МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерних наук

ЛУКОВИЧ Вікторія Андріївна

Математичне та програмне забезпечення для приховування даних у трафіку IP-телефонії / Mathematical Tools and Software for Data Hiding in IP Telephony Traffic

спеціальність: 121 - Інженерія програмного забезпечення
освітньо-професійна програма - Інженерія програмного забезпечення

Кваліфікаційна робота

Виконала студентка групи
ІПЗм-21
В. А. Лукович

_____

Науковий керівник:
д. філос. О. А. Папа

_____

Кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **А. В. Пукас**

ТЕРНОПІЛЬ - 2022

ВСТУП

Надійний захист інформації від несанкціонованого доступу є реальною проблемою, але не проблемою, яку потрібно повністю вирішити. Одним із перспективних напрямків захисту інформації стали сучасні методи стеганографії. Слово стеганофонія в перекладі з грецької буквально означає таємне письмо (steganos — таємний, таємний; phone — звук).

Стеганофонія - це низка методів, заснованих на різних принципах, які забезпечують приховування секретної інформації в тому чи іншому середовищі. Він може включати велику кількість секретних методів зв'язку, таких як невидимі чорнила, мікрофотознімки, умовне розміщення сигналів, секретні (приховані) канали, голографія тощо. В даний час розробляються методи комп'ютерної стеганофонії - самостійного наукового напрямку інформаційної безпеки, що вивчає проблему створення прихованих компонентів у відкритому інформаційному середовищі, які можуть формувати комп'ютерні системи і мережі. Головна особливість стеганофонічного підходу полягає в тому, що він не передбачає прямого повідомлення про наявність захищеної інформації.

Завдяки цим обставинам в рамках інформаційних потоків або існування традиційного інформаційного середовища можливе вирішення деяких важливих проблем і завдань щодо захисту інформації в окремих функціональних сферах. Основним визначальним моментом у стеганофонії є стеганофонічна трансформація. Донедавна стеганографія як наука вивчала переважно окремі способи приховування інформації та способи їх технічної реалізації. Різноманітність принципів, закладених у стеганофонічній методиці, докорінно гальмувала розвиток стеганофонії як окремої наукової дисципліни та не давала їй сформуватися як окремої науки зі своїми теоретичними положеннями та єдиною концептуальною системою, яка б забезпечувала досягнення нормальних якісних і кількісних оцінок. методи.

Актуальність. Дослідження та розробки в галузі стеганофонії стають все більш поширеними в сучасному інформаційному суспільстві разом із широким використанням цифрових мультимедійних форматів та існуючими проблемами управління цифровими ресурсами та контролю за використанням прав власності на комп'ютерні файли. Водночас проблема приховування інформації є важливою проблемою в умовах розвиненої інфраструктури комунікаційної мережі Інтернет-користувачів – учасників відкритої та неконтрольованої взаємодії в медіапросторі.

Структура і принципи роботи комп'ютерних систем стеганофонії подібні до стеганографічних систем. Різниця між цими спорідненими областями захисту даних полягає в середовищі формування даних і характеристиках приховування даних у стегоконтейнері.

Мета дослідження — приховати дані в трафіку ІЧ-телефонії.

Предметом дослідження є методи та комп'ютерні методи приховування даних у трафіку ІЧ-телефонії.

Методи дослідження базуються на принципах системного аналізу, апараті обчислювальної математики, методах логічного проектування та процедурних алгоритмах, методах об'єктно-орієнтованого та логічного програмування.

Метою дослідження є розробка методів і способів приховування даних у трафіку IP- телефонії для підвищення стабільності та ефективності стеганофонічних систем реального часу.

Для досягнення поставленої мети необхідно вирішити наступні взаємопов'язані задачі:

1) Дослідити передачу мовних сигналів у мережах з комутацією пакетів.

2) Проаналізувати існуючі підходи до захисту даних для IP-телефонії.

3) Проаналізувати можливості прихованої передачі мовних сигналів.

4) Дослідити особливості розвитку стеганофонічних систем, проаналізувати основні програмно-технічні прийоми їх побудови.

5) Розробити модель стегосистеми ІЧ-телефонії.

6) Розробити програмне забезпечення для стеганофонічного захисту даних у трафіку IP-телефонії.

7) Апробувати розроблені методики та прийоми, з'ясувати можливість їх застосування на практиці.

Новизна :

- Запропоновано метод приховування даних у трафіку IP- телефонії , який враховує, на відміну від відомих рішень, такі характеристики, як середній час затримки та значення максимально допустимої затримки в мережі VoIP в умовах періодично підписаного повторення.
- Запропоновано метод приховування даних у псевдовипадковому шумі, який є функцією вбудованого повідомлення та змішування отриманого шуму з основним сигналом контейнера як додатковим компонентом.

Практичний результат. В ході роботи реалізовано програмний комплекс FCITStegoVoIP, який дозволяє приховувати дані в трафіку IP-телефонії під час мультимедійного сеансу зв'язку.

Розділ 1. ОСОБЛИВОСТІ ЗАХИСТУ ДАНИХ В IP ТЕЛЕФОНІЇ

1.1 Передача голосових сигналів у мережах з комутацією пакетів

Під мережею передачі даних з комутацією пакетів (далі - пакетна мережа) розуміється сукупність методів передачі даних між комп'ютерами, в яких передача інформації між абонентами визначається за допомогою комутації пакетів. Комутація пакетів здійснюється шляхом поділу повідомлення на пакети - елементи повідомлення забезпечуються заголовком, який має фіксовану максимальну довжину, і подальшої передачі пакетів за маршрутом, визначеним вузлами мережі.

Перед передачею по мережі до повідомлення додається службова інформація – заголовок, що вказує адресу відправника та адресу одержувача. Завдяки цьому повідомлення передається від одного вузла до іншого, поки не досягне місця призначення.

Однак передача повідомлень не була повністю розширена через великі мережеві затримки під час проходження всього повідомлення від відправника до одержувача. Щоб мінімізувати черги на зміну вузлів і час обробки інформації, повідомлення розбиваються на частини певної довжини - пакети. При цьому кожен пакет отримує свій заголовок. І хоча обсяг додаткової службової інформації збільшується, мережі комутації повідомлень значно перевершують швидкість.

На відміну від мереж комутації каналів, комутація пакетів заснована на передачі інформації, попередньо записаної в пам'ять вузла комутації. Пакетні мережеві комутатори відрізняються від канальних комутаторів тим, що вони мають внутрішню буферну пам'ять для тимчасового зберігання пакетів. Дані, отримані від терміналу відправника, записуються в пам'ять вузла. При цьому дані можуть бути змінені (змінена швидкість передачі, код, додана або видалена службова інформація). Якщо вихідний порт комутатора зайнятий, то пакет деякий час знаходиться в черзі пакетів у буферній пам'яті вихідного

порту, а коли черга досягає його, він передається на наступний комутатор. Цей спосіб передачі даних має ряд переваг:

1. Ефективність використання лінії комутації пакетів вища, ніж у комутатора каналів, оскільки один сегмент вузла може динамічно розподіляти свої ресурси між блоками даних для різних програм. Якщо зібрано більше даних, ніж пропускна здатність цього каналу на вузлі передачі, дані, призначені для надсилання по певному каналу, збираються, потім буферизуються та встановлюється послідовність їх передачі. Навпаки, у мережах з комутацією каналів час, виділений кожній програмі, розподіляється у формі окремих часових інтервалів на основі синхронного часового мультиплексування. Максимальна швидкість передачі визначається пропускною здатністю цього часового інтервалу, а не пропускною здатністю всього каналу.

2. Система комутації пакетів може виконувати перетворення швидкості передачі даних.

3. Під час інтенсивного трафіку передача даних зберігається, хоча може бути затримка в доставці даних або швидкість передачі може знизитися.

4. Систему пріоритетів можна використовувати в мережах з комутацією пакетів. Якщо вузол бажає передати кілька повідомлень, він може спочатку передати дані з найвищим пріоритетом. Дані високого пріоритету будуть доставлені з меншою затримкою, ніж дані низького пріоритету.

5. У мережах з комутацією пакетів спосіб передачі даних через мережу може змінюватися навіть протягом одного сеансу зв’язку. Тобто при зміні стану мережі (перевантаження або збій окремих елементів мережі) вузол може змінити маршрут блоків даних в обхід пошкодженого зв’язку. Більш того, таких шляхів може бути багато, на відміну від систем з комутацією каналів, які мають один або два резервних шляхи. Це робить мережі комутації пакетів надзвичайно надійними та ефективними.

У системах комутації пакетів, як правило, використовується асинхронне (статистичне) мультиплексування, що дозволяє в будь-який момент часу

забезпечити необхідну пропускну здатність цифрового тракту до абонента (за умови її наявності).

Кожен пакет має поле даних, заголовок та інші службові поля, розташовані на початку або в кінці пакета. У цьому випадку заголовок — це частина пакета, яка передує даним. Частина пакета, що слідує за даними (якщо такі є), називається заголовком.

Основними моментами передачі мови по пакетній мережі є: перетворення аналогового мовного сигналу в цифрову форму, формування пакетів, передача пакетів по пакетній мережі, відновлення мовного сигналу на приймальному кінці. Таким чином, щоб організувати телефонний зв’язок як на передавальній, так і на приймальній сторонах, потрібен набір апаратних і програмних засобів, які виконують оцифрування/відновлення мови, формування пакетів і доставку цих пакетів разом із пакетами даних. у пакетну мережу.

У найбільш загальному вигляді схема організації телефонного зв'язку по мережі передачі даних з комутацією пакетів представлена на рисунку 1.1. Для наочності цієї схеми вводиться поняття пристрою одночасної передачі мови та даних, що включає весь комплекс програмно-апаратних засобів, які реалізують можливість спільної передачі мови та даних по пакетній мережі.

Для організації телефонного зв'язку по пакетній мережі необхідний комплекс апаратно-програмних засобів, функціями яких є:

1. Перетворення аналогових мовних сигналів і сигналів телефонної сигналізації в одиниці протокольної інформації (пакети або кадри).
2. Поєднання трафіку голосу та даних.

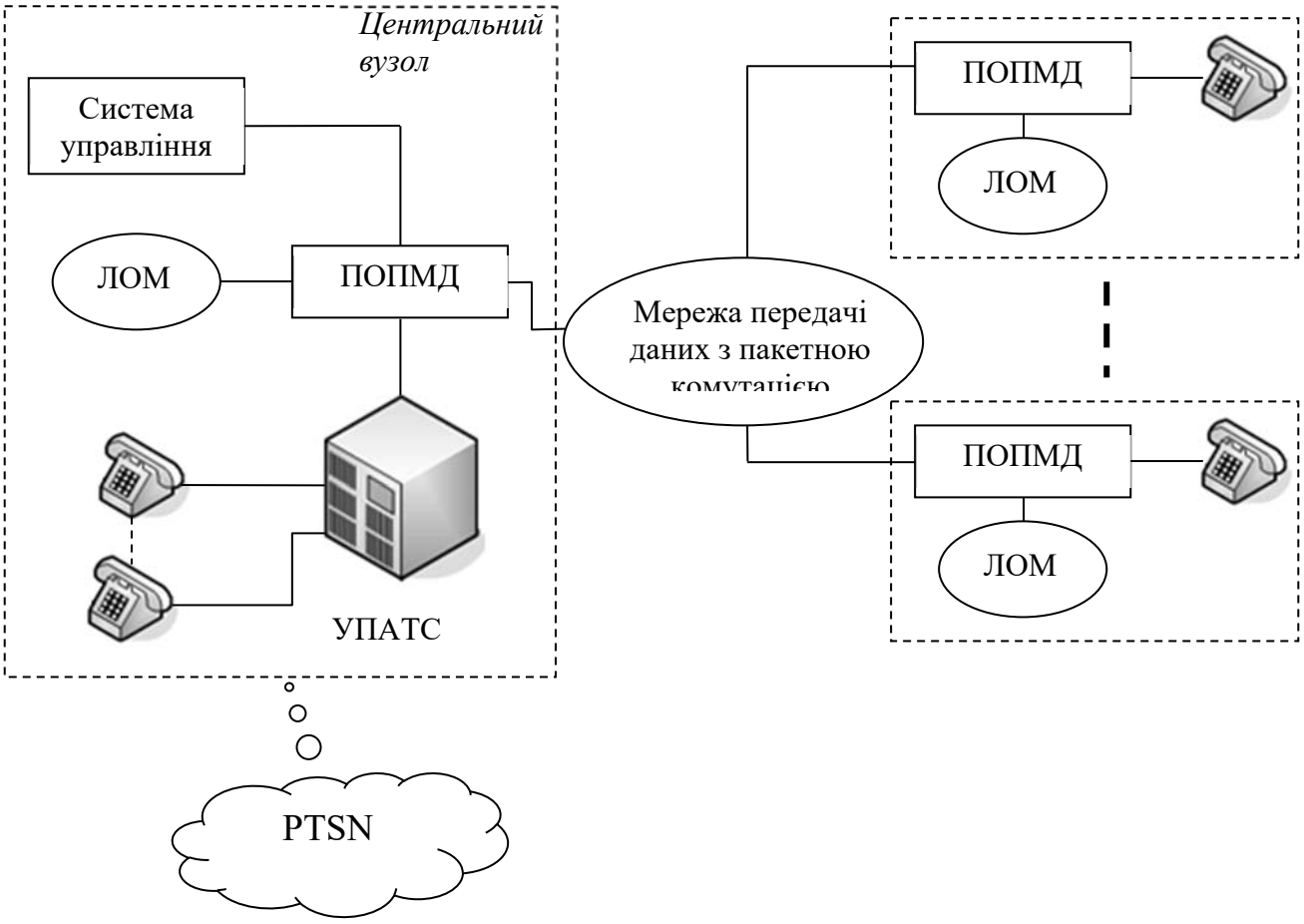

Рис. 1.1. Схема організації телефонного зв'язку по пакетній мережі.

LOM - локальна комп'ютерна мережа;

ОПМД - пристрій для одночасної передачі мови та даних;

PSTN – це комутована телефонна мережа загального користування.

Для часткової реалізації першої функції використовується DSP (процесор цифрової обробки сигналів), який необхідний для перетворення мовного сигналу в цифрову форму та формування мовних кадрів. Решта перетворень реалізуються програмно за допомогою стандартних універсальних процесорів. На малюнку 1.2. показана структура програмного забезпечення (ПЗ) для реалізації можливості передачі мови по пакетній мережі.

Це програмне забезпечення організовує інтерфейси для мовних і сигнальних сигналів, що надходять з телефону або АТС, і перетворює їх в єдиний потік інформації для передачі по мережі. Програмне забезпечення

розділене на чотири частини, щоб забезпечити чіткий інтерфейс між програмним забезпеченням DSP та іншим програмним забезпеченням для використання різних протоколів пакетної мови. Програмне забезпечення включає наступні частини для реалізації можливості передачі мови через мережу з комутацією пакетів:

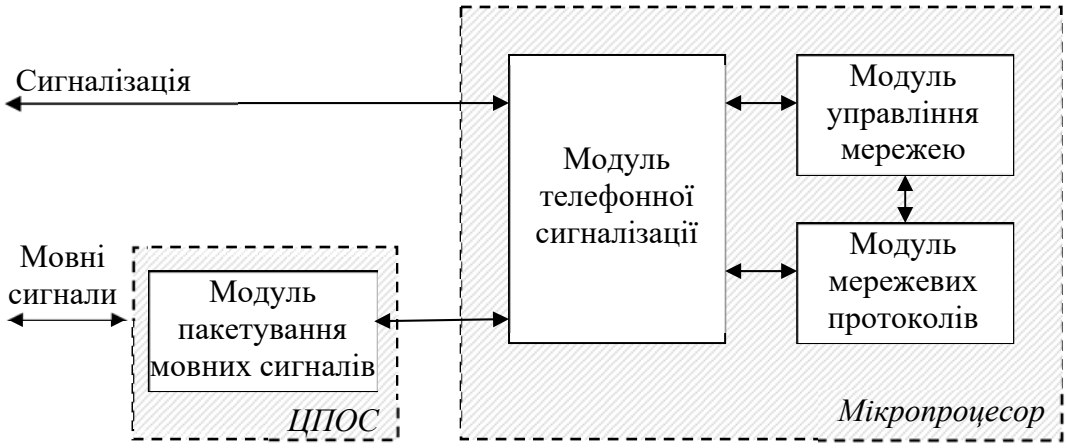

Рис. 1.2. Структура програмного забезпечення для організації телефонного зв'язку через MPD з комутацією пакетів

Це програмне забезпечення організовує інтерфейси для мовних і сигнальних сигналів, що надходять з телефону або АТС, і перетворює їх в єдиний потік інформації для передачі по мережі. Програмне забезпечення розділене на чотири частини, щоб забезпечити чіткий інтерфейс між програмним забезпеченням DSP та іншим програмним забезпеченням для використання різних протоколів пакетної мови. Програмне забезпечення включає наступні частини для реалізації можливості передачі мови через мережу з комутацією пакетів:

1. Програмне забезпечення мовного пакетування запускається на TSPOS і використовується для підготовки мовних функцій для передачі в SPD. Програмне забезпечення включає: вокодер, алгоритм ехоподавлення, алгоритм виявлення мовної активності та алгоритм усунення джиттера.

2. Програму для завантаження телефонного сигналу. Це програмне забезпечення взаємодіє з телефонним обладнанням, перетворюючи сигнали телефонної сигналізації в так звані змінні стану (встановлення з'єднання, розрив тощо), які використовуються в модулі мережевого протоколу для встановлення з'єднань.

3. Програмне забезпечення для мережевих протоколів. Це програмне забезпечення обробляє сигнальну інформацію та перетворює її з формату протоколу телефонної сигналізації на певний протокол для передачі сигнальної інформації через мережі з комутацією пакетів. Крім того, це програмне забезпечення пакує мовні кадри та сигнальну інформацію в інформаційні блоки мережевих протоколів, що використовуються в пакетній мережі.

4. Програмне забезпечення для керування мережею. Це програмне забезпечення надає інтерфейс керування мовленням для налаштування та обслуговування модулів системи мовних пакетів. Уся інформація керування визначається ASN і має синтаксис SNMP.

Передача телефонного трафіку по мережах з комутацією пакетів пов'язана з певними труднощами, пов'язаними з природними особливостями телефонної розмови. Основним небажаним явищем є затримка передачі голосового сигналу від одного абонента до іншого. Затримка спричинена двома небажаними явищами – луною та накладанням мови. Ехо означає фізичний процес відображення звукових сигналів, що надходять до диференціальної системи, яка координує 4-провідний і 2-провідний канали. Відображені таким чином сигнали повертаються до абонента і погіршують розбірливість прийнятої мови. Ехо стає серйозною проблемою, якщо затримка в поширенні звукового сигналу від джерела до приймача і назад стає більше 50 мс. У мережах з комутацією пакетів ця затримка майже завжди перевищує 50 мс, і в зв'язку з цим повинен бути передбачений механізм для усунення відлунь. Накладення мови - процес, при якому в телефоні іншої людини в момент активної розмови лунає мова одного, на відміну від ехо, коли абонент

слухає свій голос. Згідно з рекомендацією ITU-T G.114, ця проблема стає значною, якщо одностороння затримка перевищує 150 мілісекунд. Загальна мережева затримка – це величина, яка складається з наступних компонентів:

а) Накопичена затримка. Ця затримка викликана необхідністю підготувати кадр з послідовності підрахунку мови, який буде оброблений вокодером. Величина цієї затримки буде дорівнювати розміру (довжині) кадру вибраного типу вокодера. Час підготовки до підрахунку однієї мови становить 125 мкс.

У таблиці 1.1. параметри затримки наведено для деяких із найпоширеніших типів голосу.

Таблиця 1.1 Характеристики затримки вокодера

Стандартний	Тип кодування	Необхідна пропускна здатність	Накопичена затримка
G.726	ADPCM	16; 24; 32; 40 кбіт/с	125 мкс
G.728	LD-CELP	16 кбіт/с	2,5 мс
G.729	CS-ACELP	8 кбіт/с	10 мс
G.723.1	Багатошвидкісний кодер	5.3; 6,3 кбіт/с	30 мс

б) Затримка кодування. Щоб не вводити додаткову затримку в результаті фактичного процесу кодування, необхідно вибрати ЦП з такою продуктивністю, щоб затримка кодування була меншою або принаймні дорівнювала накопиченій затримці. Вибір DSP можна зробити на основі даних про складність використовуваного алгоритму кодування. Продуктивність процесора повинна бути вище або дорівнювати вказаним значенням.

в) Затримка формування пакету. Ця затримка викликана процесом підготовки мовних пакетів (як одиниць протокольної інформації). Наприклад, три мовні кадри, отримані в результаті перетворення G.729 (30 мс мови),

можуть бути зібрані в один пакет. Це призводить до затримки пакета 30 мс замість 10 мс, якщо він мав 1 кадр.

г) Затримка мережі. Ця затримка виникає, коли пакети передаються по мережі, і залежить від каналів передачі та протоколів, що використовуються в мережі, а також від буферів для усунення тремтіння. Ця затримка може становити значну частину загальної затримки, і в деяких мережах IP і Frame Relay вона становитиме 70-100 мс або більше.

Щоб забезпечити гарантовану якість голосового зв’язку, мережа має бути налаштована та керована таким чином, щоб забезпечити мінімальні затримки та тремтіння.

Коли повідомлення передаються через мережі передачі даних із комутацією пакетів, часто виникають втрати окремих пакетів. Це явище виникає в результаті спотворення пакетів в каналі зв'язку, а також при реалізації схем передачі джиттера приймального буфера. У випадку передачі даних ця проблема легко вирішується за допомогою відповідних протоколів, але у випадку передачі мови ці протоколи можуть бути незастосовними через затримку, яку вони вносять.

Набули поширення такі підходи до вирішення цієї проблеми:

а) Замініть втрачений пакет раніше отриманим пакетом. Цей підхід використовується, коли кількість втрачених пакетів невелика (до 5%).

b) Передача надлишкової інформації через використання додаткової смуги пропускання. В цьому випадку $n+1$посилка відправляється разом з n посилкою. Однак при такому підході смуга пропускання використовується нераціонально і створюються значні затримки.

1.2 Аналіз телефонії

IP-телефонія - це технологія, яка поєднує в собі переваги телефонії та Інтернету. До недавнього часу мережі з комутацією каналів (телефонні мережі) і мережі з комутацією пакетів (IP-мережі) існували майже незалежно

одна від одної і використовувалися для різних цілей. Телефонні мережі використовувалися тільки для передачі голосової інформації, а IP-мережі - для передачі даних. Технологія IP-телефонії з'єднує ці мережі за допомогою пристрою, тобто шлюзу. Шлюз - це пристрій, який з'єднує телефонні лінії з одного боку та IP-мережу (наприклад, Інтернет) з іншого.

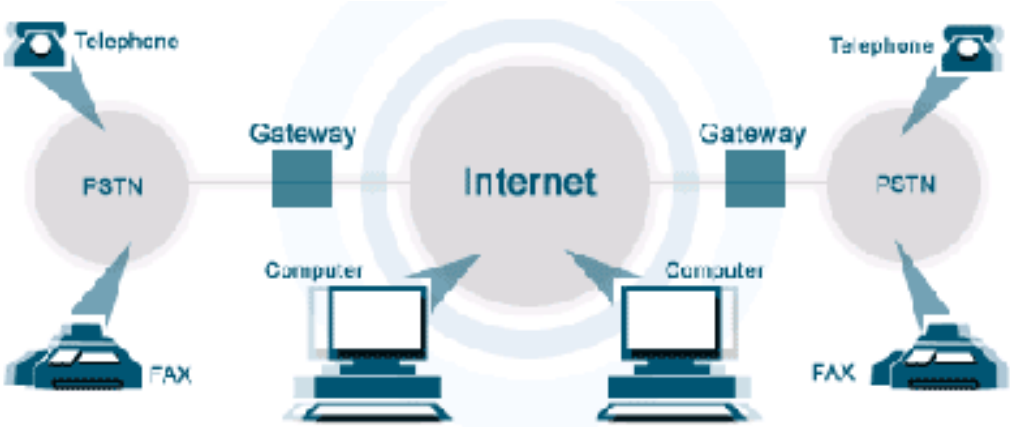

Рис. 1.3. Асиметрична схема криптосистеми

Загалом голос через мережу IP працює таким чином. Інформація про дзвінок і сигналізацію передається з телефонної мережі на мережевий пристрій, який називається телефонним шлюзом, і обробляється спеціальною платою пристрою голосового обслуговування. Шлюз, використовуючи протоколи керування сімейства H.323, передає сигнальну інформацію іншому шлюзу, розташованому на приймальному кінці IP-мережі. Приймальний шлюз забезпечує передачу сигнальної інформації до приймального телефонного обладнання згідно з планом нумерації, гарантуючи наскрізне з'єднання. Після встановлення з’єднання голос на вхідному мережевому пристрої оцифровується (якщо він не був оцифрований), кодується відповідно до стандартних алгоритмів ITU, таких як G.711 або G.729, стискається, інкапсулюється в пакети та надсилається до пункту призначення. . віддалений пристрій для використання стека протоколів TCP/IP. IP-пакети перетворюються назад на телефонний сигнал, і абонент отримує дзвінок.

Кінцеві користувачі послуги можуть навіть не знати, як здійснюється цей дзвінок.

Оскільки міжнародний телефонний оператор (міжміський) не бере участі в IP-телефонному дзвінку, вартість цього дзвінка на порядок менше, ніж вартість традиційного телефонного зв'язку.

Однак дзвінок з телефону на телефон є найбільш очевидною, але далеко не єдиною послугою, яку може надати оператор IP-телефонії. За допомогою IP-мережі можна обмінюватися цифровою інформацією для пересилання голосових або факсимільних повідомлень між двома комп'ютерами в реальному часі. За допомогою Інтернету можна буде реалізувати цю послугу в глобальному масштабі. Для IP-телефонії найчастіше використовується стандарт H.323, який визначає передачу відео та аудіо через мережі з негарантованою якістю послуг, такі як Ethernet та IP. H.323 описує декілька функцій, зокрема аудіо- та відеокодеки (кодери/декодери), протоколи зв'язку та синхронізацію пакетів.

Види IP-телефонії

Голосовий зв'язок через IP-мережу можна здійснювати кількома способами:

1. «Комп'ютер – комп'ютер». Цей варіант не є прикладом IP-телефонії, оскільки голос передається лише через мережу передачі даних без доступу до телефонної мережі. Для організації передачі трафіку користувач встановлює необхідне обладнання та програмне забезпечення, а також оплачує провайдеру роботу каналу зв'язку. Перевагою цього варіанту є максимальна економія. Недоліком є мінімальна якість зв'язку.

2. «Телефон - телефон». Для організації такого зв'язку необхідна наявність певних мережевих пристроїв і механізмів взаємодії. Голосовий трафік передається через IP-мережу, як правило, по окремому шляху. Шлюзи - це пристрої, які організовують взаємодію, з одного боку, з телефонною мережею загального користування, а з іншого - з мережею IP. Голосовий зв'язок у цьому способі, порівняно з варіантом «комп'ютер на комп'ютер»,

коштує дорожче, але його якість значно вища та зручніший у використанні. Щоб скористатися цією послугою, необхідно зателефонувати провайдеру, який обслуговує шлюз, ввести з телефону код абонента та номер і говорити так само, як під час звичайного телефонного дзвінка. Шлюз виконає всі необхідні операції маршрутизації викликів.

3. «Комп'ютер - телефон». Це відкриває більше можливостей для корпоративних користувачів, оскільки часто використовується корпоративна мережа, яка обслуговує дзвінки з комп'ютерів на шлюз, які потім передаються через телефонну мережу загального користування. Корпоративні рішення, які використовують зв’язок між комп’ютером і телефоном, можуть допомогти заощадити гроші. Ніякого додаткового обладнання кінцевому користувачеві не потрібно. Досить мати під рукою телефон з можливістю тонового набору. Це необхідно для того, щоб після дзвінка оператору вводити свій код в тональному режимі, і тоді абонент діяв не так, як звичайні. Більшість сучасних телефонів, в тому числі стільникові та стільникові, мають таку функцію. Якщо з якихось причин такого телефону немає, з функцією набору номера може впоратися біпер або, на крайній випадок, спеціальна програма, яку можна завантажити з інтернету.

4. «WEB – телефон». Ще однією новою послугою провайдерів IP-телефонії є дзвінок з веб-сайту або Surf&Call – рішення компанії VocalTec у сфері веб-телефонії, яке дозволяє здійснювати дзвінки, вибравши посилання з Інтернет-сторінки на назву абонента, на якого телефонують. Це рішення спрямоване, перш за все, на розширення можливостей електронної комерції. Surf&Call дозволяє користувачам Інтернету спілкуватися безпосередньо, наприклад, з торговим представником або спеціалістом технічної підтримки. Встановлення телефонного з'єднання відбувається при натисканні курсором на з'єднання, тобто, наприклад, назва компанії, ім'я абонента, що викликається, і т.д. на сторінці в Інтернеті. При цьому користувачеві не потрібна друга телефонна лінія чи доступ до Інтернету, необхідно лише завантажити невелике клієнтське програмне забезпечення, яке зазвичай можна знайти на тій самій

WEB-сторінці та встановлюється автоматично. З іншого боку, Surf&Call дозволяє представникам компанії відповідати на запитання, відображати WEB-сторінки та передавати необхідну інформацію, що покращить якість послуг, що надаються.

Переваги IP-телефонії.

Здешевлення телефонних розмов. Впровадження технології VOIP в комп'ютерній мережі дозволяє скоротити загальні витрати на здійснення міжнародних і міжміських телефонних розмов, а також запустити процес переходу на технології пакетної передачі мультимедіа. Крім того, завдяки можливості доступу до телефонної мережі міста використання цієї технології дозволяє звести до мінімуму оренду звичайних телефонних ліній.

Покращена якість зв'язку. Якість спілкування можна оцінити за такими основними характеристиками: рівень спотворення голосу; частота «зникнення» голосових пакетів; час затримки (між оголошенням фрази першим абонентом і моментом, коли її почує другий абонент). З усіх перерахованих характеристик якість зв'язку значно підвищилася порівняно з першими версіями рішень IP-телефонії, які допускали спотворення та переривання мови. Удосконалення кодування голосу та відновлення втрачених пакетів дозволили досягти рівня, коли абоненти настільки добре розуміють мову, що посередники не думають, що підключення здійснюється за допомогою технології IP-телефонії. Затримка, очевидно, впливає на швидкість розмови. Відомо, що затримки до 250 мілісекунд майже непомітні для людини. Сучасні рішення IP-телефонії не перевантажують цей ліміт, тому розмова не відрізняється від спілкування через звичайну телефонну мережу. Крім того, затримки зменшуються завдяки наступним трьом факторам:

• По-перше, вдосконалюються телефонні сервери (їх розробники борються із затримками шляхом вдосконалення алгоритмів роботи).

• По-друге, розвиваються приватні (корпоративні) мережі (їх власники можуть контролювати пропускну здатність і, відповідно, затримку).

• По-третє, сам Інтернет розвивається – сучасний Інтернет не був створений для спілкування в реальному часі. Інженерна робоча група Інтернету (IETF) працює з Інтернет-операторами, щоб запропонувати нові технології, такі як протокол резервування (RSVP), які дозволяють резервувати пропускну здатність.

Вирішіть проблему зайнятої лінії. Протягом тривалого часу люди, які прагнуть подорожувати всесвітньою павутиною, стикалися з проблемою зайнятості телефонних ліній під час сеансу Dial-up. IP-телефонія дозволяє дуже елегантно вирішити цю проблему. Все, що потрібно зробити абоненту – це подати на свою АТС команду з сигналом «зайнято» на номер телефону сервера IP телефону. Коли ви телефонуєте на номер абонента під час Інтернет-сесії, виклик перенаправляється на сервер IP-телефонії, який перетворює його в IP-пакети та надсилає на комп'ютер абонента. На комп'ютері абонента з'являється значок «Call In», натиснувши на який він може говорити.

Підвищення якості факсимільного зв'язку. Оскільки, в основному, факсимільне повідомлення – це потік цифрових даних, а в технології VoIP дані передаються в цифровій формі, таким чином зводячи до мінімуму передачу факсимільних повідомлень аналоговими лініями. А за рахунок того, що обладнання має можливість демодулювати сигнал перед передачею по IP-мережі та передавати факсимільне повідомлення, закодоване у форматі 64Kb в діапазоні 9,6 Kbit, знижується навантаження на канали.

Інтеграція філій в єдину інформаційну структуру. Останнім часом, з розвитком інформаційних технологій і збільшенням пропускної здатності каналів, для більш ефективного вирішення бізнес-завдань філії компанії об'єднують в одну, створюючи інтранет. Оскільки ця технологія використовує мережі передачі даних для передачі голосу, стає можливим з'єднання не тільки комп'ютерних мереж, але й телефонних мереж. Віртуальні приватні мережі (VPN). IP-телефонія — чудова технологія для побудови віртуальних приватних корпоративних мереж. Основною особливістю технології VPN є використання IP-мережі як магістралі для

передачі корпоративного IP-трафіку. Мережі VPN вирішують завдання підключення корпоративного користувача до віддаленої мережі та об'єднання кількох віддалених локальних мереж і АТС в одну корпоративну мережу для передачі голосу та даних.

Глобальний роумінг. IP-телефонія дозволяє операторам зв'язку дуже легко і з мінімальними витратами організувати роумінг послуг зв'язку. Особливо це актуально для мобільних операторів - рішення, побудоване на технологіях IP-телефонії, на порядок дешевше традиційного, і має набагато більшу гнучкість.

Комбінований доступ до Інтернету. Голосові дані, репліки повідомлень передаються за допомогою IP - основного набору інтернет-протоколів, це рішення саме по собі означає доступ до ресурсів Мережі та явну економію на оренді ліній зв'язку та оплаті послуг.

Майбутнє IP-телефонії.

IP-телефонія має три етапи розвитку. Спочатку це була, швидше, інтернет-іграшка, придатна лише для спілкування двох ентузіастів. Два комп'ютери, оснащені мікрофонами, колонками, звуковими картами і не дуже складним програмним забезпеченням, дозволяли вести двосторонню розмову в Інтернеті в реальному часі. Однак цьому способу зв'язку явно бракувало зручності звичайного телефонного зв'язку: абонентам необхідно знати IP-адресу комп'ютера посередника, узгодити час розмови, вибрати момент для кращої передачі голосу при наявності інтернет-трафіку. немає перевантажень і великих затримок. Крім того, за відсутності стандартів необхідно було встановити таке програмне забезпечення на обидва комп’ютери, щоб спосіб кодування голосу та упаковки його в пакети був однаковим. Взаємодія між комп’ютером і телефоном, підключеним до звичайної телефонної мережі, не була передбачена Азією. Однак витрати були обмежені невеликою комісією Інтернет-провайдера.

Другий етап ознаменувався появою стандартів IP-телефонії, насамперед - стандартів групи H.323. Розробники цих протоколів припускали, що дві

мережі - телефонна та IP - будуть тривалий час поряд, а це означає, що важливо регулювати їх взаємодію з урахуванням традиційних процедур встановлення з'єднання з телефонною мережею, які вже існують, так само. щодо способу передачі виклику та уніфікації самого голосу через мережу IP. Стандарти H.323 визначають дві групи протоколів - протоколи транспортної площини, також відомі як площина користувача, і протоколи площини керування викликом. На цьому етапі розвитку IP-телефонії IP (Інтернет або приватна) мережа широко використовувалася як транзит між двома локальними телефонними мережами. Ця схема дуже популярна для впровадження загальнодоступних послуг IP-телефонії в усьому світі. Для її реалізації оператору зв'язку не потрібно створювати власну дорогу транспортну інфраструктуру та мати прямий доступ до абонентів. Однак стратегічні перспективи такого підходу залишають бажати кращого через низький рівень масштабованості та вузький спектр послуг.

Масштабованість обмежена кількома факторами. Перш за все, постачальник повинен встановити численні однорангові відносини зі своїми бізнес-конкурентами. По-друге, протоколи обох площин повинні бути реалізовані в усіх аспектах мережі IP-телефонії: у шлюзах і терміналах, що викликає непотрібну складність і високу вартість для всіх цих пристроїв. Нарешті, користувачам надаються лише базові послуги обробки викликів, оскільки немає взаємодії з міжстанційними протоколами сигналізації SS7 і мережевими послугами IN Smart.
Крім того, діалог із сервером інтерактивного голосового повідомлення під час аутентифікації абонента та набору номера абонента, що викликається, досить обтяжливий – набагато зручніше просто набрати цей номер із невеликим префіксом, наприклад 8-20, і отримати доступ. до. послуги міжнародної IP-телефонії. Але цьому провайдеру потрібен прямий доступ до абонента або угода з місцевими операторами для переадресації таких дзвінків на IPTP-шлюз за допомогою інструментів Smart network (а вони ще не підтримуються всіма місцевими операторами).

Тому, щоб IP-телефонія вийшла на вищий рівень для національного або міжнародного оператора, необхідні інші стандарти та обладнання, щоб мережі, побудовані на основі протоколу IP, могли на рівні взаємодіяти з традиційними телефонними мережами.

Багато з необхідних стандартів вже з'явилися і закладені в нове покоління обладнання, яке є основою для третього етапу розвитку IP-телефонії. Така мережа може обслуговувати власних абонентів і служити транзитною мережею для традиційних телефонних мереж, надаючи повний спектр послуг, включаючи послуги мережі IN Smart. У вузлах IP-телефонії нового покоління відбувся чіткий розподіл функцій на три групи - транспортні, управління викликами та прикладні служби.

1.3 Існуючі підходи до захисту інформації в IP-телефонії

Захист інформації передбачає підтримання інформаційної безпеки, тобто стану безпеки інформаційного середовища, який досягається дотриманням конфіденційності, цілісності та доступності інформації [4]. Відповідно до [5] зазначені вимоги можуть бути виконані у випадку IP-телефонії лише за умови використання криптографічного перетворення інформації, тобто шифрування.

Конфіденційність зв'язку забезпечується впровадженням криптосистем, які відрізняються схемами розподілу ключів. Зазвичай розрізняють симетричну та асиметричну криптографію. Асиметрична криптосистема, схема якої наведена на малюнку 1.4, враховує, що кожен користувач генерує два ключа, пов'язані між собою деякими відносинами. Один важливий функціонує відкрито, інший - таємно. Повідомлення шифрується відкритим ключем, який передається кожному одержувачу, а процес дешифрування здійснюється за допомогою секретного ключа, який зберігається лише у його власника. Даний тип системи використовується як самостійний спосіб захисту і при розподілі ключів, а також метод

аутентифікації - можливість встановлення авторства інформації. Тобто асиметрична криптографія дозволяє не тільки зашифрувати інформацію, але й підтвердити , що власник конкретного ключа відправив повідомлення і ніхто інший його не переслав.

Рис. 1.4. Асиметрична схема криптосистеми

В асиметричних криптографічних системах надійність захисту інформації забезпечується не секретністю алгоритмів, а в основному математичними фактами [6, 7].

Криптосистеми з відкритим ключем займають багато часу і не можуть бути використані при шифруванні мультимедійних даних - швидкість роботи таких алгоритмів значно нижча за швидкість симетричних криптосистем [8].

Симетрична криптосистема, схема якої показана на малюнку 1.5, заснована на процесі шифрування і дешифрування за допомогою одного секретного ключа, відомого обом сторонам. У цьому випадку надійність базується на конфіденційності ключа.

Пропозиція У. Діффі та М. Гельмана щодо ідентифікації користувачів шляхом створення цифрового підпису базується на симетричних криптосистемах, які не поширені в сучасних комп’ютерних системах і мережах [8, 9].

захист інформації в IP- телефонії на основі використання спеціального протоколу захисту інформації (TLS - Transport Шар Безпека , VPN -

віртуальний Приватний Мережа) або додаткові протоколи в рамках існуючих протоколів IP-телефонії (SIP - Сесія Ініціатива протокол , специфікація N.323, Skype).

Рис. 1.5. Симетрична схема криптосистеми

захист інформації TLS наступне покоління загального криптографічного протоколу SSL (Secure Розетки Layer), який базується на асиметричній криптографії. Прикладом використання SSL є протокол HTTPS (Hypertext Переклад Протокол Secured), протокол захисту інформації TLS включає три етапи [6]:

1)діалог між двома сторонами для вибору алгоритму шифрування;

2)обмін ключами за допомогою відкритих криптосистем або аутентифікація за допомогою сертифікатів;

3)передача даних, зашифрованих за допомогою симетричних алгоритмів шифрування.

Для обміну ключами використовується комбінація алгоритмів RSA (алгоритм розроблений Р. Райвестом, А. Шаміром і Л. Адлеманом у 80-х роках), алгоритму Діффі-Хеллмана та DSA (Digital). Підпис Алгоритм). Для симетричного шифрування використовуються алгоритми RC 2 (Ron 's Code 2), RC 4, IDEA (International Подробиці Шифрування Алгоритм), ROS (Дані Шифрування Стандарт), Тримісний DES або AES (Комплекс Шифрування Стандартний). Як відомо [9, 10], ці алгоритми мають свої вразливості, що

дозволяє застосовувати лінійні та диференціальні методи шифрування для зменшення кількості операцій порівняно з повним пошуком.

Використання VPN дозволяє створити тунель між ініціатором і термінатором. Ініціатор тунелю інкапсулює мережеві пакети в новий пакет. Конфіденційність і цілісність даних досягається за рахунок шифрування не тільки початкових даних, але і всього IP-пакета. протокол VPN реалізовано не тільки програмно, а й апаратно в маршрутизаторах. Робота VPN передбачає використання відкритих ключів [11].

З'єднання VPN має низку обмежень, зокрема:

1) взаємодія програмного забезпечення (ПО) VPN і міжмережевих екранів може значно погіршити загальну продуктивність системи, оскільки весь IP-пакет зашифрований;

2) VPN на основі маршрутизатора може негативно вплинути на інший трафік, отриманий від систем, які не використовують з'єднання VPN;

3) адміністрування програмного забезпечення на основі VPN потребує додаткових ресурсів: інструментів адміністрування, каталогів тощо;

4) складність реалізації мобільності терміналів і безпосередньо абонентів при використанні стаціонарних терміналів;

5) проблеми з юзабіліті при організації конференцій щодо часових затримок, які можуть досягати 300 мс.

Всі додаткові протоколи захисту інформації в IP-телефонії можна розділити на два типи: відкриті, включаючи визнані міжнародні специфікації і стандарти, і закриті - протоколи з закритими стандартами. Так, будь-який протокол ІЧ-телефонії можна вважати закритим протоколом, закритою є інформація про те, які повідомлення структуровані.

Серед відкритих протоколів слід виділити:

• сімейство протоколів SIP (Session Initiation Protocol), розроблене IETF (Internet Engineering Task Force);

• Специфікація протоколу H.323, розроблена ITU (Міжнародний союз телекомунікацій) для IP-телефонії.

Протокол SIP RFC (Request for Comments) 3261 [12] розроблений на основі протоколу HTTP. Він належить до сьомого рівня моделі OSI. Протокол SIP спеціально розроблений для використання в IP-мережах. Для підключення IP-мережі до стільникової мережі існує модифікація протоколу SIP - протокол SIP-T, який визначає пряме і зворотне перетворення повідомлень SIP і TMzK (телефонні мережі загального користування). Цей протокол забезпечує аутентифікацію користувача.

Протокол SIPS (Session Initiation Protocol Secured) був розроблений безпосередньо для захисту інформації на основі протоколу SIP, який поєднує в собі конфіденційність автентифікації та спілкування за допомогою протоколу TLS. Він може використовуватися лише у зв'язку TSR. При цьому необхідно створити сеанс і обмінюватися ключами на всіх ділянках мережі, тобто між усіма парами SIP-серверів або шлюзів. Коли в глобальній мережі використовується протокол SIPS, час, витрачений на шифрування, становить основну частину затримки в передачі голосових даних. Протокол SIPS застосовується лише до IP-мережі та не підтримує підключення до TMzK.

Захист інформації в сімействі протоколів SIP реалізується за допомогою п’яти механізмів [13]:

1. Автентифікація за допомогою дайджесту повідомлень RFC 2617. Алгоритм MD5 використовується для отримання хеш-значення з імені, пароля та URL-адреси. Для конфіденційності мультимедійних даних використовується протокол SRTP (Secure Real-Time Transport Protocol), а для обміну ключами – протокол RFC 2327 (SDP (Session Description Protocol)).

2. Забезпечити криптографічну безпеку електронної пошти на основі стандарту S/MIME (Secure/Multipurpose Internet E-mail Extensions).

3. Використовуйте протокол TLS як для автентифікації, так і для шифрування даних.

4. Використання протоколу IPSec (протокол для забезпечення захисту даних, що передаються через Інтернет протокол IP); він дозволяє

автентифікацію та шифрування IP-пакетів і розподіл ключів за допомогою протоколу IKE (Internet Key Exchange).

5. Використовуйте протокол IPSec і ручну роздачу ключів.

Деякі оператори IP-телефонії, в тому числі TeITeI, використовують протоколи SIP в мережі PSipTN (мережа IP-телефонії, побудована на основі протоколу SIP), а також глобальну мережу Інтернет у вигляді різноманітних програмних телефонів - програмного забезпечення для персонального комп'ютера. . Крім того, ці протоколи підтримуються великою кількістю обладнання для створення корпоративних мереж IP-телефонії, наприклад Avaya і Nokia.

Специфікація протоколу N.323 орієнтована на інтеграцію з TMzK і, на відміну від SIP, містить велику кількість інших протоколів. На рисунку 1.6 показана структура H.323.

<table>
<tr><td colspan="2">Гарантована доставка інформації за протоколом TCP</td><td colspan="3">Негарантована доставка інформації за протоколом UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.225</td><td colspan="2">Потоки мови та відеоінформації</td></tr>
<tr><td>Управління з'єднанням(Q.931)</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="2">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Канальний рівень</td></tr>
<tr><td colspan="5">Фізичний рівень</td></tr>
</table>

Рис. 1.6 – Структура протоколу H .323

Для захисту інформації в специфікації H.323 використовується протокол H.235, який передбачає аутентифікацію за допомогою сертифікатів або повідомлень-токенів.

Протокол H.235 має 9 рекомендацій щодо захисту інформації, відповідно до яких можна використовувати основні методи протоколу H.235 або інших протоколів. Залежно від обраної пропозиції, H.235 дозволяє автентифікацію, захист деяких службових даних (H.225) або медіа (RTP).

Автентифікація в специфікації N.323 базується на алгоритмах HMAC-SHA1-96, цифрових сертифікатах, створених за допомогою алгоритмів SHA1 і

MD5. Конфіденційність медіа-трафіку забезпечується алгоритмами симетричного шифрування DES, 3DES і AES [14].

У той же час використання H.235 має кілька обмежень:

• складність реалізації для глобальних мереж і недостатня поширеність обладнання;

• не всі портали підтримують цей протокол, тому що використання його рекомендацій не є обов'язковим [15].

На малюнках 1.7 і 1.8 показано дві пропозиції в протоколі H.235, а саме профілі D і E.

Тип захисту інформації	RAS	H.225		H.245	RTP
Аутентифікація	HMAC-SHA1-96	HMAC-SHA1-96		HMAC-SHA1-96	
Цілісність	HMAC-SHA1-96	HMAC-SHA1-96		HMAC-SHA1-96	
Конфіденційність					DES/3DES
Розподілення ключів	Призначений пароль	Призначений пароль	Генерація та обмін за схемою Діффі-Хелмана	Вбудовані в H.235 сесійні ключи	

Рис. 1.7. Можливості захисту інформації в специфікації H .323-Profile D

Тип захисту інформації	RAS	H.225	H.245	RTP
Аутентифікація	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	
Цілісність	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	Цифровий сертифікат (SHA1/MD5)	
Конфіденційність				
Розподілення ключів	Призначений сертифікат	Призначений сертифікат		

Рис. 1.8. Можливості захисту інформації в специфікації H .323-Profile E

IPSec для захисту інформації в специфікації H.323 в межах VPN - з'єднання . У цьому випадку всі дані шифруються, але тунель (захищене з’єднання між клієнтом і сервером) створюється лише між двома кінцевими користувачами або серверами [16, 17].

H.323, як і SIP, в глобальній мережі Інтернет у вигляді різноманітних програмних телефонів (наприклад, комплексне програмне забезпечення Yate [18]) і у великій кількості обладнання Cisco , а не тільки для створення корпоративних мереж IP-телефонії.

До закритих протоколів відноситься протокол Skype , оскільки він є найпопулярнішим представником цього типу протоколів (мережа IP- телефонії Skype налічує вже понад мільярд користувачів).

Протокол Skype невідомий широкому загалу, тобто невідомо, за яким саме алгоритмом відбувається вибір портів для встановлення сеансів і формат службових та інформаційних повідомлень, що, в свою чергу, вважається негативним фактором. з точки зору інформаційної безпеки. Але аналіз повідомлень протоколу Skype , проведений у [19, 20], показав, що Skype використовує протоколи TCP і UDP для встановлення сеансів.

Недоліком протоколу Skype є необхідність підключення користувачів до Інтернету для аутентифікації (дані також передаються через Інтернет, навіть якщо комп'ютери абонентів знаходяться в одній локальній мережі). Це пов’язано зі схемою системи Skype , коли вузли з більшою пропускною здатністю робляться «мостами» (supernode), тобто виконують функцію маршрутизації передачі даних інших користувачів цього програмного забезпечення. Після реверсування клієнтського програмного забезпечення можна за допомогою модифікованого супервузла створити вузол, який може виконувати додаткові функції, крім стандартних:

• перенаправляти запити користувачів на контрольний сервер і блокувати спільний доступ доступ користувача до системи (атака на відмову в обслуговуванні);

• перехоплювати логіни та паролі користувачів;

• записати всю розмову або її частину.

В якості альтернативи можна використовувати атаку «людина посередині», тобто. де у випадку користувача А супервузол імітує

користувача B, а у випадку користувача B він імітує користувача A, замінюючи його ключі (Малюнок 1.9).

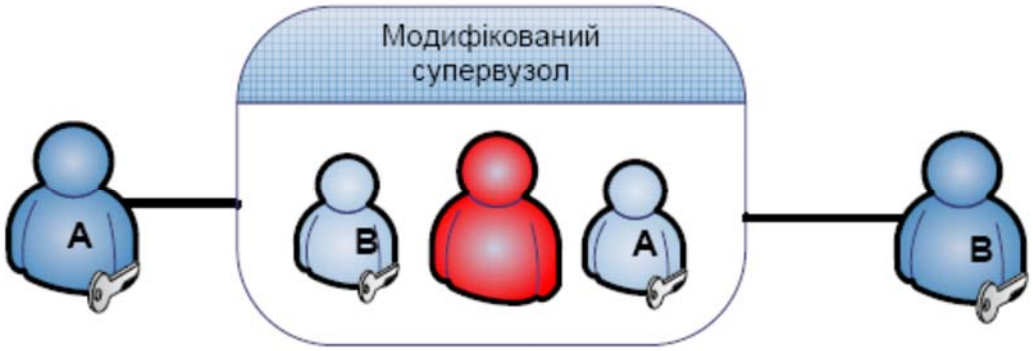

Рис. 1.9. Атака "людина посередині".

З точки зору прямого захисту інформації, Skype використовує ключі RSA і шифрування, як AES , але розробник не надає офіційних даних про алгоритми шифрування. Відомо, що захист інформації відбувається лише до підключення до ТМзК [21].

Таким чином, розподілена структура мережі Skype представляє досить значний ризик для безпеки переговорів і є одним з головних факторів, які впливають на те, чому Skype не може використовуватися як безпечне спілкування, незважаючи навіть на використання сучасних криптографічних алгоритмів [17, 18].]. . Подібні випадки відомі в історії розробки ПЗ із закритим кодом, коли програмне забезпечення мало велику кількість прогалин у системі безпеки [22].

1.4 Характеристики приховування даних в IP-трафіку - телефонія

В даний час заходи щодо забезпечення безпеки голосового зв'язку можуть бути спрямовані не тільки на запобігання несанкціонованому перехопленню голосової інформації, а й на приховування факту її передачі за допомогою стандартних технічних методів, стандартного традиційного

обміну інформацією та публічних протоколів для цих цілей. доступні канали зв'язку.

В останні роки цей напрям захисту інформації в комп’ютерних телекомунікаційних системах, який активно розвивається у всьому світі, отримав назву «стегологія».

Останнім часом особливу популярність набула така частина цього напрямку, як стеганографія, яка використовується в області приховування секретної інформації в графічних зображеннях, що передаються через комп'ютерні мережі. У той же час прогрес, досягнутий у розробці пристроїв для передачі мовних сигналів, а також комп’ютерних методів відкриває нові можливості для передачі конфіденційної інформації в аналогових і цифрових звукових сигналах і мовленні, а також. для їх прихованої передачі в інформаційних контейнерах різного типу, заснованих на використанні технологій динамічного мультимедіа, комп’ютерної та мобільної телефонії. Напрямок цифрових технологій у сфері захисту секретної інформації, яка прихована всередині або поверх відкрито передаваного звукового сигналу, тепер називається стеганофонією.

В даний час широко використовуються методи комп'ютерної стеганографії, засновані на використанні природного шуму, що містить цифрові масиви, отримані стандартними методами перетворення з аналогових аудіо- та відеосигналів. Ці шуми є помилками квантування, і їх неможливо повністю усунути. Використовуючи шумові біти для передачі додаткової секретної інформації, можна створити прихований канал передачі даних. Бітовим шумом зазвичай вважають молодші біти значень показань, які є шумом з точки зору точності вимірювання та несуть найменшу кількість інформації під час читання. Такі біти зазвичай називають найменш значущими бітами (LSB).

Одним із найпоширеніших методів стеганофонії для приховування конфіденційної інформації є метод, заснований на використанні аудіоданих (та/або будь-яких інших мультимедійних даних) NZB. Такі потоки аудіофайлів

NZB ще не є випадковими і мають певне групування послідовних нулів і одиниць, яке було подолано під час додавання інформації. Розроблено певні статистичні критерії, призначені для приховування секретного інформаційного повідомлення в НЗБ звукових сигналів.

Статистичний аналіз аудіоданих дозволив нам виявити деякі важливі властивості, які впливають на приховування секретних даних і, відповідно, на їх безпеку за допомогою аналогічних методів з використанням шумових бітів. Серед таких властивостей слід звернути увагу на:

- неоднорідність рахункових послідовностей;
- наявність певних залежностей між бітами в графі;
- наявність певних залежностей між самими графами;
- нерівність ймовірності умовних розподілів у послідовності підрахунків;
- наявність довгої серії однакових бітів;
- наявність кореляції між NCB і старшими бітами.

Ці властивості різною мірою спостерігаються в більшості аудіофайлів і можуть бути використані для побудови різних статистичних критеріїв, які визначають приховані факти в NZB. Тому подібні прийоми комп'ютерної стеганофонії все рідше використовуються на практиці.

Сьогодні можна запропонувати наступні вимоги для приховування секретної мовної інформації та для розміщення стеганофонічних маркерів у різних типах сигналів, масивів і форматів даних без вищезазначених недоліків:

- сприйняття знаків і даних, вкладених у конфіденційну інформацію, не повинно суттєво відрізнятися від сприйняття оригінального «відкритого» повідомлення, що міститься в даному знаку чи масиві;

- передані таємні мовні дані, приховані різними сигналами або неявні в їхніх параметрах, які не можна легко виявити в цих несучих сигналах широко поширеними методами та технічними методами аналізу, доступними на даний момент ;

- у деяких програмах встановлення та виявлення стеганофонічних маркерів

не повинно залежати від синхронізації цих процесів та наявності будь-якого стандарту;

- спеціальні методи встановлення та виявлення стеганофонічних маркерів повинні бути реалізовані на базі стандартної комп'ютерної техніки або спеціальних апаратно-програмних засобів на її основі;

- повинна бути передбачена можливість встановлення та ідентифікації ознак автентичності (мови) сигналів, що виявляються під час копіювання або незаконної модифікації, незалежно від типу подання та передачі цього сигналу (аналоговий чи цифровий);

- повинна бути можливість приховати конфіденційну інформацію в наборах даних незалежно від типу інформації, представленої в них.

Ось кілька прикладів таємної передачі інформації. Таким чином, можна непомітно прослухати мовний сигнал, переданий і збережений в іншому аудіо- та відеосигналі, а також поєднати технології стеганофонії з технологіями стеганографії, «розчинивши» зображення динамічного акустичного спектру. зображення - «контейнери», які мають бути представлені, синтезовані та далі озвучені на приймальному кінці публічного каналу зв'язку.

Сонограмні зображення можна використовувати як стегомаркери для передачі та зберігання мовних сигналів на паперових носіях. При реалізації таких технологій «мовного підпису», які стосуються захисту документів за змістом і обслуговуванням приблизно так само, як електронний цифровий підпис, стандартний аркуш паперу може бути надрукований у вигляді різноманітних малюнків шаблонів від 2 до 4 хвилин якісної телефонної розмови.

При цьому автентичність документа може бути встановлена не тільки за наявністю відповідних підписів і печаток, а й за інформацією, яка міститься в «мовному підписі», за допомогою сканування, синтезу та вираження основних моментів змісту документа. документа , тобто сказала відповідальна особа.

Невідповідність озвученої інформації інформації, яка міститься в документі, свідчить про фальсифікацію. Створити «мовний штамп» чи «мовний підпис» практично неможливо.

Слід зазначити, що розрахункові методи встановлення стеганофонічних маркерів і прихованої передачі секретної інформації в більшості випадків не вимагають синхронізації процесів їх введення-детектування або наявності еталонів порівняння, які тому можуть бути використані як канали зв'язку. не тільки коли вони приймають і передають сигнали та дані, а й у своїх методах зберігання.

Якщо говорити про передачу конфіденційної інформації в звуках і мові, то оцінки допустимих значень швидкості передачі конфіденційної інформації в аудіосигналах показали, що на сьогодні ці значення не перевищують 100 біт/с. Це максимальні значення, яких можна досягти різними методами приховування секретної інформації в мовних або акустичних сигналах за допомогою відповідної обробки графічних зображень їх динамічних спектрограм. Однак можна припустити, що таких швидкостей, ймовірно, буде достатньо для оперативної передачі важливих конфіденційних повідомлень у процесі мовного спілкування між двома абонентами по телефонній лінії або за допомогою прийому та передачі звукових сигналів, що містить звукові сигнали - " контейнери» з інформаційною закладкою, а також інші програми. Фактично, на таких швидкостях можна приховано передати близько трьох сторінок тексту і близько десяти чорно-білих фотографій за одну хвилину голосового сигналу під час телефонних розмов.

Як видно з проведеного аналізу, для прихованої передачі конфіденційної інформації вже використовується широкий спектр різних типів «контейнерів». Але в той же час не виключена поява нових методів прихованої передачі секретної інформації через появу інших «контейнерів», і в результаті інформаційна ефективність комп’ютерних систем передачі прихованої інформації була застосована до методи технічних стандартів. можна значно збільшити.

Виходячи з вищевикладеного, можна вважати, що в перспективі одним із перспективних напрямів захисту мовних повідомлень у каналах зв’язку є розгляд створення та розвитку комп’ютеризованих систем приховування мовних сигналів поруч або при їх спільному використанні з традиційні технології. для семантичного захисту мовних повідомлень, а саме шифрування мовних сигналів на основі криптографічних алгоритмів.

Вибір способів і конкретних способів захисту мови, як одного з видів семантичного захисту мовних повідомлень, залежатиме від практичних вимог до системи захисту мови та від технічних характеристик каналу передачі мовної інформації.

1. 5 Постановка проблеми дослідження

Можна виділити дві причини нинішньої популярності досліджень у галузі стеганофонії: обмеження на використання засобів шифрування в деяких країнах світу та поява проблеми захисту прав власності на інформацію, розміщену в цифровому вигляді. форми. Перша причина зумовила велику кількість досліджень у дусі класичної стеганографії (тобто приховування факту передачі інформації), друга – ще більшу кількість робіт у галузі так званих цифрових візуалізацій (DWA), спец. етикетка, непомітно вставлена на зображення або інший знак для контролю або іншим чином регулює його використання.

В останні роки для широкого розповсюдження мережевих методів передачі мультимедійної інформації, зокрема, потоків трафіку та голосового відео, актуальною є побудова на їх основі потокових стегосистем. Однак реалізація стегосистем з використанням модифікованих методів, наприклад, найменш значущих фрагментів початкових мультимедійних даних, обмежена тим фактом, що майже всі потоки цих даних передаються з використанням того чи іншого методу стиснення, який часто встановлюється. на психофізіологічній моделі людського сприйняття. Зокрема, якщо розглядати оцифровану мову як одне з найпоширеніших джерел мультимедійного трафіку, то в залежності від сфери застосування використовується один із варіантів диференціальної модифікації або специфічне мовне кодування. У цьому випадку використання методів стеганографії NZB є досить неефективним, а особливого значення набувають методи стеганографії, які дозволяють вбудовувати повідомлення в значні перцептивні поля, які не піддаються значним спотворенням при обробці сучасними кодеками.

Принципи побудови стеганофонічних алгоритмів показують, що сьогодні розроблено багато методів приховування повідомлень у звукових сигналах. Зокрема, в одній класичній стеганографії розроблено багато методів роботи з аудіофайлами. У зв'язку з цим , враховуючи стрімкий розвиток IP-

телефонії, комп'ютерної телефонії, мультимедійних конференцій та інших галузей, де аудіосигнал є основним видом даних для передачі, постає питання підвищення стабільності та ефективності стеганофонічних систем.

Аналіз літератури показує, що багато проблем стеганофонії ще знаходяться на початковій стадії свого вирішення. Тому актуальним є наукове завдання розробки методів і способів приховування даних у трафіку IP-телефонії для підвищення стабільності та ефективності стеганофонічних систем реального часу.

Вирішення цього завдання підвищить ефективність і безпеку прихованої передачі даних по каналах зв'язку.

Для досягнення поставленої мети необхідно вирішити наступні взаємопов’язані задачі:

1) Дослідити передачу мовних сигналів у мережах з комутацією пакетів.

2) Проаналізувати існуючі підходи до захисту даних для IP-телефонії.

3) Проаналізувати можливості прихованої передачі мовних сигналів.

4) Дослідити особливості розвитку стеганофонічних систем, проаналізувати основні програмно-технічні прийоми їх побудови.

5) Розробити модель стегосистеми ІЧ-телефонії.

6) Розробити програмне забезпечення для стеганофонічного захисту даних у трафіку IP-телефонії.

7) Апробувати розроблені методики та прийоми, з’ясувати можливість їх застосування на практиці.

2. МЕТОДИ ТА СПОСОБИ ЗАСТОСУВАННЯ ДАНИХ ДО СТЕГАНОФОНІЧНИХ ДЖЕРЕЛ

2.1 Структура стеганофонічних систем

Аналіз протоколів TCP/IP, таких як , IP, UDP, TCP, показав, що є пакети, які не використовуються або є допоміжними. Це дає нам багато можливостей, щоб приховані дані можна було приховати та передати без втрати розміру самого повідомлення. IP-заголовок має поля, доступні для використання як прихованих маршрутів. Цей метод стеганографії відіграє важливу роль для зв'язку VoIP, оскільки вищезгадані протоколи присутні в кожному пакеті. Завдання вбудовування повідомлень і вилучення їх з іншої інформації виконує стегосистема. Опишемо процес реалізації прихованої інформації, представивши стегосистему як комунікаційну систему з додатковою передачею інформації (рис. 2.1). Для цього потрібно поєднати дві фази VoIP-дзвінків: комутацію викликів (маршрутизацію) і передачу даних (кодований голос). Передача виклику здійснюється шляхом передачі сигнальних повідомлень, і цей процес називається сигналізацією. Цей процес включає одночасну перевірку автентичності та цілісності звукового сигналу та передачі повідомлення.

Рис. 2.1. Схема стегосистеми як системи передачі зв'язку з додатковою інформацією

Стегосистема виконує завдання вбудовування та вилучення повідомлень з іншої інформації, яка має такі основні особливості:

- прекодер - пристрій, призначений для перетворення прихованого повідомлення у форму, зручну для вбудовування в контейнер сигналу. (Контейнер - це послідовність інформації, що містить приховане повідомлення);
- стегокодер - пристрій, призначений для вбудовування прихованого повідомлення в інші дані з урахуванням його моделі;
- вбудований пристрій розподілу повідомлень;
- стегодетектор - пристрій, призначений для визначення наявності стегоповідомлення;
- декодер - це пристрій, який отримує приховане повідомлення.

Будь-яка стегосистема повинна відповідати наступним вимогам:

1. Властивості контейнера повинні бути змінені таким чином, щоб жодних змін не можна було виявити при візуальному огляді. Ця вимога визначає якість приховування повідомлення: для того, щоб стегоповідомлення безперешкодно передавалося по каналах зв'язку, воно жодним чином не повинно привертати увагу зловмисника.
2. Stegomessage має бути стійким до будь-яких модифікацій, у тому числі зловмисних. У процесі передачі повідомлення може зазнавати різноманітних перетворень: зменшуватися чи збільшуватися тощо. Крім того, його можна стискати, в тому числі з використанням алгоритмів стиснення з втратами.
3. Щоб зберегти цілісність вбудованого повідомлення, необхідно використовувати код з виправленням помилок.
4. Щоб підвищити надійність, вбудоване повідомлення слід тиражувати.

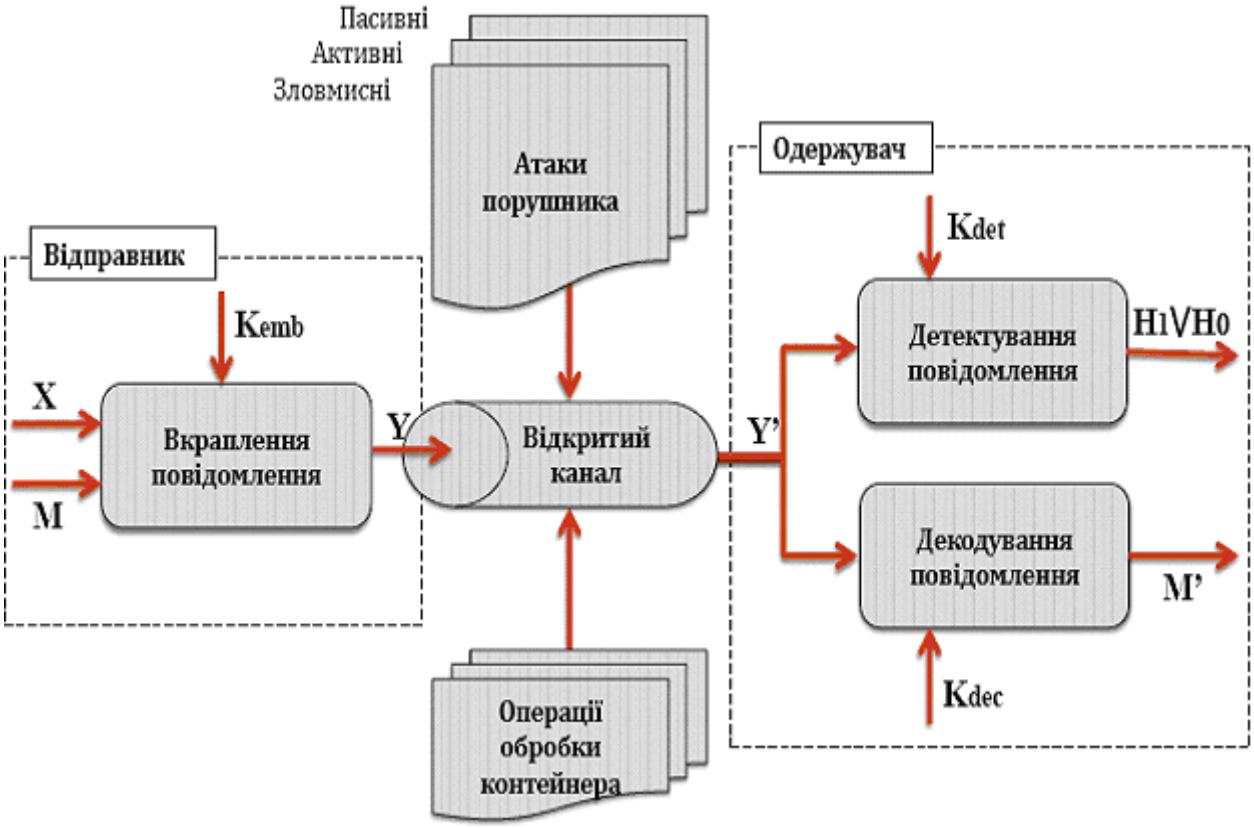

Рис. 2.2. Узагальнена модель функціонування стегосистеми

Рис. 2.3. Узагальнена модель кодів стиснення з втратами звукових сигналів

5. Виходячи зі структури стегосистеми, виникає питання, які методи застосовувати в процесі прихованої передачі мовних сигналів. 2.4 наведена узагальнена структура методів маскування мовного сигналу.

6.

Малюнок 2.4. Загальна класифікація методів маскування мовного сигналу

2.2 Методи стеганографії та критерії їх оцінки

Надсилання зашифрованих даних часто привертає додаткову увагу зловмисників. Тому для передачі важливих даних іноді використовують стеганографічні методи (рис. 2.5). Секретна інформація вкладається в контейнер шляхом відкритої передачі контейнера одержувачу (наприклад, шляхом відправки поштою або розміщення в Інтернеті). У цьому випадку потенційного зловмисника «дурять», приховуючи справжнє повідомлення. Розмір конфіденційної інформації може істотно відрізнятися (від кількох байт до кількох мегабайт). Основна вимога – конфіденційність (невидимість) прихованої інформації.

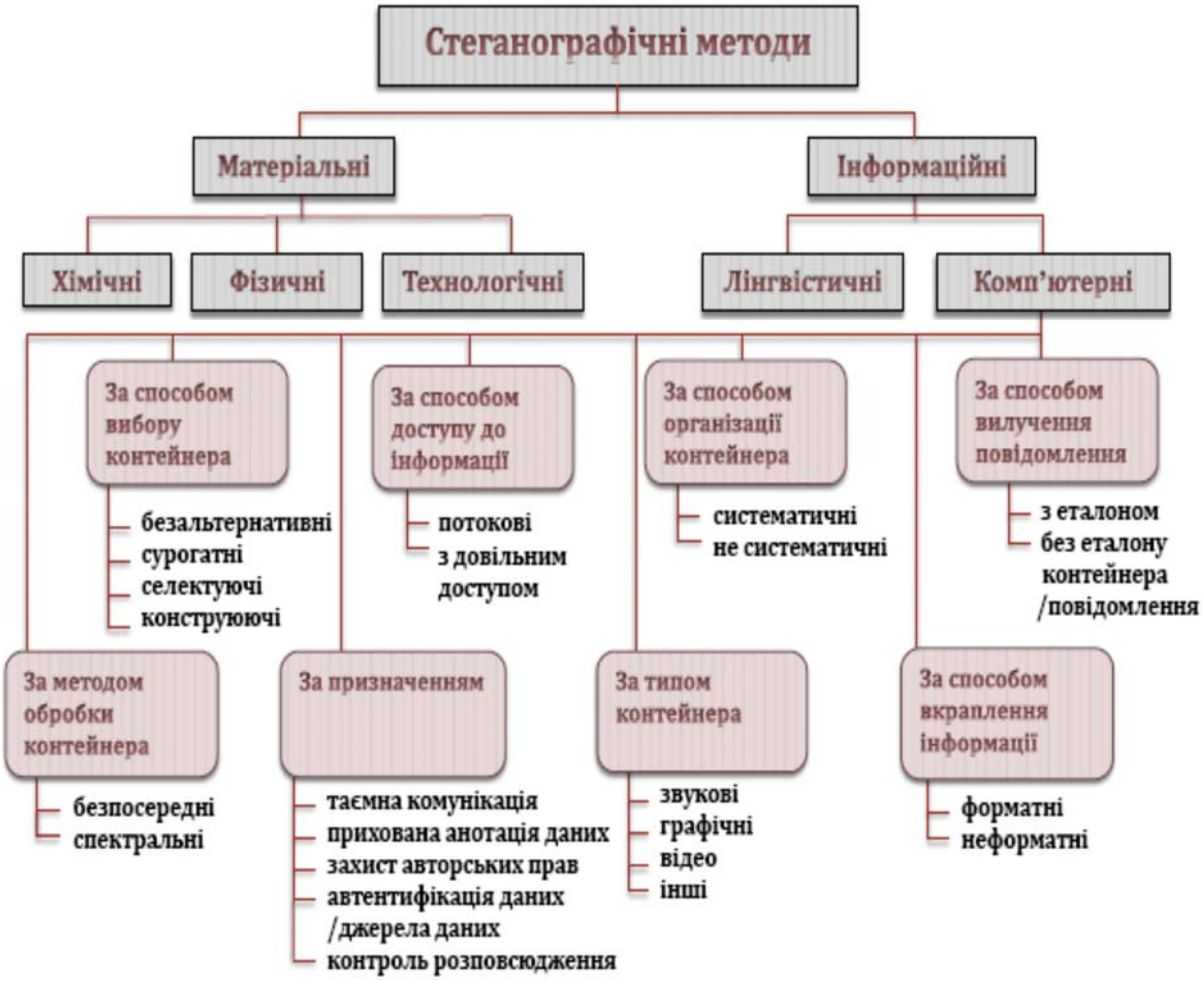

Рис. 2.5. Стеганографічні методи захисту

ЦВЗ використовується для захисту інтелектуальної власності тари (Intellectual Власність). ЦВЗ - це, як правило, невеликий обсяг інформації (наприклад, ім'я автора, товарний знак, дата видання, цифровий ідентифікатор об'єкта (Цифровий Об'єкт Ідентифікатор) тощо), який вбудовано в контейнер і може бути виявлений згодом, зокрема для підтвердження авторизації у разі несанкціонованого копіювання. CVS також можна використовувати для виявлення потенційних піратів [9]: під час розпродажів інформація про продавця та інформація про покупця вбудовуються в зображення. Головною відмінністю ЦВЗ від звичайного приховування інформації є наявність активного противника [8]. Наприклад, при використанні CDW для захисту авторських прав активний противник намагатиметься видалити або змінити

вбудовані CDW. Тому головною вимогою є стійкість вбудованих даних до атак. Секретність менш важлива, ніж таємне спілкування.

Feature Tagging (тегування). Іноді дані не вбудовуються, щоб приховати інформацію, для зручності - щоб контейнер містив корисну інформацію про його вміст: назву, опис тощо. Наприклад, імена людей на фотографії або місце, де була зроблена фотографія, можуть бути вбудовані в растрове зображення. Звичайно, при копіюванні такого файлу зображення вся ця інформація також буде скопійована. Ключові слова пошуку можуть бути вбудовані в базу даних зображень. Якщо зображення є відеокадром, для синхронізації зі звуком можна використовувати вбудовані мітки часу. Ви можете вбудувати кількість переглядів у зображення та використовувати його в додатку « оплата за перегляд » [9] .

Оцінка інструментів стеганографії є комплексною і складається з оцінок за різними критеріями (ці критерії також можна використовувати для класифікації інструментів стеганографії). Ми розділимо критерії стеганогафічних інструментів на три групи: критерії оцінки, пов’язані з: а) контейнерами; б) ті, хто обвинувачується; в) алгоритм стеганографії.

Розглянемо критерії для контейнерів. Типи контейнерів, які підтримує інструмент (зазвичай це файли певного типу, наприклад, зображення bmp, audio trZ, відео avi).

Композитний контейнер - два або більше окремих файлів, включаючи різні формати. Здатність стеганографічного інструменту використовувати контейнер стека дозволяє приховати велику кількість стегоданих. Крім того, при використанні композитного контейнера підвищується конфіденційність, оскільки частини композитного контейнера можуть передаватися різними каналами, тому, якщо одна з цих частин досягне зловмисника, він не зможе отримати секретне повідомлення через відсутність . інших частин.

Критерії, що стосуються наступного:

- типи метаданих (файли певного типу, текст);

- складені метадані (можливість приховування двох або більше окремих файлів, у тому числі різних форматів);
- stegan data compression (стиск даних перед маскуванням); шифрування метаданих (перед приховуванням);
- використовувати хеш-суму; Наявність хеш-суми збережених даних дозволяє перевірити їх цілісність після майнінгу.

Розглянемо критерії стеганографічного алгоритму (спосіб вбудовування секретних даних у контейнер).

Міцність — стійкість стеганографічного контейнера до зовнішньої обробки [2,3] (тобто до збереження стегоданих після модифікації стегоконтейнера). Цей критерій є вирішальним для захисту автора, який використовує CWZ, оскільки зловмисники намагатимуться знищити вбудований CWZ, виконуючи певне перетворення на контейнері [9].

Конфіденційність [2, 3] - стійкість до виявлення стегоданих та їх вилучення зі стегоконтейнера. Цей критерій є вирішальним для прихованої комунікації. Давайте розберемо критерій конфіденційності:

- стійкість до виявлення факту стегодатів - залежить від того, чи змінюються певні характеристики контейнера після того, як стегодаті в нього вбудовані:

- властивості контейнера (наприклад, розмір);

- аудіовізуальні характеристики контейнера (після вбудовування стегодатів можлива втрата якості зображення, збільшення кількості шумів тощо);

- структуру, основні особливості та статистичні характеристики контейнера (зміни цих характеристик часто неочевидні, але їх можна виявити, аналізуючи стегаконтейнер за допомогою спеціальних інструментів);

- проти отримання метаданих:

- шифрування стегоданих (під час попереднього шифрування даних, якщо зловмиснику вдасться отримати стегодані, він не зможе їх розшифрувати, оскільки у нього немає секретного ключа);

- наскільки складним є розподіл метаданих у контейнері.

Ємність - максимальний обсяг інформації, який може бути вкладений в контейнер заданого розміру. Як правило, місткість контейнера визначається з урахуванням конфіденційності та обмежень надійності. У [8] розглядаються два альтернативних визначення поняття стеганографічної ємності.

Зауважимо, що залежно від шкали оцінки бувають: а) бінарними (оцінюються значеннями «так» і «ні», залежно від того, чи є мета критерію притаманною стеганографічним методам чи була ... ні); б) градуйований (оцінка може отримувати певне числове значення в певному діапазоні).

Бінарні оцінки виконуються за критеріями, пов'язаними з контейнерами та стегоданими, алгоритм здебільшого покроковий. Створення єдиної градуйованої шкали для оцінки цих критеріїв виходить за рамки цієї роботи.

Розглянемо алгоритми стеганографії, класифіковані відповідно до контейнерів, для яких ці алгоритми використовуються.

Растрова графіка без палітри. LSB (Least Significant Bit) - суть методу полягає в заміні останніх значущих бітів в контейнері на біти прихованої інформації. Наприклад, розглянемо 24-розрядне растрове зображення як контейнер. Кожен піксель відповідає трьом мірам (значенням трьох компонентів кольору - червоного, зеленого і синього). Приховані дані можна записати в останній біт кожного байта (тобто один піксель зображення міститиме три біти прихованих даних). Різниця між порожньою тарою і наповненою буде візуально непомітною.

Стеганографічне зображення, отримане в результаті роботи алгоритму LSB, дуже чутливе до будь-яких модифікацій (тобто низький рівень стійкості). Мінімальна обробка цього зображення призведе до втрати вбудованої інформації.

Інформація, прихована алгоритмом LSB, може бути виявлена за рахунок виявлення аномальних характеристик розподілу значень наймолодших бітів цифрового сигналу [8], але деякі модифікації алгоритму LSB не змінюють ці характеристики. , відповідно поширювати конфіденційні дані.

Розглянемо підтипи LSB-алгоритмів для безпалітрових растрових зображень [4].

BlindHide (прихована штора). Найпростіший алгоритм: дані записуються, починаючи з лівого верхнього кута зображення до правого нижнього кута - попіксель. Програма записує приховані деталі в наймолодших бітах кольорів пікселів. Приховані дані нерівномірно розподілені в контейнері. Якщо приховані дані не заповнюють контейнер повністю, буде обрізана лише верхня частина зображення.

HideSeek (сховати — знайти). Цей алгоритм псевдовипадково розподіляє приховане повідомлення в контейнері. Він використовує пароль для створення випадкової послідовності. Трохи «розумніший» алгоритм, але все одно не враховує особливості зображення контейнера.

FilterFirst (попередній фільтр). Він виконує контейнерну фільтрацію зображень – пошук пікселів, куди буде записана прихована інформація (причому зміна наймолодших цифр найменш помітна людському оку).

BattleSteg (стеганографія морського бою). Найскладніший і просунутий алгоритм. Спочатку він фільтрує зображення контейнера, а потім записує приховану інформацію в «найкращі місця» контейнера псевдовипадковим способом (подібно до HideSeek).

Растрова графіка з палітрою. LSB. Існують певні труднощі у використанні цього алгоритму для зображень із палітрою (наприклад, GIF). Кожен піксель записується з індексом, який представляє певний колір палітри (таблиці, де записані всі кольори зображення). Навіть зміна значення наймолодшого біта цього індексу може призвести до радикальної зміни кольору пікселя. Щоб мінімізувати цей побічний ефект, палітра попередньо відсортована так, щоб різниця кольорів між сусідніми кольорами (за індексами) була мінімальною [8].

Аудіофайли LSB. Принцип дії цього методу для аудіофайлів аналогічний принципу для растрових зображень. Для аудіофайлів молодші біти кожного зразка аудіо використовуються для запису інформації про

інверсію. Полярність. У більшості мов потік повітря, який створюється під час звуковидобування, є односпрямованим. Це створює безперервну полярність мовних коливань. Слухова система людини не здатна розрізняти мовні сигнали позитивної та негативної полярності. Цей факт використовується в цьому методі.

Звуковий сигнал ділиться на сегменти (зазвичай це склади мовного сигналу), і кожному сегменту надається одна інформація. Значення біта задається зміною полярності елемента [11].

Echo Hiding (ехо-приховування). Цей метод приховує дані, додаючи відлуння до звукового сигналу. Параметри відлуння включають: початкову амплітуду, час загасання та переходу (час затримки між вихідним сигналом та його відлунням) (рис. 2). Коли зсув зменшується, два сигнали змішуються і луна перестає бути помітною для людини, як правило, якщо відстань між ними близько 1 мс [10].

Звуковий сигнал ділиться на сегменти, кожному з яких присвоюється біт. Потім параметри відлуння змінюються для кожного сегмента. Використовуються дві затримки: одна для кодування нуля, друга для кодування одиниці.

Phase Coding (фазове кодування) - вбудовування інформації в фазу сигналу. У цьому методі фаза початкового сегмента звукового сигналу модулюється в залежності від вхідних даних. Фази наступних елементів узгоджуються, щоб зберегти різницю фаз. Це необхідно, тому що людське вухо дуже чутливе до різниці фаз.

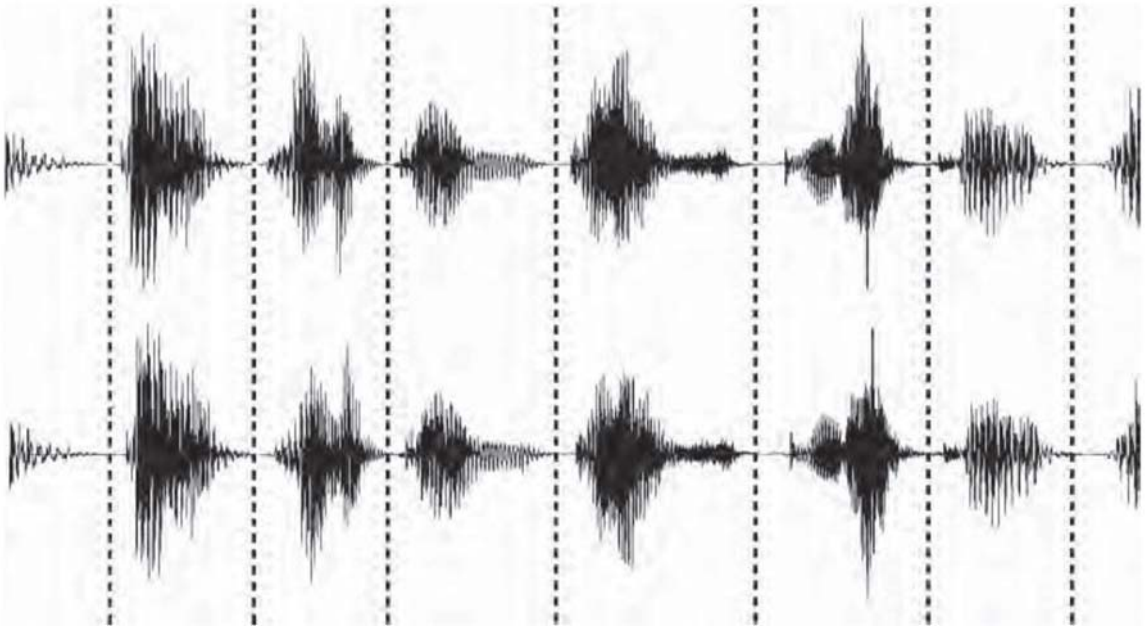

Рис. 2.6. Звуковий сигнал до (вгорі) і після (внизу) з використанням алгоритму інверсії полярності. Сегменти звукового сигналу розділені пунктирними лініями

Фазове кодування є одним із найефективніших методів кодування за критерієм відношення сигнал/шум. Основним недоліком можна вважати низьку пропускну здатність [10].

Маскування ставлення. Ефект маскування - це коли слабке, але відчутне звукове коливання стає меншим за наявності іншого, більш гучного (прихований сигнал). Ефект маскування залежить від спектральних і часових характеристик маскуючого сигналу і маскуючого сигналу [10].

Розширений спектр (SS, розширений спектр). Відповідно до методу розширення спектру, приховану інформацію намагаються максимально «розпорошити» по частотному спектру звукового сигналу. Це аналогічно системам, які використовують реалізацію LSB, яка випадковим чином розподіляє біти вхідних даних по всьому спектру. Однак, на відміну від кодування LSB, метод SS передає секретне повідомлення через частотний спектр аудіофайлу за допомогою коду, який не залежить від аудіосигналу. В

результаті кінцевий сигнал має більшу пропускну здатність, ніж насправді потрібна для передачі [13].

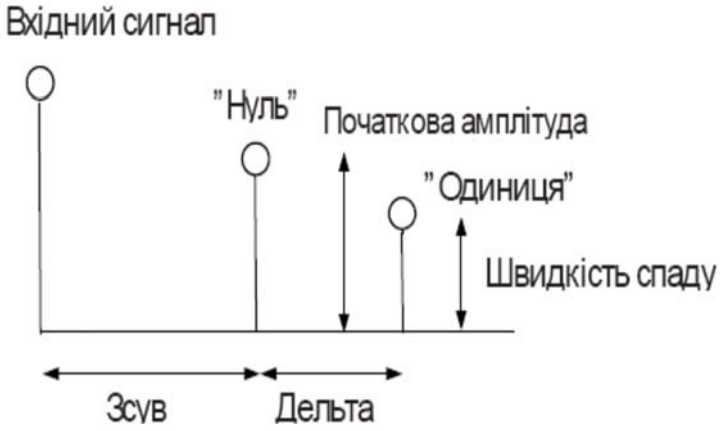

Рисунок 2.7 – Параметри ехо-сигналу

Insert Tone (вставити тон). Метод тональної вставки заснований на поганій чутності та непостійності низьких тонів за наявності компонентів значно більшого спектру.

Розглянемо приклад, коли вводяться два низькочастотні тони. Звуковий сигнал розбивається на сегменти. Для кожного сегмента розраховується його потужність f_e. Два тони різних частот додаються f_0 до кожного сегменту f_1, але з різною потужністю. Якщо необхідно записати нуль, то ступінь f_0 встановлюється 0,25 f_e, а ступінь f_1 0,001 f_0. Якщо 1, то f_1 потужність встановлюється на 0,25 f_e, а потужність f_0 на 0,001 f_1 [12]

Дискретне косинусне перетворення (DCP). Цей метод змінює коефіцієнти дискретного косинусного перетворення. Дискретно-косинусне перетворення використовується для алгоритму стиснення JPEG для перетворення блоків 8 х 8 пікселів зображення в 64 коефіцієнти DCP [14].

Один із стегоалгоритмів використовує таку функцію. Стиснуті дані зберігаються як цілі числа, але всі обчислення виконуються з числами з плаваючою комою, а потім округлюються. Помилки округлення визначають

величину втрат при стисненні. Цей алгоритм використовує рівні округлення, щоб приховати інформацію [15].

Неформатований текст [5]. Маніпуляція пробілами між словами. Різна кількість пробілів між словами може приховувати інформацію. Наприклад, нулю відповідає один пробіл, один — два.

Додавання місць відстеження. У кінці кожного речення або абзацу додається певна кількість пробілів. Наприклад, нуль пробілів у кінці речення відповідає бітовій послідовності 000, сім пробілів -111.

Змініть порядок маркерів кінця рядка. Через байдужість більшості текстових редакторів до порядку, в якому символи переходу рядка (CR) і зворотної адреси (LF) йдуть один за одним, цю пару можна використовувати для представлення однієї інформації: CR/LF може відповідати нуль, CR/LF до одиниці.

Замінити символами іншого алфавіту. Цей метод передбачає або заміну кириличного символу ідентичним латинським символом (бітове значення дорівнює нулю), або відхилення такої заміни (бітове значення дорівнює одиниці).

Морфолого-синтаксичний метод [6,7]. Послідовність речень розглядається як послідовність бітів. Функція, яка визначає, чи відповідає речення нулю чи одиниці, може бути дуже різноманітною. Наприклад, активне чи пасивне речення; чи є в реченні два іменники; чи дорівнює останній біт хеш-виразу нулю чи одиниці тощо. Метод складний у реалізації через особливості вбудовування прихованої інформації: на основі прихованої інформації створюється контейнер (можливо шляхом переформулювання речень контейнера, збереження його семантики). Особлива відмінність методу полягає в тому, що при конвертації контейнера з одного формату в інший прихована інформація зберігається навіть при друку на папері. Наприклад, інформація буде вбудована в зображення, доки зображення знаходиться в цифровій формі.

Форматування текстових символів розглядається як послідовність бітів. Форматування, яке відповідає нулю, візуально дуже близьке до форматування, яке відповідає одиниці (різниця непомітна неозброєним оком). Наприклад, нуль відповідає розміру символу 14 контактів, одиниці – 14,5 контактів, або нуль – RGB(0, 0, 0), одиниці – RGB(0, 0, 1).

Файли, що містять конфіденційні дані, стискаються та додаються в кінець стисненого файлу, щоб ці файли були «невидимими» для звичайних архіваторів. Цей метод використовує нестандартний алгоритм для створення стислих файлів і може (з відповідними змінами) також застосовуватися до інших типів файлів-контейнерів.

2.3 Аналіз прихованого програмного забезпечення Stego

У таблиці 2.1 наведено результати практичного аналізу програмного забезпечення stego.

Індикатором якості стеганографічного інструменту (і методу, відповідно), який впливає на конфіденційність, є характер шуму, який спостерігається в стегоконтейнері після приховування в ньому даних. Всі шуми можна розділити на три групи: лінійні шуми (шум присутній тільки в тій частині контейнера, де записані приховані дані; приховані дані записуються у відповідні біти контейнера, починаючи з його початку); рівномірний шум (приховані дані рівномірно розподіляються по контейнеру); контент-залежний шум (приховані дані розподіляються в контейнері таким чином, що генерований шум мінімально впливає на зміну вмісту контейнера, який сприймається людиною, тобто його аудіовізуальних характеристик).

аудіовізуальні характеристики файлів-контейнерів взагалі під час приховування даних. Так, наприклад, програма Max File Encryption певним чином приховує дані до кінця файлу-контейнера. Програма SteganoZip використовує аналогічний метод для приховування даних в архівних zip-файлах. Недоліком цього методу є те, що він змінює властивості контейнера,

тому дані, приховані таким чином, можна легко виявити шляхом аналізу розміру, структури та вмісту контейнерів.

GifShuffle використовує інший метод, який не змінює виявлений вміст контейнера, щоб приховати дані в контейнерах gif. Суть цього методу полягає в перетасуванні палітри gif-файлу для шифрування прихованих даних. Недоліком є те, що таким чином можна приховати лише невелике текстове повідомлення. Це пов’язано з розміром палітри файлів gif. Цей метод має низьку надійність для виявлення стегоданих, оскільки він змінює структуру палітри gif-файлу.

Програма Puff найкраща з точки зору практичності. Він підтримує більшість форматів даних серед інших програм (зокрема, стислі растрові та аудіоформати). Програма може використовувати стековий контейнер, що дозволяє приховати великі обсяги даних. Ви можете приховати будь-які файли або папки, і кілька одночасно. Програма архівує та шифрує приховані дані. Програма має високу продуктивність навіть при великих обсягах даних.

Програма Digital Invisible Ink Tools, завдяки можливості імітації приховування даних, показує та дозволяє візуально оцінити ефективність різних методів стеганографії. Цю програму можна використовувати для вивчення та дослідження методів стеганографії.

Програма Hiding Glyph приховує дані в контейнері 24-розрядного формату bmp за допомогою спеціального методу: ключем до пошуку прихованих даних є вихідний файл контейнера. Програма забезпечує високу місткість контейнера: співвідношення між кількістю прихованих даних і об'ємом контейнера може досягати 1:3 (хоча більшість методів не дають більше 1:8), і це візуальні характеристики зображення. виправлено - шум непомітний неозброєним оком.

Таблиця 2.1 – Аналіз програмних засобів стегосистем

		Стеганос Файл	USC Стего відео	СтегоМагі с	wbStego 4	Стего	SteganoWav	SteganoZip	NetToolsSTEG	прихований Гліф	СтеганоГ	макс	Digital Invisible	затяжка	GifShuffle	Таємничий склеп
Комерційний/Безкоштовни		З	Ф	Ф	Ф	Ф	Ф	Ф	Ф	Ф	Ф	З	Ф	Ф	Ф	Ф
	вікна	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Linux				x	x							x			
Інтерфейс: Win/Console		В	В	В	В	В	В	В	В	З	В	В	В	В	З	В
Тип файлу-контейнера	bmp	x		x	x	x				x	x		x	x		x
	jpeg	x												x		
	gif														x	
	wav	x		x			x							x		x
	mp3													x		
	avi		x													
	текст			X	X											
	html				x											
	rtf								x							
	pdf				x											
	zip							x								
	Будь-який файл											x				
	Композитний													x		x
	Деякі окремо					x										
Сотня	Тільки txt		X													
	текст			x			x		x						x	
	Будь-який файл	x		x	x	x		x		x	x	x	x	x		x
	Папка	x								x						
	Повернувся	x						x				x		x		x
	ЦВЗ				x									x		
стиснення						x		x						x		
Шифрування				x	x	x		x	x		x	x		x	x	x
Захист паролем		x	x	x	x	x		x	x		x	x		x	x	x
Атрибути зберігаються*		X				X		X		X	X	X		X		X

РОЗДІЛ 3. СТЕГО МОДЕЛЬ ДЛЯ IP-ТЕЛЕФОНІЇ

3.1 Характеристики, пов'язані з побудовою та роботою стегосистем в мережах IP- телефонії

При побудові стегосистеми IP-телефонії слід враховувати наступні положення:

1) Потенційний супротивник має повну інформацію про стеганофонічні системи та деталі їх реалізації. Єдина інформація, яка залишається невідомою ворогу, - це ключ, за допомогою якого його власник може встановити наявність прихованого повідомлення та його зміст.

2) Якщо зловмисник якимось чином дізнається про існування прихованого повідомлення, він не повинен дозволяти йому витягувати подібні повідомлення з інших контейнерів, якщо ключ зберігається в секреті (захищений криптографією).

Крім того, стегосистема повинна відповідати певним вимогам:

1) властивості контейнера повинні бути модифіковані таким чином, щоб стегоконтейнер безперешкодно проходив через канал зв'язку, незалежно від потенційних ускладнень будь-яким способом.

2) стегосистема повинна бути надійною. А саме: захистити від втрати, дублювання та порушення послідовності отримання контейнерів Stego, контролювати цілісність повідомлення.

Для врахування положень і відповідності вимогам, визначеним вище, необхідно сформувати послідовність блоків даних, придатних для вбудовування в контейнер (тут і далі М-блоки) з вихідного повідомлення. Кожен такий блок повинен бути зашифрований і, крім фрагмента повідомлення, містити достатню інформацію для забезпечення надійності стегосистеми. Крім того, вказаний М-блок повинен містити інформацію про розмір повідомлення, а М-блок є підтвердженням отримання стегоконтейнера. Визначимо загальну структуру блоку М та алгоритми відправлення та

отримання з контейнера тегів. Решта методів і методів буде визначено при описі стегосистеми на основі конкретного протоколу.

Загальна структура блоку M

Зміщення фрагмента вказує на те, де знаходиться фрагмент у вихідному повідомленні. Фрагмент ключа містить ключі старше k біт.

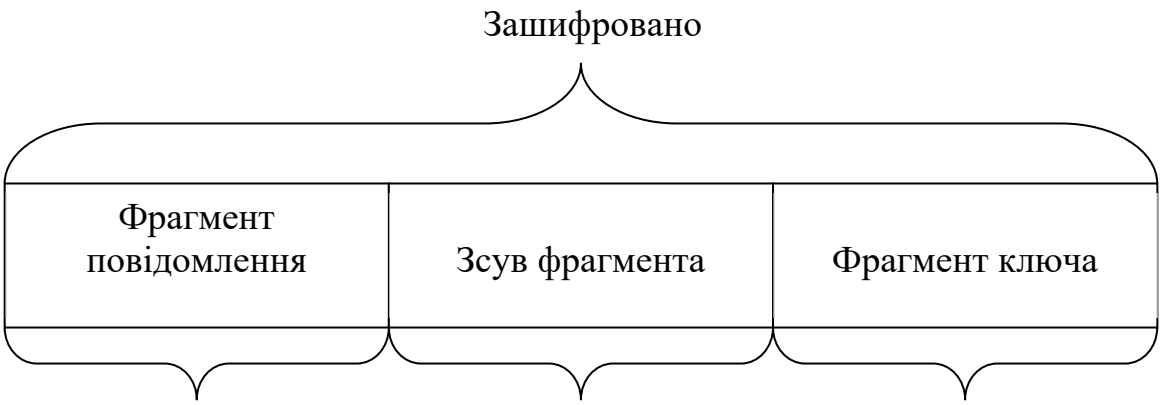

Рис. 3.1 – Загальна структура блоку M

Послідовність полів може бути довільною, і для строгого опису блочної структури M потрібно визначити тільки значення m, n і ka.

Оскільки M-блоки можуть передаватися по каналу зв’язку в будь-якому порядку, рекомендується використовувати блокчейни, які працюють у режимі електронного коду (ECB) [2]. Довжина блоку повинна відповідати довжині блоку M.

наступні кроки в процесі доставки:

1. Складіть послідовність M-блоків.

2. Візьміть блок M в контейнер.

3. Надішліть стего-контейнер адресату.

4. Зачекайте певний час від адресата, щоб підтвердити його отримання. Якщо підтвердження не надійшло, завершіть процес доставки або перейдіть до кроку 2.

5. Повторіть кроки 2-4 для кожного M-блоку послідовності формування, доки не буде досягнуто кінця цієї послідовності.

наступні кроки в процесі збереження:

1. Визначте, чи вбудовано повідомлення в отриманий контейнер. Якщо так, перейдіть до кроку 2 або зачекайте наступного контейнера.

2. Витягніть фрагмент повідомлення.

3. Підтвердьте, що стегоконтейнер знайдено.

4. Виконуйте кроки 1-3, доки не буде доведено, що було отримано все повідомлення 1.

Вилучивши крок 4 з алгоритму надсилання і крок 3 з алгоритму прийому, можна збільшити швидкість передачі повідомлення, при цьому знизивши надійність стегосистеми.

Інтернет-протокол забезпечує передачу блоків даних, які називаються дейтаграмами, від відправника до одержувача. При необхідності протокол IP також забезпечує фрагментацію і збірку дейтаграм для передачі даних по мережах з малими розмірами пакетів.

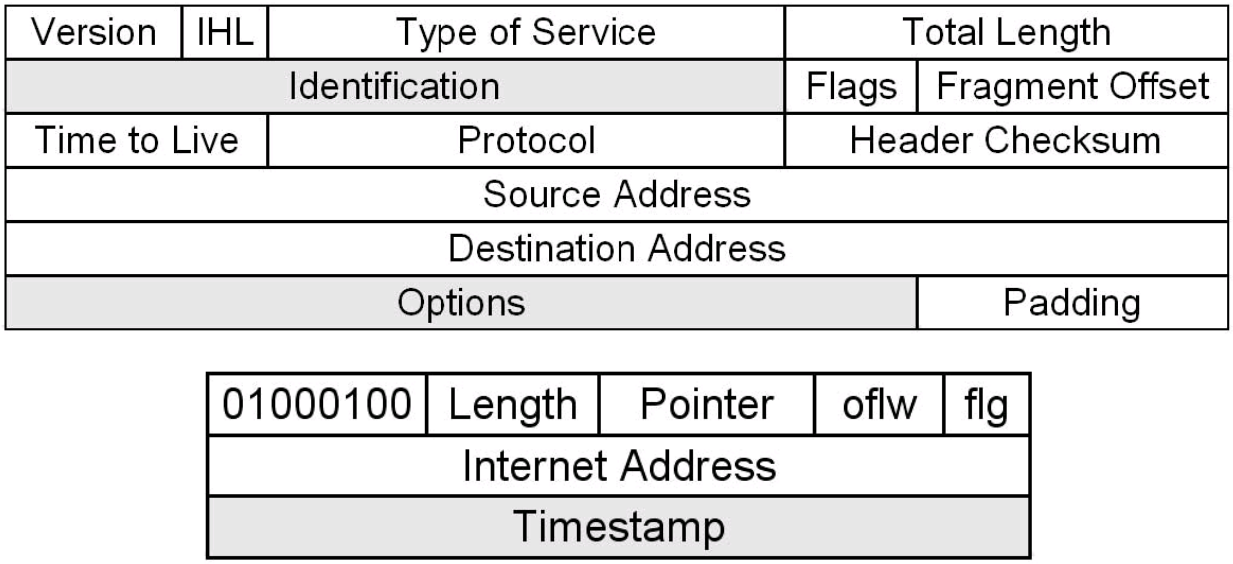

Рис. 3.2 – Структура заголовка IP-дейтаграми

Version (4 bits) - версія протоколу, в даному випадку розглядається версія 4. IHL (4 bits) - довжина заголовка Type of Service (8 bits) - тип служби, визначений за допомогою абстрактних параметрів типу служби Total Length

(16 bits) - загальна довжина дейтаграми Identifier (16 біт) - ідентифікатор, який встановлюється відправником для складання фрагментів будь-якої дейтаграми Flags (3 біти) - контрольні прапори. Fragment Offset (13 bits) - зміщення фрагмента Time to Live (8 bits) - максимальний час перебування датаграми в Інтернеті. Протокол (8 біт) - це поле показує, який протокол наступного рівня використовується з датаграмою Інтернету. Header Checker (16 bit) - засіб перевірки заголовків. Source Address (32 bits) - адреса відправника. Destination Address (32 bits) - адреса одержувача. Опції (змінна довжина) - додаткові опції.

Заповнення (змінної довжини) - заповнення, яке використовується для забезпечення того, щоб заголовок закінчувався на 32-бітній межі.

Найбільший інтерес викликають поля ідентифікатора (ID) і параметрів.

Розглянемо призначення цих ділянок докладніше. Відповідно до специфікації протоколу IP [3] ідентифікатор містить унікальний ідентифікатор пакета, який використовується для складання фрагментованих дейтаграм. Значення цього поля не залежить від значень інших полів заголовка і зберігається під час фрагментації.

Опції повинні підтримуватися всіма модулями Інтернету (хостами та шлюзами). Кожна окрема дейтаграма не обов’язково містить параметри, але все одно може їх містити. Є 8 різних варіантів, лише один з яких підходить для надсилання секретного повідомлення (перевірте специфікацію [3] для підтвердження). Це параметр позначки часу в Інтернеті. Довжина (8 біт) - кількість байтів в опції, яка включає тип, довжину, покажчик і байти oflw/flg. Покажчик (8 біт) - кількість байтів від початку цієї опції до кінця тимчасових штампів, плюс один.

Overflow (oflw, 4 біти) - кількість IP-модулів, для яких неможливо зареєструвати тимчасові штампи через брак вільного місця. Прапор (flg, 4 біти) - визначає спосіб реєстрації тимчасового штампа. Timestamp (32 bit) - мітка часу в мілісекундах. Якщо неможливо визначити час у мілісекундах , можна ввести будь-яке інше значення за умови, що найстаріший біт у полі

позначки часу має значення одиниці (що вказує на використання нестандартного значення та дає певну свободу для цього заповнення Gort).

Ми опишемо процес формування послідовності М-блоків, структуру М-блоку та процес вбудовування. Ми також визначимо М-блок, що містить інформацію про розмір повідомлення, і М-блок, який є підтвердженням отримання стегоконтейнера.

Структура М-блоку Загальна структура М-блоку визначена вище, потрібно задати лише значення змінних m, n і ka:

$m = 24 \cdot n = 16 \cdot k = 24$

Розмір повідомлення

М-блок несе інформацію про розмір повідомлення, яка містить:

- поле «фрагмент повідомлення» містить кількість блоків у сформованій послідовності (включаючи цей);

- поле «зміщення фрагмента» містить деяку випадкову послідовність бітів;

- поле "key chip" містить послідовність бітів, що відповідає рядку "siz". Формування послідовності М-блоків

1. З оригінального повідомлення створіть послідовність М-блоків, додавши блок, що містить інформацію про розмір повідомлення.

2. Визначаємо результуючу послідовність за 16-бітним алгоритмом, що дає результат, описаний у наступному прикладі.

Приклад (порядок послідовності)

Розглянемо послідовність десяткових чисел, що відповідає 16 старшим бітам М-блоків.

Послідовність виведення: 3 1 2 1 3 3 4 5 1 4 2 5 – послідовність команд: 1 2 3 4 5 1 2 3 4 5 1 3

Слід зазначити, що такий порядок призводить до того, що блок М, що містить розмір повідомлення, з’являється в довільній позиції в послідовності.

Вбудовано в поле Identity заголовка IP-дейтаграми та в опцію позначки часу в Інтернеті. При цьому необхідно враховувати наступні умови:

1) Специфікація IP-протоколу [3] вимагає, щоб ідентифікатор був унікальним протягом усього життя (Time To Live) дейтаграми. На практиці це часто реалізується шляхом збільшення значення поля ID на одиницю для кожної наступної дейтаграми.

2) Незважаючи на можливість використання нестандартної позначки часу, значення цього поля необхідно збільшувати для кожної наступної дейтаграми. Збільшення має відбуватися в певній кількості послідовних датаграм.

3) Відповідно до специфікації, відправник повинен створити параметр Internet Timestamp, щоб полів часової позначки було достатньо для розміщення всієї очікуваної інформації. Додавання тимчасових штампів не змінює розмір виділення. Якщо поле мітки часу вже заповнено, дейтаграма передається без вставки мітки часу, а лічильник переповнення збільшується на одиницю.

Розглянемо процес вбудовування докладніше. Тоді процес вилучення буде зрозумілим, і подальший опис не буде потрібен.

1. Помістіть старші 16 бітів вбудованого блоку M у поле ідентифікації заголовка IP-дейтаграми. Розташування послідовності блоків забезпечує часткове виконання першої з умов, визначених вище. Частково тому, що впорядкованість буде забезпечена, лише якщо код буде збільшено на значення більше або дорівнює одиниці для певної кількості IP-дейтаграм (кількість таких датаграм постійно або поступово зменшується)

2. У заголовку IP-дейтаграми створіть опцію Internet Time Stamp, яка містить дві позначки часу, розміщені в послідовних 32-розрядних словах (поля опцій заповнюються суворо відповідно до специфікації протоколу [3]). 48 бітів блоку M вбудовано в біти 8-31 (пронумеровані від нуля, старший біт) кожної мітки часу, старший біт встановлюється на 1, а біти 1-7 гарантують, що другі умови, визначені вище зустрічаються.

3. Щоб повністю відповідати умові, що накладається на зміну значення поля ID, разом зі стегоконтейнерами можна відправляти IP-дейтаграми, які не

містять секретного повідомлення, але гарантують, що код підняти будь-яким. Тобто для кожної наступної дейтаграми IP значення бітів 1-7 мітки часу змінюється таким чином, що результуюча 32-бітна мітка часу є більшою за мітку часу.

3. Створіть належну IP-дейтаграму, яка містить у полі «Дані» будь-які дані, які не викликають підозр щодо потенційного противника.

Підтвердженням отримання даного стего-контейнера є блок M, в якому значення полів «Message Body» і «Keyblock» збігаються зі значеннями ідентичних полів блоку M, вилученого з цього стего-контейнера, і поле " Shift Shift" більше на один. Підтвердження отримання слід надсилати з урахуванням умов, викладених у пункті «Вбудовування», бажано підтвердити, що отримано не лише один стего-контейнер, а певну їх кількість. Це число вибирається довільно і може, наприклад, відповідати кількості стегоконтейнерів, у яких збільшується значення поля ID. Загальні алгоритми надсилання та отримання повинні бути трохи змінені.

Протокол керуючих повідомлень Інтернету - Протокол керуючих повідомлень Інтернету використовує основні властивості IP так, якби це був протокол вищого рівня [4]. Однак ICMP є частиною Інтернет-протоколу.

Повідомлення ICMP зазвичай повідомляють про проблеми з обробкою датаграм і надсилаються зі стандартним IP-заголовком. Структура повідомлення залежить від його типу.

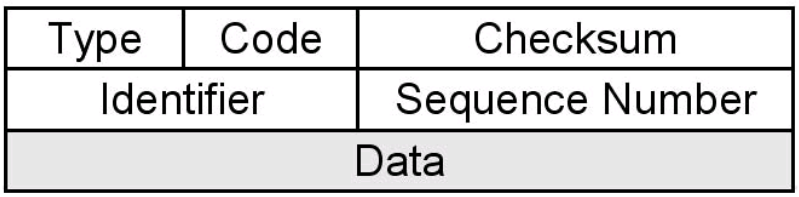

Рис. 3.3. Структура ехо-повідомлення та повідомлення-відповіді

Тип (8 біт) - тип: 8 для ехо-запиту та 0 для ехо-відповіді.

Code (8 bits) - код (впливає на заповнення полів Identifier і Sequence Number).

Checksum (16 bit) - контрольна сума. Ідентифікатор (16 біт) - ідентифікатор для співвіднесення повідомлень і відповідей на них. Sequence Number (16 біт) - службовий номер черги для кореляції повідомлень і відповідей на них.

Реквізити (змінної довжини) - додаткове інформаційне поле. Відправлений пакет складається з IP-заголовка довжиною 20 байт і, власне, ICMP-повідомлення довжиною 8 + n байт (8 байт на заголовок і n байт додаткової інформації) [5]. Зазвичай n має значення 56 (для UNIX) або 32 (для Windows). Оскільки поле додаткової інформації часто містить певні дані, корисні для налагодження, його можна використовувати для передачі секретного повідомлення.

Відповідно до специфікації протоколу ICMP [4], відповідь повинна надсилатися на всі ехо-запити. Крім того, якщо повідомлення містило додаткові дані, повідомлення повинно містити ті самі дані у відповідь на ехо. Завдання моніторингу цілісності повідомлення та підтвердження отримання стегоконтейнера вже вирішено на рівні протоколу.

Переходимо до опису стеганографічної системи, яка базується на можливості раніше відкритих дейтаграм. Виконання цієї умови повинно бути забезпечено для обох часових позначок в одній дейтаграмі, а два отриманих значення не залежать одне від одного. Звичайно, інкремент тимчасової позначки можна виконати щонайменше для 128 послідовних IP-дейтаграм.

Структура блоку M

• m = 64.

• n = k = 32 .

Загальна довжина блоку M становить 128 біт.

Розмір повідомлення

• Поле «фрагмент повідомлення» містить кількість блоків у згенерованій послідовності (включаючи цей).

• Поле «зміщення фрагмента» містить деяку випадкову послідовність бітів.

• Поле «фрагмент ключа» містить послідовність бітів, що відповідає рядку «розмір».

Формування послідовності М-блоків

Потрібно лише створити послідовність М-блоків з вихідного повідомлення, а на початку розмістити блок, що містить інформацію про розмір повідомлення. Інших обмежень щодо порядку розташування елементів цієї послідовності немає.

Додаткове інформаційне поле ICMP-повідомлення echo вбудовано. Розглянемо цей процес.

1. Створіть ехо-повідомлення ICMP, що містить додаткове інформаційне поле певної довжини. Довжина вибирається з інтервалу від 24 до 65507 байт. Однак слід враховувати, що фрагментований пакет ICMP відкрито показує, що буде передано секретне повідомлення.

2. Поставте тимчасовий штамп у верхніх 8 байтах поля додаткової інформації. Кількість байтів, що залишилися з даними, що відповідають вбудованому блоку М. При цьому, якщо довжина поля додаткової інформації перевищує мінімальну, ці дані заповнюють його циклічно.

3. Сформуйте правильну IP-дейтаграму, помістивши створене ехо-повідомлення в поле даних.

Щоб не привернути увагу потенційного ворога, кожен стего-контейнер необхідно відправляти кілька разів з певним інтервалом часу.

3.2 Спосіб приховування даних в IP- телефонії в умовах повторення підписів

Прихований мережевий канал передачі даних можна організувати на основі зміни полів IP-пакету. Основні можливості приховування даних за допомогою IP-пакетів:

- постійні дані: - ідентифікатор пакета - протокол передачі.;
- повторювані послідовності символів;

- вільний простір пакета заповнюється нульовим значенням.

Під час аналізу розподілу пакетів за довжиною було виявлено, що найбільш часто зустрічаються пакети з довжиною: 63В, 126В, 189В складають 95% від загальної кількості пакетів (рис. 3.4). Непрактично вбудовувати інформацію в пакети різної довжини.

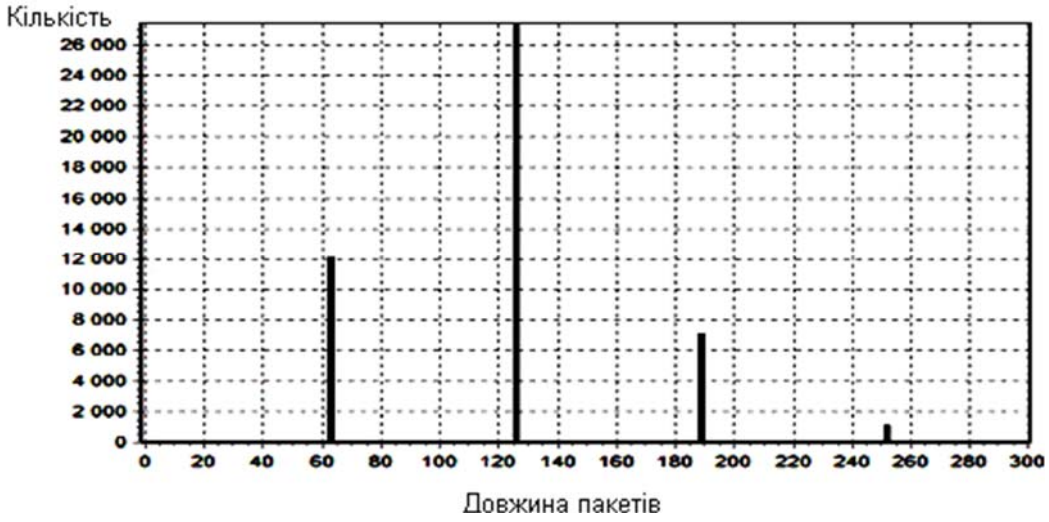

Рис. 3.4 – Аналіз розподілу довжини пакетів VoIP

На основі аналізу стандарту N.323, який забезпечить середню якість (MOS 3.5-4.0) передачі голосових сигналів, затримка не повинна перевищувати 350 мс, розроблено метод приховування даних в трафіку ІЧ-телефонії, який можна представити в наступних кроках:

1. середня затримка (*Tser)* для передачі одного пакету між абонентами А і В.

2. Середні значення затримки порівнюються зі значенням максимально допустимої затримки в мережі. Якщо *Tser < 350,* то *K= Послуга 350/T.*

3. Він визначає кількість пакетів, які можна передати від А до В без втрати якості голосового сигналу. Якщо *mod (K)>=1* , то прекодер стеганофонічної системи абонента А *mod (K) генерує* пакети, що містять секретне повідомлення в стегокодері. Кількість бітів, інкапсульованих у

пакеті, визначатиметься форматом стиснення, який використовується в ІЧ-телефонії.

4. Ми аналізуємо IP-пакети. Надходять із виділеного підключення та вибирають мережеві пакети довжиною: 63, 126, 189 В.

5. Пошук заданої послідовності символів (підписів) в IP- пакеті . Вбудовування інформації відбувається в таких випадках:

- знайти вибраний підпис в пакеті;

- наявність прихованого символу в черзі повідомлень, або пакет передається без змін.

6. IP- пакетах шляхом заміни підпису маркерами на символ секретного повідомлення.

7. Системний стегокодер абонента А позначає одне з резервних полів згенерованих пакетів, щоб стегодекодер розпізнав секретне повідомлення та передав його декодеру абонента Б.

8. Передача пакетів від абонента А до Б.

На рисунку 3.5 показано процес приховування даних методом розробки.

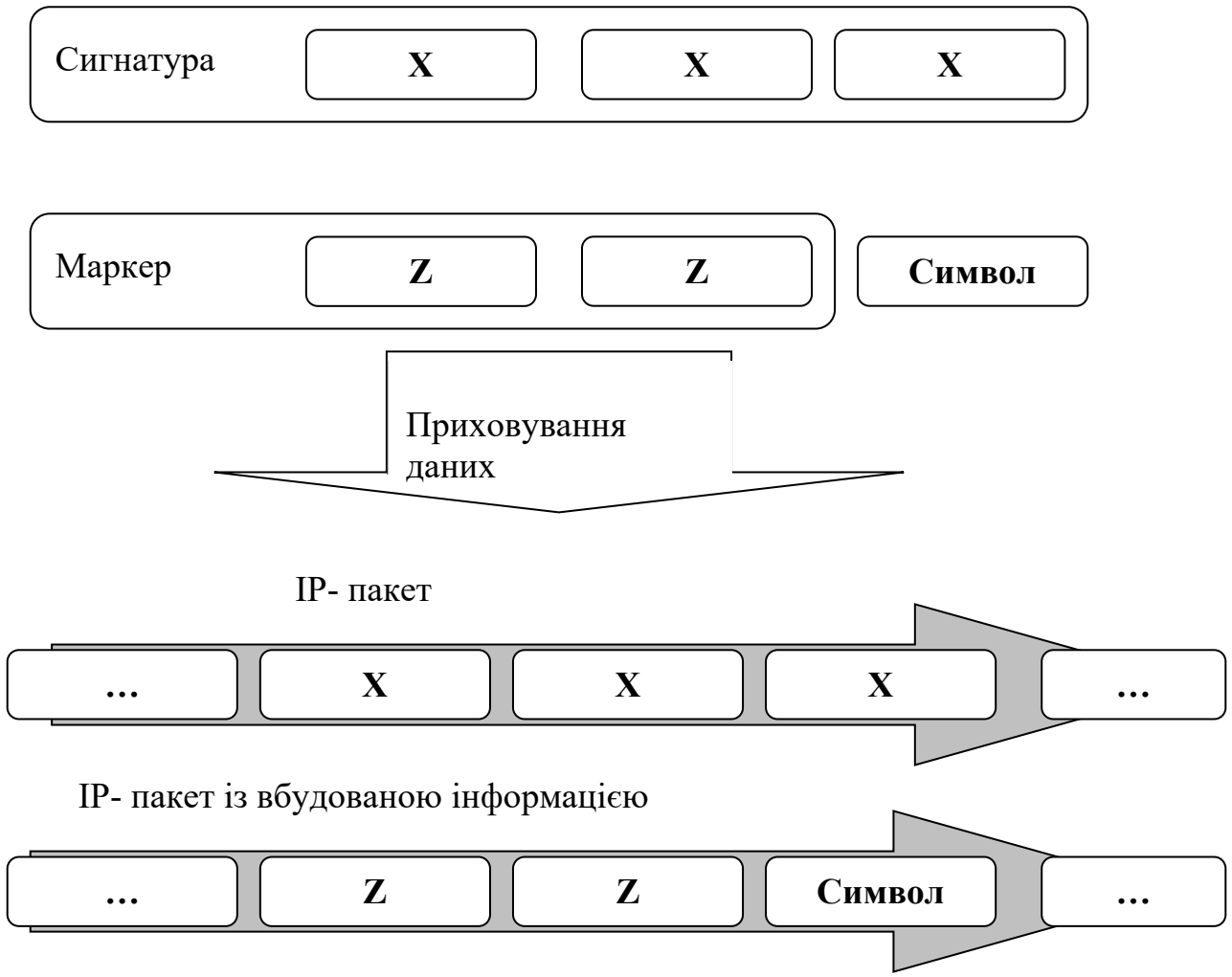

Рисунок 3.5 – Схема процесу приховування даних в IP- пакетах на основі періодичної заміни підпису

Алгоритм методу приховування даних в IP-телефонії наведено на рисунку 3.6.

Метод приховування даних на основі періодично повторюваних підписів має широкі можливості застосування в IP-телефонії, програмна реалізація та експериментальні дослідження описані в наступному розділі.

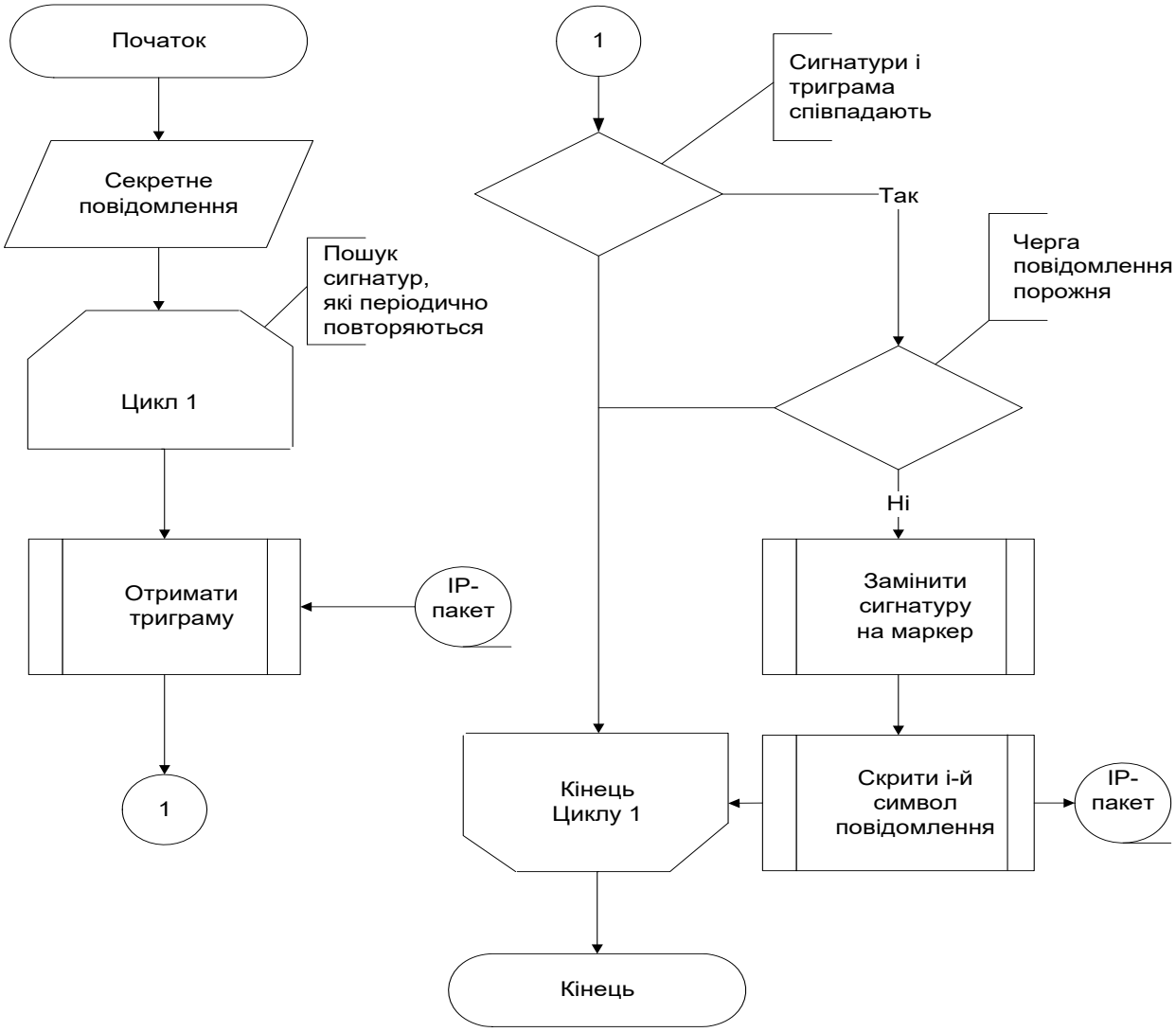

Рис. 3.6. Алгоритм приховування даних в IP-пакетах

3.3 Метод приховування даних в IP-телефонії на основі таких сигналів, як шум

Метод приховування даних на основі шумоподібних сигналів полягає у генеруванні псевдовипадкового шуму, який є функцією вбудованого повідомлення, і змішуванні отриманого шуму з основним сигналом контейнера як додатковим компонентом. В якості приймача використовується оптимальний приймач, заснований на розрахунку кореляційної функції між прогнозованим сигналом і фактично отриманим сигналом.

Пояснюємо роботу методу більш детально. Спосіб створення шумоподібних сигналів полягає в модулюванні фази тонального сигналу випадкової псевдопослідовності. У математичній інтерпретації ми отримуємо:

$$n_d(t) = sin\left(2 \cdot \pi \cdot \varpi \cdot \frac{1}{T}\right) r(t) \cdot d(t), \quad (3.1)$$

де T кількість вибірок за секунду,

ϖ - частота опорного сигналу,

$r(t)$- псевдовипадкова послідовність з мінімальною відстанню між змінами значень N_r,

$d(t)$- дані з мінімальними відстанями між змінами значень N_d.

Функції $r(t)$є копіями N та від $d(t)$набору до двійкового набору $\{-1,1\}$. Крім того, N_dпараметр повинен бути обраний таким чином, щоб дані розподілялися рівномірно по всьому сигналу контейнера. Для забезпечення завадостійкості цього методу відстань між і повинна відповідати N_rтакому співвідношенню : N_d

$$N_d > N_r \text{ в декілька разів} \quad (3.2)$$

Параметром є N_dчастота опорного сигналу ϖ і $r(t)$ключова функція цієї стегосистеми. В якості функції $r(t)$, як правило, вибирається лінійна паралельна функція, яка генерує псевдовипадкову послідовність, тому для її завдання достатньо трьох чисел.

Результуючий звуковий сигнал Його отримують шляхом змішування згенерованої послідовності далі в контейнер вихідного аудіосигналу

$$b_{m,k} = \{\hat{s}(t)\}_{t=1}^{N} \quad (3.3)$$

$$b = \{s(t)\}_{t=1}^{N} \quad (3,4)$$

$$\bar{s}(t) = s(t) + n_d(t) \quad (3,5)$$

Фільтри узгодження або кореляційні приймачі використовуються для побудови зворотної функції вилучення інформації в теорії радіозв'язку. Оскільки ці два методи є еквівалентними при цифровій реалізації, ми розглянемо кореляційний приймач у майбутньому.

Кореляційний приймач заснований на обчисленні кореляційної функції між прийнятим сигналом $\hat{s}$ і прогнозованим n_d

$$R_d = \sum_{i=1}^{N} \bar{s}_i n_d(i) \quad (3,6)$$

Оскільки задачу вилучення інформації можна представити як задачу прийому сигналу з невідомими параметрами, то для організації прийому двійкових даних необхідна наявність двох корельованих приймачів. У першому приймачі сигнал, що відповідає двійковій одиниці, вибирається n_d як прогнозований сигнал, тобто сигнал, який $n_l(i)$ взагалі i обчислюється $d(i) = 1$. У другому приймачі $n_0(i)$ вибирається сигнал, що відповідає двійковому нулю. Кореляційні функції в цьому випадку визначаються наступним чином:

$$R_0(i) = \sum_{i=N_d i}^{N_d(i+1)-1} \bar{s}_j n_0(j) \quad (3,7)$$

$$R_1(i) = \sum_{i=N_d i}^{N_d(i+1)-1} \bar{s}_j n_1(j) \quad (3,8)$$

Рішення прийняти i приховане повідомлення двійкового нуля приймається в -цій позиції if

$$R_0(i) > R_1(i) \quad (3,9)$$

інакше приймається рішення прийняти двійкову одиницю.

Якщо немає синхронізації між переданою і прийнятою послідовностями, кількість кореляційних приймачів збільшується і створюється пара кореляційних приймачів для кожної можливої зміни вихідної послідовності. В результаті складність обладнання зростає з арифметичною прогресією. Так як величини зміщення можуть досягати досить великих значень, часто намагаються знайти будь-який інший спосіб виконання умови синхронізації. В якості шумової послідовності можна використовувати видову послідовність

$$\text{k } n_d(t) > r(t)d(t) \quad (3,10)$$

Припускаючи, що передача $N_r / 3$ послідовності приймача не порушує кореляцію, засновану на кореляції між підрахунками та числами $\left[i + \frac{1}{2} N_r \right]$, де i є невід'ємним цілим числом:

$$R_d = \sum_{i=0}^{\frac{N}{N_r}} \bar{s}_{\left[\left(i+\frac{1}{2}\right)N_r\right]} n_d \left[\left(i + \frac{1}{2} \right) N_r \right] \quad (3.11)$$

До переваг методу використання шумоподібних сигналів можна віднести високу скритність і захищеність, а до недоліків – відносно низьку швидкість використання контейнерного сигналу та можливість «синхронної» атаки. Тому цей метод можна використовувати для прихованої передачі інформації по реальних каналах, навіть якщо відомо, що сигнал буде трансформуватися на шляху від відправника до одержувача, наприклад, при використанні телефонної мережі як середовища передачі.

Подальший розвиток цього методу передбачає використання відомих з психоакустики ефектів маскування частоти та часу. Шумоподібний сигнал, що містить приховане повідомлення, фільтрується за допомогою динамічного

фільтра, функція передачі якого базується на порозі частотного маскування для досягнення нечутності. Оскільки поріг частотного маскування визначається на відносно великій площі, можлива ситуація, коли на початку ділянки спостерігається тиша, а потім різке збільшення амплітуди вихідного сигналу. У цьому випадку сюжети тихі, сигнал, як і внесений шум, буде добре помітний на слух. Для запобігання цьому ефекту вводиться друга корекція на основі часового маскування, яка полягає в обчисленні контуру вихідного сигналу та подальшому накладенні цього контуру на шумоподібний відфільтрований сигнал. Результуючий контейнер аудіосигналу отримується шляхом підсумовування вихідного сигналу та шумоподібного відфільтрованого сигналу.

Інформація також витягується за допомогою кореляційного детектора. При цьому $n_d(t)$ сам шумоподібний сигнал безпосередньо вибирається як прогнозований шумоподібний сигнал або зазнає тих же перетворень, що і шумоподібний сигнал на етапі реалізації.

Цей метод має набагато вищу скритність, але в той же час він має нижчий рівень використання маркера контейнера.

РОЗДІЛ 4. ПРОГРАМНЕ РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СТЕГОСИСТЕМИ ДЛЯ IP-ТЕЛЕФОНІВ

4.1 Застосування програмного забезпечення стегосистеми для IP-телефонії

Для встановлення адекватності розроблених методів та проведення чисельних експериментів розроблено програмний комплекс FCITStegoVoIP, який реалізовано в середовищі Visual Studio 2010 на основі мови програмування C++ з використанням деяких безкоштовних модулів OpenPuff v3.30 Steganography & Водяні знаки, перелік основних модулів наведено в Додатку А .

На малюнку 4.1 показано головне вікно програми FCITStegoVoIP.

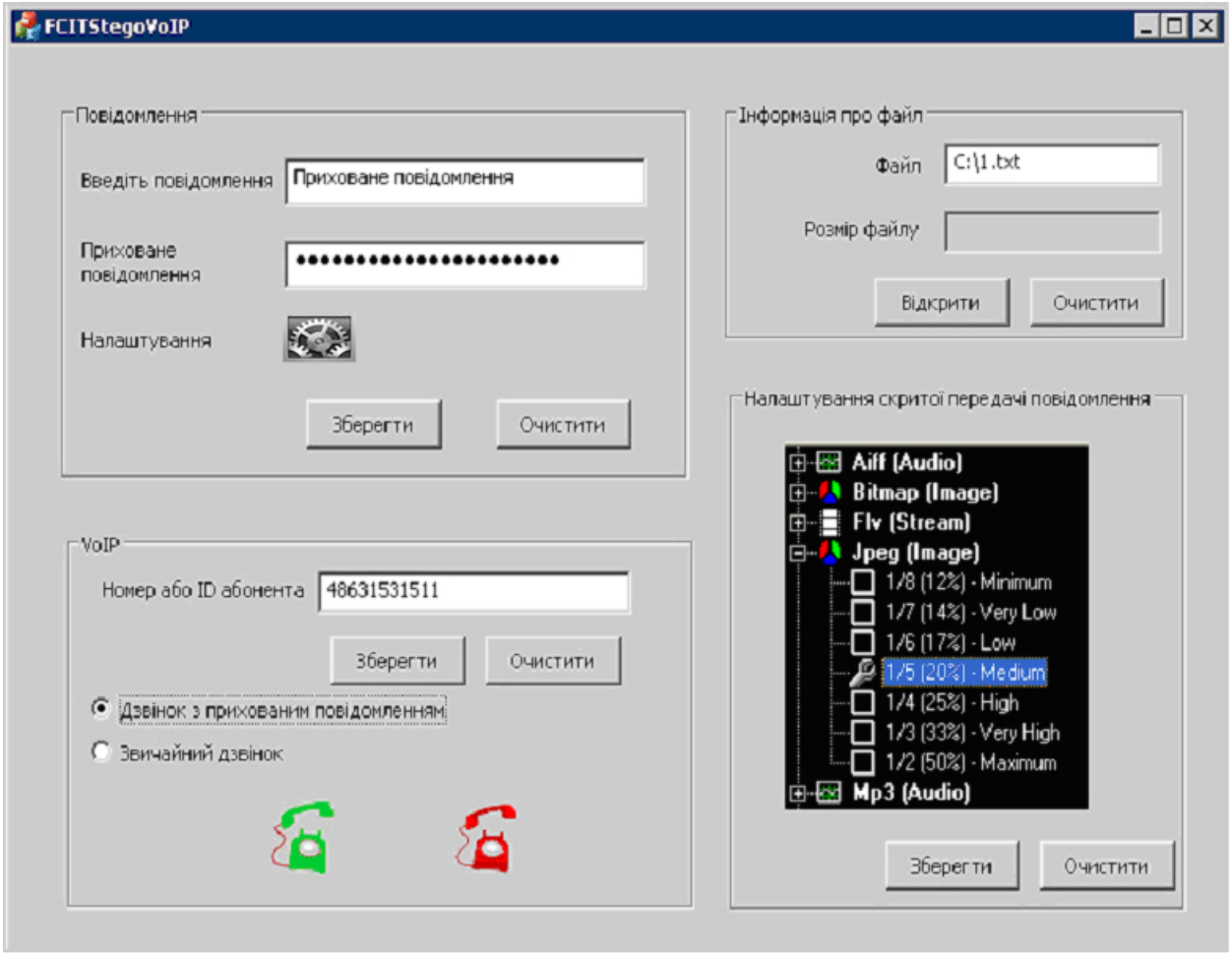

Рис. 4.1. Головне вікно програми FCITStegoVoIP

Цей комплекс реалізовано на основі архітектури клієнт-сервер, оскільки більшість стегосистем організовано саме так, але і клієнт, і сервер можуть бути рівноправними учасниками обміну конфіденційною інформацією.

У головному вікні можна ввести текст прихованого повідомлення або відкрити його з файлу, вибрати користувача для здійснення дзвінка, вибрати тип дзвінка - дзвінок з прихованим повідомленням або звичайний дзвінок, а також . як основу для налаштування характеристик передачі повідомлень - від вибору кодів стиснення до вибору типових конфігурацій для окремих груп повідомлень.

На рисунку 4.2 показано вікно клієнтської частини системи FCITStegoVoIP, до складу якого, крім модуля організації телефонної розмови, входить модуль розпакування прихованого повідомлення, можливість його збереження на локальному або мережевому диску.

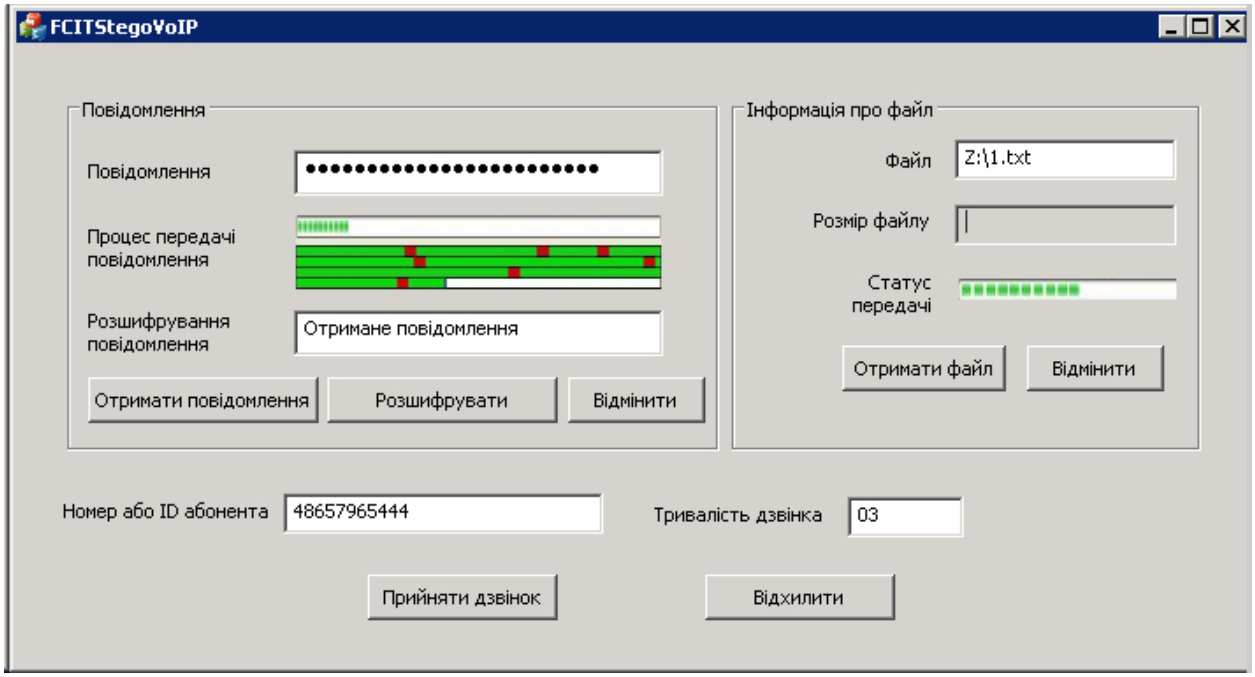

Рис. 4.2 Клієнтська частина FCITStegoVoIP

На малюнку 4.3 показано вікно для налаштування параметрів з’єднання між клієнтом і сервером, встановлення порту з’єднання та запуску та зупинки серверної частини.

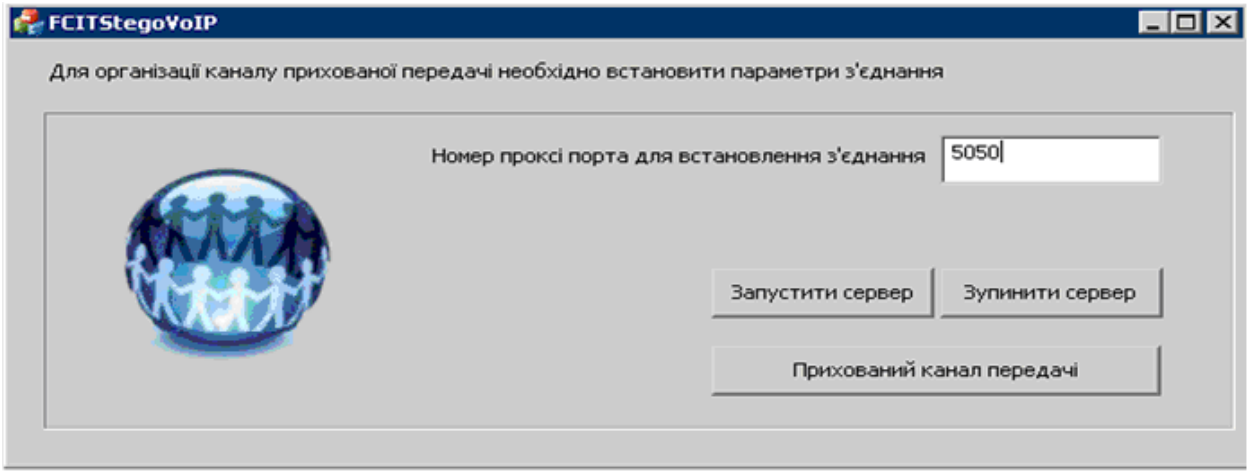

Рис. 4.3. Налаштування параметрів підключення

4.2 Дослідження моделі стегосистеми для IP- телефонії

Для оцінки можливостей використання розробленої стегосистеми в IP-телефонії було проведено кілька чисельних експериментів. У таблиці 4.1 наведено короткий опис запропонованої стегосистеми.

Таблиця 4.1 - Характеристика запропонованої системи стегоразису

Протокол	Сховати	Кордон	Переваги	Недоліки
IP	IN полі визнання і варіант Мітка часу в Інтернеті заголовок IP-дейтаграми . _	Кількість маршрутизаторів, через які проходитиме контейнер Stego, залежить від розміру опції Internet Timestamp.	Факт передачі повідомлення добре прихований. Можна використовувати можливості протоколів вищого рівня	Порівняльно жорсткий обмеження. 3 заходів вхідне повідомлення контейнери родичі складність впровадження .

У таблиці 4.2 наведено результати випробувань стегосистеми, де показано основні характеристики стегосистеми

Таблиця 4.2- Випробування стегосистеми ІЧ-телефонії

Номер Маршрути пробки	Довжина повідомлення	Інтервал	Підтвердження	Числовий подвійний	Довжина поля	Стегоконтейнери		Час доставки	Надіслани (вимірювати)
						Загалом	унікальний		
0	1024	0..60	тому	3	32	516		4503	30960
6	512		Ні				129	4013	
			тому	0..7	56	499		4793	41916
			Ні			346		2147	29064
			тому	3	32	260		2427	15600
			Ні				65	2253	
тринадцять	256		тому	0..7	56	259		2283	21756
			Ні			276		2411	23184
			тому	3	32		33	1276	7920
			Ні			132		1023	
			тому	0..7	56	161		1399	13524
			Ні			147		1140	12348

На малюнку 4.4 показані середні результати передачі прихованого потоку даних, а на малюнку показані відповідні результати, але характеризуються характеристикою переданих пакетів.

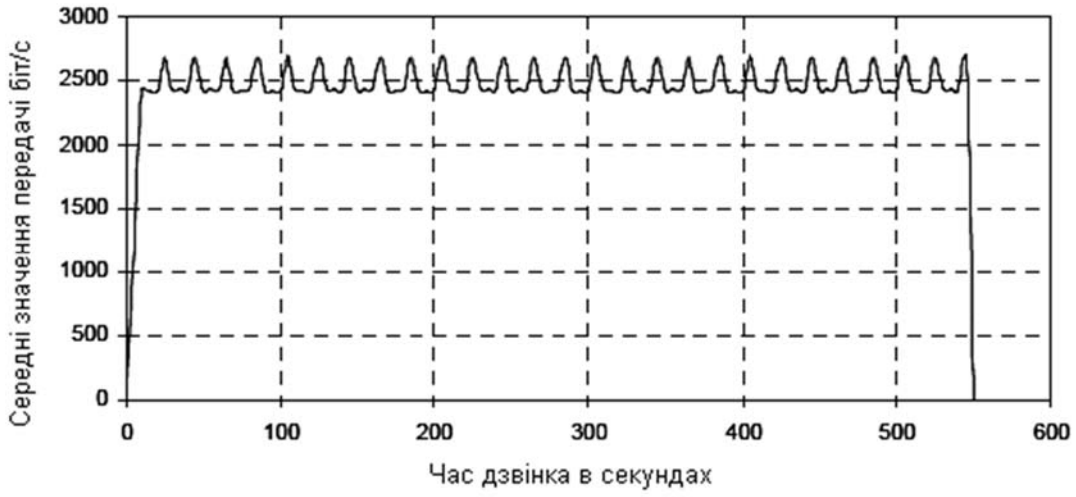

Рис. 4.4. Середні результати передачі прихованого потоку бітових даних

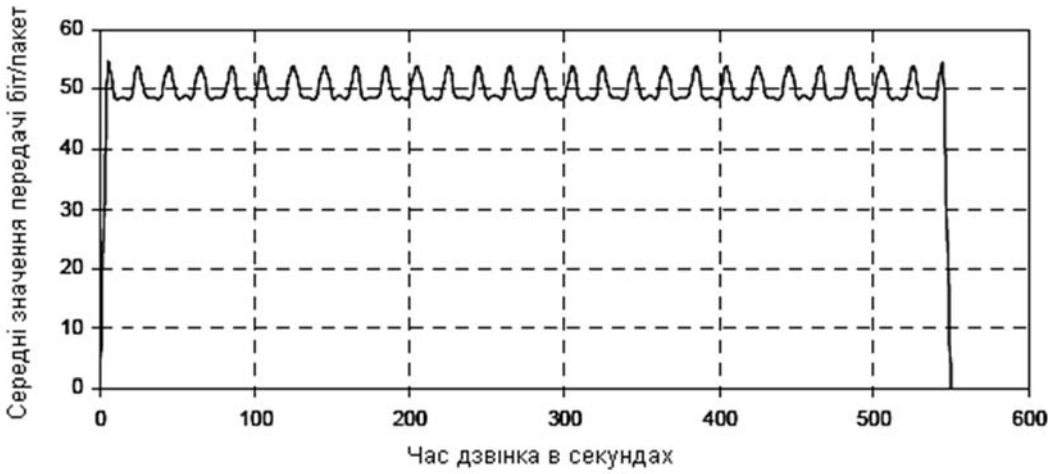

Рис. 4.5. Середні результати передачі прихованого потоку біт/пакетних даних

Проведемо порівняння розробленого методу з відомими рішеннями для оцінки можливостей його використання для прихованої передачі даних в IP-телефонії. На рисунку 4.6 наведено характеристики вихідного сигналу, а на рисунку 4.7 – сигналу, отриманого користувачем Б на виході внаслідок застосування методу молодших розрядів. На рисунку 4.8 показані характеристики прийнятого сигналу на основі застосування методу розробки. Як видно з рисунків 4.6-4.8, розроблений метод має найбільш наближені характеристики до вхідного сигналу і може бути використаний для маскування даних в IP-телефонії.

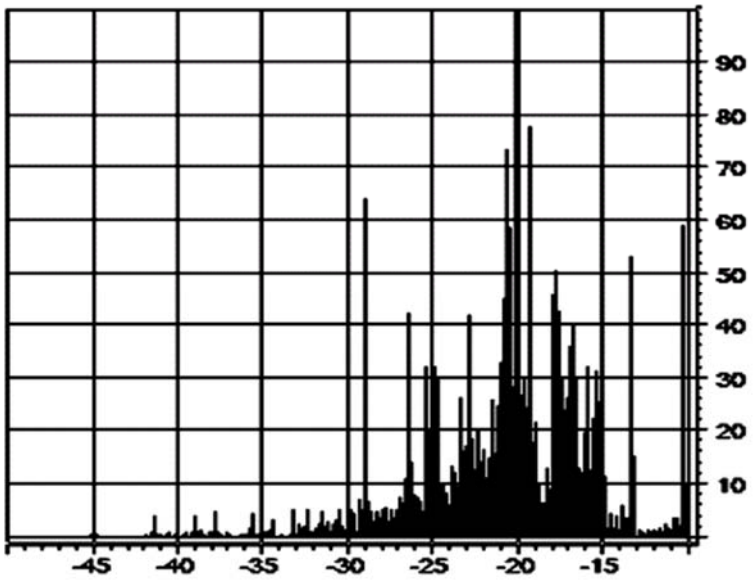

Рис. 4.6 – Вихідний сигнал

Для визначення інтервалу часу між сигналом і його відлунням необхідно розрахувати автокореляційну функцію кепстра, тобто енергетичний спектр функції.

Сплеск у функції автокореляції відбудеться приблизно через секунду δ_1 після δ_0 вихідного сигналу (рис. 4.9). Правило декодування засноване на визначенні інтервалу часу між вихідним сигналом і автокореляційним сплеском. При декодуванні приймається «одиниця», якщо значення автокореляційної функції через одну секунду δ_1 більше, ніж через одну δ_0 секунду, інакше - «нуль».

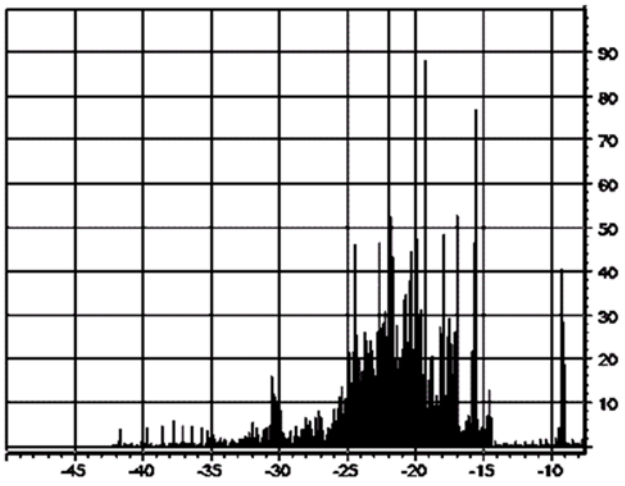

Рис. 4.7. Результуючий сигнал заснований на використанні методу заміни молодших розрядів

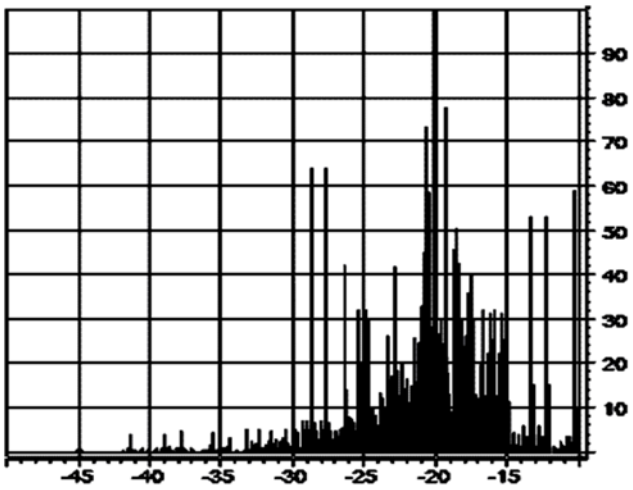

Рис. 4.8. Сигнал, отриманий на основі використання методу розробки

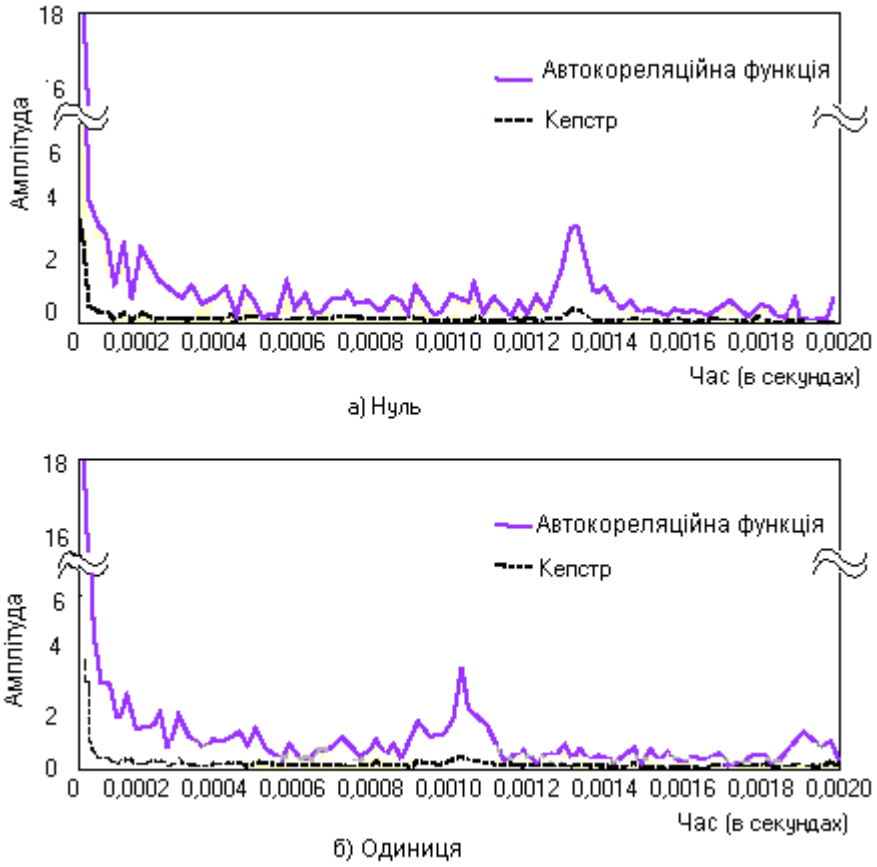

Рис. 4.9. Поведінка функції автокореляції з різною прихованою інформацією

На основі проведених експериментальних досліджень встановлено широкі можливості використання розробленої стегосистеми IP-телефонії.

ВИСНОВКИ

Виміряти приховані повідомлення в Інтернет- телефонних дзвінках - кінець етап еволюція стеганографія . методи стеганографія для приховати повідомлення там приблизно багато ну скільки _ криптографія та розробка разом з технологіями. Сучасна техніка включає в себе приховати вхідні повідомлення цифрова форма - Ти можеш виразити як зображення , і звук файли .

Перевага стеганографія закінчено криптографія це потенціал _ перехоплювачі без деталей підозра, що _ "чує" приховані повідомлення . IN VoIP трафік неможливо ідентифікувати сторонніх осіб подробиці якщо _ я не знаю впевнений, що вони _ так і два ніж функція спеціальне програмне забезпечення, призначене для розшифрування знаки

можливість передача прихований Повідомлення – це ідея в IP-телефонії, яка сьогодні активно розвивається.

У даній магістерській роботі проаналізовано характеристики передачі голосових сигналів у мережах з комутацією пакетів, проаналізовано принципи використання технології IP- телефонії та методи захисту даних.

Проведено дослідження, пов'язані з розвитком стеганофонічних систем, проаналізовано основні методи приховування мовних сигналів та методи стеганографії. Висвітлено переваги та недоліки існуючих підходів на основі критеріїв оцінки їх ефективності.

Встановлено, що мережевий канал прихованої передачі даних можна організувати на основі зміни полів IP-пакетів. Основні можливості приховування даних за допомогою IP-пакетів:

- постійні дані: - ідентифікатор пакета - протокол передачі.;
- повторювані послідовності символів;
- вільний простір пакета заповнюється нульовим значенням.

Під час магістерської роботи розроблено метод приховування даних для IP- телефонії , який враховує, на відміну від відомих рішень, такі

характеристики, як середній час затримки та значення максимально допустимої затримки в мережі в умовах, що періодично повторюються. підписаний.

Показано можливість використання методу приховування даних в ІЧ-телефонії на основі таких сигналів, як шум.

Для встановлення можливостей використання розроблених методів і алгоритмів реалізовано програмний комплекс FCITStegoVoIP на основі архітектури клієнт-сервер.

Проведено експериментальні дослідження моделі стегосистеми для IP-телефонії , в результаті чого встановлено можливості її використання .

СПИСОК ЛІТЕРАТУРИ

1. Скляр Б. Цифровий зв'язок. Теоретичні основи та практичне застосування. - М.: Видавничий дім «Вільяме», 2003. - 1104 с.

2. Гольдштейн Б. С. та ін. ІЧ-телефонія / Б. С. Гольдштейн, А. В. Пінчук, А. Л. Суховицький. - М.: Радіо і зв'язок, 2001 -336 с.

3. Бабкін В. В. та ін . Бабкін, А.А. Ланн, Б.Ц. Шаптала // Матеріали 7-ї міжнародної конференції та виставки TSO and its DSPA Application . -2005 рік. -LE. 28-32.

4. Інформаційна безпека – Вікіпедія // Вікіпедія – вільна бібліотека [Електронний ресурс]. – Режим доступу: http :// ru . Вікіпедія . org / wiki / Інформаційна_безпека.

5. Білий папір. Безпека та конфіденційність VoIP. Підвищення рівня безпеки платформ і мереж ПК Надруковано в США/1105/PMS/LKY/PP/1 50 Intel, 2006 - 8 стор.

6. TLS – Вікіпедія // Вікіпедія – вільна бібліотека [Електронний ресурс]. – Режим доступу: http :// ru . Вікіпедія . org / wiki / TLS .

7. Ботюк А. О. та ін . Переваги асиметричної криптографії / А. О. Ботюк, М. П. Карпінський, Ю. І. Кінах // Збірник доповідей II наук. - технічна конф. «Нормативно-правове та метрологічне забезпечення системи захисту інформації в Україні». – К.: НТУУ «КПІ», 2000. – С. 242 – 244 .

8. Коблиць Н. Курс теорії чисел і криптографії. - М.: ТВП, 2001 - 270 с

9. Баричев С. Г. та ін. Основи сучасної криптографії / С. Г. Баричев, В. В. Гончаров, Р. Є. Сєров. - М.: Гаряча лінія - Телеком, 2001. - 144 с.

10. Порівняння стандарту шифрування Російської Федерації з новим стандартом шифрування США [Електронний ресурс] / А. Винокуров, Є. Применко – Режим доступу: http :// www . проникливість . ru / crypto / index . htm .

11. Росляков А. В. та ін. ІЧ-телефонія /А.В.Росляков, М.Ю. Самсонова, І. В. Шибаєва. - М.: Еко-Трендз, 2003. - 252 с.