступному етапі відбувається вбудовування бітів інформаційного повідомлення шляхом модифікації складових фазового спектру. При цьому пропонується здійснювати непряму модифікацію значень фаз однієї складової відносно наступної. Приховане вбудовування даних здійснюється у двійковому вигляді, таким чином що елемент b повідомлення B, яке приховується буде приймати наступний вигляд b [0;1]. Здійснюється поділ фазового спектру на пари складових 1 та 2 та їх модифікація за таким правилом:

– якщо біт інформаційного повідомлення приймає значення b 1, то виконується умова 1 2 ;

– і навпаки, якщо біт інформаційного повідомлення приймає значення b0, то виконується умова 1 2 .

Для операції модифікації використовується наступна формула:

$$\varphi_{mod} = \varphi + \frac{1}{2} k_{mod},$$

де k_{mod} – коефіцієнт модифікації, який характеризує ступінь зміни модифікованої фази φ_{mod} відносно вихідної φ.

Отримали модифіковану фазу, після цього здійснюється перехід до частотного спектру за допомогою формули:

$$y_k = \sqrt{(y_{(kI)} + y_{(kR)})} e^{(j)\varphi_{mod}}.$$

На наступному етапі пропонується для отримати сигнал (в часовій області) .Для цього застосувати формулу зворотнього дискретного перетворення Фур'є:

$$\frac{1}{N} \sum_{k=1}^{N} y_k e^{\frac{i2\pi ki}{N}}$$

Після зворотнього дискретного перетворення Фур'є отримуємо сигнал (в часовій області).

В цьому сигналі якому буде міститися модифікована інформація.

Отримане повідомлення готове для посилання на радіостанцію.

На рисунку 3.5 представлено схему прямого маскування мовного повідомлення.

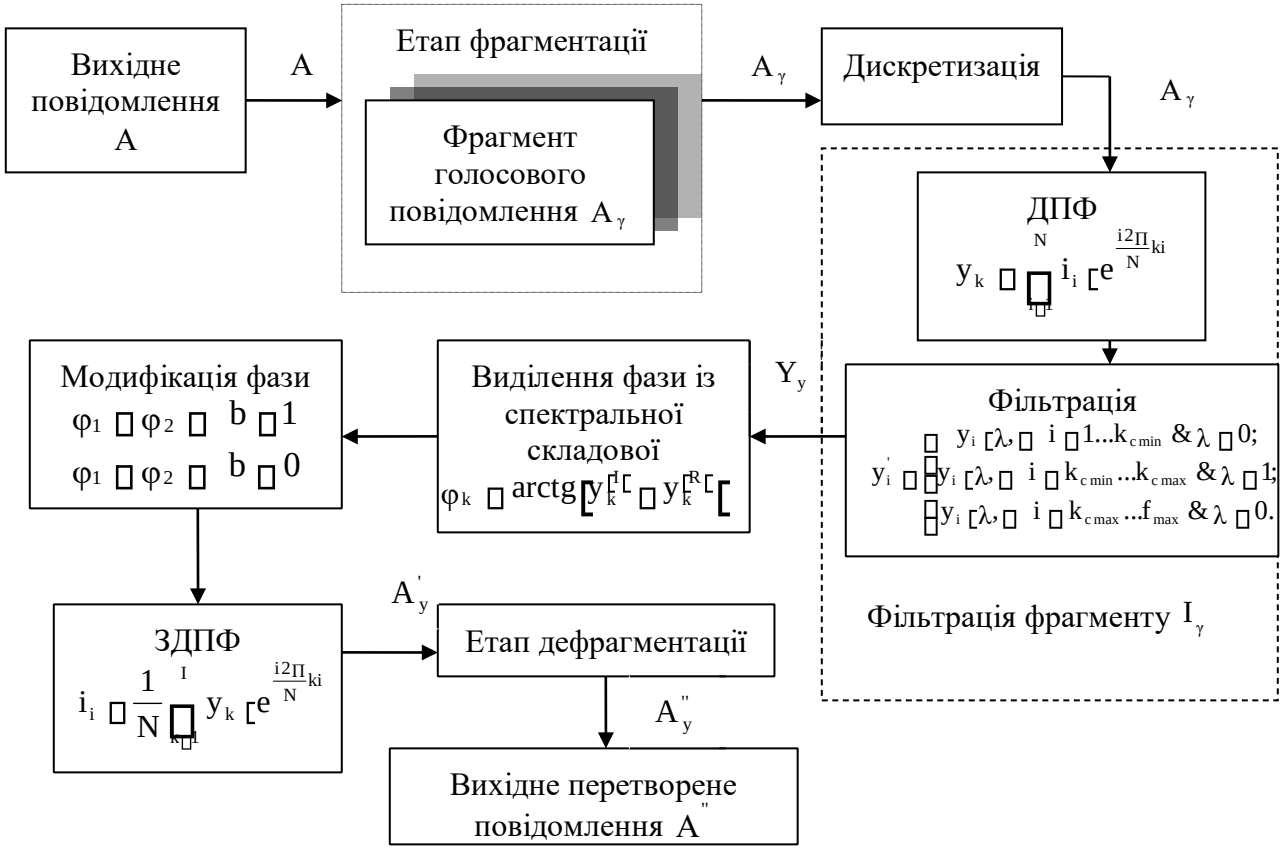

Рисунок 3.5 – Схема прямого маскування мовного повідомлення

3.2 Метод демаскування

Вилучення замаскованого повідомлення буде включати в себе наступні етапи:

1) Нехай $A_{"}$ – отримане мовне повідомлення, яке розбивається на фрагменти $A'_{\gamma}{}'$. Кількість фрагментів для голосового повідомлення $A"$ дорівнює G, яке обчислюється на основі наступного виразу:

$$G = \frac{T}{t},$$

де T– довжина голосового повідомлення $A_{"}$, секунд;
t – довжина фрагмента $A'_{\gamma}{}'$, секунд.

2) Голосове повідомлення підлягає дискретизації. Операція дискретизації задається наступним виразом:

$$I_{\gamma} = \varphi_{д}(A_{\gamma'}),$$

де I^{γ} – фрагмент голосового повідомлення $A'_{\gamma}{}'$, $\gamma = \overline{1,G}$; $\varphi_{д}$

– функціонал, який описує операцію дискретизації.

3) Наступний етап обробки фрагменту передбачає виконання цифрової фільтрації фрагмента I_{γ}. Значить необхідно отримати спектр голосового повідомлення дискретного перетворення Фур'є за допомогою формули:

$$N \quad \_\_i2\Pi ki$$

$$y_k = \sum_{i=1}^{N} i_i \cdot e^{}, \quad ,$$

де y_k – комплексна амплітуда, яка відповідає значенню сигналу на частоті k, $k = \overline{1, K}$.

i_i – і-та складова фрагмента $I_{голосового}$ повідомлення, $i = \overline{1, N}$.

Тоді операція цифрової фільтрації буде виконуватись на основі системи рівнянь:

$$\begin{cases} y_i' = \lambda, i = 1 \ldots\ldots k_{cmin} \;\&\; \lambda = 0; \; y_{i''} \\ = y_{i'} = \lambda, i = k_{cmin} \ldots k_{cmax} \;\&\; \lambda = 1; \\ = y_{i'} = \lambda, i = k_{cmax} \ldots . f_{max} \;\&\; \lambda = 0. \end{cases}$$

Де y'' – і-та спектральна компонента голосового фрагменту $I_{голосового}$ після операції фільтрації; λ – коефіцієнт фільтрації.

4) Необхідно виділити фазу із спектральної складової. Розрахунок фазового спектру буде мати наступний вигляд:

$$\varphi_k = \operatorname{arctg}\left(y_{(kI)} / y_{(kR)}\right),$$

де y_k^I – k-та компонента уявної частини спектру;

y_k^R – k-та компонента реальної частини спектру .

5) На наступному етапі здійснюється вилучення вбудованого повідомлення за допомогою формули:

$$1 \quad \varphi_1 \quad \varphi_2$$

$$b \quad 0 \quad \varphi_1 \quad \varphi_2 .$$

Після вилучення вбудованого повідомлення за допомогою формули отримуємо сигнал в якому буде міститися саме вбудоване повідомлення. Отримане повідомлення готове для посилання в апаратуру для демаскування.

На рисунку 3.6 представлено схему демаскування мовного повідомлення

Далі необхідно провести оцінку ефективності розробленого методу прихованої передачі інформації на основі розрахунку пропускної здатності каналу у різних умовах

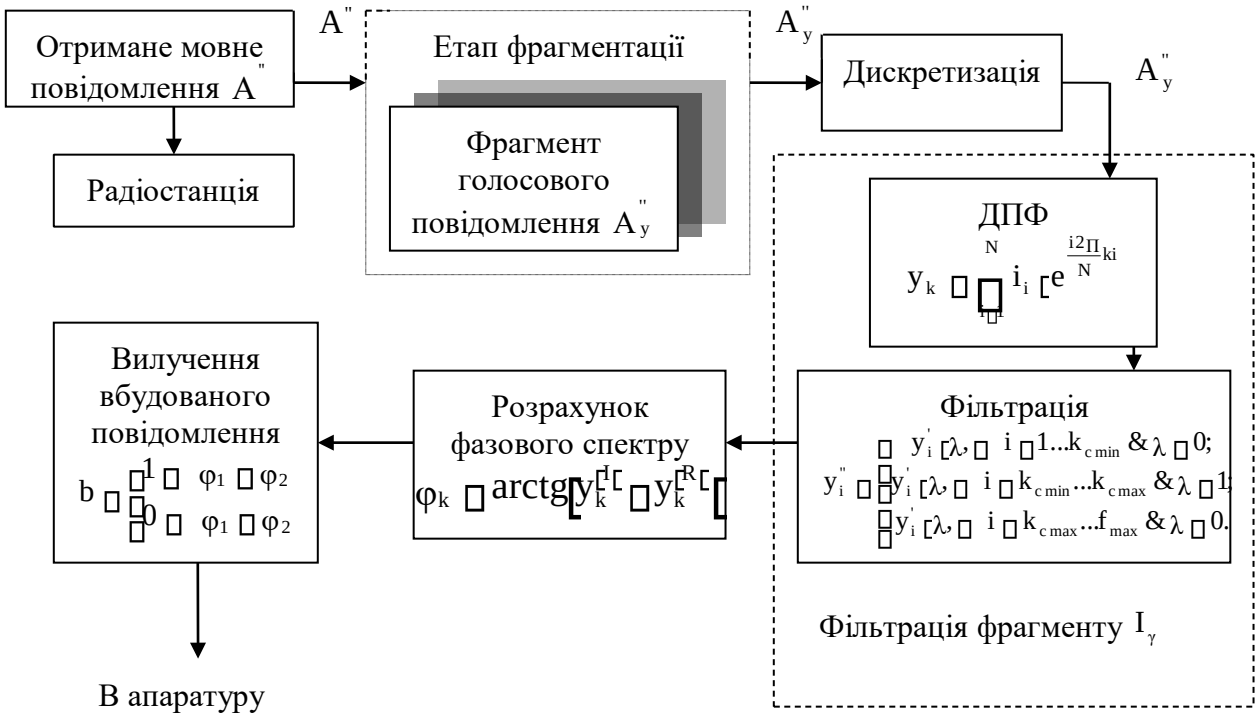

Рисунок 3.6 – Схема демаскування мовного повідомлення

3.3 Оцінка пропускної здатності розробленого методу

Оцінка ефективності розробленого методу прихованої передачі інформації проводиться на основі розрахунку пропускної здатності каналу у різних умовах. Тут під пропускною здатністю Q розуміється кількість інформації D, яка може бути передана на основі розробленої технології за одиницю часу T та вимірюється у біт на секунду:

$$Q = \frac{D}{T} \quad \text{(біт/сек.)}.$$

Розрахуємо кількість інформації, яку може бути вбудовано в фрагмент голосового повідомлення довжиною t . Враховуючи що вбудовування відбувається на основі непрямої модифікації компонент фазового спектру, для кожного фрагменту розрахуємо кількість компонент K частотного спектру. У разі якщо кількість компонент K відповідає миттєвим значенням амплітуди сигналу фрагменту повідомлення, тоді їх кількість обчислюється з урахування частоти Δf дискретизації голосового повідомлення і дорівнює:

$$N = K \cdot \frac{t}{\Delta f}.$$

В іншому випадку для кожного фрагменту буде окремо встановлюється кількість компонент частотного спектру K. Тоді для розрахунку кількості біт D яке вбудовується в фрагменті мовного повідомлення використовується наступний вираз :

$$D = \frac{K}{2}.$$

У якості приклада розрахуємо пропускну здатність Q для голосового повідомлення довжиною $T = 1$ секунд з частотою $\Delta f = 44100$ Герц . Тоді Q буде дорівнювати:

$$Q = \frac{D}{\ }.$$

T

Для даної формули необхідно розрахувати кількість біт D, яке розраховується за виразом:

$$D = \frac{K}{2}.$$

Для визначення кількість біт D, розрахуємо кількість компонент K для фрагменту :

$$K = t / \frac{1}{\Delta f} = t \cdot \Delta f = 0{,}25 \cdot 44100 = 11025$$

На основі знайденої кількості компонент K, розраховується кількість біт D для фрагменту голосового повідомлення:

$$D = \frac{K}{2} = \frac{11025}{2} = 5512 \text{ (біт)}$$

Враховуючи D та K розрахуємо пропускну здатність $Q_{фр}$ каналу для фрагменту та $Q_{мп}$ для всього голосового повідомлення:

D

$$Q_{фр} = \frac{1}{T} \cdot D = 5512 \text{ (біт/сек)},$$

$$Q_{мп} = D \cdot \gamma = 5512 \cdot 4 = 22048 \text{ (біт/сек)},$$

де D– кількість біт для фрагменту (біт); γ – кількість фрагментів у голосовому повідомленні.

Для випадку коли K не дорівнює N, пропускна здатність буде дорівнювати:

1) для K=1000:

$$Q_{мп} = \frac{K}{2} \cdot \gamma = \frac{1000}{2} \cdot 4 = 500 \cdot 4 = 2000 \text{ (біт/сек)}.$$

2) K=500:

$$Q_{мп} = \frac{K}{2} \cdot \gamma = \frac{500}{2} \cdot 4 = 250 \cdot 4 = 1000 \text{ (біт/сек)}.$$

На рисунку 3.7 у графічному вигляді наведено значення пікового відношення сигнал-шум модифікованого мовного повідомлення відносно вихідного сигналу для випадку неавторизованого доступу.

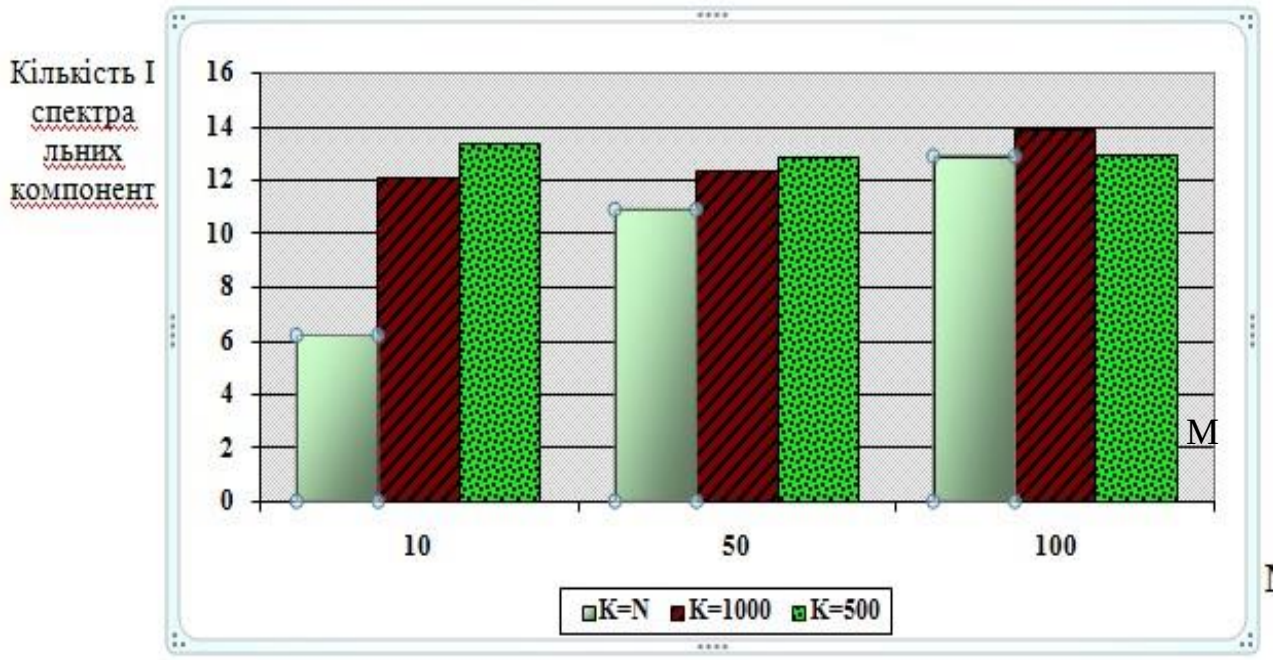

Рисунок 3.7 – Кількість І спектральних компонент

Після проведеного аналізу значень на рисунку 3.7 можна зробити наступні висновки:

– найбільше значення пікового відношення сигнал-шум спостерігається для випадку формування фрагментів мовного повідомлення з довжиною M 100 ;

– значення пікового відношення сигнал шум для різних умов функціонування розробленого методу приймає значення нижче порогу аудіо слухової розбірливості та відповідно забезпечує конфіденційність семантичного змісту мовного повідомлення.

3.4 Розробка програмного коду для проведення аналізу розробленого

методу маскування і демаскування

Метою розробки програмної реалізації розробленого методу вбудовування даних в аудіо контейнер є проведення дослідження ефективності функціонування методу для забезпечення захищеності даних.

Враховуючи, що реалізація алгоритму вбудовування передбачає проведення ортогональних перетворень з метою формування спектрального представлення складових контейнеру, для розробки програмної моделі було обрано мову програмування MATLAB.

MATLAB являє собою один з найкращих пакетів для реалізації математичних та технічних рішень і включає в тому числі функціонали для реалізації різновидів ортогональних перетворень на основі перетворення Фур'є.

Для забезпечення сприйняття аудіо контейнеру, як множини вхідних даних підключено бібліотеку Audio System Toolbox.

Перший етап розробки програмної моделі передбачає завантаження аудіо контейнеру на основі функціоналу wavread та введення основних умов виконання дослідження методу, а саме: кількість елементів у фрагменті, коефіцієнт модифікації складових та частоту дискретизації. Також будується графік вихідного аудіо повідомлення.

Лістінг 3.1 – Введення основних умов виконання дослідження методу

```
clc clear
A=wavread ('Rihana.wav'); T=length(A);  % t= 100;  % koef_mod=1.5;
%коефіцієнт модфікації непрямого вбудовування NSt=44100;
figure (1), plot(A);
 title('Вихідне мовне повідомлення до вбудовування');  % Підпись графіку
xlabel('Час, t');                                      % Підпись осі x
ylabel('Амплитуда, A');
```

Наступний етап передбачає введення частотних порогів для подальшої фільтрації при симуляції втрат при використанні аналогових каналів передачі даних.

Лістинг 3.2 – Введення частотних порогів для подальшої фільтрації

```
Fd=100; fmax=
(Fd*11000)/20000; fmin=
(Fd*100)/20000; %
figure(6), plot(A), grid
```

Для забезпечення швидкодії при реалізації методу проводиться розбиття вихідного аудіо контейнеру на фрагменти довжиною t, яка була визначена на першому етапі розробки алгоритму Будується графічне відображення для останнього фрагменту аудіо контейнеру.

Лістинг 3.3 – Розбиття вихідного аудіо контейнеру на фрагменти

```
 for l=1:(T/t)-
1;
    A1=A(t*(l-1)+1:t*(l-1)+t);
figure (2), plot(A1);
 title('Фрагмент мовного повідомлення до вбудовування'); % Підпись графіку
xlabel('Час, t');                                        % Підпись осі x
ylabel('Амплітуда, A');
```

Після фрагментування аудіо контейнеру відбувається перехід у спектральну область представлення складових контейнеру на основі функціоналу

fft з подальшим усуненням комплексної частини та побудовою спектру фрагменту аудіо контейнеру.

Лістинг 3.4 – Перехід у спектральну область представлення складових контейнеру на основі функціоналу fft

```
    Y1com=fft(A1, Fd);
    Y1= Y1com.*conj(Y1com)/20000; % усунення комплексної частини
figure (3), stem(Y1com);
    title('Спектр фрагменту мовного повідомлення');       % Підпис графіку
xlabel('Частота, f');                                    % Підпис осі
ylabel('Амплітуда, A');
```

При необхідності введення додаткових втрат в аналогову каналі при передачі даних після усуненням комплексної частини та побудови спектру фрагменту аудіо контейнеру необхідно додаткове проведення фільтрації після втрат в аналогову каналі передачі даних.

Лістинг 3.5 – додаткове проведення фільтрації після втрат в аналогову каналі передачі даних

```
          for i=1:length(Y1com);        %операція
фільтрації     if i<fmin;          Y1(1,i)=0;     else if
i>fmax;          Y1(1,i)=0;     else Y1(1,i)=Y1com(1,i);
end     end       end
```

Для зменшення втрат при непрямому вбудовування даних відбувається перехід від частотної області до фазової області для модифікації і розміщення графіку фазового спектру фрагменту аудіо контейнеру.

Лістинг 3.6 – Перехід від частотної області до фазової для модифікації фазового спектру фрагмента аудіо контейнеру

```
   Y11=sqrt(imag(Y1).^2+real(Y1).^2); % Вектор значений комплексного спектра
Y1faza=angle(Y1);       figure(4), stem(Y1faza),
  title('Спектр фаз до модифікації');                              % Підпись
графіку
 xlabel('Час, t');                                              % Підпис осі x
графіку  ylabel('Фаза, Ф');
```

У якості вбудовуваних даних генерується псевдовипадкова послідовність двійкових елементів.

Лістинг 3.7 – Генерація псевдовипадкової послідовність двійкових елементів

```
  B=round(0.75*rand(1,fix(Fd/2)));   % встраиваемая последовательность в двоичном
виде
  Faza_mod=zeros(1,Fd);
```

Наступний етап розробки програмної реалізації передбачає непряму модифікацію складових фазового спектру на основі сформульованого правила та побудову графіку модифікованого спектру після вбудовування

Лістинг 3.8 – Непряма модифікація складових фазового спектру за сформульованим правилом

```
W=length (Y1faza);      for
w=1:W/2;              x1=2*(w-
```

```
1)+1;              x2=2*(w-
1)+2;                   if
B(1,w)==1;
                if abs(Y1faza(1,x1))>abs(Y1faza(1,x2));
                    Faza_mod(1,x1)=Y1faza(1,x1)*koef_mod;
Faza_mod(1,x2)=Y1faza(1,x2)/koef_mod;                  else if
abs(Y1faza(1,x1))<abs(Y1faza(1,x2));
if Y1faza(1,x1)>0;


Faza_mod(1,x1)=(abs(Y1faza(1,x2))/abs(Y1faza(1,x1)))*Y1faza(1,x1)*koef_mod;
Faza_mod(1,x2)=Y1faza(1,x2)/koef_mod;                          else
Faza_mod(1,x1)=1*koef_mod;
                           Faza_mod(1,x2)=Y1faza(1,x2)/koef_mod;
end
                    else if Y1faza(1,x1)==Y1faza(1,x2);
if Y1faza(1,x1)~=0
                        Faza_mod(1,x1)=1*koef_mod;
                        Faza_mod(1,x2)=Y1faza(1,x2)/koef_mod;
else  Y1faza(1,x1)=koef_mod;
                           end
end                      end
end             else if
B(1,w)==0;
                if abs(Y1faza(1,x2))>abs(Y1faza(1,x1));
                    Faza_mod(1,x2)=Y1faza(1,x2)*koef_mod;
Faza_mod(1,x1)=Y1faza(1,x1)/koef_mod;                  else if
abs(Y1faza(1,x2))< abs(Y1faza(1,x1));
if Y1faza(1,x2)>0;


Faza_mod(1,x2)=(abs(Y1faza(1,x1))/abs(Y1faza(1,x2)))*Y1faza(1,x2)*koef_mod;
Faza_mod(1,x1)=Y1faza(1,x1)/koef_mod;                          else
Faza_mod(1,x2)=1*koef_mod;
                           Faza_mod(1,x1)=Y1faza(1,x1)/koef_mod;
end
                else if Y1faza(1,x2)==Y1faza(1,x1);
if Y1faza(1,x2)~=0
                        Faza_mod(1,x2)=1*koef_mod;
                        Faza_mod(1,x1)=Y1faza(1,x1)/koef_mod;
else  Y1faza(1,x2)=koef_mod;                                  end
end                end                end                    end
end   end   for i=1:Fd;
```

```
  Ymod(1,i)=Y11(1,i)*exp(1i*Faza_mod(1,i));
end
figure(5), stem(Ymod),
title('Спектр фрагменту мовного повідомлення після модифікації');  % Підпис
графіку
  xlabel('Частота, f');        % Підпис осі
ylabel('Амплітуда, A');
```

Після реалізації вбудовування відбувається повернення від спектральної області к просторово-часовому представленню на основі функціоналу ifft для зворотного перетворення Фур'є.

Лістинг 3.8 – Зворотнє перетворення Фур'є.

```
  Amod=ifft(Ymod,t);
 Amod=sqrt(imag(Amod).^2+real(Amod).^2);
figure(6), stem(Amod), grid
 title('Фрагмент мовного повідомлення після вбудовування'); % Підпись графіку
xlabel('Час, t');                                          % Підпись осі x
ylabel('Амплітуда, A');
```

На основі множини фрагментів після модифікації відбувається композиція аудіо повідомлення з вбудовуваними даними із побудовою графіку та записом у аудіо файл.

Лістинг 3.9 – Композиція аудіо повідомлення після модифікації та запис даних у аудіо файл

```
 A2((t*(l-1)+1):t*(l-1)+t)=Amod(1,1:t); %сбираємо фрагменти в масив
end figure(7), stem(A2), grid
```

```
title('Вихідне мовне повідомлення після вбудовування');    % Підпись графіку
xlabel('Час, t');                                          % Підпись осі x
ylabel('Амплитуда, A');  audiowrite('handel.wav',A2,NSt)
```

Проводиться розрахунок Q, величини пікового відношення сигнал-шум, який характеризує ступінь спотворень, які вносяться у вихідне повідомлення в процесі вбудовування. Повний код програми наведено в додатку А.

На основі аналізу розробленого методу маскування і демаскування інформації за допомогою розробленого програмного коду можна зробити висновок, що даний метод відповідає вимогам щодо забезпечення захисту даних, та може бути використано для забезпечення захисту інформаційних повідомлень під час передавання засобами зв'язку між системою управління та компонентами системи, що потребують управління.

ВИСНОВКИ

У кваліфікаційній роботі магістра розглянуто принципи функціонування сучасних комп'ютерних систем, в першу чергу таких як системи оборони, комерційні системи, де актуально стоїть питання відповідного інформаційного забезпечення конфіденційності інформації .

Проведено аналіз існуючих вітчизняних та закордонних зразків обладнання обміну інформацією.

Для повноцінного функціонування системи інформаційної підтримки запропоновано розробити метод передачі інформації з забезпеченням заданого рівня захищеності даних.

Проведено аналіз існуючих підходів до забезпечення інформаційної захищеності обміну даними. Та виділено для розв'язання завдання по створенню системи інформаційної підтримки конфіденційності інформації два методи: 1) криптографічний метод; 2) метод маскування інформації.

На першому етапі розглянуто принципи функціонування криптографічного методу. На основі аналізу встановлено, що у даному методі захисту приховується безпосередньо сама інформація, а не доступ до неї, а також алгоритми не завжди забезпечують ефективне функціонування що обумовлено рядом обмежень.

На другому етапі розглянуто принципи функціонування методу маскування інформаційних повідомлень. На основі аналізу встановлено, що на відміну від криптографічного захисту, коли у опонента існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, метод маскування дозволяє

приховати інформаційні повідомлення в контейнери та є ефективнішим засобом для забезпечення захищеності даних.

Сформульовано вимоги щодо методу приховуваної передачі даних у контейнері.

Розроблено метод прямого маскування інформації в мовному повідомленні із забезпеченням виконання вимог до розробленого методу щодо зменшення спотворень вихідного повідомлення. Для цього запропоновано вбудовування інформаційного повідомлення виконувати шляхом модифікації фази.

Розроблено метод демаскування інформації в мовному повідомленні, який передбачає вилучення замаскованого повідомлення.

Розроблено програму для проведення аналізу ефективності розробленого методу.

На основі аналізу розробленого методу маскування і демаскування інформації зроблено висновок, що даний метод відповідає вимогам щодо забезпечення захисту даних, та може бути використано для забезпечення захисту інформаційних повідомлень під час передавання засобами зв'язку між системою управління та компонентами системи.

Перевага даного методу в тому, що лише відправник і одержувач знають, що крім основного каналу передачі даних існує ще прихований, тобто приховані повідомлення кодуються всередині голосового повідомлення таким чином, що змін не помітити і тільки одержувач повідомлення може розкодувати його.

Система забезпечення конфіденційності передачі інформації у прихованому каналі, що розроблено у роботі та запропонований метод особливо актуальні для використання в корпоративних комп'ютерних системах, що базуються на засобах телекомунікаційного зв'язку і комп'ютерних мережах

передачі даних, де виникає потреба забезпечення необхідного рівня безпеки спеціальних інформаційних ресурсів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Айвенс К. Компьютерные сети [Текст] / Айвенс К. ; пер. с. англ. − СПб. : Питер, 2006. – 304 с.
2. Барский А. Б. Нейронные сети: распознавание, управление, принятие решений [Текст] / А. Б. Барский. – М. : Финансы и статистика, 2004. – 176 с.
3. Вакуленко А. Биометрические методы идентификации личности: обоснованный выбор и внедрение [Текст] / А. Вакуленко, А. Юхин. – М.: Наука, 2007. – 224 с..
4. Вилков А.С. Информационная безопасность персональных ЭВМ и мониторинг компьютерных сетей [Текст] / А.С. Вилков. – М. : МИНИТ ФСБ России, 2005. – 210 с.
5. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] – М.: Триумф, 2012. – С. 622.
6. Дональд Кнут. Искусство программирования [Текст] Том 3. Сортировка и поиск = The Art of Computer Programming, vol.3. Sorting and Searching. – 2-е издание. – М. : «Вильямс», 2007. – С. 824.
7. Никлаус Вирт. Алгоритмы и структуры даннях [Текст] . – М.: «Мир», 1989. – Алгоритмы и структуры данных. Новая версия для Оберона. – М.: «ДМК Пресс», 2010.
8. Інформація про електронний цифрови підпис [Електронний ресурс] / wikipedia.org. – Режим доступу : www/ URL: https://uk.wikipedia.org/wiki / Інформація_ про_ електронний _ цифровий підпис – 18.10.2019 г. – Заголовок з екрану..

9. Барарannик В.В. Основы теории структурно-комбинаторного стенографического кодирования кодирования: монография [Текст] / В.В. Барарannик , Э.А.Бекиров, Д.В. Барарannик . – ХНУРЕ, 2017. – 256 с.

10. Хайкин, С. Нейронные сети полный курс [Текст] / Саймон Хайкин. – М. : Вильямс, 2006. – 1104с

11. Уоссермен, Ф. Нейрокомпьютерная техника: Теория и практика [Текст] : пер. с англ. – М. : Мир, 1992. – 184 с

12. Швидке перетворення Фур'є [Електронний ресурс] / wikipedia.org. – Режим доступу : www/ URL: https://uk.wikipedia.org/wiki /Швидке_перетворення_Фур'є – 18.10.2019 г. – Заголовок з екрану.

13. Фільтр високих частот [Електронний ресурс] / wikipedia.org. – Режим доступу : www/ URL: https://uk.wikipedia.org/wiki/Фільтр_високих_частот – 18.10.2019 г. – Заголовок з екрану.

14. Фільтр низьких частот [Електронний ресурс] / wikipedia.org. – Режим доступу : www/ URL: https://uk.wikipedia.org/wiki/Фільтр_низьких_частот – 18.05.2019 г. – Заголовок з екрану

15. Сверточная нейронная сеть, часть 1: структура, топология, функции активации и обучающее множество [Электронный ресурс] / Хабрахабр. – Режим доступа : www / URL: https://habr.com/post/348000/– 05.11.2019 г. – Загл. с экрана

16. Горбань А. Н. Обучение нейронных сетей [Текст] / А. Н. Горбань. / М. : ParaGraph, 1990. – 160 с

17. Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модульностям [Текст] / Вестник МГТУ им. Н.Э. Баумана.

Сер. Приборостроение, 2012, № 3. С. 46–61.

18. Терейковський І. Нейронні мережі в засобах захисту комп’ютерної

інформації [Текст] / І. Терейковський. К. : Поліграф Консалтинг, 2007. 209 с.

19. Jeffrey L. Elman Finding Structure in Time [Text] / Luis Jeffrey // COGNITIVE SCIENCE 14, pp. 179-211 (1990).

20. Зиятдинов А.И. Принципы построения систем биометрической аутентификации [Текст] / А.И. Зиятдинов. – М.: МФТИ, 2015. – 188 с.