Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повне найменування інституту, факультету)

Кафедра телекомунікацій
(повна назва кафедри)

До захисту допущено
В.о. завідувача кафедри
_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)
"04" червня 2020_р.

Дипломна робота
на здобуття освітнього ступеня "бакалавр"
(назва ОС)
Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

на тему: Методи забезпечення інформаційної безпеки в системах IP - телефонії

Виконала: студентка 4 курсу, групи ТЗ - 62
Полковникова Світлана Михайлівна
(прізвище, ім'я, по батькові) (підпис)

Керівник Доцент, к.т.н. доцент Явіся В.С.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент
(посада, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую,
що у цій дипломній роботі немає запозичень з праць і нших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020_ року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Освітній ступінь бакалавр

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

____ Валерій_ЯВІСЯ
(підпис) (ім'я, прізвище)

"_22 "_січня_2020 р.

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

__ _____ Полковникова Світлана Михайлівна _____
1. Тема роботи___Методи забезпечення інформаційної безпеки в системах IP – телефонії _____
керівник роботи___ Доцент, к.т.н. доцент Явіся В.С._____,
затверджені наказом по університету від 30 березня 2020 р. №924-с

2. Термін подання студентом роботи___4 червня 2020_____
3. Вихідні дані до роботи__Мережа IP - телефонії_____
4.Зміст роботи
1) ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ IP- ТЕЛЕФОНІЇ) _
2) МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ IP- ТЕЛЕФОНІЇ
3) ПЕРСПЕКТИВНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ IP-ТЕЛЕФОНІЇ, ПОРІВНЯННЯ ЇХНІХ ХАРАКТЕРИСТИК ПО ПЕВНИМ КРІТЕРІЯМ
4) ВИСНОВКИ
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)
1) Загальний вигляд мережі IP- телефонії; 2) Стек протоколів H.323; 3) Стек протоколів VoIP; 4) Методи інформаційної безпеки; 5) Концептуальна модель безпеки інформації; 6) Загрози інформаційної безпеки в мережах; 7) Узагальнена схема криптосистеми; 8) Методи цифрової стеганографії; 8) Методи квантової стеганографії; 9) Узагальнена модель стегосистеми; 10) Модель аналізу загроз стійкості стегосистем; 11) Динаміка патентування відомих фірм-розробників інженерно-технічних заходів і засобів захисту та методів забезпечення інформаційної безпеки систем IP – телефонії; 12) Дінамика патентування основних відомих
методів забезпечення інформаційної безпеки систем IP – телефонії; 13) Презентація.

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання __16 жовтня 2019_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	**Примітка**
1	Аналіз отриманого завдання	01.01.2020 – 31.01.2020	Виконано
2	Постановка мети дипломної роботи та розробка попереднього змісту	01.02.2020 – 29.02.2020	Виконано
3	Формування вступної частини пояснювальної записки	01.03.2020 – 31.03.2020	Виконано
4	Формування основних відомостей про мережі IP - телефонії	01.04.2020 – 30.04.2020	Виконано
5	Формування відомостей про методи забезпечення інформаційної безпеки в системах IP- телефонії	01.05.2020 – 15.05.2020	Виконано
6	Оформлення дипломного проекту.	16.05.2020 – 31.05.2020	Виконано

Студент **_____ Полковникова С. М.**
(підпис) (прізвище та ініціали)

Керівник роботи _____ ___Явіся В. С.____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота присвячена методам забезпечення безпеки інформації в системах IP-телефонії. В даній кваліфікаційній роботі були з'ясовані типи загроз в IP-телефонії та досліджені методи боротьби з ними; визначена ступінь захисту мережи IP- телефонії в залежності від умов використання, були встановлені існуючи і перспективні методи забезпечення інформаційної безпеки в системах IP- телефонії; виявлено науково-технічні напрацювання та построєні діаграми для знаходження і теоретично обґрунтування динаміки патентування відомих фірм-розробників та інженерно-технічних заходів і засобів захисту та методів забезпечення безпеки інформації систем IP – телефонії, а також патентування вказаних методів. Стрімкий розвиток мережних-технологій привів до появи додаткових сервісів і запропонував багато послуг. Однією з найцікавіших є технологія цифрового зв'язку - IP-телефонія, яка розповсюджена в корпоративному і державному секторі, дозволяє використовувати публічну або відомчу мережу для ведення переговорів з використанням інтернет протоколу, а також передачі даних і відео в режимі реального часу. Ключові слова: мережа, комутація пакетів, протокол, IP-телефонія, VOIP-телефонія, потокова інформація, передача даних, стеганографія, контейнер, прихований канал, прихована передача інформації, стеганоаналіз, криптографія, криптоалгоритм, ключ шифрування, нерозкривні шифри, протоколи передавання інформації, метод захисту інформації патентні дослідження. Кваліфікаційна робота містить 68 сторінок, 12 рисунків та 7 таблиць. В роботі використано 62 науково-технічних видання.

ANNOTATION

Qualification work is devoted to methods of information security in IP-telephony systems. In this qualification work, the types of threats in IP telephony were clarified and methods of combating them were investigated; determined the degree of protection of the IP-telephony network depending on the conditions of use, existing and promising methods of information security in IP-telephony systems were established; scientific and technical developments and diagrams for finding and theoretically substantiating the dynamics of patenting of well-known developers and engineering measures and means of protection and methods of information security of IP systems - telephony, as well as patenting of these methods. The rapid development of network technologies has led to the emergence of additional services and offered many services. One of the most interesting is digital communication technology - IP telephony, which is widespread in the corporate and public sector, allows you to use a public or departmental network to negotiate using the Internet protocol, as well as data and video transmission in real time.
Keywords: network, packet switching, protocol, IP-telephony, VOIP-telephony, streaming information, data transmission, steganography, container, hidden channel, hidden information transmission, steganoanalysis, cryptography, cryptoalgorithm, encryption key, non-revealing ciphers, information transmission protocols , method of information protection patent research. The qualification work contains 68 pages, 12 figures and 7 tables. 62 scientific and technical publications were used in the work.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АЦП – аналогово-цифровий перетворювач;

ЦАП - цифро-аналоговий перетворювач;

АТС − автоматична телефонна станція;

ЗКС – загальноканальна сигналізація;

ІКМ– імпульсно-кодова модуляція;

ТМЗК − телефонна мережа загального користування;

Call Agent - телефонним агентом -

DNS – Domain Name Service сервіс доменних імен;

GSM – Global System of Mobile система стільникового зв’язку;

IEEE – Institute of Electrical and Electronics Engineers асоціація інженерів у галузі електротехніки та радіоелектроніки;

IP − Internet Protocol міжмережний протокол адресації;

LAN − Local Area Network локальна обчислювальна мережа;

MAC − Media Access Control ідентифікатор управління доступом до носія;

MEGACO − Media Gateway Control Protocol протокол управління шлюзами середовища;

MG − Media Gateway транспортний шлюз;

MGC − Media Gateway Controller контролер медіашлюзів;

MGCP − Media Gateway Control Protocol протокол управління шлюзами;

OSI − Open Systems Interconnection basic reference model базова еталонна модель взаємодії відкритих систем;

PBX – Private Branch eXchange приватна віртуальна телефонна мережа;

PC – Personal Computer персональний комп’ютер ПК;

RTP − Real−time Transport Protocol протокол передачі в реальному часі;

SRTP-Secure Real-time Transport Protocol розширення до протоколу RTP;

HTTP - HyperText Transfer Protocol протокол верхнього 7-го рівня;

SDP – Session Description Protocol протокол опису сеансу;

SIP − Session Initiation Protocol протокол встановлення сеансу;

TCP − Transmission Control Protocol протокол управління передачею даних, який гарантує доставку пакетів;

TDM – Time Division Multiplexing мультиплексування з розподілом за часом;

UAC – User Agent Client агентський клієнт;

VLAN – Virtual Local Area Network віртуальна локальна обчислювальна мережа;

VoIP − (Voice over IP) технологія передачі голосу в реальному часі;

CTI - концепція Computer Telephone Integration;

FNC - Federal Networking Counsil організація, відповідальна за задоволення мережевих потреб федеральних агентств США;

Token Ring - протокол передачи даних в локальній мережі (LAN), мережі Token Ring (стандарт 802.5),

FDDI - Fiber Distributed Data Interface специфікація, що описує високошвидкісні мережі з методом доступу із передачею маркера на основі оптоволокна.

ISDN - Integrated Services Digital Network цифрова мережа з інтегрованими службами;

IVR - Interactive voice response Інтеракти́вна голосова́ відповідь;

IAX2 - Inter-Asterisk eXchange protocol протокол пристосований до трансляції мережевих адрес;

OSP - Open Settlement Protocol клиент/серверный протокол, применяемый провайдерами Интернета, для авторизации, аккунтинга;

UDP - User Datagram Protocol найпростіший протокол транспортного рівня моделі OSI

RIP - Routing Information Protocol, IGRP - Interior Gateway Routing Protocol, EIGRP - Enhanced Interior Gateway Routing Protocol, IS-IS - Intermediate System-to-

intermediate System, OSPF - Open Shortest Path First, BGP - Border Gateway Protocol - протоколи маршрутизації;

TIPHON - Telecommunication and Internet Protocol Harmonization over Networks проект з розвитку IP-телефонії;

ICMP - Internet Control Message Protocol міжмережевий протокол керуючих повідомлень;

RSVP - Resource Reservation Protocol протокол резервування;

IETF - Internet Engineering Task Force –інженерна група Інтернет;

PPP - Point-to-Point Protocol протокол механізму аутентифікації;

PAP - Password Authentication Protocol, CHAP- Challenge Handshake Protocol і EAP - Extensible Authentication Protocol; RADIUS - TACACS + і Remote Access Dial-In User Service протоколи, які підтримують рішення аутентифікаці;

DoS - denial of service ДОС-атака, отказ в обслуживании;

EAP – Transport Level Security тип протоколу, застосовується у системах безпеки, які використовують сертифікати;

FEAL - Fast data Enciphtrment ALgorithm, DES - Digital Encryption Standard алгоритм блочногошифру;

CA - certificate authority сертифікаційна служба;

TranSteg - Transcoding Steganography - метод мережевий стеганографії;

HICCUPS - Hidden Communication system for CorrUPted networkS система, яка використовує недосконаліть передачі даних в мережі;

UA – Україна (Стандарт ВОИС ST.3);

RU – Росія;

US – США;

NL- Нідерланди;

CY –Кіпр;

CN –Кітай;

НДПКР- науково-дослідні і проектно-конструкторські роботи

ЗМІСТ

ВСТУП

Найціннішими ресурсами є інформаційні, вони мають відповідне матеріальне вираження і вимагають захисту від впливів, що призводять до зниження їхньої цінності. Захищати інформацію від несанкціонованого використання необхідно під час вирішення державних завдань, в комерції, під час дослідження науково-технічних проблем, розробці нових об'єктів техніки і технологій тощо.

Регулювання питань з обміну інформацією здійснюється на нормативній основі [1,2,3] законів, положень (порядків) стандартів тощо. Особливо важливими є питання інформаційної безпеки в системах телефонії.

Термін «Телефонія» охоплює науково - технічні аспекти телефонного зв'язку.

До 70-х років XX ст. розвиток телефонії носив еволюційний характер. Мережі телефонного зв'язку були аналоговими. Еволюційні зміни системи телефонного зв'язку мали характер кількісного збільшення місткості і пропускної спроможності мереж та поліпшення показників якості обслуговування [6].

Історично підтверджена актуальність досліджуваної проблеми. В літературі викладені історичні факти про проблеми з обміну інформацією [7], випадки порушення зв'язку, що мали негативні наслідки та змінювали поворот подій.

Другий період розвитку телефонії (почався в 70-і роки XX ст.), характеризується тим, що основою телефонії стали нові технології: електронна, цифрова, комп'ютерна [8].

Електронна технологія дозволила перевести усі апаратні вузли телефонії на електронну елементну і технологічну базу. Цифрова технологія об'єднала системи передачі і комутації. Застосування комп'ютерної технології стало базою у використанні комп'ютерів в ролі обладнання управління АТС, та в створенні комп'ютерних терміналів [7,8]. Інформація про другий період в історії телефонії, надана в джерелах [5,6,7,9]. Цей період характеризується радикальним характером змін і високим темпом розвитку, який збільшився впродовж декількох останніх десятиліть.

З'явилися системи і мережі з інтеграцією послуг (ISDN- Integrated Services Digital Network). Розвиваються додатки телефонії, в тому числі технологія IP – телефонії, що забезпечує передачу мови по мережах пакетної комутації. Створення єдиних програмно-апаратних платформ із зосередженням усіх функцій в одній системі (інтелектуальному сервері мережі) – є результатом напряму комп'ютерно-телефонної інтеграції.

Нова галузь виникла в середині 80-х на стику комп'ютерних і телефонних технологій. Багато винаходів з телефонії відзначається в цей період. [9 -15].

Кінець XX ст. характеризується бурхливим розвитком інформаційних технологій. Інформатизація та комп'ютеризація докорінно змінюють характерні риси суспільства. Питання інформаційної безпеки виходять на перший план у проблематиці в системах IP – телефонії. Масове впровадження нових технічних засобів і технологій з телефонії стало основою здійснення світової інформатизації та методологічним фундаментом світової науки і техніки.

Знання основних джерел небезпеки для мереж IP-телефонії, та розуміння методів усунення цих загроз допоможе покращити платформу регулювання в господарський діяльності на державному рівні. Проблематика актуальна і для інших платформ IP-телефонії.

З зростанням популярності IP-телефонії актуальнішим стає питання забезпечення безпеки в загальному вигляді і конфіденційності розмов зокрема, тому у пропонованій роботі знайшли відображення проблеми, пов'язані з розвитком і освоєнням телефонії, і з питаннями забезпечення інформаційної безпеки в її системах; а також з досліджень об'єктів попереднього та сучасного поколінь; визначенням перспективних напрямів розвитку методів інформаційної безпеки в системах IP –телефонії. Швидкий технічно-технологічний підйом в галузі телефонії, посилення конкурентної боротьби, ставлять високі вимоги до діяльності в цій галузі.

Актуальність теми. Проведений аналіз науково-технічної літератури показав, що телекомунікаційні мережі удосконалюються і стають складнішими. Спостерігається бурхливий ріст винахідницької активності в галузі телефонії за різними напрямками, серед яких гідне місце займає тенденція з пошуку нових методів забезпечення інформаційної безпеки в системах IP – телефонії та удосконаленню існуючих. Подальше дослідження в указаному напрямку є актуальним, бо цілком очевидно, що у перспективі це питання стає одним із вирішальних для стійкого розвитку економіки та безпеки держави.

Завдання. В ході виконання роботи поставлене завдання з систематизації і розширення теоретичних знань в галузі інформаційної безпеки в системах IP-телефонії, отриманих у процесі проведених досліджень, та визначення можливості використання в інформаційних технологіях і методах забезпечення інформаційної безпеки в системах IP- телефонії у процесі розв'язання завдань.

Об'єктом дослідження є методи забезпечення інформаційної безпеки в системах IP- телефонії, які є результатами науково-дослідної діяльності вітчизняних і іноземних компаній.

Предметом дослідження є IP - телефонна мережа.

Метою дослідження є визначення існуючого науково-технічного напрацювання в галузі методів забезпечення інформаційної безпеки в системах IP - телефонії; виявлення перспективних напрямків розвитку; вибір ефективних методів забезпечення інформаційної безпеки в системах IP - телефонії; виявлення прийомів, необхідних для характеристики дійсності і можливості усунення складностей в досягнення цілей.

Методи дослідження**.** В роботі виконуються дослідження, які базуються на використанні статистичних методів аналізу, принципів передачі інформації, теорії захисту інформації, а також використовувалися елементарно-теоретичний метод, історичний, логічний та методи класифікації.

Наукова новизна одержаних результатів. В результаті виконання даної роботи були з’ясовані типи загроз в IP-телефонії та визначені методи боротьби з ними; визначена ступінь захисту мережи IP- телефонії в залежності від умов використання; встановлені існуючи і перспективні методи забезпечення безпеки інформації в системах IP- телефонії; виявлено науково-технічні напрацювання; построєні діаграми для знаходження і теоретично обґрунтування динаміки патентування відомих фірм-розробників та інженерно-технічних заходів і засобів захисту та методів забезпечення інформаційної безпеки систем IP – телефонії, а також патентування вказаних методів. Виконанні порівняння відомих методів забезпечення інформації в системах IP-телефонії з висновками про переваги певних методів.

Виконані дослідження показали, що зростаюча популярність IP - телефонії і зміни, що відбуваються в структурі телекомунікаційних мереж, стали причиною здійснення активності удосконалень та впровадження широкого спектру послуг на нових технологічних основах, які будуть гарантовано надаватися з дотриманням інформаційної безпеки в IP - мережах.

1 ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ IP- ТЕЛЕФОНІЇ

1.1 Стисла характеристика IP-телефонії (VOIP).

1.1.1 Визначення IP-телефонії

IP-телефонія стала стандартом у телефонних комунікаціях, тому що це зручно, надійно, має відносно невисоку вартість в порівнянні з аналоговим зв'язком. Тенденція організації телефонних розмов по мережах передачі даних є в концепції CTI, в її межах пропонується багато послуг. Однією з найцікавіших є IP-телефонія - технологія цифрового зв’язку.

IP-телефонія розповсюджена в корпоративному і державному секторі [9-13], є популярною, але викликає застереження щодо безпеки інфраструктури мережі.

Не існує способів зв’язку з абсолютною інформаційною безпекою.

В літературі [9,12,13,14,16-21] використовують такі поняття для позначення технології передачі мови по мережах з пакетною комутацією на базі протоколу IP (Internet Protocol - міжмережевий протокол): IP- телефонія (IP Telephony); голос по IP-мережі (Voice over IP-VoIP); Інтернет-телефонія (Internet Telephony).

Стосовно організації системи зв’язку під IP- телефонією розуміють[22] технологією голосового спілкування та обмін факс-повідомленнями через мережу, що використовує протокол IP.

Виділено певні види IP телефонії: стандартна - потрібне комутаційне обладнання і термінал; бездротова IP - телефонія – потрібен спеціальний термінал, що підключений до мережі GSM або WI-FI; віртуальна IP - телефонія, без установки серверного обладнання та АТС, ресурсом є існуюча мережа, а доступ з комп'ютера підключеного до Інтернет.

Устаткування IP телефонії - це комплекс пристроїв, які мають певні функції та впливають на забезпечення інформаційної безпеки в системах IP-телефонії:

АТС для IP телефонії - основний комутаційний пристрій для підключення до традиційних послуг зв'язку і створює локальну мережу передачі даних. Комплекс обладнання володіє вибором додаткових функцій - автоматична/ручна

переадресація, внутрішній безкоштовний зв'язок, конференц-зв'язок, утримання виклику і заборона /обмеження вхідних дзвінків і інше;

сервера для IP телефонії (серверні станції) забезпечують контроль локальної мережі і об'єднують АТС і кінцевого користувача. Усередині сервера можуть перебувати цифрові і аналогові пристрої для перетворення /кодування сигналу, а також спеціальні плати для транслювання інформації на зовнішні пристрої. Завдяки уніфікованим елементам можна розширити абонентську внутрішню мережу або оснастити сервер GSM модулем для мобільного зв'язку;

телефони для IP телефонії – це кінцеві термінали для здійснення обміну інформацією між абонентами, сучасні апарати підтримують функцію відео-зв'язку, що розширює їхню функціональність;

гарнітура для IP телефонії - допоміжні пристрої є незамінними для роботи call-центрів підвищує якість сигналу, усуває ефекти луни, в порівнянні з підключеннями мікрофона через зовнішні динаміки;

програми для IP- телефонії - функціональність зв'язку неможливо забезпечити без програмного забезпечення, яке призначене для кодування і перетворення сигналу, стиснення пакетів даних, контролю за трафіком і ін.

IP - телефонія має переваги: конфіденційність (забезпечується за допомогою кодування інформації в пакети і їх передачі безпосередньо адресату); захищеність (виключена ймовірність підключення до номера сторонньої особи), тощо.

Незважаючи на переваги і функціональність, IP технологія є уразливою.

Хакери використовують сниффер – програму, що є аналізатором трафіку, тому є можливість підключитися до прослуховування лінії. Зловмисники, і перехоплюють данні, і блокують, і знищують існуючої мережі, які можуть заповнитися непотрібним трафіком, що перевантажує, роз'єднує.

Існують способи захисту каналу зв'язку: впровадження нових протоколів шифрування інформації; жорсткий контроль трафіку; додаткове стиснення пакетів даних; криптографічна автентифікація тощо.

Здійснення діяльності з надання послуг телефонного зв'язку із застосуванням технології IP-телефонії, відбувається за розробленим відповідно до Закону України "Про телекомунікації" [2], Порядком [3], в пункті 2.1 якого визначено, що IP – телефонія – це обмін інформацією голосом з використанням мережі передавання даних та IP- протоколу.

IP-протокол використовується і в мережах передачі даних з пакетною комутацією, у них є можливість передавати мовні повідомлення з використанням пакетів даних. Цей спосіб передачі мови отримав назву IP-телефонія. Вона є засобом організації і ведення телефонних розмов та передачі факсів. [9- 22].

Для передачі звукової інформації по мережі використовується технологія VoIP.

В розділі 1.1 [17] вказано, що IP-телефонія - це технологія, яка використовує мережу з пакетною комутацією повідомлень на базі протоколу IP для передачі голосу в режимі реального часу. Голосові сигнали перетворюються в пакети даних, які стискаються і посилаються через Інтернет приймальній стороні, з досягненням адресата, вони декодуються в аналоговий голосовий сигнал.

На рис.1.1 зображено загальний вигляд мережі IP- телефонії [17].

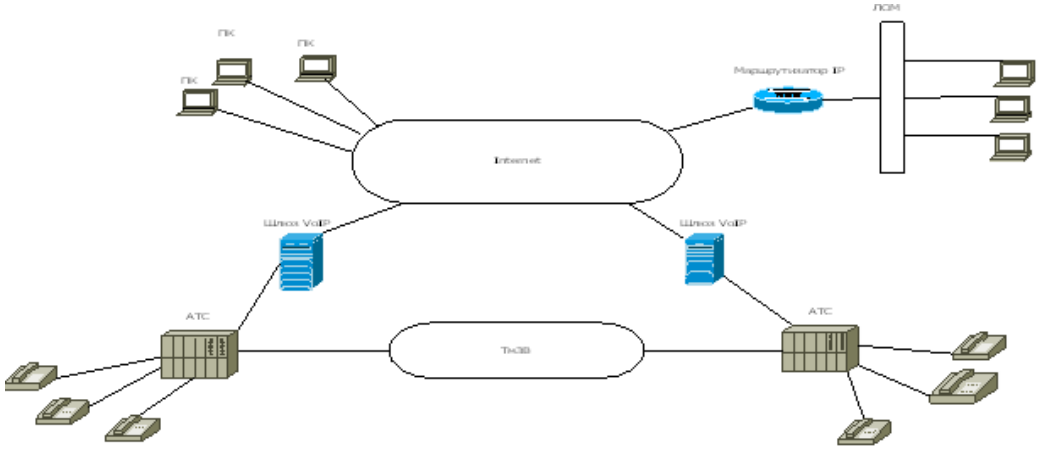

Рис.1.1 Загальний вигляд мережі IP- телефонії

Є думка, що Інтернет-телефонія - це окремий випадок IP-телефонії, при якому канали мережі Інтернет використовуються як лінії передачі телефонного трафіку і є ствердження [9], що IP-телефонія та Інтернет-телефонія стали майже синонімами, і саме так найчастіше використовують поняття. В роботах [22,23] також ці поняття вважають рівноцінними. Але різниця є: IP-телефонія для передачі голосу передбачає використання виділеного каналу зв'язку, а Інтернет-телефонія допускає використання загальних каналів зв'язку мережі Інтернет.

У світі зазвичай вживається абревіатура VoIP- Voice over IP, хоча часто використовують більш вузький термін «Інтернет-телефонія». В [26] описано про технологію Інтернет, та про визначення терміну «Інтернет», що було дано в 1995р. FNC США в такій формі: Інтернет - це частина глобальної інформаційної системи, яка логічно пов'язана унітарним адресним простором, заснованим на IP-протоколі або на його перспективних розширеннях/послідовниках; може підтримувати комунікації, використовуючи TCP/IP або його розширення/ послідовники і/або IP-сумісні протоколи; надає, використовує або робить доступними для всіх або конфіденційно сервіси високого рівня, засновані на комунікаціях і пов'язаної з ними інфраструктури. Кожна фізична мережа, що використовує технологію - Інтернет, Token Ring, FDDI, ISDN, має з'єднання типу «точка-точка» та додалися ще ATM мережа і бездротові технології.

1.1.2 Принципи пакетної передачі та інші особливості IP-телефонії

Інтернет-телефонія частково ґрунтується на існуючій мережі закріплених телефонних ліній, використовує передову технологію стиснення голосових сигналів та місткість телефонних ліній. Тому пакети даних від різних запитів та різні їхні типи, можуть переміщатися за однією лінією в один і той же час.

Принцип дії серверів IP-телефонії: якщо, сервер пов'язаний з телефонними лініями, то він може з'єднатися з будь-яким телефоном світу, а якщо сервер пов'язаний з Інтернет, то може зв'язатися з будь-яким комп'ютером в світі.

Сервер приймає телефонний сигнал, цифрує, стискає, розбиває на пакети і відправляє через Інтернет за призначенням з використанням протоколу Інтернет (TCP/IP). Для пакетів, що приходять з мережі на телефонний сервер і, що йдуть в телефонну лінію, операція відбувається в зворотному порядку. Операції відбуваються одночасно, що забезпечує повно-дуплексну розмову [10,11].

Технологія IP-телефонії об'єднує мережі з комутацією каналів зв'язку і мережі з комутацією пакетів даних, що передаються, в єдину комунікаційну мережу. Розпізнавання голосу і його передача з однієї мережі в іншу, вирішується шлюзами [22,24]. Шлюз – це пристрій, в якому, з одного боку приєднуються телефонні лінії, а з іншого боку - IP-мережа. Голос, у вигляді аналогових коливань в системі, існує в телефонній трубці, або в пристрою, який перетворює його в цифрову інформацію. На інших ділянках каналу передачі даних від одного абонента до іншого мова шифрується і передається у вигляді IP – пакетів. Шлюз забезпечує стиснення інформації, здійснює конвертацію в пакети і прямує в IP-мережу. З протилежного боку шлюз здійснює зворотні дії: розшифрування і розформування пакетів викликів [12,17].

Класифікація шлюзів представлена типами пристроїв: VoIP - переводить голосовий трафік в мережу передачі даних; GSM - переводить голосовий трафік в мережу мобільного зв'язку GSM-стандарту; VoIP GSM - переводить голосовий трафік в мережу оператора стільникового зв'язку GSM - стандарту.

Майже всі мережеві пристрої працюють відповідно до моделі OSI. За рахунок цього дані обробляються в кілька разів швидше [10,15,21,25].

Для IP-телефонії характерна модульна кількість і потужність вузлів - шлюзів, gatekeeper - можна нарощувати у відповідності з поточними потребами [26].

IP-телефонія дозволяє підвищити ефективність використання телефонних ліній; голосова інформація і дані можуть передаватися за однією мережею; є додаткові телефонні властивості (конференція, переадресація дзвінка,

автоматичний перенабір, впровадження IVR); відсутня залежність від місця розташування. IP-телефонія інтегрується з різними додатками.

При побудові інфраструктури IP-телефонії, її відокремлюють від сегментів мережі, та це не є гарантією безпеки, тому що фірми для зручності інтегрують IP-телефонію з різними додатками - з'являються нові уразливості.

1.1.3 Способи здійснення зв'язку [9, 10,11,14,26-31]

Ключовим елементом [16] Інтернет-телефонії є зв'язка «шлюз - Інтернет – шлюз». Шлюз - комп'ютер-сервер, доповнений спеціальними платами розширення і відповідним програмним забезпеченням. Він служить інтерфейсом між передавальним звук пристроєм користувача і IP- мережею.

Базові типи (сценарії) IP-телефонії.

Існує кілька варіантів IP-телефонії. Проведений аналіз відомих джерел інформації показав, що найбільш часто виділяють [17,20,27,34] три базові типи IP-телефонії: з комп'ютера на комп'ютер; з комп'ютера на телефон; з телефону на телефон.

Сценарій «комп'ютер-комп'ютер» реалізується на базі комп'ютерів, постачених засобами мультимедіа і підключених до мережі Інтернет. Аналогові мовні сигнали перетворюються в цифрову форму за допомогою АЦП. Для скорочення смуги відліки мовних даних в цифровій формі стискуються кодованим пристроєм. Після чого вихідні дані формуються в пакети, що передаються через IP-мережу в систему IP-телефонії обслуговуючого абонента. Для з'єднання між двома абонентами системи на обох кінцях одночасно реалізують як функції передачі, так і функції прийому. Цей сценарій обумовлює зосередження всіх функцій IP-телефонії в ПС користувача, але повинна бути сумісність програмно-апаратних засобів IP-телефонії різних постачальників.

Сценарій «комп'ютер-телефон»

В рамках проекту TIPHON розглядаються дві модифікації цього сценарію: від ПС (користувача IP-мережі) до телефону (абоненту ТМЗК) у зв'язку з наданням

користувачам IP-мережі доступу до телефонних послуг; від абонента ТМЗК до користувача IP-мережі з ідентифікацією, викликаються сторони на основі нумерації по E.164 або IP-адресації.

Шлюз (GW) для взаємодії мереж ТМЗК та IP може бути реалізований в окремому пристрої чи інтегрований в існуюче обладнання ТМЗК, чи IP-мережу.

Сценарій "телефон - телефон".

IP-телефонія надає віртуальну телефонну лінію через IP-доступ. Голосовий трафік передається через IP-мережу. Операції по маршрутизації виклику виконує шлюз. Типова послуга IP-телефонії за сценарієм «телефон-телефон» використовує стандартний телефон в якості інтерфейсу користувача, а замість міжміського компонента ТМЗК використовує або IP-мережу, або Інтернет.

1.1.4 Стандарти і протоколи IP-телефонії. Рівні архітектури IP-телефонії

1.1.4.1 Характеристика протоколів в IP–телефонії надана в літературі [10,11,15,17,20,23,24, 34]. Різні протоколи мають свої сильні і слабкі сторони, тому питання про створення єдиного стандарту є необхідним. Вважається, що для зв’язку абонентів Інтернет-телефонії використовувалися приватні протоколи, тому в IP-телефонії і виникла проблема - відсутність стандартів на передачу голосу. Для впровадження технології передачі голосу використовують стандарти, засновані на рекомендаціях H.323 Міжнародного Об'єднання з Передачі даних (International Telecommunications Union).

H.323 - основний стандарт, що складається з ряду рекомендацій по таким суміжним технічним питанням: якість мови, контроль викликів і специфікації приватників. H.323 є набором протоколів. Стек протоколів H.323 є одним з найпоширеніших. Це найстаріший, але найстабільніший протокол [28].

Для стека протоколів H.323 (рис. 1.2) надають транспортний сервіс протоколи IP, TCP і UDP (протоколи стека TCP / IP). IP - протокол надає кожній точці H.323 - адресу і забезпечує механізм маршрутизації H.323 - пакетів в мережі. Протокол TCP використовується для встановлення початкового з'єднання між терміналами

H.323 і шлюзами/гейткіперами. UDP використовується для передачі безпосередньо голосу через мережу.

<table>
<tr><td colspan="2">Мова</td><td colspan="3">Управління</td></tr>
<tr><td>G.7xx
(протоколи кодування і декодування)</td><td rowspan="2">RTCP</td><td rowspan="2">H.225
(RAS)</td><td rowspan="2">Q.931
(сигнали під час виклику)</td><td rowspan="2">H.245
(управління викликами)</td></tr>
<tr><td>RTP</td></tr>
<tr><td colspan="2">UDP</td><td colspan="3">TCP</td></tr>
<tr><td colspan="5">Протокол рівня передачі даних</td></tr>
<tr><td colspan="5">Протокол фізичного рівня</td></tr>
</table>

Рис. 1.2 Стек протоколів H.323

Для побудови сумісних з ТМЗК мереж IP-телефонії підходять протоколи H.323 і MGCP [10,11,34]. Протокол MGCP – це модель з централізованим управлінням викликами, визначає управління телефонними шлюзами з центрального керуючого компонента. Шлюзи взаємодіють з агентами, які здійснюють сигналізацію і обробку викликів. Протокол MGCP - це керуючий VoIP-протокол, який використовується для управління шлюзами в VoIP-мережі. Протокол MGCP набув поширення як частина архітектури Cisco AVVID. AVVID використовує саме MGCP в зв'язці з CCM для управління шлюзами.

Протокол OSP [10, 34] дозволяє різним власникам засобів зв'язку здійснювати комунікації в межах країни. Провідні компанії Ascend, GTE, AT & T і Internet Telephony Exchange Carrier (ITXC), що надають послуги IP-телефонії, підтримують протокол OSP. Компанії Lucent і Nortel теж готові підтримати стандарти на IP-телефонію, та остаточної оцінки OSP поки не дали.

Огляд протоколів в побудові IP – мережі наданий в джерелах [10,20,22, 34].

Протокол SIP приходить на зміну протоколів H.323, розробники пристроїв, що підтримують SIP, працюють над збільшенням числа функцій, мало приділяють уваги безпеці. Це негативно відбивається на IP-телефонії. Негативним щодо стандартів і IP-протоколів є: незакінченість стандартів; не має сумісності телекомунікаційного обладнання; відсутність стандартного протоколу взаємодії між контролерами.

1.1.4.2 Взаємодія протоколів VoIP описана в [17].

Універсальна мережа Інтернет будується на основі сімейства протоколів TCP/ IP і включає в себе протоколи 4-х рівнів комунікацій.

Основою стека IP- протоколів є мережевий рівень (Network layer) де реалізується принцип міжмережевого з'єднання, маршрутизація пакетів по мережі Інтернет. Програмне забезпечення IP виконує функції маршрутизації.

Реалізації міжмережевих з'єднань за IP–протоколом використовується протоколами транспортного рівня - TCP і UDP. IP – протокол визначає базову одиницю передачі даних в мережі Інтернет.

На мережевому рівні використовується IP- протокол доповнений спеціальними засобами (на маршрутизаторах повинна бути черговість з малою затримкою, повинні використовуватися схеми маркування із завданням пріоритетів - IP-пріоритети.)

Транспортний рівень (Transport layer) реалізує надійну передачу даних: основні протоколи TCP і UDP здійснюють зв'язок між машиною - відправником пакетів і машиною-адресатом [10,17,26].

У термінах передачі голосу рівень представлень забезпечує методи кодування і стиснення, що використовуються для передачі.

Прикладний рівень є найвищим рівнем моделі, пов’язаний із прикладними процесами і надає послуги, у т. ч. й залежно від виду використовуваного обладнання. Засобами прикладного рівня є набір протоколів, за допомогою яких користувачі мережі одержують доступ до ресурсів [19, 30].

Стек протоколів VoIP	
Прикладний рівень	Skype, xLite
Рівень представлень	G.729/G.711
Сеансовий рівень	H.323/SIP/SDP
Транспортний рівень	RTP/UDP/RSVP
Мережевий рівень	IP/LLQ (Low-Latency queuing)
Канальний рівень	MPPP, FR, ATM
Фізичний рівень	

Рис.1.3 Стек протоколів VoIP

Між кінцевими системами буває багато маршрутизаторів і проміжних фізичних мереж різних типів, але додаток сприймає їх як єдину фізичну мережу. Універсальність і гнучкість мереж на базі IP-протоколу дає можливість застосовувати для передачі даних, мультимедійної інформації, використовують і для передачі мовних повідомлень [19,26,30, 31].

Сеансовий рівень призначений для організації й управління сеансами взаємодії прикладних процесів відповідно до стандартів і контролює їх дотримання. Сеансовий рівень відповідає за організацію сеансів обміну інформацією між кінцевими пристроями. На цьому рівні виконуються функції, необхідні для здійснення зв'язку в мережі двох аплікацій: фіксуючі; надаючі засоби синхронізації.

Канальний рівень (Data link layer) - вказує, що протокол IP для створення фреймів може використовувати різні формати. Канальний рівень визначає правила доступу до фізичного середовища й управляє передачею інформації по каналу, під час якої виконується перевірка прийнятої інформації та виправлення помилок, відключення каналу при виникненні несправності, а також формування повідомлень про виникнення неусувних помилок для вищого рівня з відновленням передачі по закінченні ремонту техніки.

Фізичний рівень - технологія VoIP може працювати в будь-якому фізичному середовищі, що використовує звичайний протокол IP. Фізичний рівень ідентифікує канали зв'язку, управляє засобами організації фізичного з'єднання, виявляє пошкодження і передає повідомлення засобам канального рівня. Фізичний рівень виконує сервісні функції для канального рівня [19,31].

1.1.4.3 Рівні архітектури IP-телефонії описані в [20].

Архітектуру IP-технології представляють у вигляді площин: нижньої (базової мережі з маршрутизацією IP-пакетів) і верхньої (запитів зв'язку)

Нижня площина: RTP, що функціонує поверх протоколу UDP, розташованого в стеку протоколів TCP/IP над протоколом IP.

Ієрархія RTP/UDP/IP - це транспортний механізм для мовного трафіку.

В мережах з маршрутизацією IP-пакетів для передачі даних є механізми повторної передачі пакетів у разі їх втрати.

Верхня площина управління обслуговуванням виклику передбачає прийняття рішень про напрямок виклику та про встановлене з'єднання між абонентами. Інструментами управління є системи сигналізації. Системи підтримуваних декадно-крокових АТС передбачають об'єднання функцій маршрутизації і функцій створення комутованого каналу в одних декадно-крокових шукачах. Мережа з маршрутизацією IP - пакетів підтримує одночасно різні протоколи маршрутизації: RIP, IGRP, EIGRP, IS-IS, OSPF та інші.

1.1.5 Питання безпеки в мережі IP-телефонії на базі протоколів [10].

1.1.5.1 Забезпечення безпеки в мережах на базі H.323.

Як що для IP-телефонії, побудованих на базі Рекомендації ITU-T H.323, то питання безпеки розглядаються в Рекомендації H.235. В системі повинні бути реалізовані такі основні функції безпеки: автентифікація; цілісність даних; секретність; перевірка відсутності боргів.

Автентифікація користувача виконується приватником (адміністратором зони H.323), ґрунтується на використанні електронних ключів.

Криптографічний захист забезпечує цілісність даних і секретність.

Стандарти: IP-безпека (IP Security - IPSec) і безпека транспортного рівня (Transport Layer Security - TLS) є базовими стандартами для забезпечення безпеки відповідно до Рекомендації H.235. На базі Рекомендацій H.323 використовуються механізми захисту інформації каналу керування викликом Q.931, інформації каналу керування для мультимедіа комунікацій H.245 та інформації каналів передачі мультимедіа. Канал управління викликом (H.225.0) і канал сигналізації (H.245) повинні обидва працювати в захищених або незахищених режимах. Для каналу керування викликом, захист відповідний до Рекомендації H.323; безпека транспортного рівня забезпечується протоколом TSAP [порт 1300] для Q.931

повідомлень; для каналу сигналізації захисний режим визначається інформацією, переданою за допомогою протоколу початкової установки і підключення терміналів стандарту H.323.

Складність розробки і використання систем IP-телефонії на базі стандарту H.323 це основний недолік мережі, H.323 охоплює кілька рівнів моделі OSI.

1.1.5.2 Забезпечення безпеки в мережах на базі протоколів SIP і MGCP

SIP протокол використовується абонентськими пунктами для встановлення з'єднання. SIP має слабку захищеність. Для усунення цього недоліку застосовуються методи захисту інших фірм. Використовуються стандартні методи захисту, пов'язані з протоколом IP, які розроблені «інженерною групою Інтернет» (IETF) компанія Cisco Systems. Коли необхідно підтримати послуги в галузі безпеки для інших мережевих протоколів, які не мають подібних стандартних рішень, використовується метод тунелювання цих протоколів за допомогою протоколу IP. Проект стандарту «SIP security framework» (Cisco Systems), описує зовнішні і внутрішні загрози для протоколу SIP та способи захисту від них. До таких способів можна віднести захист на транспортному рівні за допомогою протоколу захисту транспортного рівня TLS або IPSec

Протокол MGCP використовує для захисту голосових даних протокол інкапсуляції зашифрованих даних ESP специфікації IPSec, а також протокол для ідентифікації відправника AH, який забезпечує автентифікацію і цілісність даних (connectionless integrity) і захист від повторень, переданих між шлюзами. Протокол AH не забезпечує конфіденційності даних, яка досягається застосуванням ESP (поряд з іншими трьома захисними функціями) [10].

Протокол MGCP не призначений для управління з'єднаннями з участю термінального обладнання користувачів (IP-телефонів). В мережі, побудованої на базі протоколу MGCP, для управління термінальним устаткуванням повинен бути присутнім сервер SIP.

1.1.5.3 Питання безпеки TIPHON і стандарту OSP.

Проект TIPHON стосується аспектів захисту і безпеки. Ідея проекту TIPHON з’явилася під впливом ринку телекомунікаційних послуг; зростаючої потреби телефонного зв'язку в мережах, що реалізують технологію маршрутизації пакетів IP. Завданням TIPHON є створення єдиної мережевої інфраструктури, привабливої для операторів різних видів зв'язку, рішення проблем взаємодії між мережами з маршрутизацією пакетів IP і мережами з комутацією каналів. [10, 33, 34]. Проект TIPHON призначений для спрощення процесу впровадження технології IP-телефонії [10, 33].

Реалізація проекту TIPHON вирішує завдання встановлення, модифікації і завершення телефонних з'єднань, включаючи процеси між мережевої взаємодії, управління безпекою виклику, запиту якості обслуговування, шифрування, автентифікації і інші [10, 33].

TIPHON передбачає первинний захист мережі від випадкових або навмисних пошкоджень. До проекту внесені механізми захисту щодо здійснення безпеки телефонного зв'язку з кінцевих пристроїв, застосуванні рекомендації ITU-T H.323. Такі механізми захисту засновані на: цифрових сертифікатах (CBSP); паролях (PBSP); шифруванні інформації. Використання цифрових сертифікатів є основним механізмом захисту, реалізація функцій безпеки показана в табл.1.1

Таблиця 1.1 Механізм безпеки TIPHON, заснований на сертифікатах

Функції безпеки	Функції обслуговування викликів		
	RAS	H225.0	H245
Аутентифікація	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А
Відмова при наявності боргів	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А
Цілісність інформації	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А	Цифрова підпис SHAI/MD5 /Процедура А
Управління ключами	Розподіл сертифіката	Розподіл сертифіката і обмін ключами для аутентифікації по алгоритму Даффі-Хофмана	Управління спільним ключем H 235 (розподіл ключа, зміна ключа)

1.2 Визначення інформаційної безпеки

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено законами, за якими трактується широке поняття «інформаційна безпека», та для питання, що розглядається, рекомендовано [28,36,37] використовувати термін «інформаційна безпека» у вузькому сенсі, як прийнято в англомовній літературі: «Інформаційна безпека – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури». Трактування поняття, що пов'язане з інформаційною безпекою, для різних суб'єктів може дуже різнитися тому пропонують [36] використовувати термін «комп'ютерна безпека».

Визначення «захист інформації» базується на основі системного підходу до інформаційної безпеки, трактується [36] так: «система захисту інформації – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз».

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають [38, 40].

1.2.1 Законодавчі вимоги і регулювання інформаційної безпеки

1.2.1.1 Українське законодавство в галузі інформаційної безпеки

Правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки складають: Конституція України, Концепція (основи державної політики) національної безпеки України, інші законодавчі акти, що регулюють відносини в інформаційній сфері.

Вітчизняне законодавство [37-40] має ряд нормативно-правових документів та законів, що призначені для забезпечення інформаційної безпеки держави.

Важливими є Закони України: Про захист інформації; Про телекомунікації; Про захист персональних даних; Про захист інформації в автоматизованих

системах; Про Державну таємницю; Указ Президента України Стратегія кібербезпеки України; Положення про технічний захист в Україні; Інструкція щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за її дотриманням та інші. До загальнодержавних нормативних актів з питань захисту інформації відносяться такі: ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття; ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт; ДСТУ 3396.2-97. Основною складовою політики національної безпеки є політика євроінтеграції. Формами зближення законодавств є гармонізація та уніфікація. Процес зближення законодавств є багатоетапним [37].

Законодавство у галузі інформаційної безпеки відповідає міжнародним стандартам і цей процес продовжує динамічно розвиватися.

Основоположними в сфері управління інформаційною безпекою є Міжнародні стандарти серії ISO (ISO/IEC 17799, ISO 27001). Це модель, яка визначає загальну організацію та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику. Аналогом стандарту ISO 27001 є ДСТУ ISO/IEC 27001:2015, який визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації» [41].

1.2.1.2 Зарубіжне законодавство в галузі інформаційної безпеки

Законодавчий рівень інформаційної безпеки найбільше забезпечений у США, де нараховується близько 500 законодавчих актів [36]. Закон про інформаційну безпеку (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988) є ключовим. Його мета - реалізація дій для забезпечення безпеки інформації у федеральних комп'ютерних системах, без обмежень всього спектра можливих дій. У 2001р. був схвалений законопроект - Computer Security Enhancement Act of 2001 (H.R. 1259 RFS), який дозволив не загострювати увагу на криптографії в цілому, а зосередитися на одному з її найважливіших додатків – автентифікації. Першим оцінним стандартом, що набув значного поширення і зробив величезний

вплив на базу стандартизації інформаційної безпеки у багатьох країнах, став стандарт Міністерства оборони США. Критерії оцінювання довірених комп'ютерних систем. За кольором обкладинки її звуть «Помаранчевою книгою». Опубліковано у 1983р. Мова йде не про безпечні, а про довірені системи, яким можна надати ступінь довіри [36,40,42].

У законодавстві ФРН основним є "Закон про захист даних" (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325). Він присвячений захисту персональних даних. Встановлюється пріоритет інтересів національної безпеки над збереженням таємниці приватного життя.

У законодавстві Великобританії є ряд стандартів BS 7799, що допомагають організаціям на практиці сформувати програми безпеки.

У сучасному світі глобальних мереж законодавча база повинна бути узгоджена з міжнародною практикою.

1.2.2 Особливості системи безпеки в IP-телефонії

В IP-телефонії передбачені два рівня безпеки: системний і викличний [34].

Для системної безпеки використовуються такі функції: запобігання несанкціонованого доступу до мережі - застосування кодового слова, яке розділяється; списки доступу, в які вносяться всі відомі шлюзи IP-телефонії; запис відмов у доступі; безпеки інтерфейсу доступу та перевірка ідентифікатора і пароля користувача, перевірка прав доступу до спеціального WEB-сервера, забезпечення безпеки виклику з необов'язковою перевіркою ідентифікатора і пароля користувача, статус користувача, профіль абонента.

При встановленні зв'язку шлюзу з іншим шлюзом своєї зони проводиться необов'язкова перевірка ідентифікатора і пароля користувача.

Сучасна технологія програмування не дозволяє створювати безпомилкові програми, тому необхідно конструювати надійні системи інформаційної безпеки.

Це вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу інформаційної системи.

Базовими елементами є: автентифікація; цілісність; активна перевірка[17].

Під автентифікацією розуміється процедура ідентифікації користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, і т. п.).

Механізми автентифікації: використання паролів; механізм автентифікації по протоколу PPP застосовується в середовищі модемного доступу і включає використання протоколів PAP, CHAP і EAP; TACACS +RADIUS - це протоколи, які підтримують рішення автентифікації; протокол Kerberos використовується в обмежених під час підтримки єдиної точки входу в мережу.

Цілісність інформації - це здатність засобів обчислювальної техніки або автоматизованої системи забезпечувати незмінність інформації в умовах випадкового і (або) навмисного спотворення (руйнування). Активна перевірка даних означає перевірку правильності реалізації елементів технології безпеки, виявляє несанкціоноване проникнення в мережу і атаки типу DoS.

1.2.3 Недоліки та вразливості IP-телефонії

Основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту є виявлення недоліків та вразливостей IP-телефонії, класифікація загроз, оцінка ймовірності реалізації конкретної загрози.

Для функціонування мережі IP-телефонії потрібна велика кількість інфраструктурних компонентів. На практиці часто використовують неспеціалізовані операційні системи для підтримки функціонування IP-мережі, такі мережі мають усі уразливості характерні для вказаних систем.

До основних загроз, яким піддається IP-телефона мережа [20,22,23], відносять такі: реєстрація чужого терміналу; підміна абонента; внесення змін до голосового, або сигнального трафіку; зниження якості голосового трафіку; перенаправлення та перехоплення головного або сигнального трафіку; підробка голосових повідомлень; завершення сеансів зв’язку; відмова в обслуговуванні;

віддалений несанкціонований доступ до інфраструктури IP-телефонії; несанкціоноване оновлення (впровадження троянської або шпигунської програми); зламування білінгової системи (для операторської телефонії).

Система реальних і потенційних загроз не є постійною, тому змінюється їхня значимість для безпеки. Класифікацію загроз подано в додатку А.

До інформаційної безпеки в мережах IP- телефонії відносять [17]: прослуховування - під час передачі конфіденційної інформації про користувачів або конфіденційних даних по незахищених каналах; маніпулювання даними, які передаються по каналах зв'язку; відмова в обслуговуванні DoS.

Щодо керованості та продуктивності IP-телефонії найбільш доцільною є така, де всі компоненти захисту вбудовані в елементи і захисні механізми IP-мережі, це дозволяє досягти відносно стійкого захисту від атак на периметрі [22,23].

Нові вразливі місця, що з’являються в програмному забезпеченні, впливають на появу нових видів атак [36], яким повинні протистояти системи безпеки.

Існує кілька способів підвищення безпеки мережі: впровадження нових протоколів шифрування інформації; жорсткий контроль трафіку; додаткове стиснення пакетів даних; криптографічна автентифікація.

Вбудована в архітектуру IP-мережі система управління викликами, може під’єднуватися до спеціально виділеної локальної інформаційної мережі інфраструктури, ізольованої від робочої мережі організації [20,22,35].

1.2.4 Визначення загроз інформаційної безпеки ІТ

1.2.4.1 В англійській мові поняття безпеки ІТ має два значення. Визначення функціональної безпеки (англ. Safety) означає, що система у повному обсязі реалізує лише ті цілі, що відповідають намірам її власника. Поняття інформаційної безпеки (англ. Security) стосується безпеки технічної обробки інформації і є властивістю функціонально безпечної системи, яка повинна запобігати несанкціонованому доступу до даних і їх втраті під час збоїв.

Принципи забезпечення інформаційної безпеки включають в себе: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграцію з міжнародними системами безпеки; економічну ефективність [38,40]. Методи забезпечення інформаційної безпеки проілюстровані на рис. 1.4.

Рис. 1.4 Методи інформаційної безпеки

1.2.4.2 Загрози безпеки інформаційних технологій

Впливи, які знижують цінність інформації, називаються несприятливими. Потенційно можливий несприятливий вплив називається загрозою.

Під час створення системи захисту інформації визначаються загрози безпеці інформації, джерела загроз, способи реалізації і мету, інші дії, що порушують безпеку. Враховуються заходи захисту інформації від неправомірних дій, що призводять до збитку.

Загроза безпеці інформації (англ. Security threat) - загрози викрадення, зміни або знищення інформації [38, 40]. Під загрозою розуміють події, які можуть принести втрати - привести до розладу, спотворення, несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається, обробляється, та програмні і апаратні засоби.

Для наочності безпеки інформації автори [36] за допомогою методів моделювання описують реальні дії щодо безпеки інформації з урахуванням їх складності на прикладі концептуальної моделі, що наведена на рис. 1.5: з одного

боку, це інформація, що захищається, а з іншого – загрози цій інформації. Загрози реалізуються шляхом способів доступу, та їм перешкоджає захист інформації.

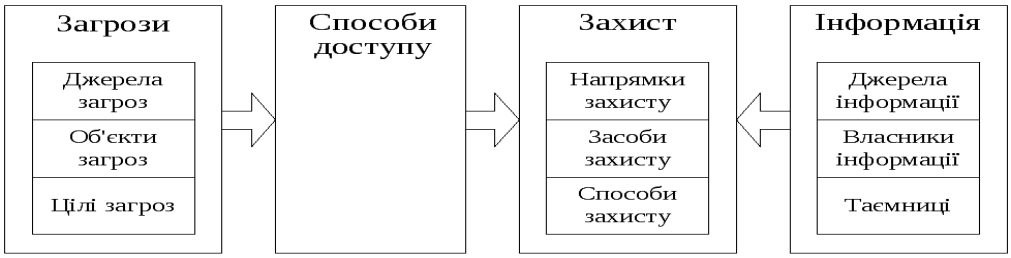

Рис. 1.5 Концептуальна модель безпеки інформації

Не існує єдиної загальноприйнятої класифікації загроз, є багато варіантів.

Загрози діляться на випадкові (або ненавмисні) і навмисні.

Джерелом перших можуть бути помилки в забезпеченні, виходи з ладу апаратних засобів, невірні дії користувачів/адміністрації локальної обчислювальної мережі, тощо. Навмисні загрози наносять шкоду користувачам/абонентам локальної мережі, вони діляться на активні і пасивні. Пасивні загрози спрямовані на несанкціоноване використання інформаційних ресурсів локальної обчислювальної мережі, не впливають на її функціонування. Активні загрози прагнуть порушити функціонування локальної обчислювальної мережі шляхом цілеспрямованого впливу на її апаратні, програмні і інформаційні ресурси. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси тощо [40].

Найнебезпечнішими є ненавмисні помилки осіб, які обслуговують інформаційні системи. Створюються вразливі місця, якими можуть скористатися зловмисники, до 65% втрат наслідок ненавмисних помилок [40]. Способи боротьби з ними – це максимальна автоматизація і строгий контроль.

Загрози доступності [40] класифікуються за компонентами ІС, на які спрямовані загрози: відмова користувачів; інформаційної системи; інфраструктури. Основними джерелами внутрішніх відмов є: порушення правил

експлуатації; вихід системи зі штатного режиму експлуатації; помилки при (пере)конфігурації системи; відмови програмного і апаратного забезпечення.

Віддалене споживання ресурсів –це може бути атака, її називають “SYN-повінь”. Атака ускладнює встановлення з’єднань з боку користувачів, сервер виглядає як недоступний. По відношенню до атаки “Papa Smurf” уразливі мережі ті, що сприймають ping-пакети з широкомовними адресами. Програма “Teardrop” “підвішує” комп’ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів. Відмови програмного забезпечення провокуються впровадженням в ІС шкідливого програмного забезпечення.

Загрози конфіденційності [40]. Конфіденційну інформацію можна поділити на службову та предметну. Службова інформація (паролі) в ІС грає технічну роль, її розкриття небезпечне, оскільки може забезпечити несанкціонований доступ до всієї інформації, зокрема предметної. Можливе розміщення конфіденційних даних у середовищі, з не забезпеченим захистом. Це є компонентом вразливих місць. Для атаки використовуються різні технічні засоби, але здійснюється доступ до даних у час найменшої захищеності.

Загрози в програмному забезпеченні [40]. Найнебезпечнішим способом здійснення атак є впровадження в ІС шкідливого програмного забезпечення, що має характеристики: шкідлива функція; спосіб розповсюдження; зовнішнє представлення. Шкідливі програми мають складну логіку, призначені для: впровадження іншого шкідливого програмного забезпечення; отримання контролю над системою; агресивного споживання ресурсів; зміни/руйнуванні програм/даних. За механізмом розповсюдження розрізняють такі види: віруси – коди, що мають здатність до розповсюдження шляхом впровадження в інші програми; «хробаки»– коди, які самостійно, викликають розповсюдження своїх копій в ІС; троянські програми – програми направлені на перехоплення даних.

Віруси розповсюджуються локально, в межах вузла мережі. «Хробаки» орієнтовані на подорожі мережею. Розповсюдження шкідливого програмного

забезпечення викликає агресивне споживання ресурсів і є шкідливою функцією. Шкідливий код, який виглядає як функціонально корисна програма, називається троянським. Перетином їхнього існувати стає оновлення бази даних антивірусних програм і інші.

Дія шкідливого програмного забезпечення буває спрямована проти доступності і інших аспектів інформаційної безпеки.

Інформаційна безпека в мережах. Телекомунікаційна мережа - організаційно-технічна система, що об’єднує систему надання послуг, систему управління, транспортну систему, мережу доступу, фізичне середовище, персонал та оброблювану інформацію.

На рівні бізнесу потенційні вороги це конкуренти та хакери. [38, 40]. Для захисту цінних даних необхідно знати весь перелік загроз безпеки. (рис.1.6).

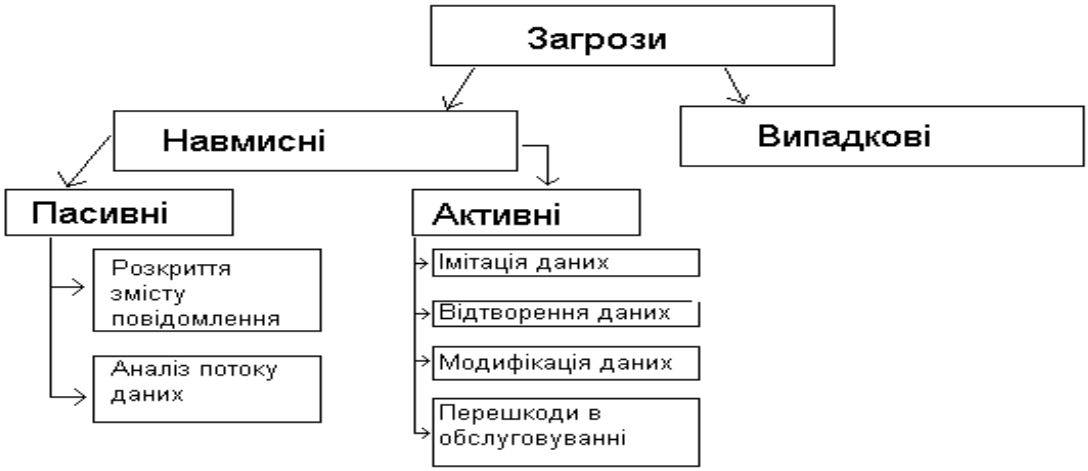

Рис. 1.6 Загрози інформаційної безпеки в мережах

Загрози інформаційної безпеки в каналах витоку інформації

Система зв’язку складається з джерела інформації, передавача, лінії зв’язку, приймача і одержувача інформації. Ці системи використовуються відповідно до свого призначення і є офіційними засобами передачі інформації, робота яких контролюється з метою забезпечення надійної, достовірної і безпечної передачі інформації, що виключає неправомірний доступ до неї з боку конкурентів. [36]. Існують умови для утворення системи передачі інформації з однієї точки в іншу

незалежно від бажання об’єкта і джерела. Такий канал називають каналом витоку інформації. Він складається з джерела сигналу, фізичного середовища його розповсюдження і приймальної апаратури на стороні зловмисника. Рух інформації здійснюється від джерела до зловмисника. При виявленні каналів витоку інформації треба розглядати всю сукупність комп'ютерного обладнання, враховувати допоміжні технічні засоби і системи.

1.3 Основні підходи до забезпечення інформаційної безпеки

Питання інформаційної безпеки розподілених систем, специфічні мережеві функції (сервіси) безпеки та необхідні для їх реалізації захисні механізми трактуються за стандартом Технічна специфікація X.800 [36].

1.3.1 Напрями захисту інформації

Захист інформації здійснюють за такими напрямами [31]: правовий – розробка норм, що встановлюють відповідальність за комп’ютерні злочини, включаючи в системах IP- телефонії та в сфері технічного захисту інформації та удосконалення законодавства; організаційний - формування політики безпеки об’єкта, його охорони, наявність плану відновлення працездатності, організацію обслуговування особами, не зацікавленими в прихованні фактів порушення, добір персоналу і покладання відповідальності, вибір місця розташування об’єкта і інші; технічний захист інформації - захист від несанкціонованого доступу до системи, шифрування файлів, резервування підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих елементів, контроль електромагнітного й акустичного стану простору, виявлення каналів витоку інформації і інші.

1.3.2 Основні класи засобів захисту інформації телекомунікаційних систем

Застосовуються такі класи засобів захисту інформації: засоби фізичного захисту - включають системи розмежування доступу, засоби захисту кабельної системи, ідентифікації об’єктів і систем електроживлення, засоби архівації, дискові масиви, системи пригнічення побічних електромагнітних

випромінювань, акустичних каналів витоку, інші; програмні засоби захисту (антивірусні програми), - криптографічні, системи розмежування повноважень, програмні засоби контролю доступу, інші; адміністративні міри захисту - контроль доступу в приміщення, розробку стратегії безпеки фірми, планів дій у надзвичайних ситуаціях і інші.

1.4 Базові елементи в області безпеки - автентифікація, цілісність і активна перевірка.

1.4.1 Забезпечення властивості для мережі

Автентифікація покликана запобігти загрозі знеособлення і несанкціонованого доступу до ресурсів і даних.

Цілісність забезпечує захист від підслуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність переданої інформації.

Активна перевірка - перевірка правильності реалізації елементів технології безпеки. Виявляє несанкціоноване проникнення в мережу і атаки типу DoS.

І для елемента мережі, і для всієї мережі треба забезпечити властивості:

конфіденційності - гарантія того, що дані будуть доступні тільки авторизованим користувачам;

цілісності - гарантія збереження правильних значень даних, що забезпечується забороною для неавторизованих користувачів будь-яким чином змінювати, модифікувати, руйнувати або створювати дані;

доступності - гарантія для користувачів одержати доступ до даних.

Виділяють в [36] виконувані ролі для цього сервісів безпеки.

1.4.1.1 Види автентифікації

У телекомунікаційних системах використовують такі види [31] автентифікації: об’єкт може продемонструвати знання якого-небудь загального для сторін секрету - слова (пароля) або факту (дати й місця події, прізвиська людини тощо); об’єкт може довести, що він володіє унікальним предметом (фізичним ключем - електронною магнітною картою, електронним ключем, смарт-картою й ін.) або

файлом; якщо об’єктом є людина, то він може довести свою ідентичність, використовуючи власні біометричні характеристики, які занесені в базу даних автентифікатора.

Використовуються варіанти автентифікації: локальна автентифікація - її можна бачити в персональних системах без підключення до мережі; пряма автентифікація - зустрічається в старих серверних системах, що використовуються у локальних обчислювальних мережах (ЛОМ), та в системах з поділом часу - мейнфреймах; непряма автентифікація - зустрічається в сучасних мережних серверних системах і в тих, що може бути реалізована, через протоколи RADIUS, TACACS, Kerberos і протокол реєстрації в домені безпеки; автономна автентифікація - зустрічається в системах з інфраструктурою відкритого ключа, що містять численні автономні компоненти, які здатні приймати точні рішення з управління доступом і якщо не можуть зв’язуватися з іншими системами для одержання авторитетних рішень з автентифікації.

Сучасні дослідження методів автентифікації визначені в роботі [44] результатами досліджень, що були проведені на основі ресурсної бази ІТС НТУУ «КПІ». Досліджені методів автентифікації, які можна використати для побудови середовища з некластеризованими ресурсами і динамічною архітектурою.

Метод EAP – TLS у системах безпеки при перевірці достовірності сертифікатів сервера та клієнта, він забезпечує найбільш надійний метод перевірки автентичності та визначення ключа.

Метод EAP - TTLS має двофазну структуру. У першій фазі створюється захищене тунельоване з’єднання, в другій відбувається передача даних для авторизації. У другій фазі може використовуватися як TLS так і старі механізми – PAP або CHAP. Метод PEAP функціонує аналогічно EAP - TTLS за принципом двофазної автентифікації. У першій фазі за допомогою протоколу TLS створюється зашифрований канал зв'язку між саплікантом та сервером. Протокол PEAP не визначає метод перевірки автентифікації, а забезпечує додаткову

безпеку для інших протоколів перевірки автентифікації EAP, наприклад EAP - MSCHAPv2, GTC чи TLS, які можуть працювати через зашифрований канал протоколу TLS. На відміну від EAP-TLS, де реалізована перевірка сертифікатів і зі сторони користувача, і зі сторони сервера, у методі PEAP – MS - CHAPv2 сертифікат видається тільки серверу, перевірка автентичності користувача є на підставі облікових даних.

Метод EAP - FAST - використовує захищений доступ облікових даних для створення тунелю TLS, в якому облікові дані клієнта і передаються.

Метод EAP - GTC метод, в якому інформація про автентифікацію знаходиться у USB - ключі або смарт - карті клієнта, за допомогою яких відбувається передача даних для автентифікації [44].

Отримані результати досліджень механізмів автентифікації 802.1x та EAP на базі порівняльного аналізу актуальних методів автентифікації для проводових і Wi-Fi мереж та аналізу сучасних операційних систем на предмет підтримки ними методів автентифікації, свідчать про можливість і доцільність використання EAP-PEAP-MSCHAPv2 для побудови гетерогенного середовища для розміщення і виконання веб сервіс - компонентів розподілених інформаційних систем на основі існуючої ресурсної бази із динамічним підключенням робочих вузлів.

1.4.1.2 Засоби ідентифікації й авторизації

Засоби ідентифікації й авторизації, що реалізуються в одній підсистемі, дозволяють визначити приналежність ресурсу мережі об’єкта та реалізувати механізм причетності для здійснення спроби обігу/впливу на ресурс. Такі засоби контролюють доступ об’єктів до ресурсів системи, надаючи об’єкту ті права, які йому були визначені відповідальною особою.

Ідентифікація може відбуватися за різними схемами, залежно від необхідності забезпечення заданого рівня безпеки, швидкості роботи підсистеми безпеки й наявності достатньої кількості системних ресурсів.

Найчастіше використовують такі схемам ідентифікації [31]: метод матриці доступу - для кожної пари суб’єкт — об’єкт у матриці доступу існує частина, у якій задаються права суб’єкта на цей об’єкт; метод використання списків доступу є модифікацією підходу з використанням матриці доступу, є економічним щодо витрат пам’яті, але вимагає більше часу на обчислення прав;

метод мітки рівня таємності і категорії доступу видаються кожному інформаційному об’єкту чи суб’єкту мітки. Рівень — це число, що визначає конфіденційність інформації й ступінь довіри суб’єкту. Цей метод є найбільш ефективним для складних розподілених систем обробки інформації. Недоліками є складність визначення конкретної множини об’єктів, що мають доступ, а також складніші правила передачі прав об’єктам.

Висновки до розділу

Незважаючи на існуючу вразливість, IP телефонія успішно розвивається, є одним з найбільш популярних і доступних видів зв'язку ринок послуг IP-телефонії останнім часом росте високими темпами. Питання, пов’язані з методами забезпечення інформаційної безпеки в IP-телефонії є актуальними.

В першому розділі надана стисла характеристика IP- телефонії і існуючих протоколів з точки зору інформаційної безпеки, розглянуті питання безпеки інформації, визначені основні загрози і основні підходи до забезпечення інформаційної безпеки, охарактеризовані базові елементи в області безпеки, описані законодавчі вимоги і регулювання інформаційної безпеки. Відзначено про відсутність єдиного підходу в трактуванні базових понять в законодавчій базі, що є негативним моментом.

2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ IP- ТЕЛЕФОНІЇ

2.1 Системи заходів для запобігання або ускладнення можливості реалізації загроз

Діяльність з забезпечення безпеки інформації систем IP-телефонії здійснюється за допомогою різних способів, засобів, прийомів, які у сукупності складають методи. Метод передбачає послідовність дій на підставі конкретного плану. Методи можуть змінюватися і варіюватися в залежності від діяльності, де використовуються, та сфери застосування [38].

Прийнято розрізняти два основних напрями забезпечення інформаційної безпеки та захисту інформації – це захист мережі і оброблюваної інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами. Методи забезпечення інформаційної безпеки в залежності від способу їх реалізації класифікують так: організаційні, технологічні, апаратні.

Технічний захист цифрової інформації забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів.

Істотна частина проблем забезпечення інформаційної безпеки та захисту інформації може бути вирішена організаційними методами, що передбачають організацію, адміністрування системи, раціональну конфігурацію [36].

Інженерно-технічний захист є сукупність спеціальних органів, технічних засобів і заходів їх використання в інтересах конфіденційної інформації.

За функціональним призначенням засоби інженерно-технічного захисту поділяються на: фізичні засоби і споруди; апаратні засоби, їх основна задача є забезпечення стійкого захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби виробничої діяльності; програмні засоби, які охоплюють спеціальні програми, програмні комплекси і системи захисту інформації в ІС; криптографічні і стеганографічні засоби.

2.2 Характеристика методів захисту інформації фізичними засобами

Фізичні засоби захисту необхідні для зовнішнього захисту засобів комп’ютерної техніки, об'єктів створення фізичних перешкод в проникнення і доступу порушників до компонентів інформаційних систем та інформації, що захищаються. Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу використання замкненого контуру захисту.

Фізичні засоби захисту - пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників. Це механічні, електромеханічні, електронні, електронно-оптичні, радіо-радіотехнічні пристрої, екрани, інші для заборони несанкціонованого доступу до засобів інформації і можливих видів злочинних дій.

2.3 Методи захисту інформації програмно - апаратними засобами

Телекомунікаційні системи виконані з передавальних і приймальних пристроїв, апаратури обробки, реєстрації, зберігання й відображення інформації. До них віднесені радіотехнічні, оптико-електронні, інфрачервоні, лазерні, акустичні, гідроакустичні засоби. Ці системи можуть бути джерелом витоку конфіденційної інформації [31].

Апаратні засоби захисту інформації є різними за принципом дії, побудовою, можливостями технічних конструкцій для припинення розголошення, захисту від витоку і протидії несанкціонованому доступу до джерел конфіденційної інформації [36]. Апаратні засоби вмонтовуються в блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки. Основні функції апаратних засобів захисту: заборона неавторизованого зовнішнього доступу віддаленого користувача; заборона несанкціонованого внутрішнього доступу до баз даних в результаті випадкових чи умисних дій персоналу; захист цілісності програмного забезпечення. Функції реалізуються шляхом: ідентифікації; автентифікації за наданим ідентифікатором; перевірки повноважень відповідності з дозволом на певні види робіт; реєстрації при

звертаннях до заборонених ресурсів; реєстрації спроб несанкціонованого доступу.

Реалізація функцій здійснюється за допомогою технічних пристроїв спеціального призначення.

Вдосконаленням процедури пошуку ЗП є застосування програмно-апаратних комплексів радіоконтролю й виявлення каналів витоку інформації, їхні можливості значно ширші, ніж у сполучених з ЕОМ сканувальних приймачів. Можливості: виявлення випромінювань радіозакладок; пеленгування; визначення дальності до джерел випромінювання; аналого-цифрова обробка сигналів для визначення їх приналежності; контроль мереж; роботи в багатоканальному режимі для одночасного контролю декілька об’єктів; постановки перешкод на частотах випромінювання радіозакладок.

Програмні методи - це програми ідентифікації користувачів паралельно захисту і перевірки повноважень, брандмауери, крипто-протоколи та ін., вони є найпоширенішими методами забезпечення безпеки інформації систем.

За їх допомогою реалізуються задачі безпеки: контроль завантаження та входу в систему за допомогою системи паролів; розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних; захист файлів від вірусів; контроль за роботою користувачів шляхом протоколювання дій. Без використання програмної складової нездійсненні ніякі групи методів.

2.4 Характеристика методів криптографічного захисту інформації.

2.4 1 Криптографічний метод - основа будь-якого захищеного зв'язку

Криптографічний метод являє собою технологію складання і розшифрування закодованих повідомлень та є важливою складовою для автентифікації; засобів забезпечення цілісності і конфіденційності[36].

Впровадження криптографічних технологій, спрямовані на забезпечення конфіденційності і працездатності мережевих додатків. Криптографічне закриття

інформації виконується шляхом перетворення інформації за алгоритмом з ключами і процедурами шифрування. Криптографічні протоколи забезпечують безпечну передачу інформації по мережі.

2.4.2 Основні визначення метода криптографічного захисту інформації

Криптографія займається методами перетворення інформації, які б не дозволили зловмиснику витягти її з повідомлень, що перехоплюються [36]. Криптографічні методи перетворення даних спрямовані на приховання інформаційного змісту. Сукупність криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів [31] представляють криптографічну систему захисту. Узагальнену схему криптографічної системи показано на рис. 2.1. [31].

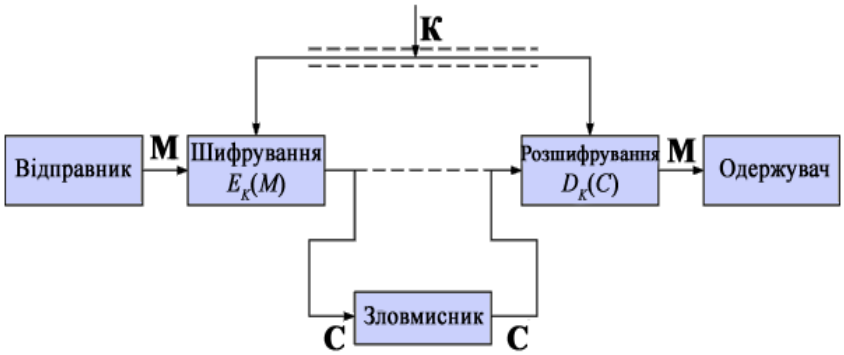

Рис. 2.1. Узагальнена схема криптосистеми

2.4.3 Характеристики метода криптографічного захисту інформації [31].

Криптографічні системи класифікуються на основі характеристик: тип операцій з перетворення відкритого тексту шифрований; число ключів, що використовуються; метод обробки відкритого тексту.

Використовують два типи шифрування: симетричне і асиметричне[31,49], а у системах забезпечення безпеки використовуються три криптографічних методи: симетричне, асиметричне шифрування та односторонні хеш-функції. Це основа створених технологій автентифікації, цілісності, конфіденційності.

При симетричному шифруванні даних застосовується один секретний ключ, який передається секретним способом до початку передачі даних.

У симетричному шифруванні застосовуються шифри: блокові і потокові.

Якщо блокові - то вихідне повідомлення ділиться на блоки постійної довжини, кожен з яких перетворюється за певними правилами в блок зашифрованого тексту.

Потокові шифри оперують з окремими бітами і байтами вихідного повідомлення і ключа. Потокові шифри мають високу крипостійкість, але використовують довгі ключі.

При симетричному шифруванні якщо ключ стане відомим хакеру, той може перехопити повідомлення і підмінити його. Для захисту від цього можна використовувати систему цифрових сертифікатів - документів, які видаються сертифікаційної службою СА і містять інформацію про власника сертифіката, зашифровану за допомогою закритого ключа цієї організації.

Крипостійкість асиметричного шифрування забезпечується складною заданою комбінацією, яку вирішити перебором кодів не можливо.

На практиці крипто-протоколів спільно використовують і симетричне, і асиметричне шифрування.

Чим більше бітів в криптографічному ключі, тим менше він вразливий[31].

Популярними є крипто-алгоритми (які забезпечують найбільш надійний захист інформації), що наведено в табл. 2.1.

Таблиця 2.1 Приклади популярних криптоалгоритмів/схем шифрування

Вид системи	Назва алгоритму	Довжина ключа, біт	Розробники технологій
Симетричні	Rijndael (AES)	128—256	J. Daemon, V.Rijmen, Бельгія
	SNOW	128, 256	Lund University, Швеція
	RC6	128—256	RSA Security, США
	3DES	168	Стандарт ANSI X9.52-1998
	MARS	128—400	IBM Corporation, США
	TwoFish	128—256	B. Schneir, США
	SERPENT	128—256	R. Anderson, E. Biham, L. Knudsen
	ГОСТ 28147-89	256	Держстандарт СРСР, стандарт гармонізовано (ДСТУ 28147:2009)
Асиметричні	RSA	1024—4096+	RSA Laboratories, США
	RSA-OAEP	1024—4096+	RSA Laboratories Europe, Швеція
	ACE Encrypt	1024—4096+	IBM Zurich Research Laboratory, Швейцарія
	EPOC	1024—4096+	Nippon Telegraph and Telephone, Японія

Крипто-алгоритми (табл.2.1) здатні забезпечити захист від: диференційного крипто-аналізу; пошуку найкращої диференційної характеристики; лінійного крипто-аналізу; інтерполяційного вторгнення; вторгнення із частковим угадуванням ключа; вторгнень на основі апаратних помилок; пошуку лазівок.

2.5 Характеристика методів стеганографічного захисту інформації

2.5 1 Основні напрями класичної стеганографії [38,48].

Розробкою засобів і методів приховування факту передавання повідомлення займається стеганографія. Стеганографія - це методи організації зв'язку, які приховують саму наявність зв'язку. До стеганографії належить безліч секретних засобів зв'язку (умовне розташування знаків, таємні канали та засоби зв'язку на плаваючих частотах тощо).

Сьогодні йде накопичення і узагальнення матеріалу по стеганографії, створення узагальнюючої теорії, вирішення малодосліджених прикладних задач[48].

2.5 1.1 Мережева стеганографія [38, 48, 52-54, 58]

Набули популярності методи, коли прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Методи отримали назву «мережева стеганографія». Мережева стеганографія - в якості носіїв секретних даних використовуються протоколи моделі OSI. У загальному вигляді мережева стеганографія є сімейством методів по модифікації даних в заголовках мережевих протоколів і в полях корисного навантаження пакетів, саме структури передачі пакетів і гібридних методів в мережевому протоколі.

Передача прихованих даних в мережевій стеганографії здійснюється через приховані канали, що можуть існувати у відкритому каналі, в якому існує надмірність. Приховувані дані називають стеганограммой.

Пропускна здатність прихованого каналу, ймовірність виявлення та стеганографічна вартість є основними параметрами мережевої стеганографії.

Ймовірність виявлення - визначається за можливістю виявлення стеганограми в носії. Аналіз статистичних властивостей, отриманих даних і порівняння їх з типовими значеннями для цього носія є способом виявлення стеганограми. Стеганографічна вартість характеризує ступінь зміни носія після впливу на нього стеганографічного методу [38].

Методи [58] модифікації пакетів включають методи: зміни даних в полях заголовків протоколу (засновані на модифікації полів заголовків IP, TCP, SCTP); модифікації корисного навантаження пакета (застосовуються алгоритми стеганографічних технік по прихованню даних); змішаних технік.

Модифікація структури передачі пакетів здійснюється методами, в яких змінюється: порядок послідовності пакетів; затримка між пакетами; та методом навмисної втрати пакетів у разі пропуску порядкових номерів.

Головна ідея методів модифікації полів заголовків (поля IP, TCP протоколів) [58]полягає в їх використанні для стеганограми за рахунок деякої надмірності - не використання полів при передачі пакетів. Стеганографія легко реалізовується, має хорошу пропускну здатність і низьку вартість. Використання полів не порушують функцію пакету. Дані містяться у відкритому вигляді; можна ще посилити захист кріптографією.

Метод мережевої стеганографії, призначений для приховання повідомлень VolP, називається TranSteg - метод мережевий стеганографії зі стисненням корисного навантаження мережевого пакету за рахунок перекодування. У TranSteg стиснення даних, використовується, щоб звільнити місце під стеганограму: відбувається перекодування голосових даних з високого бітрейта в більш низький бітрейт, з мінімальною втратою якості голосу, і після стиснення вносяться дані в місце, що звільнилося в області корисного навантаження пакету [58]. Метод дозволяє отримати хорошу стеганографічну пропускну здатність в 32 кб/с і найменшу різницю в затримці пакета.

SCTP (Stream control protocol) - транспортний протокол нового рівня з контролем пакетів, замінить TCP і UDP в мережах майбутнього. Цей протокол реалізується в операційних системах BSD, Linux, HP-UX, SunSolaris, підтримує мережеві пристрої операційної системи CiscoIOS і може бути в Windows. SCTP-стеганографія використовує особливості даного протоколу: мультипоточність, використання множинних інтерфейсів. Методи SCTP- стеганографія поділяються на три групи: в яких змінюється вміст SCTP - пакетів; в яких змінюється послідовність передачі SCTP - пакетів; які впливають на вміст пакету, їх порядок під час передачі (змішані) [58].

Суть гібридного (мішаного) методу на основі SCTP-протоколів полягає в використанні механізмів протоколу, в яких організовують навмисний пропуск пакетів в потоці, без повторної посилки. В цей пакет додається стеганограма, і він повторно відправляється[58].

Метод RSTEG заснований на механізмі повторної посилці пакетів, суть: коли відправник посилає пакет, то одержувач не відповідає пакетом з прапором підтвердження, спрацьовує механізм повторної висилки пакетів і повторно надсилається пакет зі стеганограмою всередині, на який також не приходить підтвердження. При наступному спрацьовуванні даного механізму надсилається оригінальний пакет без прихованих вкладень, на який приходить пакет з підтвердженням про вдале отримання.

LASCK (Lost Audio Packets Steganografy) - стеганографія навмисних затримок аудіо пакетів. Метод здійснюється через VolP. Зв'язок через IP-телефонію складається з двох частин: сигнальної і розмовної. В обох передається трафік в обидві сторони. Використовується сигнальний протокол SIP і RTP (RTCP-керуючого протоколу). Кінцеві точки SIP обмінюються SIP повідомленнями, які проходять через SIP сервера [58-62]. Користувачі знаходять один одного, а потім є фаза розмови - аудіо (RTP) потік в обох напрямках. При навмисному виклику

втрат погіршується якість зв'язку, це викликає підозру. LASK має складність виявлення і реалізації.

У технічній літературі [38,57] характеризують типові методи мережевій стеганографії, що включають зміну властивостей одного з мережевих протоколів, використання взаємозв'язку між різними протоколами з метою надійного приховування передачі секретного повідомлення. Виділяють методи стеганографії: WLAN-стеганографія - ґрунтується на методах передачі стеганограм в бездротових мережах (Wireless Local Area Networks). Приклад: - система HICCUPS; LACK - стеганографія - приховування повідомлень при розмові з використанням IP-телефонії[38, 57-62].

Методи IP і TCP виділяються відносно інших методів: в якості носіїв стеганограми використовуються найпоширеніші і стандартні протоколи; в надають пропускну здатність 49 біт/1 пакет; реалізуються на будь-якій операційній системі, реалізація не вимагає довгих налаштувань і підготувань; зміни в пакеті не вплинуть на поведінку в мережі, якщо не фрагментований.

2.5.1.2 Комп'ютерна стеганографія - заснована на особливостях комп'ютерної платформи (стеганографічна файлова система StegFS для Linux, приховування даних в невикористовуваних областях форматів файлів, підміна символів в назвах файлів, текстова стеганографія і т. п.).

Метод використання зарезервованих полів комп'ютерних форматів файлів - суть в тому, що частина поля розширень, що не заповнена інформацією, за замовчуванням заповнюється нулями. Використовують «нульову» частину для запису своїх даних. Недоліком цього методу є низький ступінь скритності і малий обсяг інформації, що передається.

Метод приховування інформації в невикористовуваних місцях гнучких дисків - інформація записується в невикористовувані частини диска, наприклад, на нульову доріжку. Недоліки: маленька продуктивність, передача невеликих за обсягом повідомлень.

Метод використання особливих властивостей полів форматів, які не відображаються на екрані - метод заснований на спеціальних «невидимих» полях для отримання виносок, покажчиків. Недоліки: маленька продуктивність, невеликий обсяг інформації, що передається.

Використання особливостей файлових систем - при зберіганні на жорсткому диску, файл завжди займає ціле число кластерів. Ті, що ні на що не використовуються можна використовувати для зберігання інформації. Недолік: легкість виявлення.

2.5 1.3 Цифрова стеганографія [38,48,52-54]

Цифрова стеганографія - заснована на приховуванні/впровадженні додаткової інформації в цифрові об'єкти/спотворення об'єктів. Внесення спотворень здійснюється нижче порога чутливості середньостатистичної людини і не призводить до помітних змін. В відцифрованих об'єктах, які мають аналогову природу, присутній шум квантування; при відтворенні об'єктів з'являється ще аналоговий шум і нелінійні спотворення апаратури, це сприяє непомітності прихованої інформації. Цифрова стеганографія (рис.2.2).

Рис.2.2 Методи цифрової стеганографії

Приховування даних у просторовій області [51] здійснюється за допомогою наступних методів:

Метод заміни найменш значущого біта (заміна останніх значущих бітів в контейнері на біти приховуваного повідомлення); метод псевдовипадкового

інтервалу (довільний розподіл бітів секретного повідомлення по контейнеру, відстань між вбудовуваними бітами визначається псевдовипадково); метод псевдовипадкової перестановки (генератор псевдовипадкових чисел утворює послідовність індексів та зберігає k-й біт повідомлення в пікселі з індексом kj, секретні біти рівномірно розподілені по всьому бітовому просторі контейнера); метод блокового приховування полягає в тому, що зображення-оригінал розбивається на неперетинні блоки довільної конфігурації, для кожного з яких обчислюється біт парності. У кожному блоці виконується приховування одного секретного біта.

Приховування даних в аудіо-сигналах [51,52] можливе при використанні наступних методів:

кодування найменш значущих біт (тимчасова область) відбувається шляхом використання звукового сигналу із заміною НЗБ кожної точки здійснення вибірки, представленої двійковою послідовністю;

фазового кодування полягає в заміні фази вихідного звукового сегмента на опорну фазу, характер зміни якої відображає дані, які необхідно приховати;

розширення спектру використовує технологію РСПП, яка розширює сигнал даних, помножуючи його на сигнал несучої та псевдовипадкову шумову послідовність, що характеризується широким частотним спектром;

приховування даних з використанням ехо–сигналу-полягає у вбудовуванні даних в аудіо сигнал-контейнер введенням ехо-сигналу, змінюють параметри ехо-сигналу: початкової амплітуди, швидкості загасання і зсуву.

До методів приховування даних в тексті [51, 52] належать: синтаксичні та семантичні методи. До синтаксичних методів [52] відносять методи зміни пунктуації та методи зміни структури і стилю тексту. Семантичні методи подібні до синтаксичних, вони визначають два синоніми, котрі відповідають значенням приховуваних біт. Для цього потрібна таблиця синонімів.

Методи довільного інтервалу ґрунтуються на трьох методах (заміни інтервалу між реченнями, заміни кількості пробілів у кінці текстових рядків, зміни кількості пропусків між словами вирівняного за шириною тексту). Для приховування даних вони використовують вільне місце в тексті. У деяких джерелах [52] описані вище методи відносять до лінгвістичної стеганографії.

Лінгвістична стеганографія [51,52] – напрям, який вивчає методи приховування конфіденційної інформації в непримітний текст, застосовуючи мовні властивості та лінгвістичні ресурси. Лінгвістичні методи стеганографії поділяються на дві основні категорії: умовне письмо і семаграми. До умовного письма відносять: жаргонний код, геометричну систему, нульовий шифр і шифр «решітка». Жаргонний код передбачає використання непривертаючих увагу слів, які мають зовсім інше реальне значення, а текст складається так, щоб виглядати максимально непримітно і правдоподібно. Жаргонні коди включають в себе нанесення піктограм, таємну термінологію, яка передає зміст внаслідок того, що ключ відомий тільки певним особам.

При застосуванні геометричної системи мають значення слова, розташовані на сторінці в певних місцях або в точках перетину геометричної фігури заданого розміру. Нульовий шифр приховує повідомлення відповідно до певного, заздалегідь підготовленого, набору правил. Шифр «решітка» застосовує шаблон для приховування повідомлення-контейнера. Слова, які з'являються в отворах шаблону, є прихованим повідомленням.

Іншу категорію лінгвістичних методів становлять семаграми – таємні повідомлення, в яких значеннями шифру є символи, крім літер і цифр. Візуальна семаграма використовує звичайні фізичні об'єкти для передачі повідомлення. Текстова семаграма приховує повідомлення, змінюючи зовнішній вигляд тексту-контейнера.

Перевагою методів лінгвістичної стеганографії є можливість передавання повідомлення великої довжини, а недоліками – можливість випадкового вияву кодуючого алгоритму та складність процесу кодування повідомлення.

Квантова стеганографія [52,55] аналогічно традиційним аналогам має за мету приховування самого факту передачі інформації. Квантова стеганографія ще не набула масовості, але пропонуються моделі, що використовують квантові властивості. Даний напрям є синтезом класичної і квантової інформатики і заснований на злитті понять квантової фізики та класичної теорії інформації. Хуліо Джі-Бенаклач [52] запропонував ідею приховування таємних повідомлень у формі синдрому помилки при застосуванні квантових коригуючих кодів. Однак, протокол, що був наданий, не дає можливості непримітно приховувати конфіденційну інформацію в квантовому каналі. Пізніше, Керті [52] запропонував три стеганографічні системи, які використовують квантові інформаційні характеристики. Класифікація методів квантової стеганографії зображена на рис.2.3.

Рис.2.3 Методи квантової стеганографії

Перша система приховує один класичний біт в шумоподібний кубіт (наприклад, молодший біт квантових значень), заміною кубіта. Друга система приховує два класичних біта в один шумоподібний кубіт шляхом заміни кубіта із

щільним кодуванням. Безпека системи залежить від ідентичності між квантовим шумом та справжнім білим шумом (матриці щільності).

У третій системі кубіт передається через класичний стеганографічний канал за допомогою квантової телепортації [52]. Безпека цієї системи аналогічна, що лежить в основі класичної стеганографічної системи. Жоден з цих протоколів не забезпечує передачу непримітних повідомлень через відкритий класичний канал або загальний квантовий канал в умовах секретності. Наторі [52] трактує елементарні поняття квантової стеганографії, яка є модифікацією надщільного кодування.

Мартіном [52] було введено поняття квантового стеганографічного зв'язку, а запропонований ним протокол квантового розподілу ключів (КРК) є варіантом протоколу Беннета і Брассара (BB84), в якому він приховує стеганографічний канал (контейнер).

Квантова стеганографії є значно стійкішою за традиційну тим, що перехопити і декодувати конфіденційну інформацію, закодовану у квантові стани, теоретично неможливо (теоретико-інформаційна стійкість).

Перевагами методів цифрової стеганографії є: простота реалізації; висока стійкість до атак, візуальна незмінність між модифікованим і первинним повідомленнями; є вільне програмне забезпечення для їхньої реалізації.

Недоліками цифрової стеганографії є: чутливість до найменших спотворень контейнера; ймовірність виникнення помилок при детектуванні; складність вбудовування інформації в контейнер великого об’єму послання.

2.5.1.4 Алгоритми вбудовування прихованої інформації [52]

Алгоритми розділено на підгрупи: працюючі з самим цифровим сигналом (метод LSB0); «впаювання» прихованої інформації - відбувається накладення приховуваного зображення (звуку, тексту) поверх оригіналу; використання особливостей форматів файлів - запис інформації в метадані або в інші зарезервовані поля файлу, що не використовуються.

За способом вбудовування інформації стегоалгоритму можна розділити на лінійні (адитивні), нелінійні та інші. Алгоритми адитивного впровадження інформації полягають в лінійній модифікації вихідного зображення, а її витяг в декодере проводиться кореляційними методами. У нелінійних методах вбудовування інформації використовується скалярне/векторне квантування. Серед інших методів певний інтерес представляють методи, які використовують ідеї фрактального кодування зображень.

Метод мережевий стеганографії з модифікацією полів в TCP заголовку, в якому буде передаватися секретне повідомлення. У заголовку протоколу з метою стеганографії використовують поля, які можна змінити без функціонування пакета. Наприклад, поле «Номер послідовності» (SN - SeguenceNumber), яке виконує два завдання. Перше - якщо встановлено прапор SYN, то це початкове значення номера послідовності - ISN (InitialSeguenceNumber), і перший байт даних, які будуть передані в наступному пакеті, буде мати номер послідовності, рівний ISN + 1. В іншому випадку, якщо SYN не встановлений, перший байт даних, який передається в даному пакеті, має цей номер послідовності. Важливо знати, що це значення не зміниться за час шляху пакета від відправника до одержувача. Поле «Номер послідовності» дозволяє створювати послідовність довжиною в 32 біта. За методом Роуланда, передане повідомлення кодується відповідно до таблиці ASCII і множиться на певне число (ключ), кратне двом для зниження ймовірності виявлення, потім вноситься в генерований TCP пакет в поле «Номер послідовності» і пакет відправляється. При досягненні пакетом адреси призначення, одержувач повинен зберегти всі прийшли TCP пакети, з яких він повинен вилучити значення в поле «Номер послідовності», після чого поділити на заздалегідь відомий йому ключ. Метод легко виявити. А якщо даний ключ передавати одночасно з TCP пакетом, в IP заголовку, це підвищить складність виявлення стеганограми. Наступною дією є внесення призначення носія С поле «Номер послідовності» TCP заголовка. Необхідно внести значення

зашифрованого ключа (inv (z) 16) в поле IP заголовка. Для організації операції використовується метод мережевий стеганографії з модифікацією полів IP заголовка. Незмінними під час шляху пакета залишаються тільки поле «Ідентифікатор», довжина якого становить 16 біт і 1 біт в поле «Прапори», який відповідає за прапор DF (Donotfragment - НЕ фрагментировать). Зміна полів не несе змін в пакеті, тому що не проводитися фрагментація пакета, а за умовою треба мати мінімальне значення MTU і не перевищувати його при створенні і відправці пакета.

Під час систематизації та класифікації сучасних стеганографічних напрямів установлено, що виділяють чотири основні напрями стеганографії: класична, цифрова, лінгвістична та квантова. Кожен напрям представлений конкретними методами приховування конфіденційної інформації.

2.5.2 Потужні засоби приховування інформації, контейнери

Стеганографічні методи дозволяють приховати інформацію в різних об'єктах (контейнерах): в текстових документах, в графічних файлах. Відео файлах, в звукових файлах, на HTML- сторінках, в субтитрах фільмів, в повідомленнях, переданих за допомогою SMS MMS, чатів, месенджерів і блогів. Текстові повідомлення можуть бути в невикористовуваних областях Flash-пам'яті, жорстких і оптичних дисків. Число різновидів контейнерів, які використовуються на практиці, велике. Кожен вид контейнера може існувати в різних форматах. Для приховування інформації можуть використовуватися різні методи (алгоритми), стеганографічні завдання є багатовимірними.

Для більшості сучасних методів, використовуваних для приховування повідомлення в цифрових контейнерах, є залежність надійності системи від обсягу вбудованих даних. При збільшенні обсягу вбудованих даних знижується надійність системи. Контейнер, що використовується в стегосистемі, накладає обмеження на розмір вбудованих даних.

Контейнер - будь-яка інформація, призначена для приховування таємних повідомлень. [51,52]. Порожній контейнер - контейнер без вбудованого повідомлення; заповнений контейнер - контейнер, що містить вбудовану інформацію. Вбудоване (приховане) повідомлення - повідомлення, що вбудовується в контейнер.

2.5.3 Стеганографічна система (стегосистема)

Стегосистема - сукупність засобів і методів, які використовуються для формування прихованого каналу передачі інформації. При побудові стегосистеми враховуються наступне: зловмисник має повне уявлення про стеганографічну систему і деталях її реалізації, а залишається невідомим ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення; якщо зловмисник дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати повідомлення в інших даних до тих пір, поки ключ зберігається в таємниці; зловмисник повинен бути позбавлений технічних та інших переваг в розпізнаванні або розкритті змісту таємних повідомлень Узагальнена модель стегосистеми представлена на рис. 2.4 [50, 52]

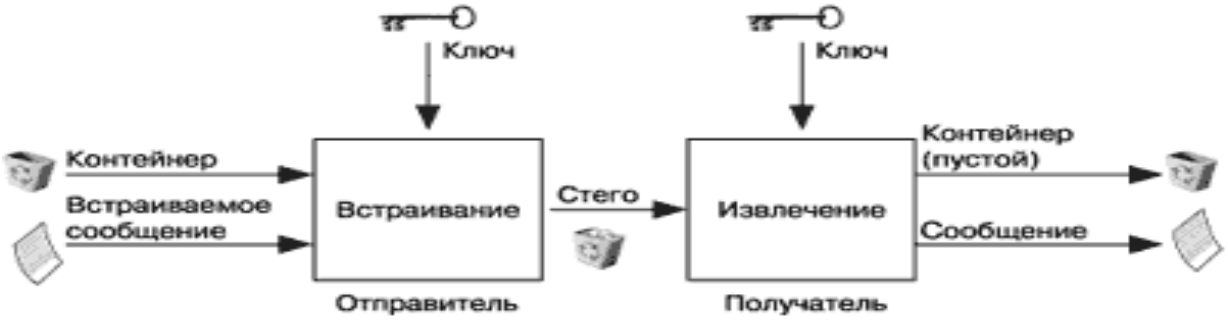

Рис. 2.4 Узагальнена модель стегосистеми

Стегоключ/ ключ - секретний ключ для приховування інформації. Залежно від кількості рівнів захисту (вбудовування попередньо зашифрованого повідомлення) в стегосистемі може бути один або кілька стегоключів. За аналогією з криптографією, по типу стегоключа стегосистеми можна поділити на

два типи: з секретним ключем; з відкритим ключем. У стегосистеми з секретним ключем використовується один ключ, який визначений до початку обміну секретними повідомленнями, або переданий по захищеному каналу. У стегосистемі з відкритим ключем для вбудовування і вилучення повідомлення використовуються ключі, які розрізняються, що за допомогою обчислень неможливо вивести один ключ з іншого. Один ключ - відкритий передається вільно по незахищеному каналу зв'язку. Схема працює і при недовірі відправника і одержувача.

На рис. 2.5 [56] зображено підсумовуючу модель аналізу загроз та стійкості стегосистем.

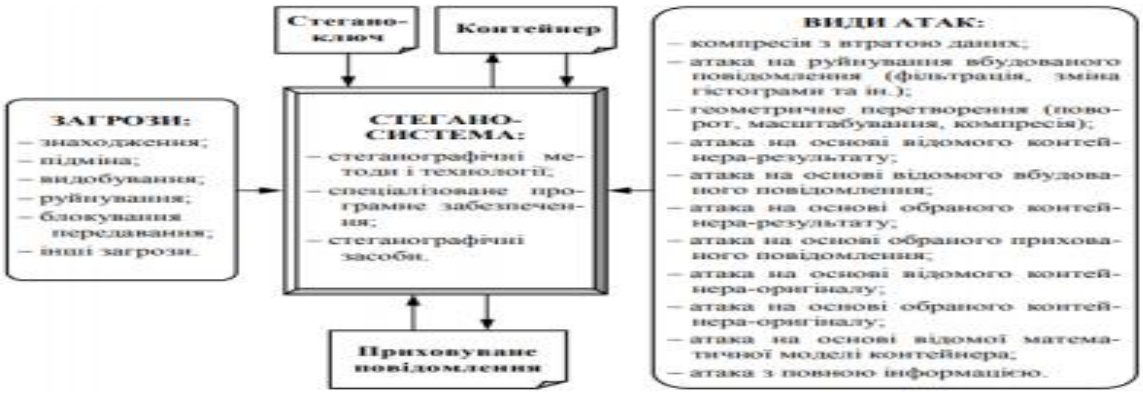

Рис.2.5 Модель аналізу загроз стійкості стегосистем

Систематизація інформації щодо стійкості стеганографічної системи та захисту від зовнішніх впливів полегшує оцінити рівень існуючих досягнень в галузі забезпечення інформаційної безпеки. Проведений аналіз потребує подальших фундаментальних досліджень, а також дозволяє підвищити ефективність створення нових захисних системи стійких до атак.

Висновки до розділу

Самостійні технічні рішення безпеки не можуть забезпечити абсолютний захист від загроз. Для підвищення ефективності забезпечення безпеки інформації систем IP-телефонії потрібен комплексний підхід. Але навіть придбання систем

для забезпечення безпеки саме по собі повністю не вирішує проблему. Абсолютну гарантію безпеки не дає жоден метод.

В цьому розділі розглянуті програмно-апаратні методи, а також методи криптографії і стеганографії, що використовуються для забезпечення безпеки інформації в системи IP-телефонії, які використовуються в інфраструктурі мережи. Постійний і обов'язковий аналіз рівня захисту та комплексний підхід, разом з постійним вдосконаленням систем інформаційної безпеки, дозволить створити захищену систему.

3 АНАЛІЗ МЕТОДВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ IP- ТЕЛЕФОНІЇ

3.1 Науково-технічна ситуація щодо програмно-апаратних (апаратно-програмні) методів забезпечення інформаційної безпеки систем IP – телефонії

Забезпечення інформаційної безпеки систем IP - телефонії - одна з найважливіших проблем нової технології зв'язку. В залежності від різновидів Ip-телефонії вибираються методи забезпечення інформаційної безпеки.

Перспективними методами захисту інформації в системах IP – телефонії визначаються апаратно-програмні методи, тому що в цьому зацікавлені в першу чергу самі виробники обладнання для IP-телефонії, що його реалізують, та користувачів для здійснення успішної економічної та комерційної діяльності використання надійної і безпечної системи IP – телефонії є безперечним. Найчастіше користується попитом апаратні-програмні системи двох американських компанії Cisco та Avaya. Це конкуруючі компанії.

3.1.1 Порівняння науково-технічної бази з організації корпоративної IP-мережі та методів забезпечення інформації в системах IP-телефонії конкуруючих американських компаній Cisco та Avaya Inc.

Компанії Cisco та Avaya Inc пропонують принципово різні підходи до організації корпоративної IP-мережі. Ця різниця пояснює їхню відмінність в лідерстві в різних регіонах. Сучасний стан ринку IP-телефонії свідчить про життєздатність обох підходів.

У технічній літературі (http://citforum.ck.ua/security/articles/ipsec/ Безпека IP-телефонії) описані результати тестування систем IP-телефонії. Взяти участь в тестуванні брали компанії Cisco і Avaya.

Компанія Cisco довела, що вона здатна побудувати VoIP-мережу, яка може серйозно протистояти витонченим хакерським атакам.

Команда "хакерів" виявила вразливості захищеного варіанту Схеми IP-телефонної мережі компанії Avaya, однак Компанія Avaya заявила, що для

ліквідації цієї уразливості заплановано встановити програму на ПО управління. Підсумкова оцінка безпеки для останнього рішення компанії від Avaya, враховуючи порівняно не велику небезпеку виявлених вразливостей, - "Сталий"

Порівняння їхньої науково-технічної бази з організації корпоративної IP-мережі та методів забезпечення інформації в системах IP-телефонії представлені в таблиці 3.1.

Таблиця 3.1 Порівняння науково-технічної бази з організації корпоративної IP-мережі та методів забезпечення інформації в системах IP-телефонії конкуруючих американських компаній Cisco та Avaya Inc.

Характеристики	**Cisco**	**Avaya Inc**
Спеціалізація	Проектування, розробка, розгортання і адміністрування корпоративних мереж зв'язку для широкого спектру компаній	
Підходи до організації корпоративної IP-мереж	Дотримується революційного підходу до реалізації своїх рішень - швидкий перехід від традиційних аналогових мереж до IP-мереж.	Пропонує побудову конвергентних мереж з використанням існуючої телефонної мережі і нарощування додаткового функціоналу- дає VoIP-технологія, за рахунок застосування апаратних і програмних рішень
Особливі характеристики	Рішення Cisco використовуються в основних галузях вітчизняної економіки. Пройден аудит системи управління якістю (Quality Management System) на відповідність українському законодавству, отримано серійні сертифікати відповідності системи УкрСЕПРО на ввезене обладнання Cisco. Проведено експертизу рішень на предмет технічного та криптографічного захисту інформації ДССЗЗІ, отримано понад 20 експертних висновків на свої продукти.	Колишній підрозділ корпоративних мереж зв'язку компанії Lucent Technologies - самостійною з 2000р. У 2007р. Придбала за $ 8,2 млрд. приватні інвестиційних компанії TPG Capital та Silver Lake Partners. На 2018 має більше 130 тис. клієнтів в 220 тис. точках світу. Придбала систему мережевого управління Nortel Enterprise і патенти: US 20050007951; 7173934; 6496502. Поширила портфель патентів на комунікаційні додатки в сфері рішень для уніфікованих комунікацій (бездротовий зв’язок) - є більш ніж 4400 патентів і заявок на винаходи.

1) Компанії Cisco та Avaya Inc. пропонують принципово різні підходи до організації корпоративної IP-мережі. Ця різниця пояснює їхню відмінність в

лідерстві в різних регіонах. Сучасний стан ринку IP-телефонії свідчить про життєздатність обох підходів.

Компанія Cisco застосовує засоби захисту: на другому і третьому рівнях - моделі EMBOC (комутатори Catalyst); четвертому і п'ятому - міжмережеві екрани і системи виявлення вторгнень; шостому - шифрування RTP голосових потоків; сьомому рівні - за допомогою серверних додатків Cisco Security Agent.

2) Рішення компанії Avaya мають обмежений набір засобів безпеки на другому-третьому рівнях і вище, за винятком шостого рівня. Компанія Avaya пропонує надійну схему шифрування RTP трафіка (рівень 6) і підтримує його для всіх своїх IP-телефонів. Рішення компанії з максимально задіяними засобами безпеки мають більш ефективні засоби захисту на третьому, четвертому і шостому рівнях, хоча і не позбавлені ряду вразливостей.

З огляду на апаратно-програмні методи щодо інформаційної безпеки відомими є такі фірми, табл.3.2.

Таблиця 3.2. Відомі фірми (компанії) в галузі апаратно-програмних методів

Назва фірми (компанії)	Досягнення
Siemens Enterprise Communications, Німеччина	Світовий лідер в сегменті корпоративного зв'язку з сильними позиціями в області систем уніфікованих комунікацій, центрів обробки викликів і захищених мереж, має патенти у багатьох країнах, під час за тематикою виявлено патенти на винаходи і корисні моделі: UA 46781, RU 2636113, 2619206, 2554532, 2313186
Platan Sp. z o.o. Польща	Провідний польський виробник цифрових IP АТС і телекомунікаційних серверів. ООО «Інфотел-Дистрибуція» є Ексклюзивним Дистриб'ютером компанії **Platan Sp. z o.o. в Україні**
Digium Inc. США	Компанія розробила платформу IP-телефонії з відкритим вихідним кодом Asterisk, виробник плат інтерфейсів комп'ютерної телефонії, сумісних з цією платформою. Комплекс має всі можливості АТС, а також завдяки підтримці VoIP - протоколів, програмне рішення Asterisk може працювати з будь-яким обладнанням IP-телефонії. Має представництво у Києві
Gigaset Communications GmbH	Світовий виробник бездротових телефонів і європейський лідер у виробництві DECT-телефонів. Розробляє, виробляє і реалізовує високоякісні продукти під брендом Siemens Gigaset, включаючи DECT-телефони, VoIP пристрої
Gigaset Pro	Якісна підтримка DECT роумінгу, що покриває VoIP DECT зв'язком великі території. Якісно підтримує стандарт SIP, має найкраще VoIP рішення. Є представництво у Києві
2NTELECOMUNIKACE, Чехія	Успішний європейський виробник, розробляє і виробляє продукти для реалізації різних рішень в галузі телекомунікаційних технологій, безпеки і контролю доступу
Компанія Yealink, Китай	Професійний розробник і виробник обладнання VoIP - IP телефонів. Продукти повністю сумісні зі стандартом SIP і сумісність з більшістю IP-АТС. Телефони Yealink мають безліч функцій, які спрощують зв'язок, і працюють з

	усіма IP-PBX, що підтримують протокол SIP. В більш ніж 140 країнах вибирають обладнання Yealink, тому що воно має підвищену надійність, безпеку, якість та ергономіку комунікаційних мереж
Корпорація ZyXEL Communications, Тайвань	Провідний розробник мережевих рішень на базі інтернет-технологій. Напрямки діяльності: рішення для широкосмугового доступу, рішення для універсальних конвергентних мереж (NGN) і мережевої безпеки. Має представництво у Києві і Львові

3.1.2 Патентна активність в галузі програмно-апаратних методів забезпечення інформаційної безпеки систем IP – телефонії.

3.1.2.1 Патентна активність іноземних фірм.

Інформаційні ресурси у все в більшій мірі стали ареною суперництва за лідерство, тому фірми патентують цікаві, цінні технічні рішення. Так, основна архітектура IP – телефонії запатентована виробниками, що є дуже не зручно, тому що це стало гальмом для науково-технічного розвитку в галузі інформаційної інфраструктури.

Запатентовані окремі елементи, наприклад сервіси безпеки самі по собі не можуть гарантувати надійність програмно-технічного захисту.

Тільки перевірена архітектура здатна зробити ефективним об'єднання сервісів, забезпечити керованість ІС, здатність протистояти новим загрозам. Але описані в патентах окремі рішення не можуть бути основою вирішення проблеми архітектурної безпеки мережевих конфігурацій. Потрібно дотримуватися принципів: впровадження єдиної політики безпеки; забезпечення конфіденційності і цілісності під час мережевих взаємодій; формування сервісів, щоб кожен компонент мав повний набір захисних засобів та був єдиним цілим.

3.1.2.1 Патентна активність вітчизняних фірм, компаній, організацій

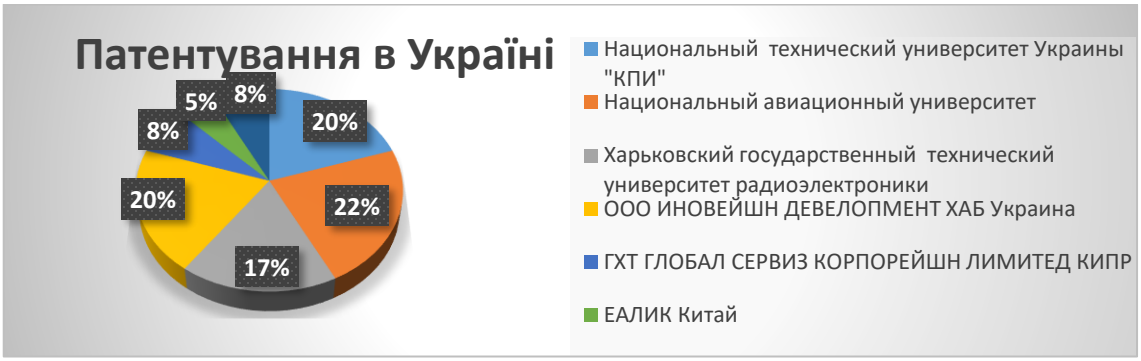

Рисунок 3.1 Динаміка патентування відомих фірм-розробників інженерно-технічних заходів і засобів захисту та методів забезпечення інформаційної безпеки систем IP – телефонії

Стосовно національних компаній, які за дослідженою тематикою патентують об’єкти промислової власності, серед всіх патентовласників визначаються найбільш активними наукові організації (див. рис.3.1).

3.1.3 Порівняння напрямів відомих методів захисту інформації за певними крітеріями в системах IP – телефонії

Захист інформації спрямовано на забезпечення інформаційної безпеки в системах IP- телефонії полягає у створенні системи заходів, що забезпечує збереження властивостей інформації і системи IP- телефонії.

Порівняння напрямів відомих методів за певними критеріями показано в таблиці 3.3.

Таблиця 3.3 Порівняння характеристик методів захисту інформації

Показники	**Моральноетичні методи**	**Адміністративні (організаційні) методи**	**Технічні (фізичні) методи**	**Програмно-апаратні методи**
1	**2**	**3**	**4**	**5**
Надійність захисту	Забезпечують в комплексі з адміністративними (організаційними) методами	Забезпечують в комплексі з застосуванням інших видів захисту: технічного, програмного.	Використання замкненого контуру захисту;структуро-ваної кабельної системи Надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії /стрибків напруги електромережі є установка джерел безперебійного живлення.	Забезпечуються компле ксно: адміністративними і технічними методами; криптографічний і стега-нографічний захист; заборона неавторизованого зовнішнього доступу віддаленого користувача і несанкціонованого доступу до баз даних.
Стійкість, потужність механізму захисту	Закріплення обов'язків. Морально-етичні норми не є обов'язковими і не всі затверджені в законодавчому порядку. Не можливо забезпечити абсолютну стійкість із-за незабезпечення повноти організаційних	Не можливо забезпечити абсолютну стійкість, із-за великої кількості адміністративних правил обтяжує працівників і послабляє організаційні зв'язки між системою і за окремими ланками.	Є втрата стійкості, із-за змін якісних параметрів системи. Забезпечується зовнішнім захистом засобів, об'єктів створення фізичних перешкод в проникнення і доступу порушників до компонентів інформаційних систем та інформації, що захищаються: засоби захисту кабельної і системи електроживлення.	Із-за змін якісних параметрів системи. Додатково криптографією (криптоалгоритм сильний, неможливо розшифрувати без секретного ключа, від якого залежить безпека переданого повідомлення. Алгоритм треба використовувати для шифрування даних/потоків

	зв'язків системою і з ланками.			
Складність реалізації	Несистемність-захищаються складові елементи системи, ці захисти слабо між собою пов'язані. Порушення організаційних зв'язків між системою і окремими ланками.	Несистемність - захищаються складові елементи системи, захисти слабо між собою пов'язані. Порушення організаційних зв'язків між системою і окремими ланками.	Несистемність - захищаються складові елементи системи, ці захисти слабо між собою пов'язані, тому використовуються різноманітні фізичні засоби захисту, призначені для створення перешкод на шляху зловмисників.	Несистемність, бо захищаються складові елементи системи, і ці захисти слабо між собою пов'язані. Основною причиною складності реалізації є людний фактор.
Запобігання порушень у роботі системи та загроз несанкціонованого доступу до інформації	Посилення норм поведінки, що складаються з поширенням ЕОМ, мереж і іншими. Підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців.	Процеси функціону-вання ІС, використання ресурсів, діяльність персоналу, порядок взаємодії користувачів із системою; удосконалення карного і цивільного законодавства, судочинства; заходи під час добіру і під-готовки персоналу; при будівництві та облаштуванні об'єктів охорони; при проектуванні, модифікації програмного забезпечення;розробка правил захисту інформації	Для усунення загрози потрібне: дослід-ження апаратних за-собів і їх випромі-нювання і атестування, категорування засобів, об'єктів з видачою дозволу на експлуатацію. Використання в ЕОМ у системі вводу-виводу BIOS апаратного паролю, що блокує завантаження і роботу ПК, не зовсім надійним є захист від загроз НСД, частка BIOS-носія паролю може замінена (вузли BIOS уніфіковані) з відомим паролем.	За допомогою технічних пристроїв спеціального призначен-ня: джерел безперебі-йного живлення апаратури,пристроїв стабілізації у мережі електроживлення; екранування апаратури ліній зв'язку, в яких знаходиться комп'ютерна техніка; прис-трої ідентифікації і фіксації терміналів і користувачів пристосувань несанкціонованого доступу до комп'ютерної мережі; засоби захисту портів комп'ютерної техніки
Використання в комплексі з іншими методами	З адміністративними засобами	Здатні доповнити законодавчі норми	З апаратними і програмними методами.	З технічними криптографічними стеганографічними

На підставі аналізу матеріалів, що є в таблиці 3.3 можна зробити висновок:

1) Програмно – апаратні методи мають перевагу над іншими методами тому, що передбачають комплексну систему захисту інформації;

2) Сучасні методи захисту розвиваються в цьому напряму.

3) Програмно – апаратні методи більш ефективні ніж інші методи тому, що вони основані на синтезі програмних, апаратних засобів та криптографічних і стеганографічних методів, і є можливість регулювання та узгодження змін в системі зв'язків ланок захисту в залежності від змін якісних параметрів системи.

4) Це знижує втрати стійкості і ефективності захисту, запобігає порушенням у роботі системи та загрозам несанкціонованого доступу до інформації.

5) Комплексна система захисту інформації забезпечує на належному рівні основні показники: надійність захисту, стійкість і потужність. Указані показники залежать від таких факторів: сильний криптографічний алгоритм з використанням різних статистичних закономірностей зашифрованого повідомлення або інші способи аналізу; безпека переданого повідомлення повинна залежати від секретності ключа, але не від секретності алгоритму.

3.2 Науково-технічна ситуація щодо криптографічних та стеганографічних методів

Основні умови забезпечення мережевої безпеки ефективними заходами можуть бути лише тоді, коли покриваються всі рівні мережевої інфраструктури.

Проблема захисту інформації від несанкціонованого доступу вирішувалася здавна [51], основними шляхами вирішення є криптографія та стеганографія.

3.2.1 Рішення задач захисту інформації в сучасних системах IP-телефонії неможливо без аналізу структури протоколів передачі даних, що в них застосовуються, на предмет встановлення їх відповідності потребам збереження конфіденційності телефонних переговорів та формування вимог до комплексного захищеного протоколу обміну голосовими повідомленнями абонентів високої стійкості. Захист інформації полягає в підтримці стану захищеності інформаційного середовища, яке досягається шляхом дотримання конфіденційності, цілісності та доступності інформації. Дотримання вимог (у випадку IP-телефонії) може бути майже гарантованим у разі використання криптографічних перетворень інформації.

3.2.2 Основні перспективні криптографічні методи

3.2.2.1 Під час використання основних схем побудови криптосистем, видів з’єднання абонентів, алгоритмів шифрування та протоколів VoIP для комплексного захищеного VoIP- протоколу, цікавою є інформація з світового

конкурсу шифрів-кандидатів на AES - новий криптографічний стандарт. Організатором є Національний інститут стандартів и технологій США та Аналіз схем поточного шифрування, конкурс NESSIE.

За результатами конкурсу AES (США) можна відзначити високу якість розробок, що визначають науково-технічний прогрес в сфері криптографії.

У другому колі брали участь 5 дуже сильних шифрів-фіналістів: "Serpent" від Андерсона (Англія), Кнудсена (Данія) і Біхам (Ізраїль); "Mars" від Копперсміта, Геннаро і ін. З IBM (США); "Rijndael" від Реймі і Дамена (Бельгія); "RC6" від Райвест, Робшоу і ін. З RSA Security (США); "Twofish" від Шнайера, Келсі та ін. (США). Найскладнішу конструкцію (ускладнює аналіз стійкості, це є недоліком) мають Mars і Twofish; найбільш просту конструкцію - Rijndael і RC6, в основі алгоритмів лежать недостатньо глибоко вивчені криптоперетворення; Serpent володіє найбільш прозорою "консервативною" конструкцією, та обрано великий запас міцності. Жоден з шифрів не вдалося розкрити. Криптоалгоритми протестовані в різних втіленнях: як програмно - на мовах ANSI C, асемблер, Java та ін. в умовах різних архітектур; і в апаратно - в смарт-картах і FPGA-чіпах. Найменш продуктивним шифром серед алгоритмів-фіналістів виявився MARS. На передостанньому місці - RC6, він як і MARS пригальмовує в розгортанні кріптоключа. В мережевих додатках типу шлюзів VPN і в протоколах IPsec швидкість роботи з ключами є найважливим фактором продуктивності, власне шифрування потоку з великою швидкістю виконують всі алгоритми-фіналісти. Шанси на перемогу продемонстрував бельгійський шифр Rijndael. Алгоритм має теоретичне обгрунтування стійкості, швидко працює в програмних і апаратних реалізаціях. За результатами конкурсу був прийнятий в 2001р федеральний стандарт США (FIPS 197), новий стандарт блочного шифрування AES-Rijndael.

3.2.2.2 Для розробки нових європейських стандартів ЄС пішло цим же шляхом. В рамках проекту NESSIE (New European Schemes for Signature, Integrity, and Encryption) є конкурс на розробку європейських криптографічних стандартів.

Програма NESSIE ширше і передбачає створення криптографічних примітивів: алгоритми блочного і поточного шифрування; алгоритм несиметричного шифрування; алгоритм формування MAC-кодів і хеш-функцій; цифровий підпис; ідентифікаційна схема. Одним проектом бажають стандартизувати основні механізми безпеки.

Аналіз результатів випробувань є цікавим для криптографічного кола. У технічній літературі багато уваги приділяється питанням практичної реалізації схем блочного і поточного симетричного шифрування. Різні алгоритми шифрування постійно застосовуються в корпоративних мережах для захисту. Всі канали та сервери в таких системах є захищеними та підданими обробці з того чи іншого алгоритму шифрування. Ці системи вимагають обов'язкового поточного шифрування каналів зв'язку на мережевому рівні і вище, що забезпечує захист переданого трафіку при передачі по скомпрометованим провайдерським каналам. Потокові шифри забезпечують неохідну швидкість шифрування на канальному, мережевому і транспортних рівнях. [56-58].

3.2.2.3 Науково-технічні напрацювання криптографічних методів забезпечення інформаційної безпеки систем IP – телефонії.

Існує багато готових алгоритмів шифрування з високою криптостійкістю, шифрувальникові треба створити свій унікальний ключ для додання інформації необхідних криптографічних якостей, що використовується і для шифрування, і в процесі розшифрування. Над проблемою працюють винахідники.

За результатами проведеного попереднього патентного пошуку виявлено 34 патентів України на удосконалення криптографічних методів забезпечення інформаційної безпеки.

3.2.3 Порівняння стеганографічних методів приховування конфіденційних повідомлень, що застосовуються в техніці зв'язку

Дані, які передаються між користувачами по IP-телефонії, повинні залишатися конфіденційними. Глобальна мережа повиннна гарантувати захист користувача і

його даних від будь-якого роду атак і загроз. Інформаційна безпека не тільки стає обов'язковою, вона ще є однією з характеристик інформаційних систем. Масове використання мереж призвело до розробки програмних систем захисту інформації від несанкціонованого доступу. З'явилися спеціалізовані системи, (перевірка автентифікації, створення електронного цифрового підпису), з'явилися спеціалізовані програмні продукти відповідного призначення (програми F5, StegHide спеціалізуються на стеганографічних методах) [59-63].

3.2.3.1 Порівняння стеганографічних методів конфіденційних повідомлень, що застосовуються в техніці зв'язку наведено в табл. 3.4.

Таблиця 3.4 Порівняння характеристик стеганографічних методів використання надмірності аудіо та візуальної інформації

Показники	**Методи заміни в просторовій області** / метод заміни молодших біт (LSB- метод)	**Методи, що діють в частотній області**	**Широкосмугові методи**	**Статистичні методи**
Методи використання надмірності аудіо та візуальної інформації				
Галузь застосування	Забезпечують швидкодію і значний обсяг вбудованих даних, доцільно використовувати при передачі прихованих повідомлень. Для прихованого зв'язку доцільно використовувати методи заміни у простор.області	Застосовуються в техніці зв'язку для забезпечення високої завадостійкості.Для прихованого зв'язку доцільніше використовувати методи заміни у частотній області	Застосовуються в техніці зв'язку для забезпечення високої завадостійкості і складності процесу перехоплення та виявлення. Та в технологіях ЦВЗ є найбільш ефективнішим застосування ніж у статистичних методів.	Застосовуються в техніці зв'язку для забезпечення високої завадостійкості і складності процесу перехоплення та виявлення
Особливості методу	Базується: молодші розряди графічних, аудіо і відео форматів несуть мало інформації і їх зміна не познача-ється на якості переданого зобра-ження/звуку. Вико-ристання для коду-вання конфіденційної інформації	Дані приховуються у коефіцієнтах частотного представлення контейнера. Найчастіше використовують ся перетворення, які застосовуються у алгоритмах стиснення із втратами (дискрет-не косинусне перет-творення в стандарті JPEG і вейвлет перет вореня- в JPEG2000).	Суть даних методів полягає в розширенні смуги частот сигналу, до ширини спектру, більшої ніж це необхідно для передачі інформації Для розширення діапазону існують два способи: метод прямого розширення спектру, за допомогою псевдо – випадкової послідовності, і метод стрибкоподібного пе-реналаштування частоти.	Приховують інформацію – змі-нюють статистичні властивості зображення./ідея алгоритму Patchwork базується на припу-щенні-значення пікселів неза-лежні і однаково розподілені. Генерується секрет. ключ для ініціалізації генератора псев-довипадкових чисел, які вказу- ють на місце в зображенні, для внесення біт. У відповідності зі стегоключем вибирається n пар пікселів у яких значення яскравості змінюється

Стеганостійкість	Є нестійкими до відомих видів спотворень. Забезпечують меншу стій кість до геометричних пе ретворень і виявлення ка-налу передачі (порівняно з методами частотній області). Розподіл прихованих біт по всьому контейнері зумовлює високу стійкість до випадкових спотворень.	Забезпечують більшу стійкість до геометричних перетворень і виявлення каналу передачі (порівняно з методом LSB) є стійкішими до спотворень та операцій цифрової обробки	Стійкість до випадкових та умисних спотворень.	Забезпечує високу стійкість до операцій цифрової обробки
Якість **приховування повідомлени**	Безперешкодне проходження стеганоповідомлення по каналу зв'язку не привертає увагу атакуючго. Якість залежить від об'єму даних	Якісні приховування, якщо приховати менший об'єм даних	Принцип дії - "розчинити" секретне повідомлення в контейнері і зробити неможливим його виявлення.	забезпечує високу якість приховування
Надійність	Для зниження компрометуючих ознак потрібна корекція статистичних характеристик. надійність методів заміни в просторовій області залежить від рівня частотних спотворень контейнера.	Оскільки є можливість в широкому діапазоні варіювати якість стисненого зображення, що робить неможливим визначення походження спотворення.	Оскільки сигнал, розподілений по всій смузі спектра, його важко виділити. Наявність секретного ключа у що використовують псевдовипадкове кодування, підвищує їх надійність.	Важкість виявлення прихованих даних без відповідного секретного ключа. Наявність секретного ключа у що використовують псевдовипадкове кодування, підвищує їх надійність.
Переваги	Простота реалізації та можливість таємної передачі великого об'єму інформації	Приховання може проводитися і початкове зображення, і одночасно із стисненням зображення контейнера.Стегосистеми, у яких враховані особливості алгоритму сти снення, є нечутливими до компресії контейн.	Корисна інформація розподіляється по всьому діапазону, тому при втраті сигналу в деяких смугах частот в інших смугах залишається достатньо інформації для її відновлення.	Можливість прихованої передачі великого обсягу інформації. Можливість захисту авторського права, прихованого зображення товарної марки, реєстрауіних номерів і т.п.

Недоліки	За рахунок введення додаткової інформації спотворюються статистичні характеристики файлу-контейнера і приховане повідомлення легко виявити за допомогою статистичних атак, таких як оцінка ентропії та коефіцієнтів кореляції. Недоліком методу є також його чутливість до операцій цифрової обробки: стиснення, застосування фільтрації, конвертації кольорів, геометричних перетворень,додаткового зашумлення та зміни формату контейнера.	Можуть приховати менший обсяг даних	Можливість стегоаналізу за рахунок цифрової обробки з використанням шумозгладжуючих фільтрів.	За рахунок введення додаткової інформації потворюютья ститстичні характеристики цифрових потоків. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик

Методи приховування даних у нерухомих зображеннях є нестійкими до більшості відомих видів спотворень: конвертування зображення у інший формат із компресією призводить до часткового або повного руйнування повідомлення.

Загальним принципом алгоритмів методів приховування даних у просторовій області полягає у заміні надлишкової, малозначної частини зображення біта секретного повідомлення. Для витягу повідомлення необхідно знати алгоритм, по якому воно розміщувалося у зображенні. Основною перевагою методу є простота реалізації та можливість таємної передачі великого об'єму інформації. Однак за рахунок введення додаткової інформації спотворюються статистичні характеристики файлу-контейнера і приховане повідомлення легко виявити за допомогою статистичних атак. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик. Недоліком є чутливість до операцій цифрової обробки: стиснення, фільтрації, конвертації кольорів, геометричних перетворень, додаткового зашумлення, зміни формату контейнера.

3.2.3.2 Стеганографічниі методи (мережева стеганографія) використання спеціальних властивостей комп'ютерних форматів даних з трафіком VoIP, порівняння характеристик стеганографічних методів використання

Популярними методами стали методи в яких прихована інформація передається через комп'ютерні мережі з використанням особливостей роботи протоколів передачі даних. Особливістю є те, що повідомлення приховуються в елементах управління протоколів зв'язку і в результатах зміни логіки протоколу. Цей напрям називають мережева стеганографія, він активно розвивається. В якості носіїв секретних даних використовуються мережеві протоколи OSI - мережевій моделі взаємодії відкритих систем. Методи мережевій стеганографії включають зміну властивостей мережевих протоколів. Мережева стеганографія охоплює широкий спектр методів. Серед них стали популярними методи модифікації даних в заголовках мережевих протоколів і в полях корисного навантаження пакетів, зміни структури передачі пакетів в мережевих протоколах стали базовим інструментом для мережеваю стеганографії, порівняння їхніх характеристик надано в таблиці 3.5. Порівнювалися методи модифікації пакетів, методи стеганографії, які змінюють структуру і параметри передачі пакетів та змішані (гібридні) методи стеганографії.

Таблиця 3.5 Порівняння характеристик методів мережевій стеганографії

Показники	**Методи**				
	RSTEG	LACK	TranSteg	HICCUPS	SCTP
Реалізація	Реалізація методу складна. Заснований на повторній посилки пакетів. Даний метод досить складно реалізувати, особливо ті його алгоритми, які базуються на перехопленні і виправлення пакетів звичайних користувачів.	Реалізація методу занадто склад на, і може бути неможливою в межах деяких операційних систем.	Реалізація методу зана дто складна Голосові дані висо ого бітрейта перекодуються в низький бітрейт,поможливості - з мінімальними втратами якості, а на звільнене місце вносяться дані стеганограми,також TranSteg про водить перестиснення вихідних даних з втра тами для звільнення місця під стеганограм.	Володіє найменшою складністю реалізації. Мережі з розділяється середовищем передачі даних, особливо локальні мережі з шинною топологією, використовують різні механізми доступу до середовища, CSMA,CSMA/CD, CSMA/CA , Token Bus.– можуть «чути» кадри з даними	Реалізація методу середня реалізується в таких операційних системах як BSD, Linux, HP-UX та SunSolaris, а також підтримує мережеві пристрої операційної системи CiscoIOS і може бути використаний в Windows
Особливість	Метод з використанням ретрансляції пакетів є гібридним. Відправник посилає пакет, але одержувач не відповідає пакетом з прапором підтвердження. Спрацьовує механізм повторної посилки пакетів, і тепер посилається пакет зі стеганограммой всередині, на який також не приходить підтвердження. При наступному спрацьовуванні даного механізму надсилається оригінальний пакет без вкладень	Функціонування – передавач вибирає один з пакетів голосового потоку, і його корисне навантаження замінюється бітами секретного повідомлення – стеганограмой, яка вбудовується в один з пакетів. Потім вибраний пакет навмисно затримується. Кожен раз, коли надмірно затриманий пакет досягає одержувача, незнайомого з стеганографічної процедурою, він відкидається..	Полягає в стиснен ні корисного навантаження мереже евого пакету за рахунок перекодування і може застосо вуватися скрізь, де існує можливість стиснення з втрата ми/ без відкритих даних. Саме стиснення потрібно для обмеження ро- зміру переданих даних, т.к. прихо-ваний канал зв'яз-ку має обмежену пропускну здат-ність.	HICCUPS з розподілом смуги пропускання для мереж з розділеннимсередовищем передачі даних, використовує недосконалості середовища передачі — шуми і перешкоди, які є природними причинами спотворення даних Обов'язкова умова для перехоплення кадрів - доступ до фізичного середовища..	використовує характерні особливості протоколу, такі як мультіпоточность і використання множинних інтерфейсів (multi-homing). Методи зміни вмісту SCTP-пакетів засновані на тому, що кожна частина STCP-пакета може мати змінні параметри
Вартість	Висока	Дуже висока	Дуже висока	Сама висока	Сама низька
Складність виявлення	Володіє високою складністю виявлення і по в'язана з використовуваним механізмом ре алізації методу.На ос нові RTO характеризу ється високою складні стю виявлення; на ос - нові SACK більш легко виявляємий Через різке збіль-шення час тоти ретранслювання пакетів або виникнення незвичайних затримок при передачі, стеганограми можуть вик ликати підозри у спостерігача	Володіє середньою складністю виявлення	Володіє високою складністю Складність виявлення безпосередньо залежить, наприклад, від місця розташування спостерігача, в якому він може переглядати VoIP-трафіку).	Має самую високу складність виявлення полягає у: використанні захищеної телекомунікаційної мережі, обладнаної криптографічними механізмами, для створення стеганографічної системи;	Володіє самою низькою складністю Виявлення даного методу будується на основі статистичного аналізу адрес мережевих карт, використовуваних для пересилання пакетів, з метою виявлення прихованих зв'язків.
Продуктивність	Залежить від деталей процедур зв'язку (розмір корисного навантаження пакета, частота, з якою генеруються сегменти і т.п.).	Залежить від деталей процедур зв'язку	Залежить від деталей процедур зв'язку	Залежить від деталей процедур зв'язку	Залежить від деталей процедур зв'язку
Пропускна спроможність	Пропускна здатність висока RSTEG є гібридним. пакетів. На основі RTO характеризується	Пропускна здатність не менше, а іноді і вище, ніж у інших алгоритмів, що	володіє найвищою пропускною здатністю у 32кб/с при найменшій різниці в	знаходиться на третьому місці по пропускній здатності; новий протокол з розподілом пропуск-	пропускна спроможніст не велика

	низькою пропускною здатністю, на основі SACK володіє максимальною для RSTEG пропускною здатністю	використовують аудіо-пакети	бітрейті голосового потоку	ної здатності для стеганографических цілей, заснованого на пошкоджених кадрах.	
Переваги	Його стеганографічна пропускна здатність приблизно дорівнює пропускній здатності методів з модифікацією пакету, і при цьому вище, ніж у методів зміни порядку передачі	Працює з VoIP. Зв'язок че-рез IP-телефонію складається з частин: сигналь-ної і розмовної. В них відбувает-ься передача ін-формації в обид-ві сторони.Вико-користовується SIP і RTP- протя-гом сигнальної фази виклику кін цеві точки SIP об мінюються SIP-повідомленнями. Вони проходять через SIPсерве-ри.Після з'єднан-ня у фазі розмо-ви, де аудіопотік RTP йде в обох напрямках між зухвалим і вик-ликаним. І саме тут ефективний LACK	змінює корисне навантаження VoIP-пакета, користується успіхом за рахунок популярності програм, що забезпечують голосовий та відеозв'язок через Інтернет.	Загальновідомий метод ініціалізації алгоритму шифру-вання У мережі можна створити три прихованих каналу даних в кадрі MAC: – HDC1: канал засно-ваний на векторах ініціалізації шифру; – HDC2: канал засно-ваний на MAC-адреси; – HDC3: канал на основі значень механізму цілісності (У мережах, де безпека не забезпечується, використовуються тільки HDC2 і HDC3. Більшість провідних мереж не підтримують безпеку на рівні MAC, на відміну від бездротових	
Недоліки	Втрати пакетів у мере-жі ретельно контролю ються,а RSTEGвикори стовує легальний тра-фік, збільшуючи зага-льні втрати. Щоб пере конатися, що за гальна втрата пакетів у мере-жі нормальна і RSTEG частка не надто висо-ка над іншими сполу-ками мережі,рівень ре трансляції в цілях сте-ганографії повинен ко нтролюватися і дина мічно адаптуватися.	При умисному вик-лику втрат виникає погіршення якості зв'язку, що може викликати підозру як у звичайних користувачів, так і у прослуховуючого спостерігача.	варто віднести складність його реалізації: потрібно з'ясувати, які кодеки використовуються для формування голосового потоку, і підібрати кодеки з найменшою різницею втрати якості мови (що неминуче знижуватиметься).	«Прослухову-вання» переданих в середовищі кадрів з даними та можливість відправлення пошкоджених кадрів з неправильними значеннями кодів корекції — найважливіші мережеві функції для HICCUPS.	Боротися ж з організацією прихованого каналу передачі, заснованому на цьому принципі, можна змінюючи адреси відправника і одержувача в випадково обраному пакеті, який міститься в повторно запропонованому блоці.
загальні ознаки	1 Жоден із реальних методів стеганографії не є досконалим. 2 Незалежно від методу, прихована інформація може бути виявлено: чим більше прихованої інформації внесено в потік даних, тим більше шансів, що вона буде виявлена методами стегоаналізу. Більш того, чим більше пакетів використовується для посилки прихованих даних, тим сильніше зростає частота ретранслированных пакетів, що істотно полегшує виявлення прихованого каналу зв'язку 3 характеристики перебувають у найтіснішому взаємозв'язку. Так, наприклад, складність виявлення буде прямо залежати від якості реалізації, а отже — складності реалізації. 4 Спільною рисою всіх методів мережевої стеганографії є створення з їх допомогою прихованих каналів передачі інформації в будь-якому відкритому каналі, в якому є якась надмірність.				

Для характеристики методів, що описані табл. 3.5 використана інформація з джерел [59-62].

Виконане порівняння характеристик деяких стеганографічних методів використання спеціальних властивостей комп'ютерних форматів даних з трафіком VoIP, табл. 3.5 свідчить про таке:

1) Зазвичай використовуються два підходи: навмисні затримки аудіо пакетів LACK (Lost Audio Packets Steganography) (колонка 3 табл. 3.5) і ретрансляція пакетів RSTEG (Retransmission Steganography) (колонка 2 табл. 3.5).

2) Метод модифікації мережевих пакетів Transcoding Steganography (TranSteg), що змінює корисне навантаження VoIP-пакета, користується успіхом за рахунок популярності програм, що забезпечують голосовий та відеозв'язок через Інтернет(колонка 4 табл. 3.5). Складність виявлення безпосередньо може залежити від місця розташування спостерігача, де він переглядає VoIP-трафік.

3) SCTP (колонка 3 табл. 3.5) (Stream control transport protocol) - транспортний протокол з контролем пакетів, реалізується в операційних системах BSD, Linux, HP-UX та SunSolaris, а також підтримує мережеві пристрої операційної системи CiscoIOS і може бути використаний в Windows.

4) SCTP-стеганографія (колонка 6 табл. 3.5) використовує характерні особливості даного протоколу, такі як мультіпоточность і використання множинних інтерфейсів (multi-homing). Методи зміни вмісту SCTP-пакетів засновані на тому, що кожна частина STCP-пакета може мати змінні параметри.

5) Система HICCUPS(колонка 5 табл. 3.5) Система HICCUPS (HIdden Communication system for CorrUPted NetworkS) - стеганографічна система з розподілом смуги пропускання для мереж з розділяється середовищем передачі даних (shared medium). HICCUPS використовує недосконалості середовища передачі - шуми і перешкоди, які є природними причинами спотворення даних

Більшість видів цифрової стеганографії знаходиться на стадії розробки та експериментів. Поки не можна зробити остаточні виводи щодо основних хаактеристик і точно стверджувати про надійність і швидкість передачі прихованих даних за допомогою протоколів, але ця тема є цікавою і новою.

6) На підставі аналізу матеріалів таблиць 3.4 і 3.5 можна зробити висновок, що найбільш поширене практичне застосування комп'ютерної стеганографії є використання надмірності аудіо та візуальної інформації, хоча популярність

голосових розмов в Інтернеті призводить до безперервного росту обсягів трафіку VoIP, очікується стрімкий розвиток стеганографічних методів, які використовують канали мережевої стеганографії для прихованої передачі.

3.2.3.3 Науково-технічні напрацювання стеганографічних методів забезпечення інформаційної безпеки систем IP – телефонії

Велика кількість вітчизняних та зарубіжних публікацій присвячена аналізу головної характеристики стегосистеми – її стійкості.

Серед останніх досліджень і публікацій варто виділити дослідження, що стосуються аналітичного огляду великої кількості алгоритмів вбудовування, запропонованих за останні роки класифікації стегосистем та методів вбудовування, математичного опису та структурної схеми стеганографічної системи захисту інформації на основі теорії секретних систем, проблем цифрової обробки сигналів при вбудовуванні інформації, підвищення пропускної здатності стегоканалу, забезпечення стійкості та непомітності вбудовування.

Кожен з пропонованих раніше методів відрізняється своїми якісними характеристиками, проте пошук оптимального співвідношення місткості контейнера і його спотворення триває досі. Для розширення стеганографічних задач використовують нові та удосконалюють старі методи.

Найефективнішим способом забезпечення конфіденційності інформації є суміщене використання стеганографічних і криптографічних засобів [51]. Тенденції розвитку засобів інформаційної комунікації, що спостерігаються зараз, сприяють значному збільшенню швидкості та обсягів передачі й обробки інформації, а також забезпеченню організації дистанційного доступу до глобальних інформаційних ресурсів та появі нових типів каналів зв'язку[56]. Приховування ж самого факту наявності секретних даних при їх передачі, зберіганні або обробці є завданням стеганографії. При цьому завдання виявлення інформації стає не таким важливим і вирішується в більшості випадків стандартними криптографічними методами. Під приховуванням існування

інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності секретного повідомлення, але і унеможливлення виникнення підозр стосовно цього, оскільки в останньому випадку проблема інформаційної безпеки адресується стійкості криптографічного коду [51,56].

У реальних системах складність перебудови алгоритмів впровадження повідомлень в залежності від ключа привела до того, що в більшості рішень стеганографічні ключі не використовуються. Побудова реальних ключових стеганосістем є складним завданням, що вимагає розробки легкоперебудовуємих алгоритмів приховування інформації, що є нереальним.

Сучасне використання стійких криптоалгоритмів разом з стеганографічним алгоритмом дозволяє досягти високої пропускної здатності створюваного стеганоканала з порівняно високою стійкістю проти спотворень в каналі і можливих атак противника.

3.2.3 За результатами попереднього пошуку за дослідженою тематикою установлено, що найбільш патентів на об’єкти промислової власності видано на удосконалення криптографічного методу забезпечення інформаційної безпеки, надругому місці апаратні методи, тощо (див. рис. 3.2).

Рисунок 3.2 Дінамика патентування основних відомих методів забезпечення інформаційної безпеки систем IP – телефонії

Висновки до розділу

В цьому розділу розглянуто перспективні методи, що використовуються для забезпечення інформаційної безпеки в системах IP-телефонії, виділено їх і визначено, що серед перспективних методів захисту інформації в системах IP – телефонії є методи основані на синтезі програмних, апаратних засобів та криптографічних і стеганографічних методів, які стали майже найголовніші для здійснення успішної економічної та комерційної діяльності фірм, виділено конкуруючі американські компанії Cisco та Avaya Inc, визначено різниці в підходах до організації корпоративних IP-мереж взагалі та визначено клас захисту обладнання їхнього виробництва, що є вирішальним фактором у виборі обладнання того чи іншого виробника, крім стандартних - ціна, продуктивність, функціональність. В цьому розділі описані основні характеристики, переваги й недоліки, були описанні нові криптографічні і стеганографічні методи. Здіснений порівняльний аналіз стеганографічних методів показав, що з найбільш поширеного практичного застосування комп'ютерної стеганографії є використання надмірності аудіо та візуальної інформації, хоча популярність голосових розмов в Інтернеті призводить до безперервного росту обсягів трафіку VoIP, і очікується стрімкий розвиток стеганографічних методів, які використовують канали мережевої стеганографії для прихованої передачі.

Не зважаючи на велику кільсть відібраних для подальшого аналізу документів, не вдалося виявити ні одного методу абсолютного забезпечення інформаційної безпеки систем IP – телефонії, тому відомі фірми ведуть дуже активні пошуки рішень щодо забезпечення інформаційної безпеки IP – телефонії.

Динаміка патентування відомих фірм-розробників інженерно-технічних заходів і засобів захисту та методів забезпечення інформаційної безпеки систем IP – телефонії, свідчить про те, що найбільш активними в цьому напряму досліджень є вітчизняні наукові організації, які найбільш всього патентують об’єкти промислової власності.

ВИСНОВКИ

Технологія IP–телефонії знаходиться у сфері діяльності інформаційного простору, в якому відбувається інформаційно-технічне протистояння, де головними об’єктами нападу і захисту є системи телекомунікаційні, управління і зв'язку, різні радіоелектронні засоби, та інформаційні ресурси. Для цього використовуються спеціальні засоби знищення, перекручення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж і комп'ютерних систем. Інформаційна технологія IP–телефонії має недоліки, пов’язані з безпекою інфраструктури мережі (прослуховування дзвінків, зміною їхнього змісту, схильність IP–системи до DoS–атак і т. п.).

З’явився небезпечний вид інформаційних загроз, який прискорено розвівається, відповідно сфер впливу проглядаються загрози: атака на бізнес (комерційне шпигунство, крадіжки баз даних, інформаційні дії який з метою підриву репутації тощо.) та контролюючі життєдіяльність суспільства пристрої (крадіжка, злом систем, нелегальне придбання можливості безкоштовно користуватися сервісами, видалення і зміна інформації про себе та \ або замовника та ін.) Ці правопорушення направлені проти конфіденційності, цілісності та доступності комп’ютерних систем, мереж і даних.

Комп'ютерні шахрайства, крадіжки вимагання та інше не є новими видами протиправних діянь, та засоби за допомогою яких вони здійснюються постійно удосконалюються, тому вже на етапі підготовки проекту IP–телефонії необхідно визначитися які механізми захисту інфраструктури доцільніше використовувати.

В результаті виконаного аналізу загроз в IP–телефонії, були визначені вразливості технології та загальні заходи захисту інформації, виявлені перспективні методи забезпечення інформаційної безпеки та науково-технічні напрацювання. Використання цих матеріалів допоможе створювати надійну

систему захисту інформації вже на початкових стадіях роботи. Виходячи із історичних та статистичних даних, виявлено, що найважливішими моментами для користувачів є доступність, масштабованість, ціна, простота і надійність використання IP-телефонії, якість при передачі голосу; серед вимог є захист від прослуховування. З огляду на вищезазначене можна стверджувати про зростання потреби розвитку методів забезпечення інформаційної безпеки IP-телефонії.

Найбільш досконалий захист від прослуховування забезпечує використання IP–телефонів із вбудованими засобами шифрування інформації та додатковий захист надає шифрування трафіку між телефонами і шлюзами. Але така функціональність збільшує тривалість проходження сигналу, що необхідно враховувати при побудові захищеної лінії зв'язку. Для передачі мовних сигналів і даних з локальних віртуальних мереж використовується загальна фізична пропускна смуга. При зараженні вузла вірусом або черв'яком може статися переповнювання мережі трафіком. Проте якщо вдатися до відповідно налагоджених механізмів QOS, трафік IP–телефонії має пріоритет при проходженні через загальні фізичні канали, і DoS–атака виявиться безуспішною. Атаки типу «відмова в обслуговуванні» на застосування IP–телефонії (наприклад, на сервери оброблення дзвінків) і на середовище передачі даних є серйозною проблемою. Протокол RTP (Real-Time Protocol) у IP–телефонії відповідає про атаки на середовище передачі даних. Для захисту мереж використовуються як вбудовані в мережеве устаткування механізми забезпечення інформаційної безпеки, так і додаткові рішення.

Відбиті в дипломній роботі перспективні напрямки методів забезпечення інформаційної безпеки в IP–телефонії допомагатимуть під час створення надійної системи захисту інформації вже на початкових стадіях роботи.

Розроблені пропозиції щодо захисту інформації можуть широко використовуватися для підвищення рівня інформаційної безпеки IP–телефонії.

Слід зазначити, що з розвитком технологій буде збільшуватися і обсяг інформації що в них обертається. Тому необхідність забезпечення конфіденційності, цілісності, доступності інформації буде тільки зростати.

Одним з головних недоліків є те, що регламентуючі документи є неоднозначними, мають різноманітні трактовки понять, які здатні значно ускладняти розуміння методів забезпечення інформаційної безпеки IP–телефонії, це може призвести до некоректного виконання процесів і істотно впливати на рівень інформаційної безпеки.

Проведене дослідження наочно показує, що безпека мереж IP - телефонії є відкритою для досліджень проблемою в новій технології зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України про захист інформації
2. Закон України Про телекомунікації
3. Порядок взаємоз'єднання та взаєморозрахунків операторів щодо здійснення діяльності з надання послуг фіксованого міжнародного, міжміського телефонного зв'язку із застосуванням технології IP-телефонії
4. ДСТУ 3575-97 Патентні дослідження.
5. Щербина Л. П. Телефонные аппараты / – М.: ВАС, 1972. – 235 с.
6. История развития телефона и телефонной связи. [Електронный ресурс].- Режим доступа: https://knowledge.allbest.ru/radio.
7. Ларин Д.А. Изобретение телефона и первые проекты в области защиты телефонных переговоров. 2017. [Електронный ресурс].- Режим доступа: https://cyberleninka.ru/
8. Островский А.В. История средств связи. Учебное пособие. СПб., 2009
9. Обоснование целесообразности внедрения новой технологии предоставления услуг связи на базе IP-телефонии. Понятие и история развития IP-телефонии. Технические и Економический аспекты данного вида связи. Оборудование для Интернет-телефонии Cisco Systems. [Електронный ресурс].- Режим доступа: http://www.allbest.ru/.
10. Технология IP-телефонии. Основные характеристики технологии IP-телефонії. 2011. [Електронный ресурс].- Режим доступа: https://otherreferats.allbest.ru/radio/00150003_2.html.
11. Avtandilko A. Основы IP-телефонии, базовые принципы, термины и протоколы. **13 июня 2013.** [Електронный ресурс].- Режим доступа: **https://habr.com/ru/post/183152/**
12. Каргин А.С. IP-телефония. 2012. [Електронный ресурс].- Режим доступа: // http://www.allbest.ru/
13. Киселёв В. Н. IP-телефония. 2005. [Електронный ресурс].- Режим доступа: *https://www.docsity.com / ip-telefoniya.*
14. Устюжанин К.В Доклад на тему «IP-телефония» Киров [Електронный ресурс].- Режим доступа: 2009// *https://works.doklad.ru/view*
15. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония. Москва «Радио и связь», 2001.
16. Feoktistova Olga. Простыми словами: Что такое SIP-телефония. 17.05.2017
17.Лекція 10. Інформаційне забезпечення мобільних систем ТК. [Электронный ресурс] - Режим доступа: http://www.its.kpi.ua/itm/ternovoy/discipline

18. Черкасов Д. Основи технології VoIP та IP-телефонії Національний Університет «Києво-Могилянська Академія» 2017
19. Кузнецов А.Е.,Пинчук А.В,Суховицкий А.Л. Построение сетей IP- телефони / Компьютерная телефония, 2010, №6. – с. 166-194.
20. Пархоменко В.Л., Алєксєєва І.В., Лемеш С. Б. Методи побудови системи зв'язку на основі IP -технологій./Вісник АМУ серія «Техніка» Вип.5 – 2012
21. Тарнавський Ю. А. Кузьменко І. М. Організація компютерних мереж. Підручник. КПІ ім. Ігоря Сікорського, 2018
22. Кузьменко І.С., Грицюк Ю.І. Використання IP- телефонії в інфраструктурі мережі та особливості її захисту від посягань зловмисників. Львів Україна/Вісник Національного технічного університету України «КПІ». Серія радіотехніка. Радіоаппаратобудування.- 2013.-№55.
23. Деребенцева К. Защитная IP- телефония. [Електронный ресурс].- Режим доступа: https://citicity.ru/15561/
24. Платов М. Что важно знать об IP- телефонии. [Електронный ресурс].- Режим доступа: https://www.oppenet/docs.RUS/voip.asterisk/1.html
25. Еталонная модель OSI. [Електронный ресурс].- Режим доступа: http://bourabai.kz/einf/Glava101-4.htm
26. VoIP - система зв'язку, що забезпечує передачу мовного сигналу по мережі Інтернет або по будь-яких інших IP-мережах. [Електронный ресурс].- Режим доступа: inmad.vntu.edu.ua › portal › static.
27. Русаков М. Видеокурс по основам HTML. [Електронный ресурс].- Режим доступа: srs.myrusakov.ru **;** Основные сценарии IP-телефонии. [Електронный ресурс].- Режим доступа: **https://studopedia.ru/3_28675_osnovnie-stsenarii-IP-telefonii.html**
28.Галатенко, В.А. Основи інформаційної безпеки. Інтернет-університет інформаційних технологій – ІНТУІТ.ру, 2007. [Електронный ресурс].- Режим доступа: **http://citforum.ck.ua/nets/articles/voip_cisco/2.shtml**
29. IP- телефония. Обзор технологий. [Електронный ресурс].- Режим доступа: **https://www.price.od.ua//articles.phtmlid/**
30. Росляков А.В. IP-телефонія; Москва, 2008.
31. Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. Телекомунікаційні системи та мережі.Том 1. Друге видання. Виправлено та доповнено. 2018[Електронный ресурс].- Режим доступа: **http://www.znanius.com/3591.html**

32. Стів Мак-Квері, Келлі Мак-Грю, Стівен Фой. Передача голосових даних по мережах Cisco Frame Relay, ATM и IP; Київ, 2007
33. Проект TIPHON (Telecommunication and Internet Protocol Harmonization over Networks). 2014. [Електронный ресурс].- Режим доступа: **https://www.ds77.ru/news/1229903/**; http://www.mini-server.ru/books/ip-telephony/75-ip2/1130-8-6-mexanizmy-bezopasnosti-v-proekte-tiphon
34. Баскаков И.В., Пролетарский А.В., Мельников С.А., Федотов Р.А. IP-телефония в компьютерных сетях [Електронный ресурс].- Режим доступа: https://bstudy.net/713477/informatika/obespechenie_bezopasnosti_baze_protokola; http://mayoroven.ru/docum/intuit/course-35
35. Гайворонський М.В. Безпека інформаційно-комунікаційних систем. К. Вид. группа ВНВ, 2009.-608с.
36.Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки. Вінниця ВНТУ 2009. [Електронный ресурс].- Режим доступа: https://studfile.net/preview/6012701/
37. Вдовиченко О.О. Методи забезпечення інформаційної безпеки. 2017. [Електронный ресурс].- Режим доступа: https://informatika.udpu.edu.ua/?page_id=3405
38. Wikipedia.org/wiki/Інформаційна_безпека.
39. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. -Київ. 2004. 508 с.
40. Головач М. Кібернетична безпека. - Київ. 2015. [Електронный ресурс].- Режим доступа: https://studfile.net/preview/5009924
41. Майданюк Н., Чугуєва О. Стандарт ISO 27001: огляд. Інформаційна безпека в сучасному суспільстві 29-30 листопада 2018р.Львів.
42. Дорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно “Критериев оценки надежных компьютерных систем TCSEC (Trusted Computer Systems Evaluation Criteria)”, США, “Оранжевая книга”. – Бизнес и безопасность, 1998, № 1.
43. Громаков Ю.А. Стандарты и системы подвижной радиосвязи, - М.: Мобильные телесистемы и Эко-Трендз, 1997, 240 с.
44. Майборода О.В., Алєксєєв М.О. Використання аутентифікації 802.1X для побудови високопродуктивного обчислювального середовища з некластеризованими ресурсами. / НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «Київський політехнічний інститут» ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НДІ Телекомунікацій. / Шоста

міжнародна науково-технічна конференція та Четверта студентська науково-технічна конференція «Проблеми телекомунікацій» присвячені Дню науки і Всесвітньому дню телекомунікацій 24–27 квітня 2012рік. Матеріали конференції м. Київ
45. Максимів О. Аналіз стану забезпечення конфіденційності інформації про користувача в Інтернеті .Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
46.Вараксін О.О., Василіву Є.В., Горохов С.М., Кільдишев В.Й., Кононович В.Г. Кібербезпека мереж наступного покоління. Навчальний посібник. Одеса.2013.
47.Щербак Г.В., Мельникова Л.І., Рубан І.В., Садовий К.В., Сумцов А.В.Сучасні телекомунікаційні мережі у цивільному захисті. Підручник. Харків 2007. 255с.
http://www.univer.nuczu.edu.ua/tmp_metod/107/STKMvCZ.pdf
48. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации. Учебное пособие. / ИУНЛ ПГУТИ. Самара.2010. – 330с
49. Бройдо В.Л., Ильина О.П. Вычислительные системы, сети и телекоммуникации. Учебник для вузов 4-е изд.- СПб. Питер, 2011-560 с.
50. Чунарьова А.В., Потапенко Є.О. Система стеганографічного захисту інформації. [Електронний ресурс]. Режим доступу: http://www.rusnauka.com/10_DN_2013/Informatica/4_132640.doc.htm.
51. Конахович Г.Ф. Компьютерная стеганография / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: «МК-Пресс», 2006. – 288 с.
52.Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. (НАУ) Сучасні стенографічни методи захисту інформації. Науково-технічний журнал НАУ «Захист інформації» №1, 2011
https://www.researchgate.net/publication/311663916_SUCASNI_STEGANOGRAFICNI_METODI_ZAHISTU_INFORMACII
53.Грибунин О.В. Основные положения стеганография.-М. Солон. Пресс, 2002.-261с.
54. Барсуков В.С. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности XXI века. – М «Специальная техника» 2007-225с.
55. Корченко О.Г., Василіу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації // Науково-технічний журнал "Захист інформації". – 2010, № 1. – С. 77-89.

56. Липка Т.Б. Модифікація методу стеганографії з використанням матриці судоку Київ – 2018 https://ela.kpi.ua/handle/123456789/23212
57. Коркач И.В., Пирогова Ю.И.Использование технологий IP-телефонии для скрытой передачи информации.// Информационная безопасность человека, общества, государства.-.2012. — Т. 9, № 2. — С. 124–128.
58. Песков О.Ю.. Халабурда Ю.Г. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи. Известия ЮФУ. Технические науки. https://cyberleninka.ru/article/n/primenenie-setevoy-steganografii-dlya-skrytiya-dannyh-peredavaemyh-po-kanalam-svyazi/viewer
59. Горпенюк А.Я., Стороженко А.О. Дослідження та порівняльнийй аналіз стеганографічних методів для впровадження даних у цифрові файли http://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/3733/horpeniukayastorozhenkoao.pdf
60. Романчук Р. О. Методи комп'ютерної стеганографії для цифрових контейнерів у вигляді зображення. 2018. https://ela.kpi.ua/bitstream/123456789/23826/4/Romanchuk_magistr.pdf
61. Юдін О.К., Зюбіна Р.В., Фролов О.В Аналіз стеганографічних методів приховування інформаційних потоків у контейнері різних форматів. https://cyberleninka.ru/article/n/analiz-steganografichnih-metodiv-prihovuvannya-informatsiynih-potokiv-u-konteyneri-riznih-formativ/viewer
62. БелкинаТ.А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности / Т. А. Белкина.// Молодой ученый. — 2018. — № 11 (197). — С. 36-44. — URL: https://moluch.ru/archive/197/48821/ (дата обращения: 16.05.2020).
63. Овчарук І.В., Пристінська А.А. Аналіз чутливості зорового прийняття інформації людиною на основі стеганографічного методу A LSB file:///C:/Users/USER/Downloads/Vodt_2017_1_24.pdf

Додаток А

Класифікація загроз

Таблиця Класифікація загроз безпеки [31]

Класифікаційна ознака	Класифікаційні групи
За джерелом погрози	1) внутрішні — джерело на території України; 2) зовнішні — джерело розташоване за кордоном держави
За природою виникнення загроз	1) викликані політикою держави; 2) ініційовані іноземними державами; 3) що надходять від кримінальних структур; 4) що надходять від конкурентів або контрагентів
За ймовірністю реалізації	1) реальні — можуть здійснюватися в будь-який момент часу; 2) потенційні — можуть реалізуватися у разі формування певних умов
Стосовно людської діяльності	1) об'єктивні — формуються незалежно від цілеспрямованої діяльності; 2) суб'єктивні — створюються свідомо, наприклад, розвідувальною, підривною й іншою діяльністю, організованою злочинністю
За об'єктом зазіхання	1) на інформацію; 2) на майно; 3) на фінанси; 4) на персонал; 5) на ділове реноме
За можливістю прогнозування	1) що прогнозуються на рівні господарюючого суб'єкта; 2) що не піддаються прогнозу
За наслідками	1) загальні — відбуваються на всій території України або більшості її суб'єктів; 2) локальні — мають вплив на окремі об'єкти
За величиною нанесеного (очікуваного) збитку	1) катастрофічні; 2) значні; 3) що спричиняють труднощі