МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Український державний університет науки і технологій

Кафедра «Електронні обчислювальні машини»

«ДО ЗАХИСТУ»

Завідувач кафедри
_____ Жуковицький І. В.
(підпис) (ПІБ)
«21» 12 2021 р.

ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології
(шифр) (назва)

Спеціальність 123 Комп'ютерна інженерія
(код) (повна назва)

Тема Дослідження та розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу

Theme Research and development of demonstration means of steganographic information protection and steganalysis

Керівник дипломної роботи	доцент		Остапець Д. О.
	(посада)	(підпис)	(ПІБ)
Консультант розділу з БЖД	доцент		Саблін О. І.
	(посада)	(підпис)	(ПІБ)
Нормоконтролер	доцент		Шаповалов В. О.
	(посада)	(підпис)	(ПІБ)
Студент групи	КС2021		Холодарь К. С.
	(група)	(підпис)	(ПІБ)
Student			Kholodar Karyna
			(family name)

Дніпро
2021

Міністерство освіти і науки України

Український державний університет науки і технологій

Кафедра «Електронні обчислювальні машини»

ДОВІДКА

За результатами перевірки випускної кваліфікаційної роботи здобувача вищої освіти Холодарь Карини Сергіївни

на тему:

«Дослідження та розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу»

в роботі не виявлено порушень академічної доброчесності.

Керівник ВКР, к.т.н., доц. каф. ЕОМ Д.О. Остапець

Український державний університет науки і технологій

Факультет Комп'ютерних технологій і систем кафедра Електронні обчислювальні машини
Спеціальність Комп’ютерна інженерія

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
_____
(підпис)
«___»_____20__ р.

ЗАВДАННЯ

до дипломної роботи на здобуття освітнього ступеня _____«магістр»_____
(освітнього ступеня)

студента групи КС2021 _____Холодарь Карини Сергіївни_____
(номер групи) (ПІБ)

1 Тема дипломної роботи Дослідження та розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу_____
_____
_____

затверджена наказом по університету від «31»__08__2021 р. № 508ст.

2 Термін подання студентом закінченої роботи_____

3 Вихідні дані до дипломної роботи_____
_____
_____
_____

4 Зміст пояснювальної записки (перелік питань до розробки) _____
_____
_____
_____
_____

5 Перелік креслень (демонстраційного матеріалу) _____
_____
_____
_____
_____
_____
_____
_____
_____

6 Розділи та консультанти

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека у надзвичайних ситуаціях	Саблін О. І.		

КАЛЕНДАРНИЙ ПЛАН

Назва розділу	Термін виконання	Обсяг розділу, %

Дата видачі завдання: «___»_____ 20___ р.

Керівник дипломної роботи _____ Остапець Д. О.
(підпис) (ПІБ)

Завдання прийняв до виконання _____ Холодарь К. С.
(підпис) (ПІБ)

РЕФЕРАТ

Холодарь К. С. Дослідження та розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу. – Український державний університет науки і технологій, кафедра електронних обчислювальних машин. – Дипломна робота. – 85 с., 33 рис., 4 табл., 39 джерел, 3 додатки.

Об’єктом дослідження в даній дипломній роботі є мережева стеганогафія та стегоаналіз з використанням у якості стегоконтейнерів ICMP та IP пакетів.

Метою дипломної роботи є розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу з використанням мережевої стеганографії. Здійснено огляд та аналіз методів та засобів стеганографії, дано характеристику мережевої стеганографії та стегоаналізу. Обрано метод модифікації полів у заголовках ICMP та IP пакетів. Описано організацію, інформаційну структуру та функції розроблюваних програмних засобів. Наведено алгоритми роботи, діаграми класів, написано та відлагоджено програмне забезпечення. Розроблено інструкцію та методику з використання засобів у цілях навчання. Проведено аналіз даних, що передаються, на предмет виявлення стеганоаналітиком. Розроблені програмні засоби можуть використовуватися для прихованого обміну даними та у навчальному процесі.

СТЕГАНОГРАФІЯ, СТЕГОАНАЛІЗ, МЕРЕЖА, ОБМІН ІНФОРМАЦІЄЮ, ICMP, IP, ПРОТОКОЛИ ПЕРЕДАЧІ ІНФОРМАЦІЇ, ОДНОРАЗОВИЙ БЛОКНОТ, C++.

ABSTRACT

Kholodar K.S. Research and development of demonstration means of steganographic information protection and steganalysis - Ukrainian State University of Science and Technology, department of electronic computing machines. - Diploma project. - 85 p., 33 fig., 4 tables, 39 sourses, 3 appendixes.

The subject of research in this project is network steganography and stegoanalysis using ICMP and IP packets as stegocontainers.

By the method of diploma robots is the development of a demonstration of steganographic information and steganalysis from the victorious steganography of steganography. A review and analysis of methods and tools of steganography, a description of network steganography and stegoanalysis. The method of modification of fields in ICMP headers and IP packets is chosen. The organization, information structure and functions of the developed software are described. Algorithms of work, diagrams of classes are given, the software is written and debugged. The instruction and a technique on use of means for the purposes of training are developed. An analysis of the transmitted data for detection by a steganoanalyst was performed. Developed software can be used for covert data exchange and learning.

STEGANOGRAPHY, STEGANALYSIS, NETWORK, INFORMATION EXCHANGE, ICMP, IP, INFORMATION TRANSMISSION PROTOCOLS, DISPOSABLE NOTEBOOK, C ++.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ОС – операційна система

VoIP – Voice over IP

TranSteg – Transcoding Steganography

TCP – Transmission Control Protocol

SCTP – Stream control transport protocol

RSTEG – Retransmission Steganography

LACK – Lost Audio Packets Steganography

IP – Internet Protocol

ID – Identifier

ICMP – Internet Control Message Protocol

HICCUPS – Hidden Communication system for CorrUPted networks

ВСТУП

На сьогодні проблема захисту інформації з обмеженим доступом від несанкціонованого доступу актуальна як ніколи. Для вирішення цієї проблеми було створено безліч криптографічних засобів для захисту інформації, що включають в себе засоби шифрування та захищені протоколи передачі даних на їх основі. Ці засоби призначені для захисту інформації під час передачі по відкритих каналах, але цей захист можна посилити, почавши передавати інформацію по прихованим каналах, щоб потенційні зловмисники не змогли виявити самого факту передачі. Прихований канал може існувати в будь-якому відкритому каналі, в якому існує деяка надмірність. Приховувані дані називаються стеганограмою.

Галузь мережевої стеганографії та стеганоаналізу достатньо нова та до кінця не вивчена. Але питання надійної передачі інформації у мережі піднімається щодня. Тому тема дипломної роботи є актуальною.

Тема дипломної роботи затверджена наказом по університету №508ст від 31.08.2021 р.

Метою дипломної роботи є розробка засобів демонстрації стеганографічного захисту інформації та стегоаналізу з використанням мережевої стеганографії. Розроблені програмні засоби можуть використовуватися для прихованого обміну даними та у навчальному процесі.

Основні положення роботи доповідались та були схвалені на 81-ій науково-практичній конференції студентів та молодих вчених УДУНТ, XIV та XV Міжнародних науково-практичних конференціях «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» у 2020 – 2021 рр.

Представлена дипломна робота складається зі вступу, 5 розділів та висновків.

У розділі 1 представлений огляд та аналіз методів стеганографії. Розглянуто загальну структуру стеганосистеми та її складових. Наведено особливості використання контейнерів різного типу та вимог до них. Наведено

характеристику методів мережевої стеганографії. Для описаних методів проведено порівняльний аналіз за невідьемними характеристиками. Наведено методи стеганографічного аналізу.

У розділі 2 наведено організацію комплексу, та розроблено його інформаційну структуру. Здійснено опис пакетів передачі даних та процес обміну даними між абонентами.

У розділі 3 здійснено вибір середовища та мови програмування для розробки програмного забезпечення, описано функції ПЗ, розроблено алгоритми їх роботи, на основі яких розроблено програмне забезпечення.

У розділі 4 наведена методика використання розроблених засобів, проаналізовано пакети передачі стеганограм та представлена можливість для використання ґпз у навчальному процесі.

У розділі 5 сформовані основні вимоги безпеки при виконані робіз з персональним компьютером. Проведено оцінку робочого місця програміста-розробника на підставі вимог до робого місця. Розглянуто основні шкідливі виробничі фактори при роботі за персональним компьютером, сформовано основні дії працівників у надзвичайних ситуаціях.

В додатках А, Б, В наведено вихідний код програм.

1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ СТЕГАНОГРАФІЇ

1.1 Загальні відомості та поняття стеганографії

З появою писемності завдання забезпечення конфіденційності та достовірності повідомлень, що передаються, набуло особливої актуальності. Справді, словесне або жестове повідомлення доступне незнайомцю лише на короткий час, коли воно «в дорозі», одержувач може не сумніватися в його достовірності, тому що він бачить свого співрозмовника.

Інше питання, коли повідомлення написано - воно вже живе окремим життям та має свій шлях, який часто дуже відрізняється від шляху його творця. Повідомлення, написане на папері, існує в матеріальному світі набагато довше, і у людей, які хочуть прочитати його зміст проти волі відправника та одержувача, набагато більше шансів це зробити.

Тому саме після появи писемності з’явилося мистецтво криптографії, мистецтво «таємного письма» - низка методів, призначених для секретної передачі записаних повідомлень від однієї людини іншій [1, 2].

Дані про перші методи криптографії дуже уривчасті. Існує гіпотеза [3], що стародавні шумери одними з перших почали використовувати стеганографію, оскільки вчені виявили численні глиняні клинописні таблички. Особливістю цих табличок були два шари інформації: одна записка була покрита шаром глини, що містила іншу інформацію.

Однак у цієї теорії є противники [4]. Вони вважають, що це була не спроба приховати інформацію, а просто особливість листа. У Стародавній Греції для письма використовували вощені дерев’яні дошки. Трактат Геродота «Історія» описує засоби, за допомогою яких перський цар Ксеркс завоював Грецію. Повідомлення було подряпано на дошці під шаром воску, тому сама дошка виглядала як порожня заготівля для написання.

Інший епізод, який стосується того ж часу, - це передача повідомлення за допомогою голови раба. Щоб передати таємне послання, голили голову раба, наносили татуювання, а коли волосся відростало, його відправляли з повідомлення.

У Китаї писали листи на смужках папірусу. Потім, щоб приховати повідомлення, шари тексту листа згортали в кульки, покривали воском, а потім заковтувалися посильними.

Темне середньовіччя породило не тільки інквізицію: посилення стеження привело до розвитку як криптографії, так і стеганографії. Саме в середні століття вперше було застосовано спільне використання шифрів і стеганографічних методів.

В 1499 абат Іоанн Тритемій описав безліч способів прихованої передачі даних у своєму трактаті «Steganographia» [5]. Саме в цій книзі вперше було запроваджено поняття стеганографії.

При цьому тайнопис ділився на два види: шифрування (криптографія) та приховування інформації (стеганографія). Слово «стеганографія» походить від грецьких слів «steganos» – прихований та «graphein» – писати.

Стеганографія – це метод організації зв'язку, який власне приховує саму наявність зв'язку [6]. На відміну від криптографії, де зловмисник точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в нешкідливі послання так, щоб неможливо було запідозрити сам факт існування вбудованого таємного послання.

Стеганографія являє собою своєрідне доповнення до криптології. Приховування повідомлення методами стеганографії суттєво знижує ймовірність виявлення самого факту обміну повідомленням. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту [7].

Як і будь-який новий напрямок, стеганографія, незважаючи на велику кількість відкритих публікацій і щорічні конференції, довгий час не мала єдиної термінології.

До недавнього часу для опису моделі стеганографічної системи використовувалася запропонована 1983 році Сіммонс так звана "проблема ув'язнених". Пізніше, на конференції Information Hiding: First Information

Workshop в 1996 році було запропоновано використовувати єдину термінологію і обговорені основні терміни. К. Шеннон надав загальну теорію тайнопису, яка є базисом стеганографії як науки. У сучасній стеганографії існує два основних типи файлів: повідомлення-файл, який призначений для приховування, і контейнер-файл, який може бути використаний для приховування в ньому повідомлення. При цьому контейнери бувають двох типів. Контейнер-оригінал (або "порожній" контейнер) – це контейнер, який не містить прихованої інформації. Контейнер-результат (або "заповнений" контейнер) - це контейнер, який містить приховану інформацію. Під ключем розуміється секретний елемент, який визначає порядок занесення повідомлення в контейнер.

Основні положення сучасної стеганографії є наступними [7, 8]:

– методи приховування повинні забезпечувати автентичність і цілісність файлу.

– передбачається, що противнику повністю відомі можливі стеганографічні методи.

– безпека методів ґрунтується на збереженні стеганографічних перетворень основних властивостей відкрито переданого файлу при внесенні до нього секретного повідомлення і деякої невідомої противнику інформації - ключа.

– навіть якщо факт приховування повідомлення став відомий противнику через спільника, витяг самого секретного повідомлення являє складну обчислювальну задачу.

У зв'язку зі зростанням ролі глобальних комп'ютерних мереж стає все більш важливим значення стеганографії. Аналіз інформаційних джерел комп'ютерної мережі Internet дозволяє вставити висновок, що в даний час стеганографічні системи активно використовуються для вирішення наступних основних завдань:

– захист конфіденційної інформації від несанкціонованого доступу;

– подолання систем моніторингу та управління мережевими ресурсами;

– камуфлювання програмного забезпечення;

– захист авторського права на деякі види інтелектуальної власності.

Стеганографічна система або стегосистема - сукупність засобів та методів, що використовуються для формування прихованого каналу передачі інформації.

Контейнер – будь-яка інформація, призначена для приховування таємних повідомлень.

Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер або стегоконтейнер, що містить вбудовану інформацію.

Узагальнена модель стегосистеми представлена на рис. 1.1.

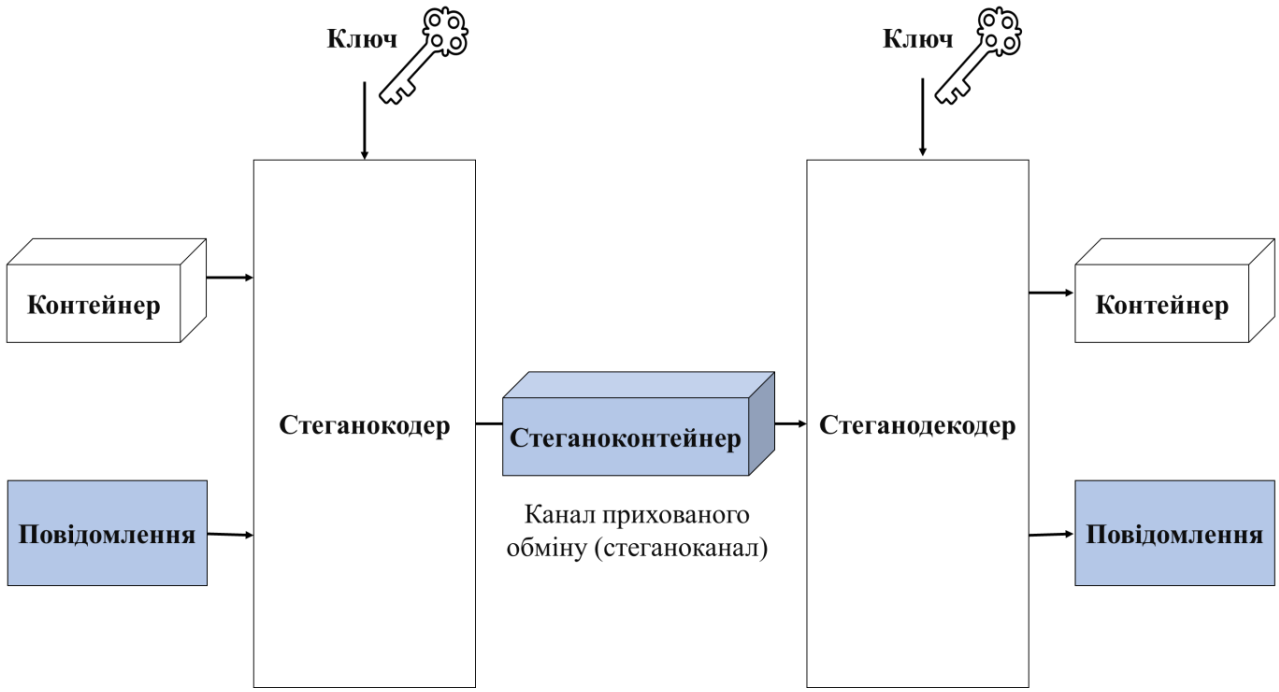

Рисунок 1.1 – Узагальнена модель стегосистеми

Стеганографічний канал або просто стегоканал – канал передачі стего.

Стегоключ або просто ключ - секретний ключ, необхідний приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистемі може бути один або декілька стегоключів [8].

При побудові стеганосистеми повинні враховуватись наступні положення [9]:

– властивості контейнера повинні бути модифіковані, щоб зміну неможливо було виявити під час візуального контролю, вона жодним чином не повинна привернути увагу атакуючого;

– противник має повне уявлення про стеганографічну систему та деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному противнику, є ключ, за допомогою якого тільки його власник може встановити факт присутності та зміст прихованого повідомлення;

– якщо противник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних до тих пір, поки ключ зберігається в таємниці;

– потенційний противник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні чи розкритті змісту таємних повідомлень.

За аналогією з криптографією, за типом стегоключа стегосистеми можна поділити на два типи:

– з секретним ключем;

– з відкритим ключем.

У стеганосистемі з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу.

Різні ключи використовуються у стеганосистемах з відкритим ключем для вбудовування і вилучення повідомлення, котрі віждрізняються настільки, що неможливо витягти один ключ з іншого за допомогою обчислень. Таким чином, один ключ (відкритий) може вільно передаватися по незахищеному каналу зв'язку. Також ця схема добре працює у разі взаємної недовіри між відправником і одержувачем.

1.2 Особливості використання контейнерів різного типу та вимоги до них

У більшості сучасних методів, що використовуються приховування повідомлення в цифрових контейнерах, має місце зворотна залежність надійності системи від довжини, приховуваного повідомлення (рис. 1.2).

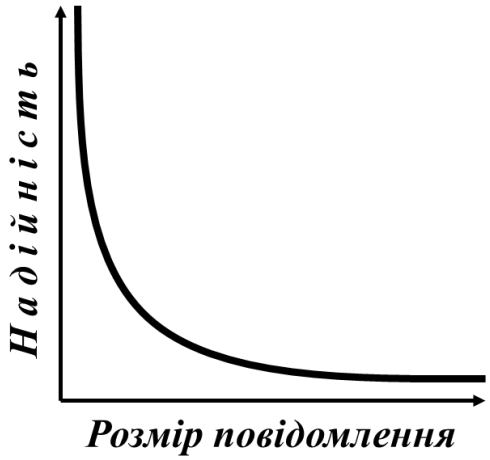

Рисунок 1.2 – Залежність надійності системи від розміру, приховуваного повідомлення

Ця залежність вказує на те, що збільшення обсягу вбудованих даних знижує надійність системи (на той самий розмір контейнера). Таким чином, контейнер, який використовується в стегосистемі, накладає обмеження на обсяг вбудованих даних.

Довжини контейнерів можна розділити на два типи: безперервні (потокові) та обмеженої (фіксованої) довжини. Особливістю потокового контейнера є те, що неможливо визначити його початок чи кінець [10]. Більше того, неможливо заздалегідь дізнатися, якими будуть наступні біти шуму, що призводить до необхідності включення бітів, які приховують повідомлення, в потік, а самі приховані біти вибираються спеціальним генератором, який регулює. відстань між послідовними бітами потоку.

Найважче для одержувача в безперервному потоці даних – визначити, коли починається приховане повідомлення. Якщо є потоковий контейнер для сигналів синхронізації або кордонів пакетів, приховане повідомлення починається відразу після них. У свою чергу, у відправника можуть виникнути

проблеми, якщо він не впевнений, що потік контейнера буде достатньо довгим, щоб вмістити все секретне повідомлення.

Перевагою використання контейнерів фіксованої довжини для відправника полягає у тому, що він заздалегідь знає розмір файлу і може вибрати біти, що приховують, у відповідній помилковій випадковій послідовності. З іншого боку, контейнери фіксованої довжини, як згадувалося вище, мають обмежену ємність, і іноді вбудоване повідомлення може не поміститися у файл-контейнера.

Інший недолік полягає в тому, що відстані між бітами, що приховують, рівномірно розподілені між найбільш коротким і найбільш довгим заданими відстанями, в той час як істинний випадковий шум буде мати експоненційний розподіл довжин інтервалу. Звичайно, можна породити псевдовипадкові експоненційно розподілені числа, але цей шлях зазвичай дуже трудомісткий. Однак на практиці найчастіше використовуються саме контейнери фіксованої довжини як найбільш поширені і доступні. Можливі наступні варіанти контейнерів [11]:

– контейнер генерується самою стегосистемою. Такий підхід можна назвати конструюючою стеганографією.;

– контейнер вибирається з кількох контейнерів. У цьому випадку створюється велика кількість альтернативних контейнерів, тому що потім обирається найбільш підходящий для приховування. Такий підхід можна назвати селектуючою стеганографією.даних. Такий підхід можна назвати селективною стеганографією. При виборі оптимального контейнеру з безлічі згенерованих найважливішим вимогою є природність контейнера. Єдина проблема полягає в тому, що навіть оптимально організований контейнер дозволяє приховати невелику кількість даних у дуже великому обсязі контейнера;

– контейнер надходить ззовні. В даному випадку відсутня можливість вибору контейнера і для приховування повідомлення береться перший

контейнер, що не завжди підходить для вбудованого повідомлення. Цей підхід можна назвати безальтернативною стеганографією.

1.3 Класифікація методів стеганографії

Сучасну стеганографію в загалом класифікують на три розділи [12]:

– класична;

– комп’ютерна;

– цифрова.

На рис. 1.3 представлена класифікація сучасної стеганографії за використанням методів реалізації.

Рисунок 1.3 – Методи сучасної стеганографії

Класична стеганографія – це методи, що використовувались ще до появи сучасних комп’ютерних систем, та методи що не потребують участі обчислювальних машин/комп’ютерів.

Два протилежні розділи стеганографії класичній – комп’ютерна та цифрова. Комп'ютерна стеганографія включає в себе методи, що базуються на властивостях комп'ютерної платформи та використання спеціальних властивостей комп'ютерних форматів даних. Цифрова стеганографія – напрямок сучасної стеганографії, заснований на прихованні або впровадження додаткової інформації у цифрові об'єкти. При цьому виникають деякі спотворення файлів-контейнерів.

В епоху великого розвитку мережевого обміну даними цифрова стеганографія являє собою найбільший інтерес, з точки зору захисту інформації, як найбільш перспективний напрям.

Одним із прикладів цифрової стеганографії є мережева стеганографія, де у якості носія даних, що приховуються, використовуються протоколи моделі OSI. Саме дослідження у цьому напрямі є більш актуальними, і вони зумовлені також рішенням завдання приховування інформації від незаконного вилучення, копіювання, тощо, так як, це може понести не лише матеріальні збитки та порушення державної таємниці, але й загрозу життю людини.

1.4 Характеристика методів мережевої стеганографії

У мережевій стеганографії роль носія виконує пакет, що передається по мережі.

Основні параметри мережевої стеганографії – це пропускна здатність прихованого каналу, ймовірність виявлення та стеганографічна вартість.

Пропускна здатність – обсяг секретних даних, який може бути надіслано в одиницю часу.

Ймовірність виявлення визначається по можливості виявлення стеганограм у певному носії. Найбільш популярний спосіб виявити

стеганограму – це аналіз статистичних властивостей, отриманих даних та порівняння їх із типовими значеннями для цього носія.

Стеганографічна вартість характеризує рівень зміни носія після впливу на нього стеганографічного методу.

На рис. 1.4 приведена класифікація методів мережевої стеганографії.

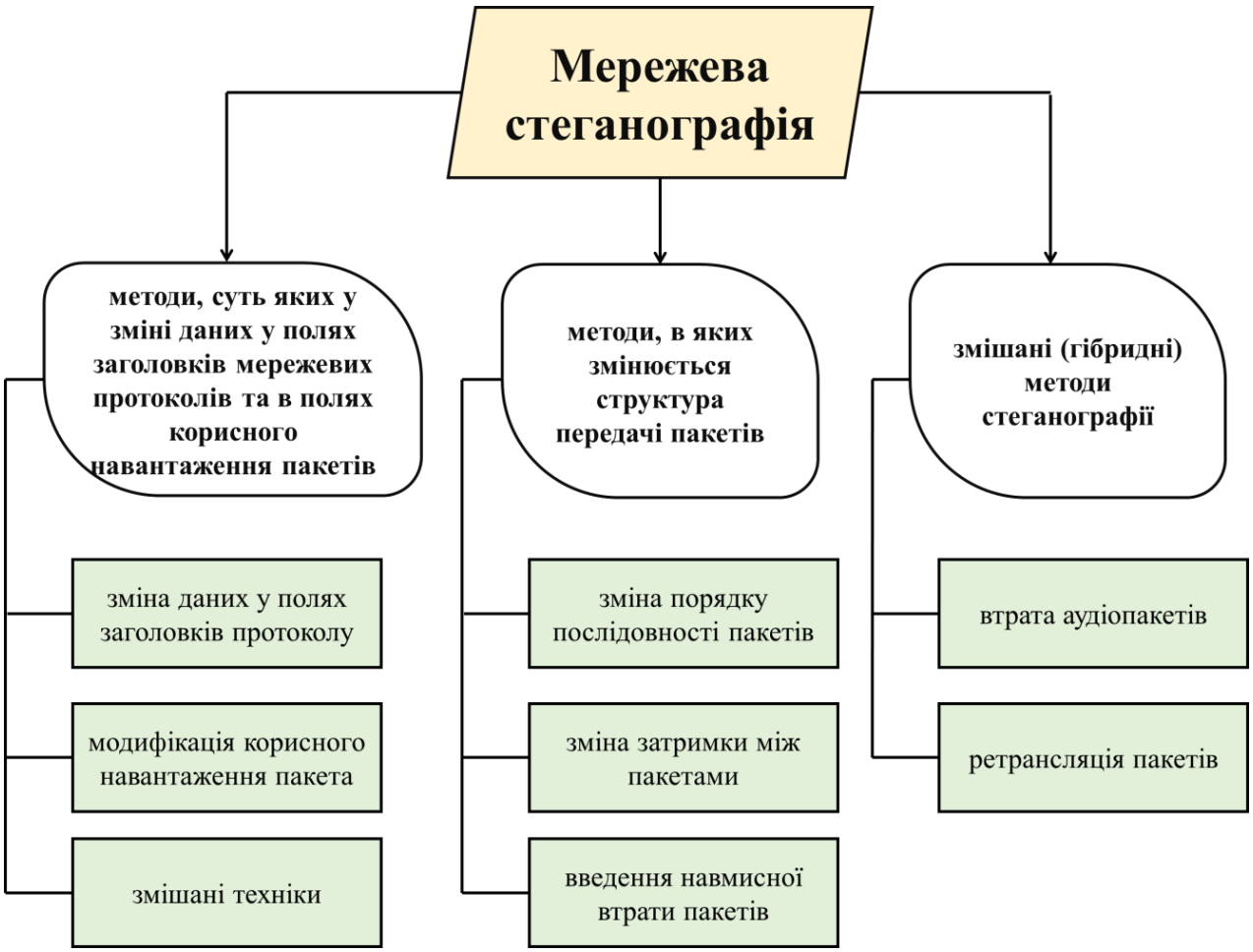

Рисунок 1.4 – Класифікація мережевих методів стеганографії

Головна ідея методів модифікації полів заголовків полягає у використанні деяких полів заголовків для внесення до них стеганограми.

Це можливо за рахунок деякої надмірності в даних полях, тобто існують певні умови, в яких значення даних полях не будуть використовуватися при передачі пакетів. Найчастіше використовуються поля заголовків IP та TCP протоколів [13].

Перевагами даного методу є відправка без змін інформації від відправника до отримувача, але це також обмежує кількість інформації, що передається. Головними недоліками є те що данні, що передаються,

знаходяться у відкритому доступі, та можуть бути легко зчитані спостерігачем (зловмисником).

Метод модифікації мережевих пакетів, що змінюють корисне навантаження VoIP пакету TranSteg реалізується за рахунок перекодування [14]. TranSteg, також, використовується в реалізації стиснення відкритих даних (наприклад, потокові відео). Метод дозволяє отримати добру стеганографічну пропускну здатність у 32 кб/с з найменшою різницею в затримці пакету. Недоліком являється складність реалізації методу, також при стиснені втрачається якість мовленої інформації.

Метод із застосуванням механізмів SCTP-протоколу полягає на використанні таких характерних характеристик як багатонитковість та використання множинних інтерфейсів [15]. Суть змішаного методу на основі SCTP протоколу ґрунтується на використанні певних механізмів протоколу, які дозволяють організувати навмисне пропускання пакетів у потоці, без його повторної посилки. Пізніше до пакету додається стеганограма, і він повторно відправляється.

Використання змішаного методу з використанням модифікації пакетів представлена в системі HICCUPS [16]. Система використовує недоліки обміну даними у мережевому середовищі, такі як поміхи та шум в середовищі зв’язку, а також звичайну схильність даних до спотворення. Цей метод має низьку смугу пропускання (залежить від мережі), громіздку реалізацію, низьку стеганографічну вартість і високу складність виявлення. Проте аналіз кадрів з невірною контрольною сумою може призвести до виявлення використання даного методу.

Змішаний метод стеганографії RSTEG заснований на механізмі повторної посилки пакетів [16, 17]. Його стеганографічна пропускна здатність приблизно дорівнює пропускній здатності методів з модифікацією пакетів та при цьому вище, ніж у методів зміни порядку передачі пакетів.

Метод LACK – це стеганографія з використанням навмисних затримок аудіопакетів [14]. Цей метод також реалізується через VoIP. Зв'язок через IP-телефонію складається з двох частин: сигнальної та розмовна.

Даний метод має певні переваги. Пропускна здатність більша в порівнянні з іншими алгоритмами, що використовують аудіопакети. Але при навмисному виклику втрат виникає погіршення якості зв'язку, що може викликати підозру або у звичайних користувачів, або у зловмисника, що прослуховує [18]. Виходячи з представлених методів стегоаналізу LACK, можна зробити висновок, що метод має середню складність виявлення. Реалізація методу складна і може бути неможлива в межах деяких операційних систем.

Таємна передача інформації у сегментахTCP ґрунтується на зміні довжини TCP-сегменту таким чином, щоб значення довжини даних, що передаються TCP-сегментом, містило у собі інформацію о конфіденційному тексті. Вибір TCP-сегментів в якості контейнерів дозволяє досягти того, що ні в заголовку TCP-сегменту, ні в заголовку IP-дейтаграми біти секретного тексту не містяться в явному вигляді [18, 19, 20].

Також одним із важливих службових протоколів стеку TCP/IP є ICMP, який призначений для розсилки повідомлень про помилки та інші виняткові ситуації, а також перевірки зв'язку, трасування маршрутів та багато іншого. Незважаючи на те, що ICMP відноситься до службових протоколів, наявність або відсутність даних у полі корисного навантаження пакета само по собі не може бути використане як ознака прихованої передачі інформації [21].

Також у заголовка TCP - висока стеганографічна вартість . Будь-яка зміна в будь-якому з полів, не передбачена специфікацією, тягне за собою порушення протоколу TCP . А явне порушення протоколу призводить до виявлення стеганограми. Як мінімум, з'являється можливість довести, що вона там є. Тому на думку автора використання того методу стеганографії з можливістю приховування інформації всередині заголовка TCP шляхом прямої

зміни полів – не ефективним і складним через високу стеганографічну вартість і ймовірність виявлення.

Дивлячись на різну вагу характеристик методів стеганографії їх по різному використовують для реалізації програмних забезпечать. Таким чином першим продуктом був CovertTCP [22] реалізований у 1997 році, головною метою котрого було приховування каналів обміну з використанням заголовків TCP та IP протоколів (табл. 1.1).

Таблиця 1.1 – Порівняльний аналіз відомих методів мережевої стеганографії

Метод мережевої стеганографії / Характеристика	**HICCUPS**	**LACK**	**RSTEG**	**TranSteg**	**Використання SCTP multihoming**	**Використання протоколів SCTP (гібрид)**	**Модифікація блоків даних у SCTP протоколах**	**Модифікація полів у заголовках TCP та IP пакетів**	**Модифікація полів у заголовках ICMP и IP пакетів**
Відносна пропускна здатність	висока	висока	середня	дуже висока	дуже низька	низька	низька	середня	середня
Відносна ймовірність виявлення	дуже низька	низька	середня	низька	висока	середня	дуже висока	висока	низька
Відносна стеганографічна вартість	дуже висока	висока	висока	низька	середня	середня	дуже низька	висока	низька
Відносна складність реалізації	дуже висока	висока	висока	середня	середня	середня	дуже низька	низька	низька
Популярність використання	+	+	+	+	-	+	+	+	-

Головна перевага використання IP та ICMP – низька стеганографічна вартість. У RFC 792 [23] вказано те, що поле ID заголовку ICMP може приймати будь-які значення, на розсуд кожної конкретної реалізації echo request / echo respond. Теж саме відноситься до поля ID заголовку IP [20]. Тобто його зміна взагалі ніяк не впливає на протокол у цілому.

Саме тому у даній дипломній роботі буде розглядатись метод реалізації стеганографії за допомогою ICMP та IP протоколів.

1.5 Характеристика методів мережевого стегоаналізу

Завдання вилучення прихованого повідомлення з контейнера, навидь при оптимальних умов атаки, може бути дуже складним. Однозначно стверджувати про факт існування прихованої інформації можна лише після її виділення у явному вигляді. Іноді метою стеганографічного аналізу є не відновлення алгоритму взагалі, а пошук, наприклад, конкретного стеганоключа, використовуваного для вибору бітів контейнера в стеганоперетворенні [24].

Одним з головних завдань стеганоаналізу є дослідження можливих слідів застосування стеганографічних засобів та розробка методів, які б виявляти факти їх використання. Застосування спеціального стеганографічного перетворення вимагає індивідуального підходу до стеганоаналітика.

Стегоаналітичні методи за широтою аналізу контейнерів поділяються на вузьконаправленні та універсальні (рис. 2.1).

Рисунок 2.1 – Стеганоаналітичні методи

Вузьконаправленний стегоаналітичний метод використовує знання цільової стеганографічної техніки, та може підходити лише для конкретного виду стеганографії.

Універсальний метод використовується для виявлення кількох видів стеганографії. Зазвичай, універсальні методи не вимагають знання операцій вкладання. Тому його ще називають – сліпий метод.

Вузьконаправлені способи, тобто. орієнтовані одним певним алгоритмом, у плані знаходження зашифрованих даних є ефективнішими. У той же час вони мають серйозний недолік – у разі навіть невеликої і малозначної зміни алгоритму, дані вже можуть залишитися нерозпізнаними. Перевагою сліпих (універсальних) методів є широкий спектр алгоритмів приховування, над якими вони можуть працювати. У той же час ці методи потребують «навчання», від якості якого залежать їх стегоаналітичні можливості [25].

Методи мережевого стеганоаналізу ті самі, що і в звичайному стеганоаналізі, але з поправкою на специфіку контейнерів.

Збирання статистики, пошук аномалій та закономірностей: невірний порядок пакетів, порушення протоколів, порушення стандартів і т.д, будь-які відхилення від норми – це непряма підозра факту передачі інформації.

1.6 Висновки за розділом

Розглянуті основні поняття стеганографії, особливості використання контейнерів та класифікація методів стеганографії та стегаоаналізу.

Проведено порівняльний аналіз методів мережевої стеганографії. Завдяки цьому аналізу став можливим вибір конкретного методу реалізації стеганографії, а саме приховування інформації у заголовках ID протоколів передачі ICMP та IP.

2 ОРГАНІЗАЦІЯ ТА ІНФОРМАЦІЙНА СТРУКТУРА РОЗРОБЛЮВАЛЬНИХ ЗАСОБІВ

2.1 Структура заголовків дейтаграм

Жодна з поширених ОС (Windows/Linux) не надає зручний інтерфейс для роботи з мережевими пакетами на рівні нижче транспортного.

Наприклад, у Windows можна отримати максимум інтерфейс сокетів, тобто надається IP адреса та Порт, та функції "прийняти", "відправити".

Всі інші функції по формуванню покатів ОС бере на себе та не дозволяє програмісту втручатись у цей процес. Тобто засобами Windows змінити за бажанням вміст заголовків IP та TCP – неможливо. Для цього необхідно працювати з мережевою картою, в обхід мережевого стеку операційної системи.

У дипломній роботі буде розглядатись утиліти ping та підвиди ICMP – echo request / echo respond. Головна перевага IP та ICMP протоколів, як і було зазначено раніше, – низька стеганографічна вартість. У специфікації RFC 729 [23] вказано те, що поле ID заголовку ICMP (рис. 2.1)може приймати будь-які значення, на вибір кожної конкретної реалізації echo request / echo respond. Теж саме відноситься і до поля ID заголовку IP [20] (рис. 2.2). Тобто їх зміна в загалом не впливає на протокол у цілому. До того ж echo request / echo respond простіше реалізувати з використанням бібліотек для роботи з мережевою картою на пряму.

Відповідно [24], поле ID заголовку ICMP, використовується для ідентифікації сеансу пінгу, а Sequence Number – для співставлення запиту та відповіді, тобто щоб можливо було зрозуміти на котрий запит прийшла отримана відповідь.

Приклад: Відправка 5 echo request повідомлень, отримання 5 echo respond. Якби використовувався ping Linux, то у всіх 10 пакетів буде однаковим поле ID (рис 3.2).

Тобто цей метод підходе для вирішення складної задачі, як ідентифікація отримувачем пакетів, у котрих присутня стеганограма, від тих, в яких її нема.

Рисунок 2.1 – Формат заголовку ICMP «Ехо-повідомлення та повідомлення у відповідь на ехо»

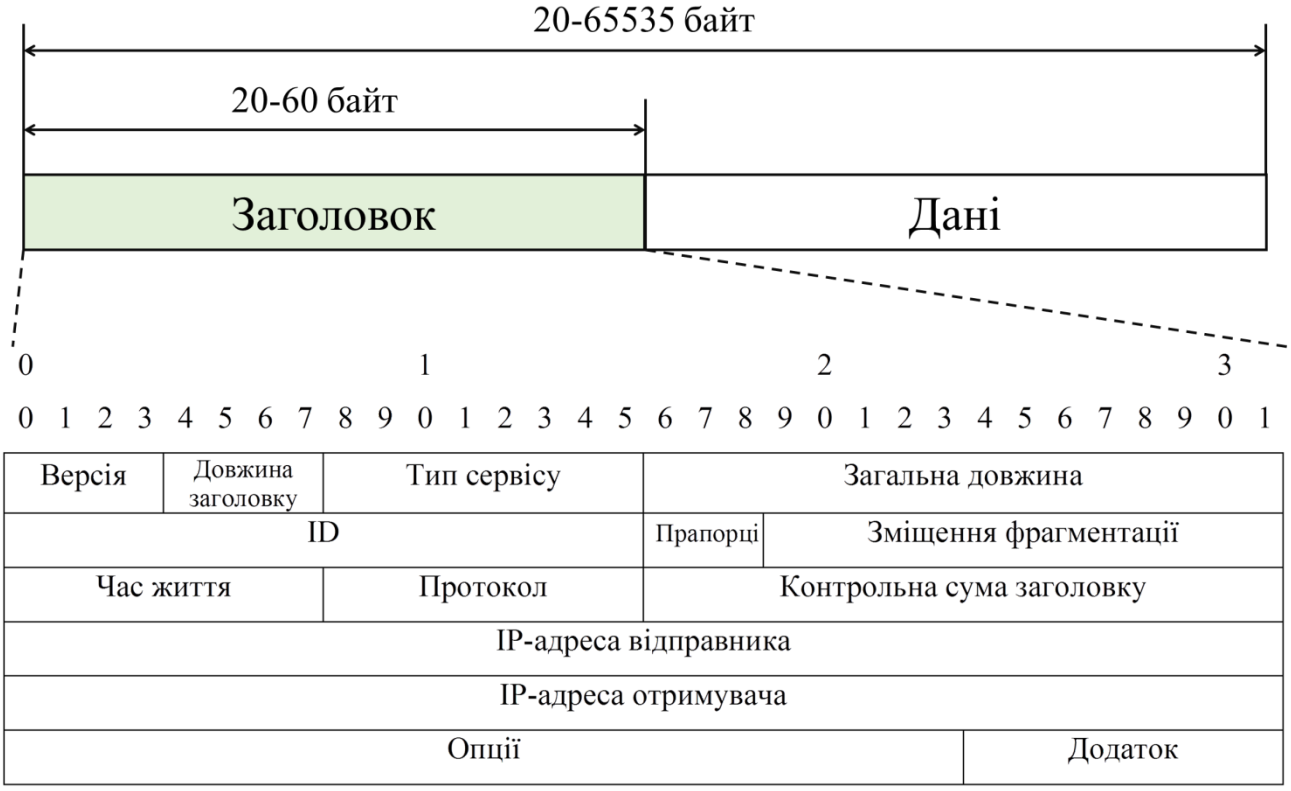

Рисунок 2.2 – Формат заголовку IP-дейтаграми

Саме данні у вигляді стеганограми можливо помістити у поле ID заголовку IP пакету, а маркер ідентифікації у поле ID заголовку ICMP пакету.

2.2 Вибір криптографічних функцій

У роботі є необхідність використання криптографічних функцій/шифрування для наступного:

– формування стеганоключа;

– шифрування/дешифрування даних, що передаються.

Стеганоключ формується з загального секретного ключа до котрого застосовується алгоритм формування контрольної суми RFC 1071 [25]. Алгоритм дозволяє отримати 2 байти (16 біт) інформації, котра у подальшому буде використовуватись як маркер ідентифікації.

Шифрування даних буде відбуватись завдяки методу шифрування – одноразовий блокнот (XOR) [26]. Шифр являється абсолютно стійким, так як розмір ключа дорівнює або більше тексту для шифрування. І це є невід'ємним фактором при виборі алгоритму шифрування. Також алгоритм простий у реалізації для мов високого рівня.

2.3 Схема взаємодії між абонентами

Обмін інформацією відбувається між двома абонентами – відправник та одержувач (рис 2.3).

Обмін загальним секретним ключем відбувається за межами реалізації розроблювального комплексу.

На підставі загального секретного ключа формується стеганоключ завдяки використання алгоритму контрольної суми, та отримується 2 байти інформації – це маркер за котрим отримувач буде розрізняти прослухуванні пакети від тих що адресовані йому, від тих що ні. Маркер вставляється у поле ID заголовку ICMP пакету.

Дані, що передаються, відправником шифруються алгоритмом одноразового блокнота (XOR). У якості ключа виступає загальний секретний ключ. Шифротекст (стеганограма) розбивається на блоки по 2 байт та вставляються у поле ID заголовку IP пакету. Сформовані пакети передаються одержувачу. Обсяг даних, що передаються, штучно зменшено до 20 байт, так як масова відправка пакетів з одного джерела може викликати підозру, що являє собою непряму підозру факту передачі інформації.

Одержувач прослуховує трафік на предмет наявності пакетів ICMP з необхідним ID (маркером), та при знаходженні витягує та розшифровую

стеганограму. Також для підтримки видимості дотримання протоколу отримувач відправляє ICMP-відповідь.

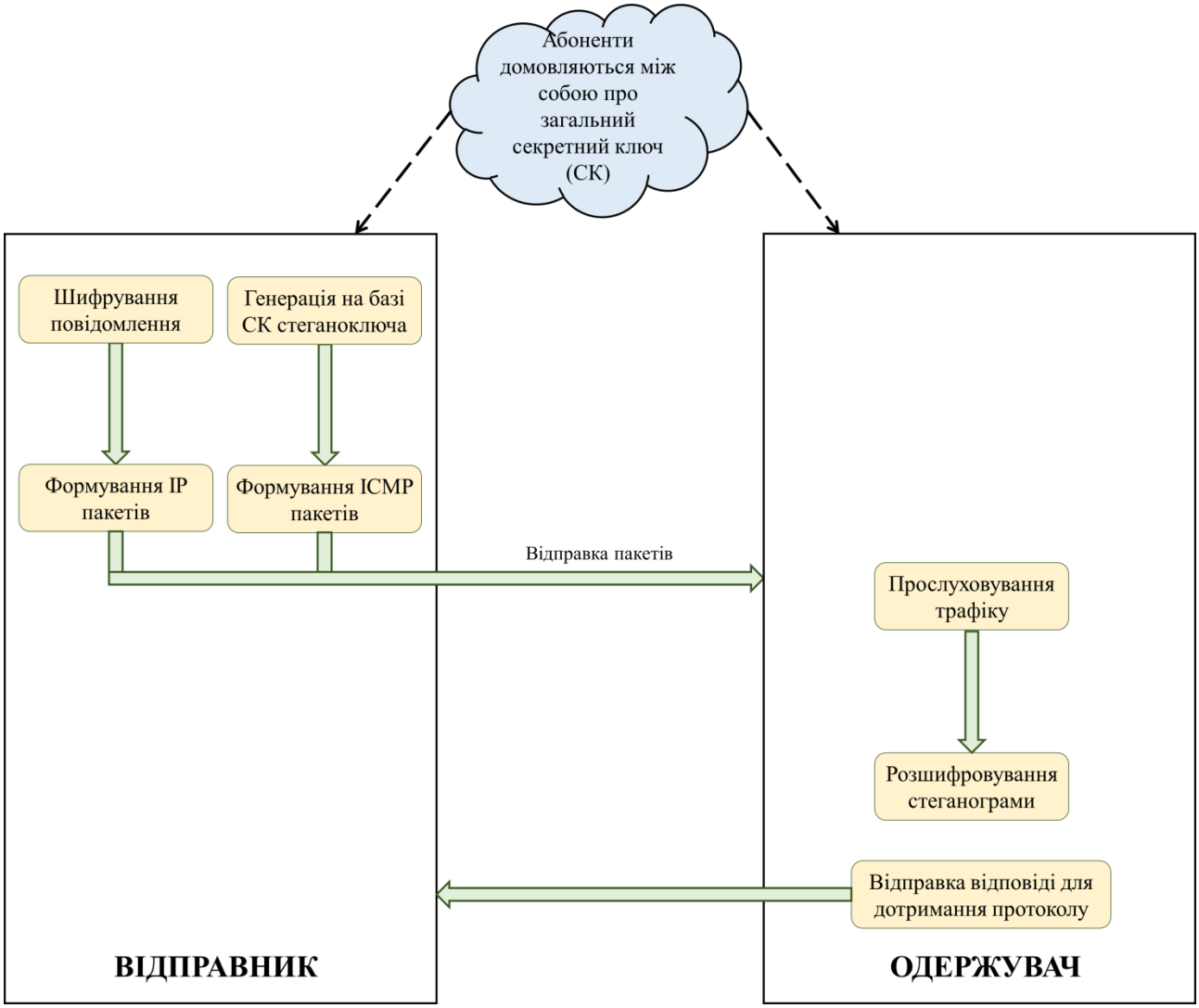

Рисунок 2.3 – Схема взаємодії між абонентами

ICMP-пакети вкладаються у IP-дейтаграми, котрі у подальшому входять до складу канального кадру (рис. 2.4).

У методі використання ICMP протоколу непогана здатність передачі даних. В середньому довжина ICMP пакету приблизно 100 байт та на кожні 100 байт ми можемо надіслати - 2 байти стеганограми.

Наприклад, візьмемо метод з використанням TCP/IP пакетів. У мережах Ethernet не можна передавати кадр більше 1514 байт – віднімаємо заголовки e Ethernet, IP, TCP і отримуємо 1460 байт. Відповідно до RFC 793 [19] стандарту TCP, значення sequence number та acknowledgment number слугує для підтвердження передачі. Нехай sequence number дорівнює 1000, розмір

корисного навантаження TCP = 200 байт, тоді у відповідь має прийти acknowledgment number = 1201.

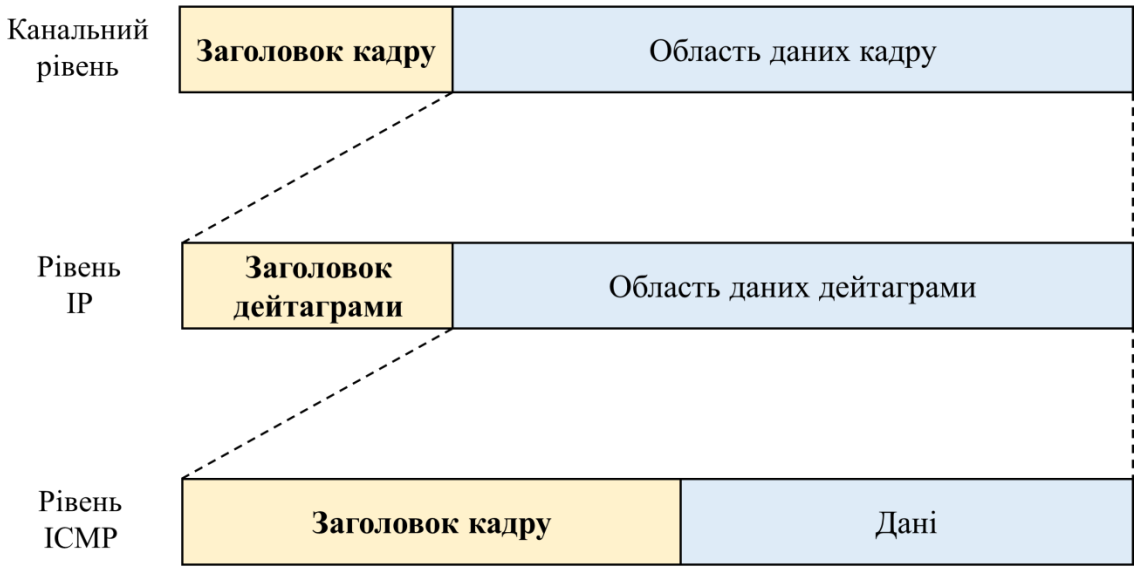

Рисунок 2.4 – Схема вкладення ICMP –пакетів до кадру

З цього випливає, що значення sequence number при передачі одного кадру не може бути збільшено на число більше максимального розміру пакета Ethernet, тобто 1460. Якщо збільшити sequence number на значення більше 1460, за допомогою додавання до оригінального sequence number стеганограми – стеганоаналітик може щось запідозрити. Оскільки для кодування 1460 нам потрібно 11 біт, за умови максимального дотримання стандарту RFC 793 ми можемо в заголовку TCP передавати лише 10 біт інформації. Якщо sequence number відрізняються більш ніж на 1460, то той же Wireshark починає розглядати ці TCP сегменти як частини різних TCP потоків, тобто вони нібито не належать різним процесам, але при цьому всі прямують в один порт і Wireshark буде їх помічати різними кольорами. Це привертає увагу аналітика і є непрямим підтвердженням факту передачі. І ще один важливий момент – аналітик може помітити невідповідність розміру пакета і значення acknowledgment number, якщо не змінювати розмір відповідно до числа, що додається до sequence number. Разом – використовуючи TCP пакети можливо надіслати 10 біт даних, за середньої довжині пакетів від 100 до 1000 байт. Тобто при максимальній довжині пакету TCP, пропускна здатність за методом

модифікації ICMP/IP заголовків у 16 разів вища, ніж при використанні методом модифікації TCP/IP.

2.4 Висновки за розділом

Розглянуті формати пакетів передачі ICMP/IP та їх вкладання до кадру, криптографічні функції.

Розроблено схему взаємодії між абонентами з використанням обраних стеганоконтейнерів та криптографічних функцій. Також представлена оцінка ефективності використання протоколів ICMP та TCP.

3 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Вибір засобів реалізації

Для реалізації засобу демонстрації мережевої стеганографії за методом модифікації полів у заголовках ICMP/IP пакетів обрано середовища розробки Visual Studio 2019, мова програмування C++ стандарту C++11[27].

Середовище розробки Visual Studio 2019 обрано за наступними критеріями:

– підтримка мови C++;

– зрозумілий інтерфейс;

– можливість рефакторингу коду.

Компілятори C++ є на кожній операційній системі, більшість програм легко переноситься з платформи на платформу, з середовищем розробки та бібліотеками не виникає проблем.

Мова програмування C++ була обрана за головним критерієм – необхідність використання бібліотеки WinPcap, котра призначена для використання разом з мовами C/C++.

Бібліотека WinPcap [28] використовується для реалізації роботи з мережевими даними, що надходять на мережеву карту комп’ютера.

Для реалізації аналізу трафіку, тим самим демонстрації обміну повідомленнями використовується – WireShark [29], так як це програмне забезпечення підтримується на різних ОС та різних їх версіях.

3.2 Діаграма класів

Програма складається з 4 основних класів (рис. 4.1), та допоміжних класів (рис. 4.2), що використовуються для обробки помилок.

Клас ICMP packet є похідним від IP packet , або успадковує його. Це просто масив із вказівниками на різні місця цього масиву для зручнішої роботи із заповненням полів пакету. Є клас Adapter – в його основі лежать функції з

бібліотеки WinPcap , яка є надбудовою над packet.lib: Adapter – надбудова над WinPcap.

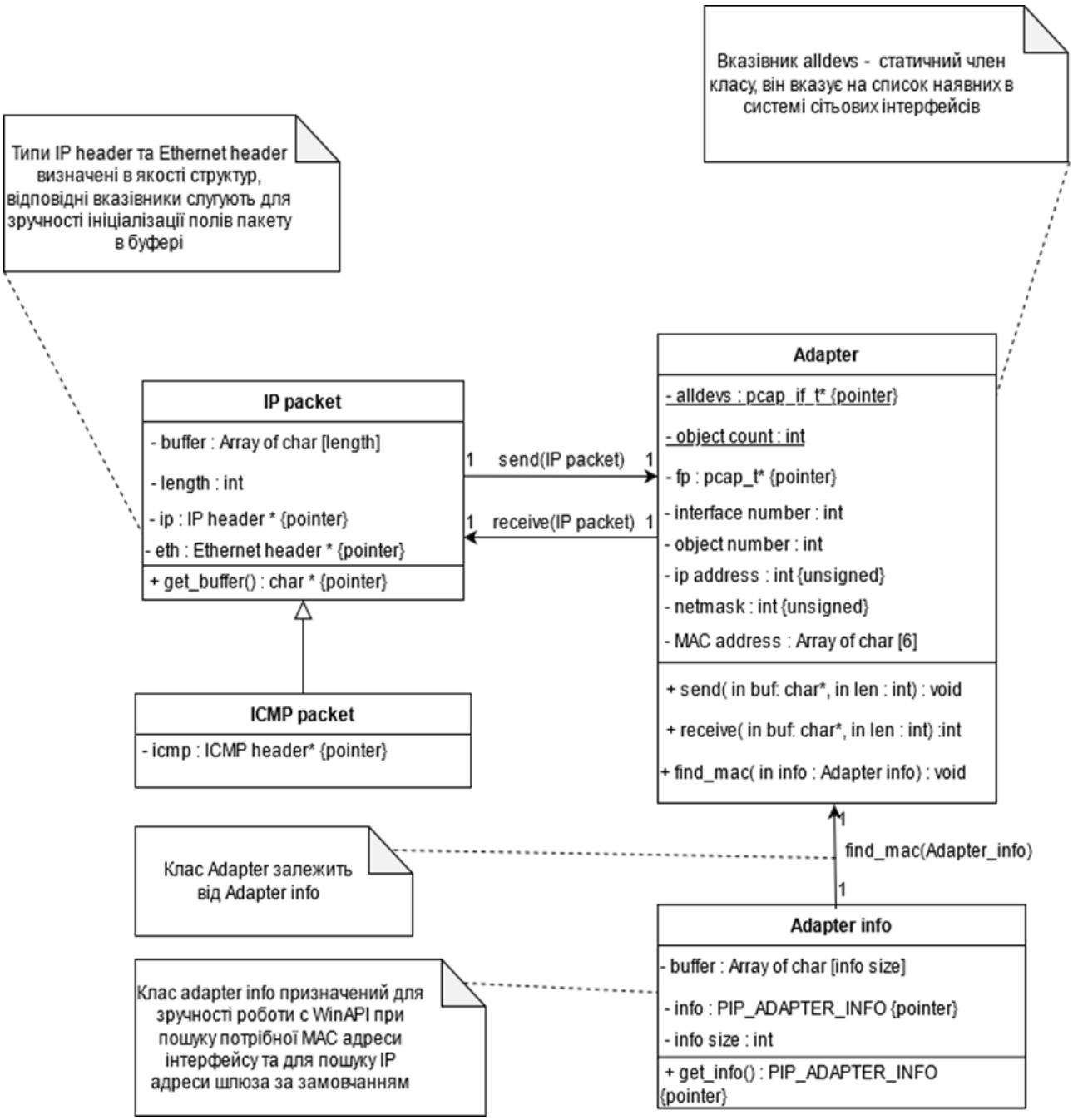

Рисунок 3.1 – UML діаграма класів

Проблема WinPcap в тому, що вона не дозволяє дізнатися MAC адреси інтерфейсу, хоча дозволяє посилати пакети через нього. Щоб дізнатися MAC треба чи за допомогою функції з packet.lib безпосередньо у мережевої карти, або дізнаватись у Windows. Тому Adapter info це надбудова над інтерфейсом WinAPI.

Також на рис. 3.1 вказано через які методи взаємодіють класи ПЗ.

winpcap_adapter::adapter	Клас призначений для більш зручної работи з мережевими інтерфейсами напряму в обхід интерфейсу сокетів Windows
winpcap_adapter::adapter_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter
winpcap_adapter::adapter_info	Клас призначений для зручного користування наявним інтерфейсом WinAPI для пошуку детальної інформації о встановленому мережевому обладнанні
winpcap_adapter::adapter_info_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter adapter_info
packet::ethernet_header	Структура описує структуру заголовку протоколу Ethernet пакету на канальному рівні
packet::icmp_header	Структура описує структуру заголовку протоколу ICMP пакету на мережевому рівні згідно RFC 792
packet::ip_header	Структура описує структуру заголовку протоколу IP пакету на мережевому рівні згідно RFC 791
packet::ip_packet	Клас створений для зручної роботи з редагування мережевих пакетів перед відправкою та після їх перехоплення з можливістю редагування заголовків канального та мережевого рівня
packet::icmp_packet	Клас наслідуваний від ip_packet, призначений для роботи с пакетами типу ICMP
packet::MAC_address	Об'єднання, для зберігання MAC-адрес
packet::packet_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter
packet::u_16	Об'єднання, для доступу до байтів в середині типу unsigned short
packet::u_32	Об'єднання, для доступу до байтів в середині типу unsigned int
packet::u_64	Об'єднання, для доступу до байтів в середині типу unsigned long long

Рисунок 3.2 – Скріншот «Ієрархія класів з описом»

packet	
u_16	Об'єднання, для доступу до байтів в середині типу unsigned short
MAC_address	Об'єднання, для зберігання MAC-адрес
ethernet_header	Структура описує структуру заголовку протоколу Ethernet пакету на канальному рівні
u_32	Об'єднання, для доступу до байтів в середині типу unsigned int
u_64	Об'єднання, для доступу до байтів в середині типу unsigned long long
ip_header	Структура описує структуру заголовку протоколу IP пакету на мережевому рівні згідно RFC 791
icmp_header	Структура описує структуру заголовку протоколу ICMP пакету на мережевому рівні згідно RFC 792
ip_packet	Клас створений для зручної роботи з редагування мережевих пакетів перед відправкою та після їх перехоплення з можливістю редагування заголовків канального та мережевого рівня
packet_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter
icmp_packet	Клас наслідуваний від ip_packet, призначений для роботи с пакетами типу ICMP
winpcap_adapter	
adapter	Клас призначений для більш зручної работи з мережевими інтерфейсами напряму в обхід интерфейсу сокетів Windows
adapter_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter
adapter_info	Клас призначений для зручного користування наявним інтерфейсом WinAPI для пошуку детальної інформації о встановленому мережевому обладнанні
adapter_info_error	Допоміжний класс для обробки помилок та виключень, які можливо виникнуть при роботі з об'єктами класу adapter adapter_info

Рисунок 3.3 – Скріншот «Класи, структури, об'єднання та інтерфейси з описом»

3.3 Розробка алгоритмів програмного забезпечення

Програмне забезпечення (ПЗ) має наступні функції:

– шифрування та дешифрування даних, що передаються;

– відображення всіх локальних мережевих інтерфейсів;

– вибір за абонентом: приймати, чи відправляти повідомлення;

– вибір текстового файлу для відправки;

– перегляд отриманого повідомлення;

– зберігання останнього повідомлення без втручання абоненту;

– вивід підказок по роботі з ПЗ.

Головною функцією ПЗ – є функція main() (рис. 3.4). Завдяки цій функції відбувається безпосередній запуск процесів, звернення до інших функцій, та реалізовано завершення процесів ПЗ.

Блок 1 – Початок роботи комплексу.

Блок 2 – Обробка вхідних параметрів.

Блок 3 – Перевірка на виникнення винятку.

Блок 4 – Відкриття необхідних файлів, застосування фільтру до обраного інтерфейсу.

Блок 5 – Перевірка на виникнення винятку.

Блок 6 – Встановлення прапорців.

Блок 7 – Якщо прапор встановлено на відправлення даних, надсилаємо API запит.

Блок 8 – Виклик функції SendStg.

Блок 9 – Якщо прапор встановлено на одержання даних, виклик функції WaitEchoRequest.

Блок 10 – Перевірка на виникнення винятку.

Блок 11 – Вбудована обробка винятків.

Блок 12 – Завершення роботи.

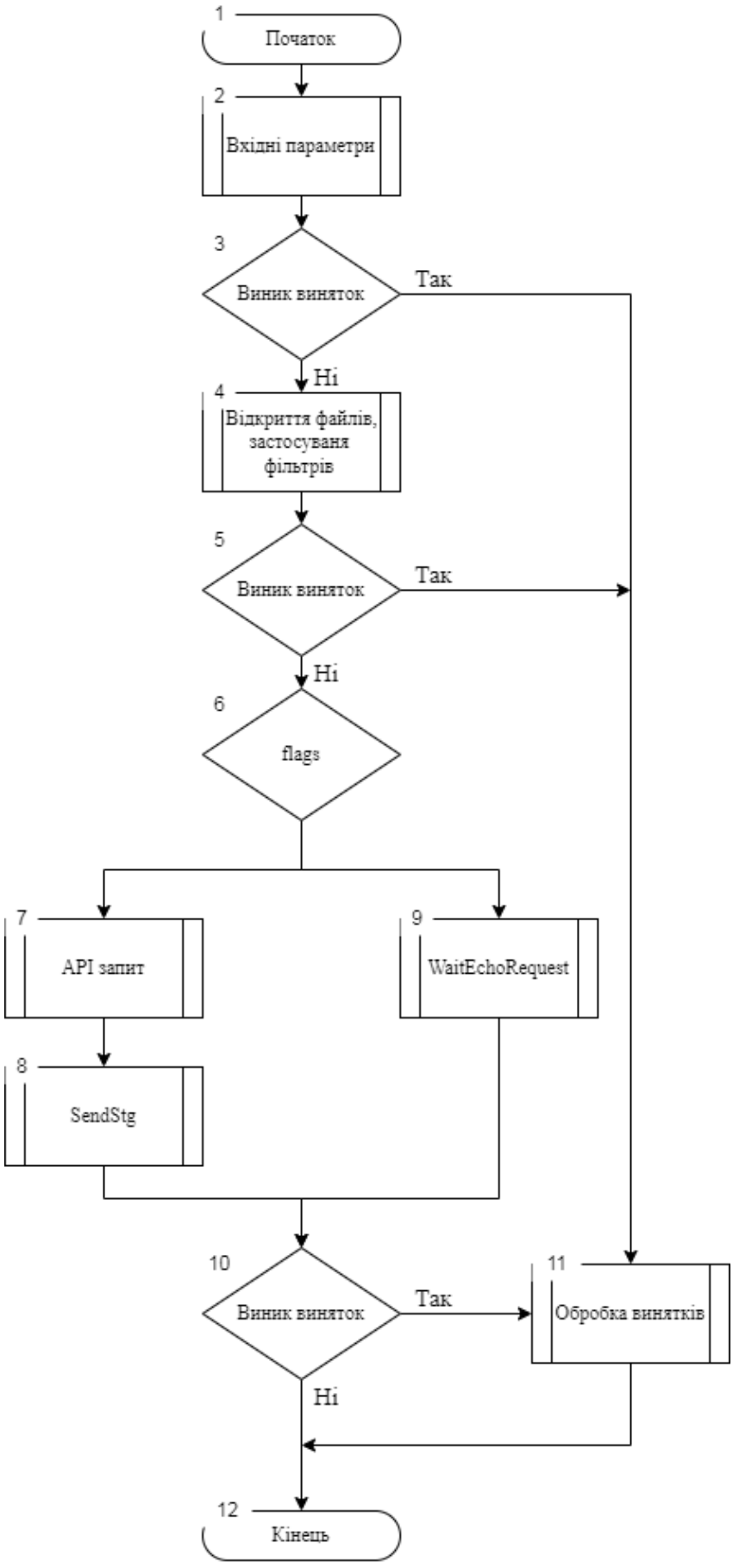

Рисунок 3.4 – Блок-схема функції main()

Блок-схема функції StgSend, до котрої звернення відбувається у функції main(), наведена на рис. 3.5. Якщо абонент обирає роль відправника, то алгоритм йде до цієї функції.

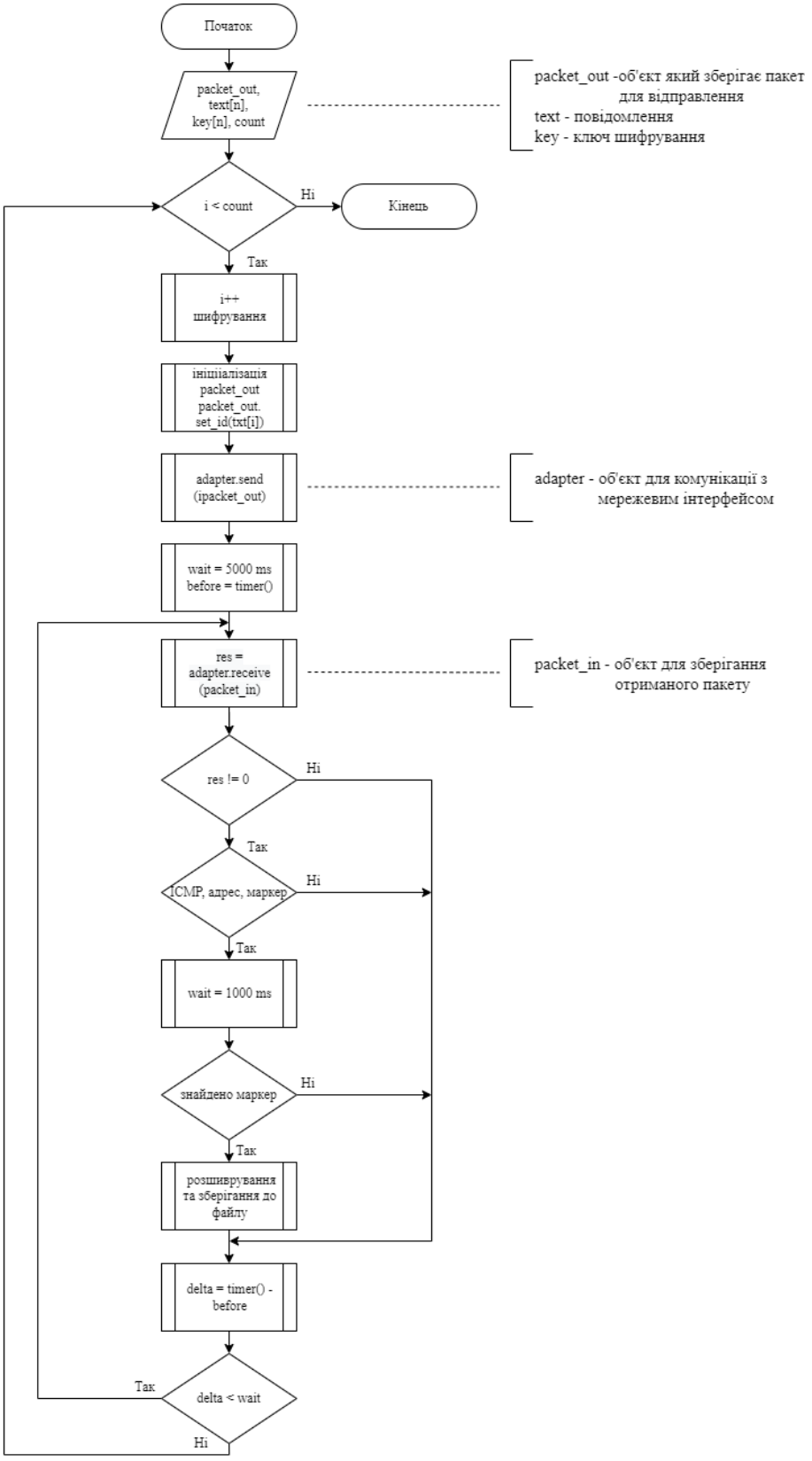

Рисунок 3.5 – Блок-схема функції StgSend

Блок-схема функції WaitEchoRequest, до котрої також йде звернення у функції main(), наведена на рис. 3.6. У випадку, коли абоненту необхідно одержати дані, алгоритм йде по цій вітці.

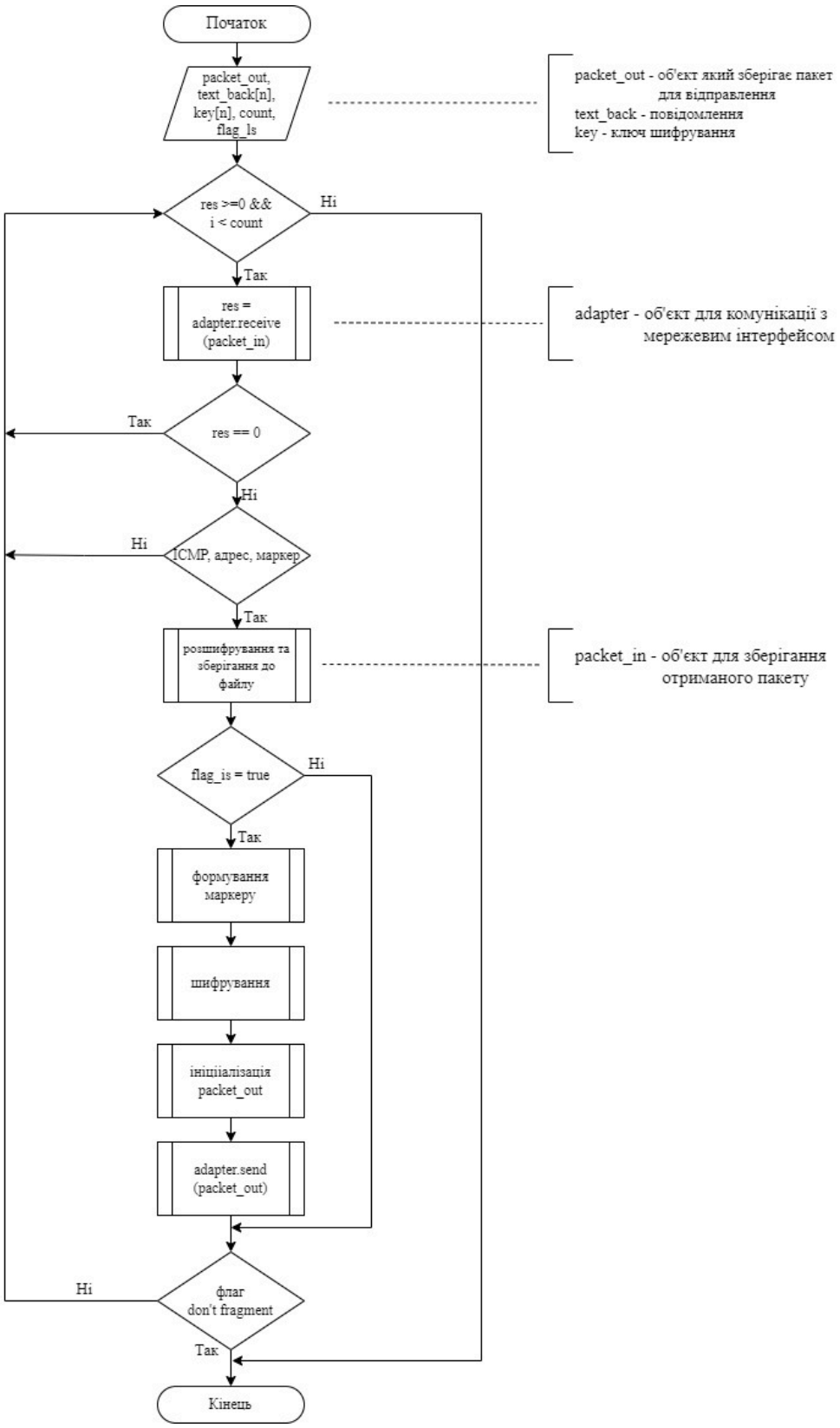

Рисунок 3.6 – Блок-схема функції WaitEchoRequest

Реалізація процесу відбувається завдяки взаємодії об’єктів під час виконання програми. Взаємодію об’єктів наведено у вигляді UML-діаграми (рис. 3.7).

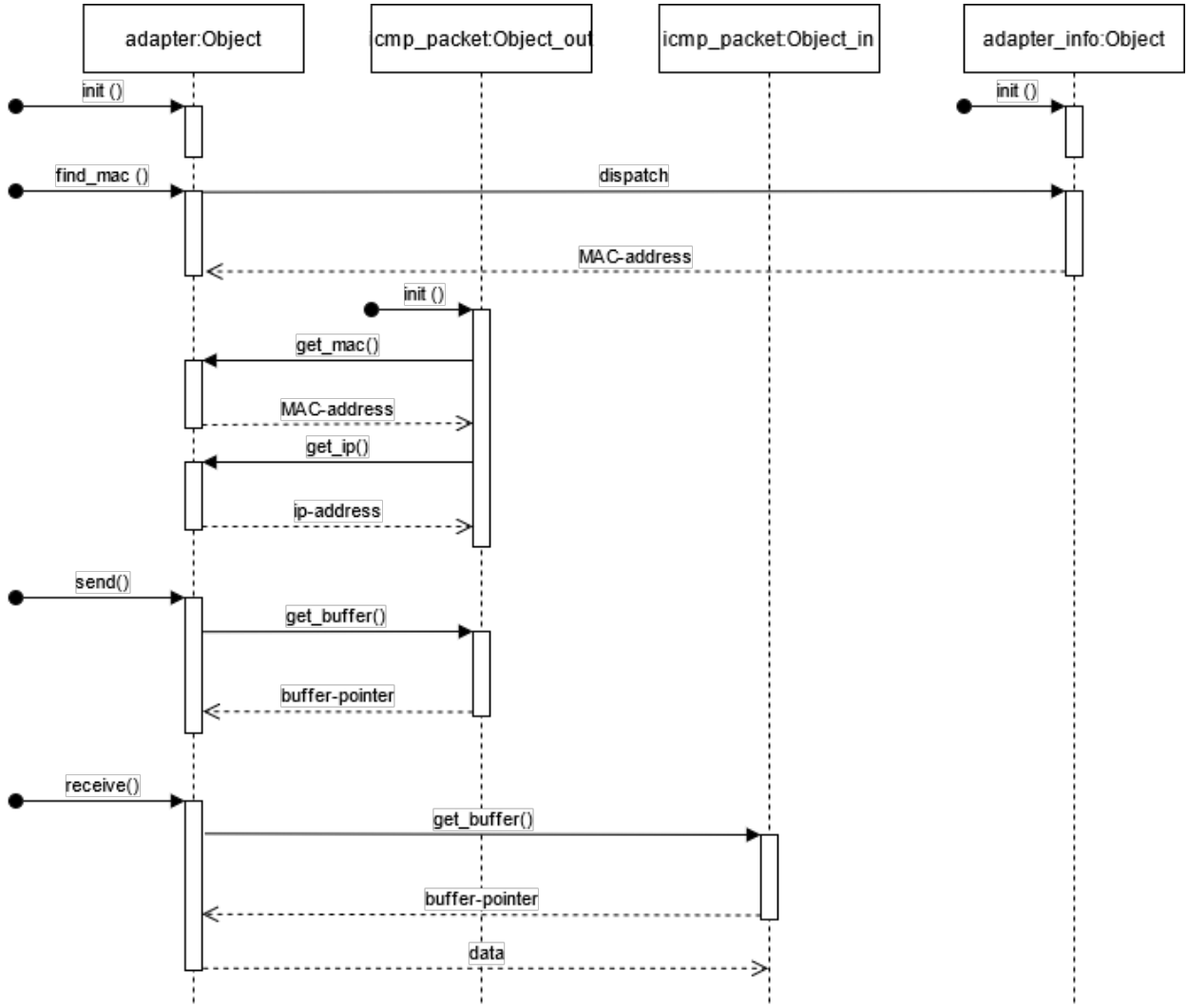

Рисунок 3.7 - UML sequence діаграма взаємодії об’єктів під час виконання

Вихідний код реалізованого програмного забезпечення наведено у Додатках А, Б, В.

3.4 Висновки за розділом

Розглянуто та обрано засоби для реалізації програмного забезпечення. Представлено діаграму класів розробленого ПЗ з описом їх взаємодії.

Також представлено функціонал ПЗ, головну функцію проекту та діаграму взаємодії об’єктів під час використання.

Комплекс дозволяє реалізувати обмін даними за методом модифікації полів у заголовках ICMP/IP пакетів.

4 МЕТОДИКА ВИКОРИСТАННЯ РОЗРОБЛЕНИХ ЗАСОБІВ

4.1 Інструкція з використання

4.1.1 Ініціювання

Розроблене ПЗ є консольним, тому звернення до нього відбувається через командну строку (рис. 5.1): **шлях до exe файлу > NetStg2.exe** .

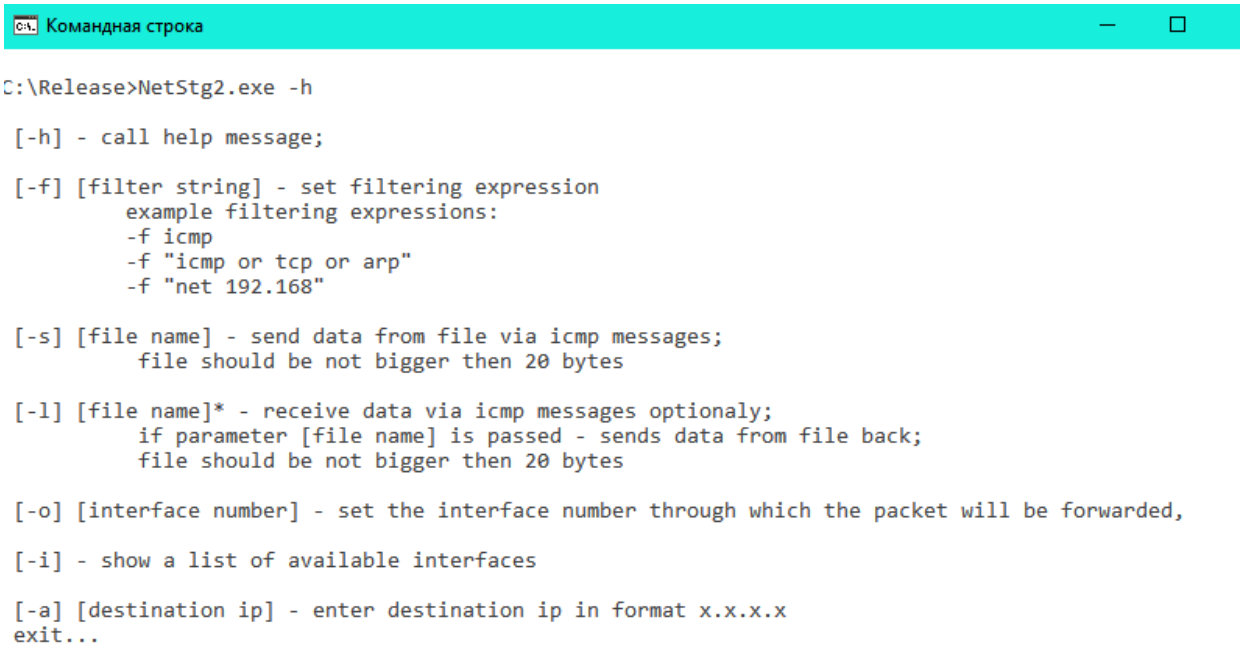

Рисунок 4.1 – Запуск програми, виклик допомоги

4.1.2 Одержувач

Першою дією абоненту є вибір необхідного інтерфейсу з наявних для обміну даними (рис 5.2). Звернення до виводу цієї інформації відбувається за допомогою: **NetStg2.exe –i**.

```
C:\Release>NetStg2.exe -i
0 - rpcap://\Device\NPF_{36123D6C-6DE7-46A1-9D02-D84448A666B8}
        Description: Network adapter 'Qualcomm Atheros QCA9377 Wireless Network Adapter' on
local host
        Loopback: no
        Address: 192.168.0.108
        Address: 255.255.255.0
        Address: 192.168.0.255

1 - rpcap://\Device\NPF_{6F421C95-6EC4-471B-8BEA-61937C4E231C}
        Description: Network adapter 'Microsoft Wi-Fi Direct Virtual Adapter' on local host
        Loopback: no
        Address: 169.254.195.240
        Address: 255.255.0.0
        Address: 169.254.255.255

2 - rpcap://\Device\NPF_Loopback
        Description: Network adapter 'Adapter for loopback traffic capture' on local host
        Loopback: yes

 exit...
```

Рисунок 4.2 – Список доступних інтерфейсів (одержувач)

Для отримання повідомлення абонент активує режим прослуховування (рис. 5.3): **NetStg2.exe –o *«номер інтерфейсу прослуховування»* -l** .

```
C:\Release>NetStg2.exe -o 0 -l

0-rpcap://\Device\NPF_{36123D6C-6DE7-46A1-9D02-D84448A666B8}
        Description : Network adapter 'Qualcomm Atheros QCA9377 Wireless
Network Adapter' on local host
        ip address  : 192.168.0.108
        ip netmask  : 255.255.255.0
        mac address : 0.0.0.0.0.0

 Waiting for ICMP requests ...
```

Рисунок 4.3 – Режим прослуховування (очікування даних)

Якщо обмін повідомленням пройшло вдало, то буде відображатись потік отриманих ICMP-відповідей та зміст повідомлення (рис. 5.4).

```
Waiting for ICMP requests ...
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
ICMP-request from 192.168.0.103 was received - ICMP-reply has been sent;
received message : Kholodar' Karyna
```

Рисунок 4.4 – Потік ICMP-відповідей та зміст отриманого повідомлення

Отримані дані зберігаються у текстовому документі received.txt до наступного отримання повідомлення (рис. 5.5).

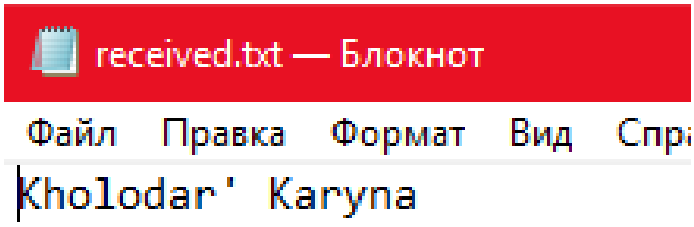

Рисунок 4.5 – Зміст текстового документу після отримання повідомлення

4.1.3 Відправник

Для передачі повідомлення абоненту, перш за все, необхідно надрукувати текстовий файл об’ємом до 20 байт (рис 4.5).

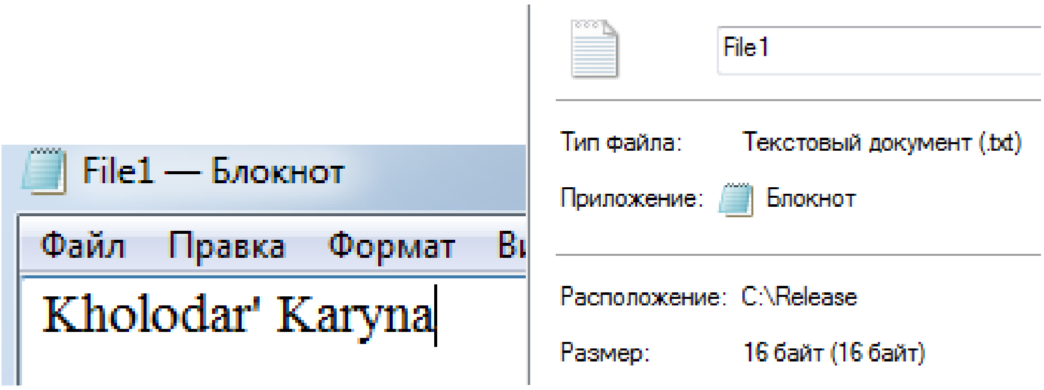

Рисунок 4.5 – Зміст та розмір даних, що передаються

Наступним етапом йде вибір інтерфейсу через котрий буде здійснюватися обмін даними (рис 4.6).

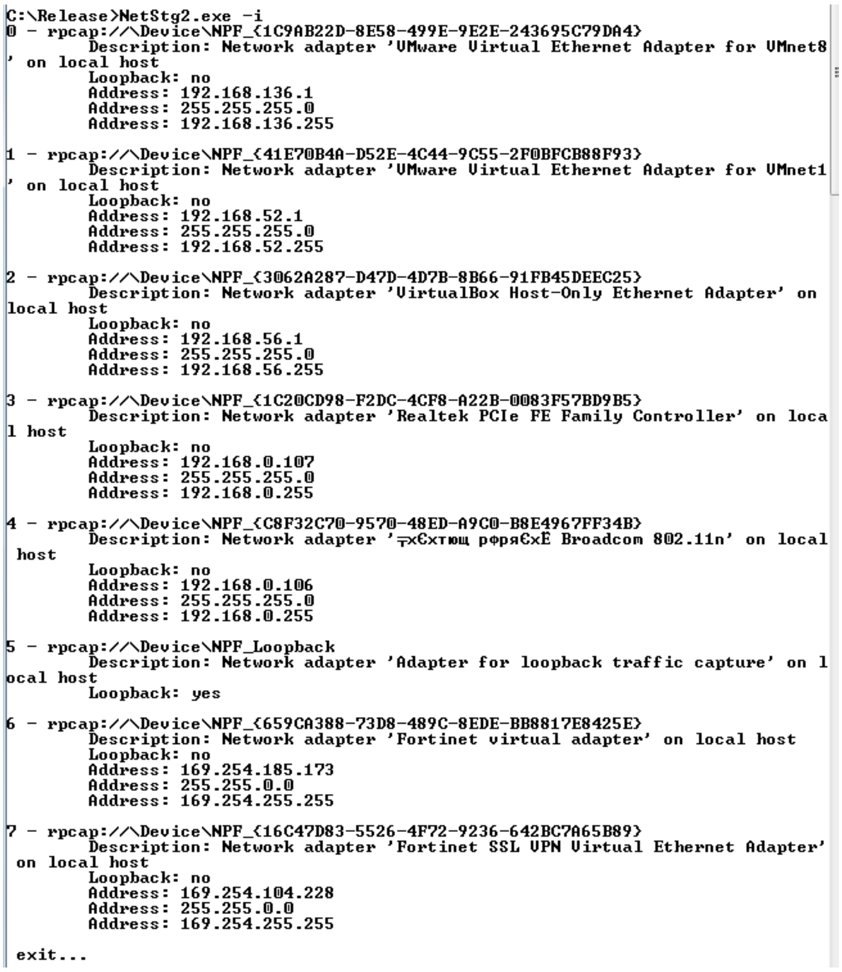
C:\Release>NetStg2.exe -i
0 - rpcap://\Device\NPF_{1C9AB22D-8E58-499E-9E2E-243695C79DA4}
Description: Network adapter 'VMware Virtual Ethernet Adapter for VMnet8
' on local host
Loopback: no
Address: 192.168.136.1
Address: 255.255.255.0
Address: 192.168.136.255
1 - rpcap://\Device\NPF_{41E70B4A-D52E-4C44-9C55-2F0BFCB88F93}
Description: Network adapter 'VMware Virtual Ethernet Adapter for VMnet1
' on local host
Loopback: no
Address: 192.168.52.1
Address: 255.255.255.0
Address: 192.168.52.255
2 - rpcap://\Device\NPF_{3062A287-D47D-4D7B-8B66-91FB45DEEC25}
Description: Network adapter 'VirtualBox Host-Only Ethernet Adapter' on
local host
Loopback: no
Address: 192.168.56.1
Address: 255.255.255.0
Address: 192.168.56.255
3 - rpcap://\Device\NPF_{1C20CD98-F2DC-4CF8-A22B-0083F57BD9B5}
Description: Network adapter 'Realtek PCIe FE Family Controller' on loca
l host
Loopback: no
Address: 192.168.0.107
Address: 255.255.255.0
Address: 192.168.0.255
4 - rpcap://\Device\NPF_{C8F32C70-9570-48ED-A9C0-B8E4967FF34B}
Description: Network adapter '╤х€хтющ рфряЄхЁ Broadcom 802.11n' on local
host
Loopback: no
Address: 192.168.0.106
Address: 255.255.255.0
Address: 192.168.0.255
5 - rpcap://\Device\NPF_Loopback
Description: Network adapter 'Adapter for loopback traffic capture' on l
ocal host
Loopback: yes
6 - rpcap://\Device\NPF_{659CA388-73D8-489C-8EDE-BB8817E8425E}
Description: Network adapter 'Fortinet virtual adapter' on local host
Loopback: no
Address: 169.254.185.173
Address: 255.255.0.0
Address: 169.254.255.255
7 - rpcap://\Device\NPF_{16C47D83-5526-4F72-9236-642BC7A65B89}
Description: Network adapter 'Fortinet SSL VPN Virtual Ethernet Adapter'
on local host
Loopback: no
Address: 169.254.104.228
Address: 255.255.0.0
Address: 169.254.255.255
exit...

Рисунок 4.6 – Список доступних інтерфейсів (відправник)

Після вибору інтерфейсу, відправник переходить до етапу обміну даними за допомогою команд (рис 5.7): **NetStg2.exe –o *«номер інтерфейсу передачі» -s «назва текстового файлу»*.txt –a «*IP адреса отримувача*»** .

```
C:\Release>NetStg2.exe -o 3 -s File1.txt -a 192.168.0.108

3-rpcap://\Device\NPF_{1C20CD98-F2DC-4CF8-A22B-0083F57BD9B5}
        Description : Network adapter 'Realtek PCIe FE Family Controller' on loc
al host
        ip address  : 192.168.0.107
        ip netmask  : 255.255.255.0
        mac address : 0.9.f.aa.0.1

MAC-address resolution - OK
```

Рисунок 4.7 – Вибір інтерфейсу, даних та адреси отримувача для обміну

Якщо обмін даними пройшов вдало, то буде відображено потік отриманих ICMP-відповідей від одержувача та повідомлення про те, що всі пакети успішно передані (рис 4.8).

```
1. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
2. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
3. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
4. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
5. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
6. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
7. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
8. Sending ICMP request -> 192.168.0.108
  received ICMP reply from 192.168.0.108
 All packets has been sent
```

Рисунок 4.8 – Потік отриманих ICMP-відповідей від одержувача

4.1.4 Стеганоаналіз

За достовірністю процесу обміну даними між одержувачем та відправником можна спостерігати за допомогою інструменту захвату та аналізу мережевого трафіку Wireshark.

Використовуючи атаку типу «людина посередні» аналітик (зловмисник) має можливість сканування трафіку між абонентами.

Знаючи IP адреси абонентів, аналітик виставляє фільтр на увесь трафік: **(ip.src == *“адреса відправника”*) and (ip.dst == *“адреса отримувача”*)** .

Таким чином відображається трафік між двома абонентами (адресами) (рис. 4.9). Напрям трафіку за бажанням, та для повноти картини змінюється.

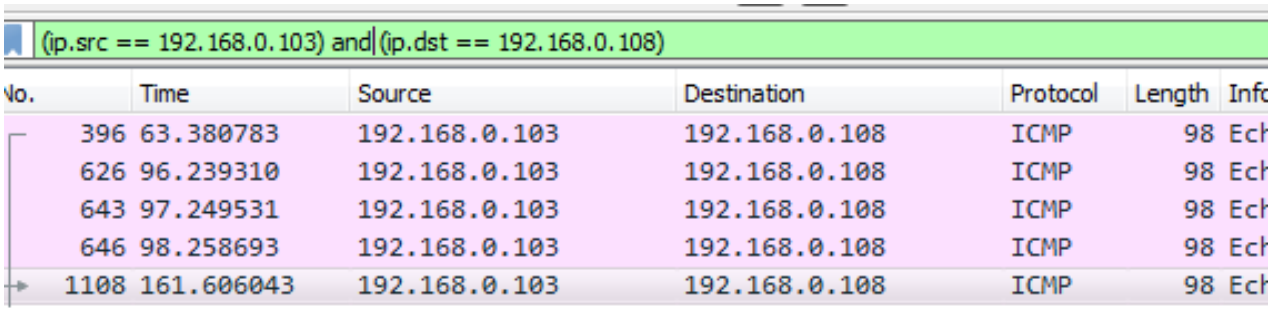

Рисунок 4.9 – Скріншот відображення захвату пакетів між двома абонентами

4.2 Аналіз даних

За допомогою Wireshark зробимо аналіз даних, що передаються, для прикладу, що наведений вище.

Відправник надіслав текст у вигляді: **Kholodar’ Karyna**

Це повідомлення займає 16 байт. Програмно дані розбиваються на блоки по 2 байти, тобто ми маємо 8 ICMP-запитів, та 8 ICMP-відповідей (рис. 4.10).

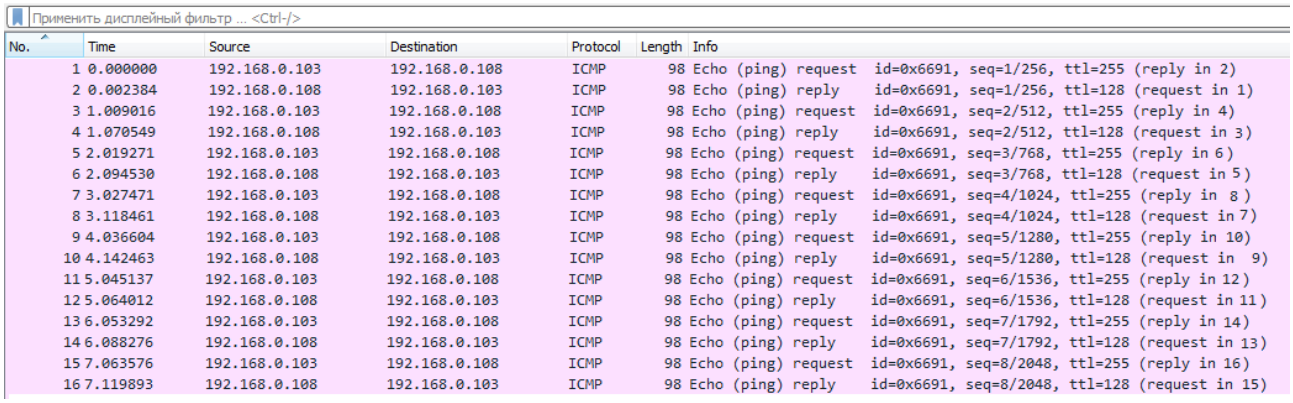

Рисунок 4.10 – Скріншот процесу захвату ICMP пакетів програмою Whireshark (приклад 1)

Іншим прикладом буде виступати передача даних відправником у вигляді 2 байтного повідомлення: **hi** . Аналогічно першому прикладу, повідомлення повинно розбиватись на блоки, але ми маємо лише 2 байти повідомлення, тому повинні отримати 1 ICMP-запит/відповідь (рис. 4.10).

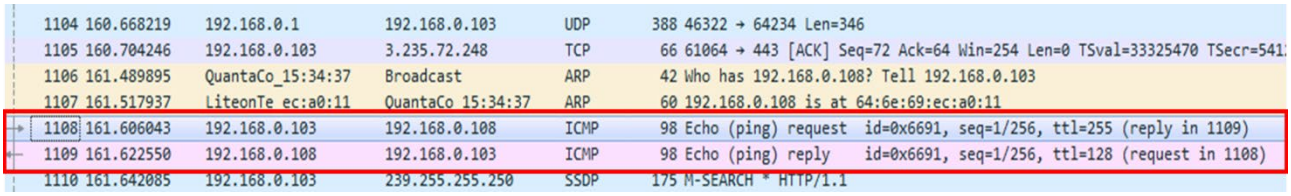

Рисунок 4.10 - Скріншот процесу захвату ICMP пакетів програмою Whireshark (приклад 2)

Також за допомогою Wireshark можливо переглянути вміст полів заголовків ICMP/IP (рис. 4.11). Як було приведено раніше, у другому розділі, структуру вкладання ICMP-пакетів у кадр, саме за такою схемою реалізується відображення кадру у Wireshark.

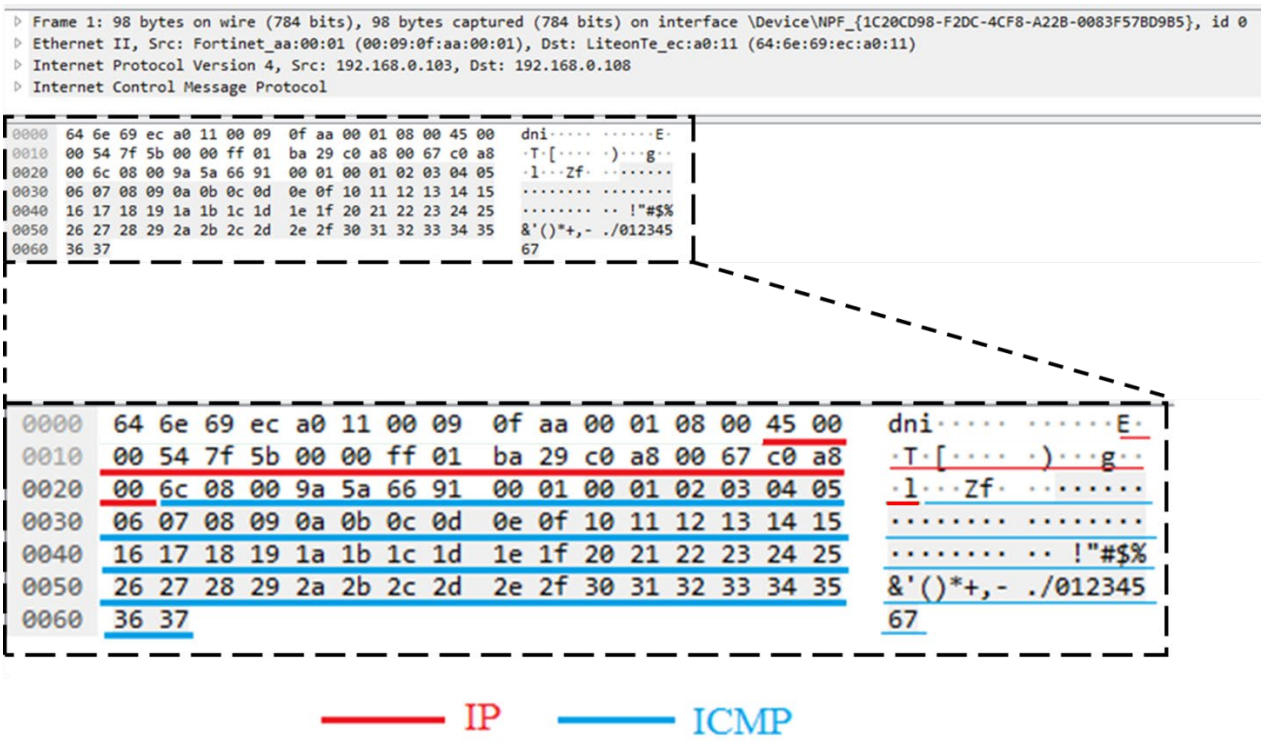

Рисунок 4.10 – Скріншот представлення ICMP-пакету у Wireshark (з поясненням)

Переглядаючи всі пакети, дійсно можна побачити як в заголовку ID IP передається інформація, а у ID ICMP незмінний маркер (рис 4.11).

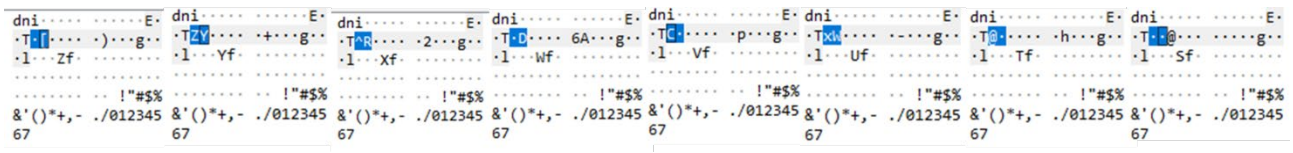

Рисунок 4.11 – Наявність даних, що передаються, та маркеру у заголовках ID

Використовуючи стандартну утиліту ping ми можемо порівняти пакети, що надсилаються абонентами та ICMP-пакети в котрих не має прихованої стеганограми (рис. 4.12).

ping **Стеганограма**

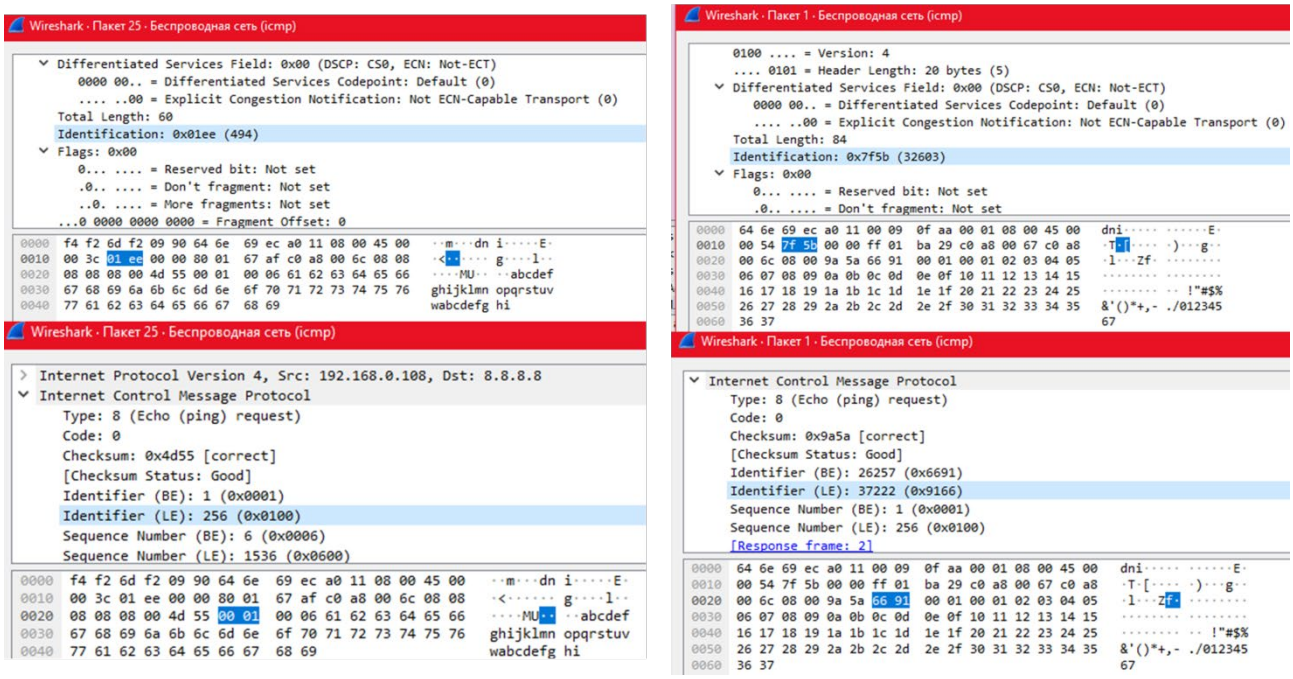

Рисунок 4.12 – Скріншоти відображення IP-дейтаграми та ICMP-пакету при використанні утиліти ping та з вкладеною стеганограмою

Таким чином видно, що ICMP/IP пакет з прихованою стеганогрмою відрізняється від стандартного пакету. Якщо аналітик має відповідні знання то він може встановити наявність прихованих даних.

4.3 Можливості використання розроблених засобів у навчальному процесі

Розроблені засоби можна використовувати у навчальних цілях для ознайомлення студентів із базовими поняттями у області мережевої стеганографії та стеганоаналізу.

Варіант виконання: робота із ознайомлення виконується по групам з трьох студентів. Два студенти виступають у ролі абонентів – відправник та одержувач, третій у якості аналітику/зловмиснику.

Запуск розроблених засобів відбувається на двох віртуальних машинах – гостьових ОС. Хост-комп’ютер буде виступати у якості концентратору, та на ньому запускається Wireshark.

Студентам-абонентам видаються контрольні повідомлення. Студент-аналітик налаштовує Wireshark на прослуховування необхідного інтерфейсу. Через віртуальні машини студенти-абоненти встановлюють обмін даними. Для додаткового навантаження на мережу на віртуальних машинах запускаються браузери та відповідні сайти.

Після обміну даними студент-аналітик, використовуючи фільтри до трафіку, відокремлює підозрілі пакети, та аналізуючи їх вміст визначає наявність стеганограми.

У якості додаткового методичного матеріалу можна використовувати інструкцію наведену у розділі 4.1.

4.3 Висновки за розділом

Представлено інструкцію з використання розроблених засобів з прикладом вхідних та вихідних даних.

Проведено аналіз даних на характерних прикладах.

Наведено можливості використання розроблених засобів в цілях навчання.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Вимоги безпеки праці під час виконання робіт на робочому місці

Питання охорони праці є дуже важливим, та воно має вирішуватися на всіх етапах трудового процесу, незалежно від професійної діяльності. Визначення основних положень що стосуються реалізації конституційного права громадянина на охорону її життя і здоров'я у процесі трудової діяльності міститься у законі України «Про охорону праці» згідно з Постановою Верховної Ради України № 77-VIII від 28 листопада 2014 року [30].

Відповідно до НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів», що затверджено: наказ Держнаглядохоронпраці України №4 від 9 січня 1998 року [31], та НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час робот з екранними пристроями», затверджені наказом Міністерства соціальної політики України "Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями" № 207 від 14 лютого 2018 року[32], вимоги безпеки під час роботи з електронно обчислювальною машиною з відео-дисплейними терміналами (далі - ВДТ) і периферійними пристроями (далі – ПП) наступні:

– Очищати перед початком роботи щодень екран від пилу та інших забруднень;

– Щодня перед початком роботи оператор ЕОМ повинен перевірити своє робоче місце на наявність ознак пошкодження обладнання;

– Перед початком роботи оператор ЕОМ повинен перевірити правильність підключення обладнання ЕОМ до електромережі;

– Перед початком роботи оператор ЕОМ повинен перевірити правильність організації робочого місця;

– Обладнання, принесене у холодну пору року з вулиці в робоче приміщення, можна підключати до електричної мережі тільки після того, як

температура обладнання зрівняється з температурою повітря відповідного робочого приміщення.

– Забороняється:

o виконувати на робочому місці, ремонт та налагодження ЕОМ;

o відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ЕОМ або їх технічне налагодження;

o працювати з ВДТ, у яких під час роботи з'являються нестабільне зображення на екрані, нехарактерні сигнали тощо;

o зберігання біля ЕОМ дискет, паперу, інших носіїв інформації, запасних блоків, деталей тощо;

o допускання попадання вологи на поверхню системного блоку;

o доторкання до задньої панелі системного блоку при включеному живленні;

o вимикання живлення під час виконання активного завдання;

o приймання напоїв та їжі на робочому місці;

– Про виявлення несправності обладнання або інших факторів, які створюють загрозу для життя або здоров’я працівників, необхідно негайно інформувати свого безпосереднього керівника.

Згідно [32] робочі місця програмістів-розробників мають бути розроблені з урахуванням можливості здійснити рухи або зміну положення тіла.

Гранично допустимий рівень випромінювання від екранних пристроїв не може бути перевищеним. Маються на увазі супутні в роботі приладів та пристроїв вібрація, шум, перевищення або зниження комфортної температури для роботи, чинники забруднення, стан працездатності, поведінки, що не підвладні здатності адаптації програміста-розробника.

Робоче місце програміста-розробника повинно мати відповідний до [32] рівень ергономіки, відповідати антропологічним та психофізіологічним нормам а також характеру службових обов’язків.

Робоче місце програміста-розробника з екранним пристроєм має бути достатньо освітленим і мати відповідний рівень контрасту між екраном та довкіллям за витримкою «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [33], що є частиною «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» №7 затверджених Головним державним санітарним лікарем України від 10 грудня 1998 р. [33].

Мікроклімат у виробничих приміщеннях з робочими місцями програмістів-розробників з екранними пристроями має постійно відповідати вимогам «Санітарних норм мікроклімату виробничих приміщень» ДСН 3.3.6.042-99 [33], що було затверджено постановою Головного державного санітарного лікаря України від 01 грудня 1999 року №42.

Стіл на робочому місці або поверхня повинні мати низьку відбивну здатність, достатньо ергономічні розміри та мати гнучкість при розміщенні клавіатури, екрана, документів, обладнання, тощо.

Крісло на робочому місці повинне бути стійким та дозволяти програмісту-розробнику займати зручне положення. Воно повинне мати здатність до регулювання висоти та нахилу. Має бути передбачена підніжка для тих, якщо це необхідно для зручності.

Не допускається підчас роботи програміста-розробника, на його робочому місці здійснювати технічне обслуговування, технічне налагодження або зміни у конструкції, у склад якої входить екранний пристрій.

Забороняється взаємодія з екранними пристроями підчас роботи програміста-розробника, якщо виникають нестабільне зображення на екрані, нехарактерна поведінка та інші виведення з ладу.

Екранні пристрої не повинні викликати ризик для програміста-розробника.

Електромагнітне випромінювання видимої частини спектру має бути відповідати незначному впливу на безпеку життя та здоров’я програміста-

розробника. Символи повинні мати достатню чіткість та інтервали, а між рядками належну дистанцію.

Не допускається миготіння зображення чи інші прояви нестабільності. Контрастність та яскравість символів повинна мати здатність до регулювання.

Не допускається мерехтіння зображення або інша нестабільність. Контраст та яскравість символів мають бути налаштовані.

Екрани повинні мати можливість нахилу або повороту, якщо цього вимагає програміст. Для розміщення екрану можна використовувати підставку або регулювальний стіл.

При виборі клавіатури перевагу слід віддавати клавіатурі, що може відкидатися або відділена від екрану для зручного положення тіла програміста-розробника та уникнення втоми рук або їх частин. Відображення на поверхні клавіатури не допускається. Тому поверхня клавіатури повинна бути матовою. Положення клавіш клавіатури повинно відповідати достатньому рівню ергономіки розробника.

Обладнання не має виділяти тепло в такій кількості, що може порушити комфортний мікроклімат на робочому місці програміста-розробника.

Розробка робочого місця програміста має супроводжуватись добиранням програмного забезпечення і обладнання, що вирішує відповідні завдання, має простоту керування програмістом-розробником, або відповідає рівню знань програміста-розробника.

5.2 Шкідливі виробничі фактори на виробництві

Правильна оцінка небезпечних і шкідливих виробничих факторів значно впливає на забезпечення безпечних умов праці. Фактори виробничого середовища, надмірне розумове та фізичне навантаження, нервово-емоційна напруга, а також різне сполучення цих причин можуть впливати на однакові по складності зміни в організмі людини.

У приміщенні на програміста-розробника можуть негативно впливати наступні фізичні та психофізіологічні фактори:

– підвищена або знижена температура;

– підвищена або знижена вологість;

– недостатня освітленість;

– підвищений рівень шуму;

– підвищена іонізація повітря;

– підвищений рівень електромагнітних випромінювань;

– нервово-психічні перевантаження.

Одним з найважливіших факторів, що впливають на здоров’я людини є організація робочого місця. Так у нормативно правовому акті з охорони праці НПАОП 22.1-1.01-96 «Правила охорони праці для видавництв і редакцій», що затверджено наказом Державного комітету України по нагляду за охороною праці № 122 від 18 липня 1996 року [35] йдеться мова про об’єм виробничих приміщень для програмістів. Відповідно [35] об’єм виробничих приміщень на одного працівника повинна складати 20 м3, а площа приміщень - не менше 6 м2 з урахуванням максимального числа працівників в одну зміну.

Відповідно до санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, що затверджено Постановою Головного державного санітарного лікаря України №42 від 1 грудня 1999 року [34] робота програміста за енерговитратами відноситься до категорії легких робіт, зокрема до категорій Іа та Іб.

Мікрокліматичні умови виробничих приміщень характеризуються наступними такими показниками, як: температура повітря, швидкість руху повітря, відносна вологість повітря, інтенсивність теплового (інфрачервоного) опромінення, температура поверхні.

У таблиці 1 наведено оптимальні мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт, відповідно до [31].

Таблиця 1. – Оптимальні мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт

Період року	Категорія робіт	Температура повітря	Відносна вологість	Швидкість руху, м/сек.
Холодний період року	Легка Іа	22 – 24	60 – 40	0,1
	Легка Іб	21 – 23	60 – 40	0,1
Теплий період року	Легка Іа	23 – 25	60 – 40	0,1
	Легка Іб	22 – 24	60 – 40	0,2

У таблиці 2 наведено допустимі мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт, відповідно до [32].

Таблиця 2. – Допустимі мікрокліматичні умови виробничого приміщення, для категорій Іа та Іб легких робіт.

Період року	Категорія робіт	Температура, град.С				Відносна вологість (%)	Швидкість руху, м/сек.
		Верхня мережа		Нижня мережа			
		На постійних робочих місцях	На непостійних робочих місцях	На постійних робочих місцях	На непостійних робочих місцях		
Холодний період року	Легка Іа	25	26	21	18	75	не більше 0,1
	Легка Іб	24	25	21	18	75	Не більше 0,2
Теплий період року	Легка Іа	28	30	22	20	55 – при 28 град.С	0,2-0,1
	Легка Іб	28	30	21	19	60 – при 27 град.С	0,3-0,1

Температура на постійному робочому місці зіставляє +18˚С у холодний період, що не відповідає допустимим мікрокліматичним нормам.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ВДТ ЕОМ і ПЕОМ [31, 39], мають відповідати вимогам що наведені у таблиці 3.

Таблиця 5.3 – Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот для програміста

Вид трудової діяльності	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц									
	31,5	63	125	250	500	1000	2000	4000	8000	Рівні звуку, еквівалентні рівні звуку, дБА/дБАекв.
Програмісти ЕОМ	86	74	61	54	49	45	42	40	38	50

Устаткування, що становить джерело шуму відповідно до [36], слід розташовувати поза приміщенням для роботи ЕОМ, а також для забезпечення допустимих рівнів шуму на робочих місцях слід застосовувати засоби звукопоглинання.

Відповідно до державних будівельних норм ДБН В.2.5-28:2018 «Природне і штучне освітлення», що затверджено наказом Мінрегіону №264 від 3 жовтня 71 2018 року [35] нормативним параметром природного освітлення є коефіцієнт природного освітлення (КПО). Коефіцієнт природного освітлення встановлюється в залежності від розряду виконуваних зорових робіт. Робота програміста відноситься до робіт середньої точності (IV розряд зорових робіт, мінімальний розмір об'єкту розрізнення складає 0,5-1,0мм), для яких при використанні бокового освітлення КПО=1,5%. Для IV розряду зорових робіт мінімальна освітленість складає 300-500 лк.

Розрахунок штучного освітлення для робочої кімнати площею 16,43 м2 , ширина якої складає 3,1 м, довжина – 5,3 м, висота – 3,7 м за методом коефіцієнта використання світлового потоку.

Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, необхідно визначити світловий потік, що падає на робочу поверхню за формулою (1):

$$F = \frac{ESKZ}{n}, \tag{1}$$

де F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк Е = 300 Лк;

S – площа освітлюваного приміщення;

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації(К = 1,5)

Z – відношення середньої освітленості до мінімальної (Z =1,1);

n – коефіцієнт використання світлового потоку, (залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін (ρст.) і стелі (ρстелі), значення коефіцієнтів дорівнюють ρст = 30 % і ρстел = 50%).

Обчислимо індекс приміщення за формулою (2):

$$i = \frac{S}{h(A+B)}, \quad (2)$$

де S – площа приміщення, S = 16,43 м2 ;

h – розрахункова висота підвісу, h = 2,9 м;

А – ширина приміщення, А = 3,1 м; В – довжина приміщення, В = 5,3 м.

Підставивши значення отримаємо: i = 0,67. Знаючи індекс приміщення, знаходимо n = 0,25. Підставимо всі значення у формулу для визначення світлового потоку F:

$$F = \frac{300 * 16{,}43 * 1{,}1 * 1{,}5}{0{,}25} = 32531{,}4 \text{ Лм}$$

Для освітлення використані люмінесцентні лампи типу ЛБ 40-1, світловий потік яких F=4320 Лм. Розрахуємо необхідну кількість ламп у в світильниках за формулою (3):

$$N = \frac{F}{F_Л}, \quad (3)$$

де N – кількість ламп, що визначається;

F – світловий потік;

Fл – світловий потік ламп

$$N = \frac{32531{,}4}{4320} = 7{,}5 = 8$$

В приміщені кожен світильник комплектується двома лампами, тобто необхідно використовувати 4 світильника з 2 працюючими лампами. Схема розташування світильників наведено на рис. 5.1.

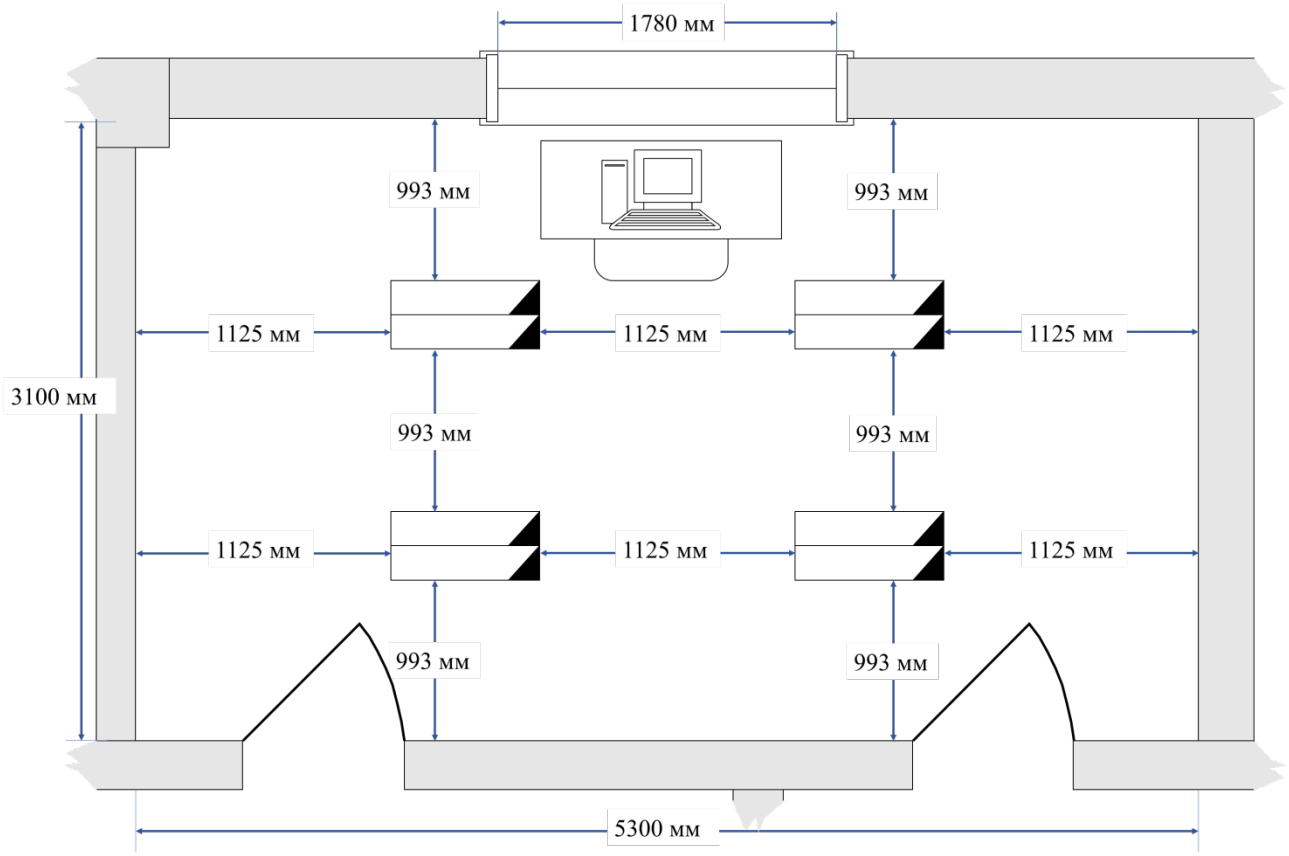

Рисунок 5.1 – Схема розташування освітлення у робочій кімнаті

Таким чином повністю задовольняються достатні умови штучного освітлення.

Приміщення, які оснащенні для роботи з обчислювальною, зараховують до категорії приміщень з підвищеною небезпекою, оскільки є велика вірогідність ураження електричним струмом. Осередком підвищеної електричної небезпеки є блоки , корпус пристрою, сервера і прилади в разі виникнення несправності (наприклад, при порушенні захисного механізму, ізоляції проводів, включення в мережу і виключення з мережі вилок електроживлення).

У кімнати, де одночасно використовується понад п'яти обчислювальних машин монтується аварійно-резервне реле напруги, який має змогу вимкнути повністю живлення техніки, окрім освітлення.

Ні в якому разі не можна допускати підключення комп’ютерного обладнання до звичайної електричної мережі, особливо з використанням перехідників.

Електронно-обчислювальні машини мають відповідати чинних стандартів в Україні, нормативних актів охорони праці. Електронно-обчислювальні машини іноземного походження додатково мають відповідати вимогам національних стандартів держав-виробників і мати в наявності певні позначення на корпусі, в паспорті або іншій експлуатаційній документації.

За методом захисту користувачів від ураження електричним струмом електронно-обчислювальної машини повинна відповідати 1 класу захисту відповідно до ДСТУ 2267-93 «Вироби електротехнічні. Терміни та визначення» [37].

Окрім цього, мають місце в застосуванні наступні технічні засоби захисту від пошкоджень електричним струмом в кімнаті з електронно-обчислювальними машинами, як:

– електрична ізоляція струмоведучих кабелів;

– захисне заземлення;

– захисне відключення.

Вся техніка, що має заземлюватись, повинна бути приєднана до заземлювальної шини окремими провідниками.

Основною вогненебезпечною проблемою в кімнаті з комп’ютерними пристроями несе в собі електричне обладнання. Під час роботи з електричними пристроями мають дотримуватись правил та вимог охорони праці. Весь прилягаючий інвентар (меблі, корпуси апаратури, покриття) не має бути вироблено з легкозаймистих матеріалів, бо можуть стати основною причиною спалаху пожежі.

Приміщення має повністю відповідати вимогам з вогнестійкості будівельних конструкцій, плануванні будівель та устаткованістю комплексного протипожежного захисту.

Система профілактичних пожежних перевірок представляє собою забезпечення пожежної безпеки наступних установ: обладнання, електроустановок, систем опалення та вентиляції, запобігання утворення та внесення джерел запалювання, запобігання появи вогненебезпечного середовища. Система пожежного захисту передбачає застосування мало займистих матеріалів, ізоляції займистого середовища, обладнання засобами гасіння пожежі, пожежної сигналізації та сповіщення про пожежу відповідним органам, застосування засобів індивідуального та загального захисту операторів, організацію пожежної безпеки об'єкта. Приміщення повинно мати в наявності засоби гасіння пожежі, а саме: воду, хімічну і механічну піну, негорючі гази і пари, порошкоподібні речовини, покривала з негорючих матеріалів і ін.

Будівлі, де розташовані робочі місця операторів, мають бути не нижче II ступеня вогнестійкості згідно з ДБН В.1.1-7:2016 «Пожежна безпека об`єктів будівництва. Загальні вимоги» [38].

5.3 Дії працівників в надзвичайних ситуаціях

У випадку Аварійної ситуації програміст зобов’язаний:

– при виявленні будь-яких неполадок в роботі персонального комп'ютера програміст повинен припинити роботу, вимкнути комп'ютер і повідомити про це безпосереднього керівника для організації ремонту;

– при попаданні людини під електричну напругу негайно вимкнути електричне живлення, до прибуття лікаря надати долікарську медичну допомогу;

– при будь-яких випадках порушень роботи технічного обладнання негайно викликати представника технічної служби;

– при нещасному випадку, отруєнні, раптовому захворюванні необхідно негайно надати першу допомогу потерпілому, викликати лікаря або допомогти

доставити потерпілого до лікаря, а потім повідомити керівника про те, що трапилося;

– у випадку виникнення різі в очах, різкого погіршення зору, виникнення головного болю, больових почуттів у пальцях та кистях рук, посилення серцебиття – негайно припинити роботу з використанням ЕОМ, повідомити про те, що сталося, свого безпосереднього керівника й звернутися до медичної установи;

– при загорянні обладнання негайно відключити його від електромережі, ужити заходів щодо ліквідації вогню за допомогою вуглекислотного або порошкового вогнегасник.

План евакуації ділянки №4 2 поверх АТ «ДАЗ» представлено на рис 5.2.

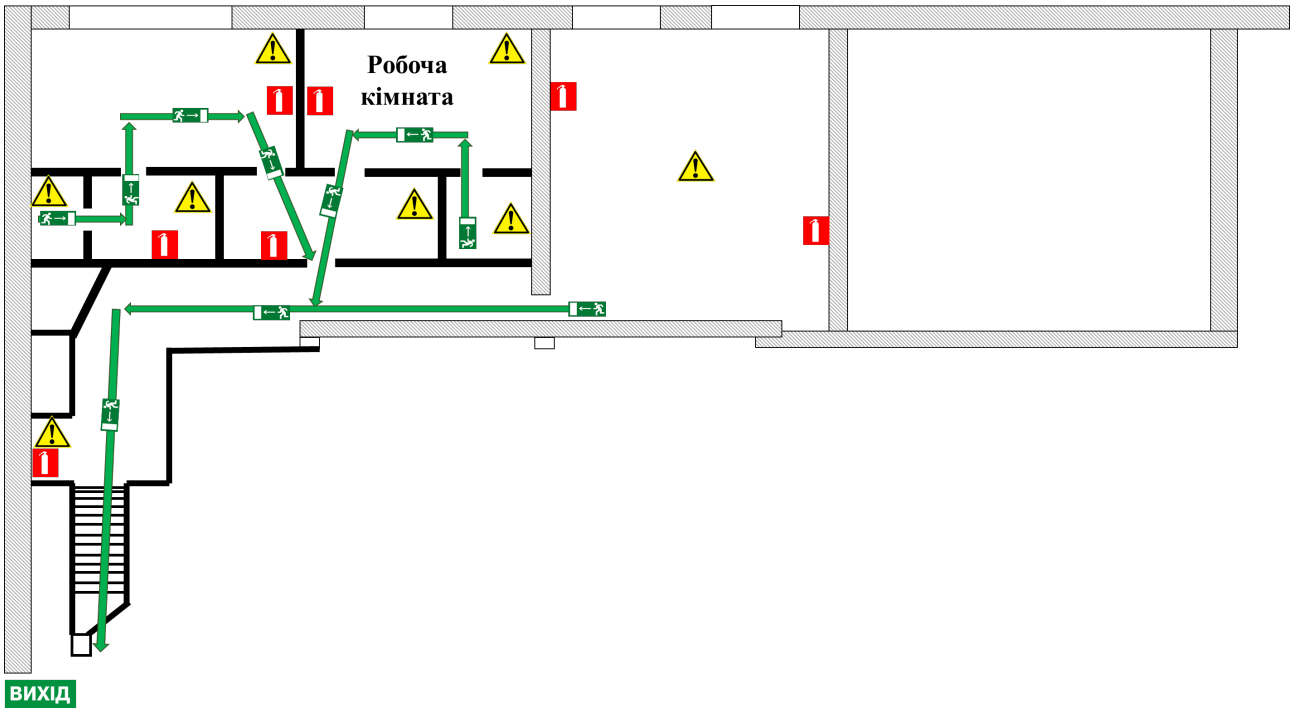

Рисунок 5.2 – План евакуації

Згідно з [40] загальними правилами надання до медичної допомоги э наступними:

– Перш за все оглянути місце пригоди і впевнитись в особистій безпеці і безпеці постраждалого;

– Провести первинний огляд постраждалого;

– Викликати швидку медичну допомогу;

– Провести вторинний огляд постраждалого, з метою виявлення інших проблем (пошкоджень), які потребують надання домедичної допомоги (розпочніть із загального огляду всього тіла, починаючи з голови).

Надання першої домедичної допомоги постраждалим при ураженні електричним струмом [40]:

1) Як можливо швидко відокремити потерпілого від джерела струму.

2) Викликати швидку, якщо це необхідно.

3) Покласти та/або зігрійте людину.

4) Закрити опіки – якщо у потерпілого є опіки, їх треба накрити стерильною марлею (якщо є під рукою) або чистою гладкою тканиною. Звичайно, тільки в тому випадку, якщо стан людини дозволяє зняти або розрізати одяг на обпалених місцях.

5) Якщо з'являються ознаки шоку – блювання, слабкість, сильна блідість, – трохи підняти ноги, підклавши під ступні валик з речей.

6) Якщо потерпілий погано дихає або не дихає зовсім, негайно починайте робити штучне дихання рот в рот.

7) Якщо у людини немає пульсу і відсутній серцебиття, крім штучного дихання, необхідний непрямий масаж серця.

Надання першої домедичної допомоги постраждалим при пожежі [40]:

1) Якщо горить одяг, його слід скинути або погасити полум'я, щільно накривши людини ковдрою або будь–яким шматком тканини. Обпалені ділянки одягу акуратно розрізати і скидати по частинах, у запобігання подальшої травматизації шкіри.

2) Якщо закрита рана необхідно охолоджувати водою уражену ділянку протягом 10 хвилин.

3) На поверхню рани слід накласти стерильну пов'язку.

4) Забезпечити потерпілому спокій.

5) Дати випити велику кількість рідини (чай, вода і тому подібне).

6) Негайно викликати бригаду невідкладної допомоги.

7) При можливості знеболити потерпілого.

5.4 Висновки за розділом

Розглянуто питання охорони праці та безпеки у надзвичайних ситуаціях відповідно до сучасних НПАОП та ДСН.

Розглянуто робоче місце програміста з точки зору питання про шкідливі виробничі фактори. Отримано, що робоче місце має достатнє освітлення але не відповідає допустимим мікрокліматичним умовам праці.

Розроблено загальні правила що до надання загальної першої медичної допомоги, медичної допомоги при ураженні електричним струмом та медичної допомоги постраждалим від пожежі.

ВИСНОВКИ

В дипломній роботі виконано дослідження та розробку програмних засобів демонстрації мережевої стеганографії та стеганоаналізу з використанням методу модифікації полів у заголовках ICMP/IP пакетів.

Розроблене програмне забезпечення мережевої стеганографії можна використовувати для прихованого обміну даними у мережі, а також в навчальному процесі студентів при проведені лабораторних або практичних занять з відповідних дисциплін.

Розглянуто структуру стеганосистеми та наведено загальний огляд методів мережевої стеганографії. Проведено порівняльний аналіз цих методів за п’ятьма характеристиками та обрано метод модифікації полів у заголовках ICMP/IP пакетів.

Обрано тип полів та криптографічні функції для реалізації програмного засобу. Розроблено інформаційну структуру взаємодії користувачів. Описано основні етапи обміну даними.

Здійснено вибір середовища та мови програмування для розробки програмного забезпечення та розроблено алгоритми роботи зі сторони відправника та одержувача. На основі алгоритмів було розроблено програмне забезпечення.

Зазначено, що розроблений програмний засіб стеганогрфії може бути використано у навчальних цілях, для чого наведена інструкція з використання.

Зазначено, що розроблений програмний засіб стеганогрфії може бути використано у навчальних цілях, для чого наведена інструкція з використання.

Сформовані основні вимоги безпеки при виконані робіт з персональним комп’ютером. Проведено оцінку робочого місця програміста-розробника на підставі вимог до робочого місця. Розглянуто пожежну безпеку та методи надання загальної медичної допомоги при уражені струмом та постраждалим при пожежі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гребенников В. В. Стеганография. История тайнописи [Текст] / В. В. Гребенников. – М.: ЛитРес, 2019. – 160 с.

2. Жельников В. Криптография от папируса до компьютера [Текст] / В. Жельников. - М., 1996. – 330 с.

3. Попов М. Вперед в прошлое. Криптография [Електронний ресурс] / М. Попов // Мир фантастики. - 2007. - № 50. - Режим доступу: http://old.mirf.ru/Articles/print2292.htm

4. Барабаш А. Стеганография. Древняя тайнопись в цифровую эпоху [Електронний ресурс] / Режим доступу: http://www.webcitation.org/66M340RTC

5. Колобова А.К., Д.Г. Колобов, А.С. Герасимов Стеганография от древности до наших дней [Електронний ресурс] / А.К. Колобова, Д.Г. Колобов, А.С. Герасимов – 2015. – PDF, 145 КБ.

6. Конахович Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

7. Бернет С. Криптография. Официальное руководство RSA Security [Текст] / С. Бернет, С. Пейн – М. «Бином», 2012. – 325 с.

8. Серов Р.Е. Основы современной криптографии [Текст] / Р.Е. Серов, В.В. Гончаров, – Москва, Горячая линия – Телеком, 2011. – 443 с.

9. Zollner J. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding [Електронний ресурс] / J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf - Dresden University of Technology, 01062 Dresden, Germany - 1998. – Режим доступу: https://www2.htw-dresden.de/~westfeld/publikationen/zoellner.et.al.ihw98.pdf

10. Shapiro J. Embedded Image Coding Using Zerotrees Of Wavelet Coefficients [Електронний ресурс] / IEEE Transactions on Signal Processing, 1993. – Vol. 41, No. 12. – Режим доступу: https://web.stanford.edu/class/ee398a/handouts/papers/Shapiro%20-%20EZT.pdf

11. Said A., Pearlman W. A New Fast And Efficient Image Codec Based On Set Partitioning in Hierarchical Trees [Text] / IEEE Transactions on Circuits and Systems for Video Technology, 1996. – Vol. 6. – P. 243-250.

12. Грибунин В.Г Цифровая стеганография [Текст] / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // М.: СОЛОН-Пресс – 2002. – PDF 3,71 МБ.

13. Enrique Cauich Data Hiding in Identification and Offset IP fields / , Enrique Cauich, Roberto Gómez, Ryouske Watanabe [Текст] / – California University at Irwing, Computer Science and Engineering 204B University of California, Irvine, CA 92717 USA.

14. Mazurczyk, W. Hiding Data in VoIP In Proc [Текст] / Mazurczyk, W., Lubacz, J., Szczypiorski K.// The 26th Army Science Conference (ASC 2008), Orlando, Florida, USA, December 1-4, 2008.

15. Mazurczyk, W. Hiding Information in Retransmissions [Текст] / W. Mazurczyk, M.Smolarczyk, K. Szczypiorski // Warsaw University of Technology, Institute of Telecommunications Warsaw

16. Szczypiorski, K.: HICCUPS: Hidden Communication System for Corrupted Networks [Текст] / In Proc. of: ACS'2003, October 22-24, 2003, Miedzyzdroje, Poland, pp. 31-40

17. Павлин Д. В. О Сетевойстеганографии. Реализацияалгоритма rsteg [Текст] / Д. В. Павлин, А. И. Макосий, О. Н. Жданов // Журнал – Решетковские чтения, 2014

18. Пескова О.Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи [Текст] / О.Ю.Пескова, Ю. Г. Халабурда // Известия ЮФУ: Технические науки. – Ростов-на-Дону. – №12, Том 137. – 2012. – С.167-176.

19. RFC 793 - TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION [Електронний ресурс] / Режим доступу: https://datatracker.ietf.org/doc/html/rfc793

20. RFC 791 - INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION [Електронний ресурс] / Режим доступу: https://datatracker.ietf.org/doc/html/rfc791

21. Галушка В.В. Сетевая стеганография на основе ICMP-инкапсуляции [Електронний ресурс] / В.В. Галушка, С.Б. Петренкова, Я.В. Дзюба, В.А. Панченко // Донской государственный технический университет, Ростов-на-Дону – 2018. – Режим доступу: https://cyberleninka.ru/article/n/setevaya-steganografiya-na-osnove-icmp-inkapsulyatsii/viewer

22. Craig H. Rowland Covert Channels in the TCP/IP Protocol Suite [Текст] / First Monday, Volume 2, Number 5 - 5 May 1997. – Режим доступу: https://journals.uic.edu/ojs/index.php/fm/article/view/528/449

23. RFC 729 - TELNET BYTE MACRO OPTION [Електронний ресурс] / Режим доступу: https://datatracker.ietf.org/doc/html/rfc729

24. RFC 792 - INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION [Електронний ресурс] / Режим доступу: https://datatracker.ietf.org/doc/html/rfc792

25. RFC 1071 - COMPUTING THE INTERNET CHECKSUM [Електронний ресурс] / Режим доступу: https://datatracker.ietf.org/doc/html/rfc1071

26. Габидулин Э. М. Защита информации [Текст] / Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И. // Учебное пособие — М.: МФТИ, 2011. — 225 с.

27. Working Draft, Standard for Programming Language C++11 [Електроний рисурс] / Режим доступу: http://open-std.org/jtc1/sc22/wg21/docs/papers/2012/n3337.pdf

28. WinPcap [Електроний рисурс] / Режим доступу: https://www.winpcap.org/default.htm

29. WireSharkЕлектроний рисунок [Електроний рисурс] / Режим доступу: https://www.wireshark.org/

30. Про охорону праці [Текст]: Закон України згідно з Постановою Верховної Ради України № 77-VIII від 28 листопада 2014 року

31. НПАОП 40.1–1.21–98 «Правила безпечної експлуатації електроустановок споживачів» [Текст]: Затверджено: наказ Держнаглядохоронпраці України № 4 від 9 січня 1998 року

32. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час робот з екранними пристроями» [Текст]: Затверджено: наказ Міністерства соціальної політики України «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» № 207 від 14 лютого 2018 року

33. ДСанПІН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [Текст]: Затв. Постанова Головного державного санітарного лікаря України від 10 грудня 1998 р. № 7

34. ДСН 3.3.3-042-99 Державні санітрані норми мікроклімату виробничих приміщень [Текст]:. Постанова Головного державного санітарного лікаря України від 01.12.1999 №42.

35. НПАОП 22.1-1.01-96. Правила охорони праці для видавництв і редакцій [Текст]: Затверджено наказом Державного комітету України по нагляду за охороною праці від 18.07.96 № 122.

36. ДБН В.2.5-28:2018 «Природне і штучне освітлення» [Текст]: Затверджено наказом Мінрегіону № 264 від 3 жовтня 2018 року

37. ДСТУ 2267—93 Вироби електротехнічні. Терміни та визначення [Текст]: Наказ від 12.11.1993 № 169

38. ДБН В.1.1-7:2016 «Пожежна безпека об`єктів будівництва. Загальні вимоги» [Текст]: Наказ від 31.10.2016 № 287.

39. ДСН 3.3.6-037-99 Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку»[Текст]: Наказ від 01.12.1999 № 37

40. Ненько С. К., Полівода Л. А. Надання першої медичної допомоги при надзвичайних ситуаціях [Електроний рисурс] / Херсон: «Навчально-

методичний центр цивільного захисту та безпеки життєдіяльності Херсонської області», 2014, 28 с. – Режим доступу: https://ks.nmc.dsns.gov.ua/files/documents/first-medical-aid.pdf