МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Метод фільтрації трафіку для підвищення захищеності мережі від зовнішніх загроз»

Виконавець: _____ Валентин ХІВРИЧ
(підпис)

Керівник: _____ Віталій КУРУШКІН
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Хіврича Валентина Романовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Метод фільтрації трафіку для підвищення захищеності мережі від зовнішніх загроз»
затверджена наказом ректора від «28» вересня 2023 р. №1965/ст
2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.
3. Вихідні дані до роботи: телекомунікаційна мережа
4. Зміст пояснювальної записки: зовнішні загрози безпеці та методи протидії; оцінка потенційної небезпеки зовнішніх загроз; принцип роботи системи фільтрації трафіку; метод фільтрації трафіку для підвищення захищеності мережі від зовнішніх загроз;
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: метод додавання до чорного списку введеної користувачем url-адреси; метод пошуку адрес у списку заборонених; результати виконання модульних тестів; реалізація замірів часу завантаження сторінок; результати повторного модульного тестування; діаграма зміни часу завантаження сторінки після ввімкнення мережевого фільтра

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	02.10.2023-04.10.2023	Виконано
2	Вступ	05.10.2023-08.10.2023	Виконано
3	Зовнішні загрози безпеці та методи протидії	09.10.2023-22.10.2023	Виконано
4	Оцінка потенційної небезпеки зовнішніх загроз	23.10.2023-05.11.2023	Виконано
5	Принцип роботи системи фільтрації трафіку	06.11.2023-10.11.2023	Виконано
6	Метод фільтрації трафіку для підвищення захищеності мережі від зовнішніх загроз	11.11.2023-30.11.2023	Виконано
7	Охорона праці	01.12.2023-06.12.2023	Виконано
8	Охорона навколишнього середовища	07.12.2023-17.12.2023	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	18.12.2023-31.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професор Батир ХАЛМУРАДОВ		
Охорона навколиш-нього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “29" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Валентин ХІВРИЧ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Метод фільтрації трафіку для підвищення захищеності мережі від зовнішніх загроз» містить 84 сторінки, 27 рисунків, 2 таблиці, 49 використаних джерел.

ФІЛЬТРАЦІЯ ТРАФІКУ, ЗАХИСТ МЕРЕЖІ, ЗОВНІШНІ ЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА, БРАНДМАУЕРИ, СИСТЕМИ ВИЯВЛЕННЯ/ЗАПОБІГАННЯ ВТОРГНЕННЯМ, VPN І БЕЗПЕКА МЕРЕЖІ, КЕРУВАННЯ ДОСТУПОМ, ШИФРУВАННЯ ТРАФІКУ, ПЕРЕТВОРЕННЯ МЕРЕЖЕВИХ АДРЕС, ЗАХИСТ ВІД ВІДМОВ В ОБСЛУГОВУВАННІ (DOS/DDOS), ПРОТОКОЛИ ЗАХИСТУ (TLS/SSL), МОНІТОРИНГ МЕРЕЖЕВОГО ТРАФІКУ, ІНТЕГРОВАНІ СИСТЕМИ БЕЗПЕКИ, ЗАХИСТ ВІД ЗЛОВЖИВАННЯ (МАНІПУЛЮВАННЯ) ТРАФІКОМ, АНАЛІЗ ТРАФІКУ, ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ, СПОСТЕРЕЖЕННЯ ЗА МЕРЕЖЕЮ, БЕЗПЕКА КІНЦЕВИХ ТОЧОК, БЕЗПЕКА ВЕБ-ДОДАТКІВ.

Метою кваліфікаційної роботи є аналіз зовнішніх загроз у сфері інформаційної безпеки, оцінювання рівня їхньої потенційної небезпеки, дослідження методів фільтрації трафіку як способу захисту від зовнішніх загроз і розробка прототипу такого фільтра.

Об'єкт дослідження - зовнішні загрози у сфері інформаційної безпеки, системи фільтрації інтернет-трафіку.

Предмет дослідження - безпека інформації в частині несанкціонованого доступу до неї із зовнішнього середовища (зовнішні загрози) і можливість її підвищення за рахунок використання фільтра інтернет-трафіку.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IPS - Intrusion Prevention System (Система запобігання вторгнень).

IDS - Intrusion Detection System (Система виявлення вторгнень).

FW - Firewall (Брандмауер).

ACL - Access Control List (Список керування доступом).

DMZ - Demilitarized Zone (Демілітаризована зона).

DoS - Denial of Service (Відмова в обслуговуванні).

DDoS - Distributed Denial of Service (Розподілена відмова в обслуговуванні).

VPN - Virtual Private Network (Віртуальна приватна мережа).

TLS/SSL - Transport Layer Security/Secure Sockets Layer (Протоколи захисту транспортного рівня / Протоколи безпеки сокетів).

URL - Uniform Resource Locator (Одинаковий локаційний ідентифікатор).

DNS - Domain Name System (Система доменних імен).

IP - Internet Protocol (Інтернет-протокол).

NAT - Network Address Translation (Перетворення мережевих адрес).

WAF - Web Application Firewall (Брандмауер для веб-додатків).

MTU - Maximum Transmission Unit (Максимальна одиниця передачі).

QoS - Quality of Service (Якість обслуговування).

RDP - Remote Desktop Protocol (Протокол віддаленого робочого столу).

SIEM - Security Information and Event Management (Система управління інформацією та обробки подій безпеки).

LDAP - Lightweight Directory Access Protocol (Протокол доступу до легкодоступного каталогу).

IoT - Internet of Things (Інтернет речей).

IoE - Internet of Everything (Інтернет всього).

APT - Advanced Persistent Threat (Складна тривала загроза).

BYOD - Bring Your Own Device (Бери свій пристрій).

CoPP - Control Plane Policing (Керування трафіком у керуючому плані).

DLP - Data Loss Prevention (Запобігання втратам даних).

EPP - Endpoint Protection Platform (Платформа захисту кінцевих точок).

IoT Security - Internet of Things Security (Безпека Інтернету речей).

NIDS - Network Intrusion Detection System (Система виявлення вторгнень в мережу).

OT - Operational Technology (Операційна технологія).

PKI - Public Key Infrastructure (Інфраструктура з відкритим ключем).

RAT - Remote Access Trojan (Троян для віддаленого доступу).

Sandboxing - Isolated testing environment (Ізольоване тестування).

SaaS - Software as a Service (Програмне забезпечення як послуга).

UAC - User Account Control (Керування обліковими записами користувачів).

UEBA - User and Entity Behavior Analytics (Аналітика поведінки користувачів та сутностей).

VLAN - Virtual Local Area Network (Віртуальна локальна мережа).

WPA/WPA2/WPA3 - Wi-Fi Protected Access (Захищений доступ Wi-Fi - рівні 1, 2, 3).

ВСТУП

Актуальність теми. Нині переважна більшість компаній, державних структур і кінцевих користувачів використовують інформаційні системи (ІС) для зберігання, оброблення та обміну інформацією. Відповідно, зростає як кількість людей, що використовують ІС, так і потужності обчислювальних систем, а разом з цим постійно існує проблема захисту інформації, що зберігається і передається, від несанкціонованого доступу. Захист інформації - це практика запобігання несанкціонованому доступу, використанню, розкриттю, викривленню, викривленню, зміні, дослідженню, запису або знищенню інформації.

Комп'ютери та інформаційні системи використовуються практично в усіх сферах діяльності в останні десятиліття. Збільшення обсягів даних, що зберігаються в інформаційних системах, глобалізація комп'ютерних мереж, підвищення доступності сучасних технологій - усе це неминуче призводить до того, що інформація, розміщена в інформаційній системі, стає вразливою до несанкціонованого доступу або повного її знищення. Таким чином, під час роботи з ІС велика увага приділяється, або, принаймні, має приділятися повноцінному захисту інформації, що зберігається і передається.

У сучасних умовах практично неможливо створити інформаційну систему, повністю ізольовану від зовнішнього середовища. Безумовно, існують і застосовуються системи закритого типу, і для завдань певного типу це або єдиний, або виправданий варіант реалізації захисту інформації від зовнішніх загроз. Однак здебільшого такі чинники, як глобалізація комп'ютерних мереж, масове впровадження бездротових способів зв'язку, перехід до поширених сховищ і обчислювальних систем та багато інших, однозначно визначають необхідність підключення ІС до глобальної мережі в тій чи іншій мірі.

За наявності в інформаційної системи виходу в глобальну мережу неминуче з'являється велика кількість зовнішніх загроз безпеці інформації, і виникає необхід-

ність у забезпеченні захисту ІС від таких загроз. Запорукою успішної боротьби з несанкціонованим доступом до інформації та перехопленням даних слугує чітке уявлення про канали витоку інформації в зовнішнє середовище, тобто, про наявні та можливі зовнішні загрози безпеці інформації. Одним із способів захисту від зовнішніх загроз, що надходять із зовнішньої мережі, є фільтрація вхідного і вихідного інтернет-трафіку на предмет виявлення небажаної інформації або небажаних джерел інформації та запобігання виникненню загрози.

Актуальність дослідження зумовлена постійно зростаючим числом кіберзлочинів та інших зовнішніх загроз збереженню інформації, а, отже, і збільшенням збитків компаній, пов'язаних з усуненням наслідків втрати інформації та відновленням нормального режиму роботи. При цьому, хоча і постійно створюються нові способи і методи захисту цифрової інформації, також наростає і потужність сучасних комп'ютерів, у зв'язку з чим більшість чинних способів захисту постійно виявляються уразливими, нікчемними для потужніших комп'ютерів, і потрібно запроваджувати дедалі новіші та новіші вимоги до захисту інформації, що зберігається на комп'ютерах.

Метою кваліфікаційної роботи є аналіз зовнішніх загроз у сфері інформаційної безпеки, оцінювання рівня їхньої потенційної небезпеки, дослідження методів фільтрації трафіку як способу захисту від зовнішніх загроз і розробка прототипу такого фільтра.

Наукова гіпотеза дослідження полягає в тому, що підхід до захисту інформації наразі здебільшого полягає в захисті від відомих загроз, а також навчанні кінцевих користувачів для виключення людського фактора. Розглядається ефективність впровадження та використання фільтрації трафіку для забезпечення більш надійного захисту.

Наукові завдання дослідження:

- проаналізувати види зовнішніх загроз і методи їхньої дії;
- оцінити рівень потенційної небезпеки зовнішніх загроз;
- дослідити методи фільтрації трафіку як способу захисту від зовнішніх загроз;
- розробити прототип фільтра трафіку;

- провести тестування розробленого прототипу;
- оцінити результати тестування, порівняти їх з наявними системами фільтрації, зробити висновки.

Методи дослідження, які використані в цій роботі:

- огляд і вивчення статей, нормативних актів і досліджень, присвячених захисту інформації від зовнішніх загроз;
- аналіз інформації, статистичне дослідження;
- розробка прототипу програми;
- тестування прототипу додатка, оцінка та порівняння результатів.

Об'єкт дослідження - зовнішні загрози у сфері інформаційної безпеки, системи фільтрації інтернет-трафіку.

Предмет дослідження - безпека інформації в частині несанкціонованого доступу до неї із зовнішнього середовища (зовнішні загрози) і можливість її підвищення за рахунок використання фільтра інтернет-трафіку.

Отримані результати мають велике **практичне значення** для покращення безпеки мережі та захисту інформації в організаціях та корпораціях:

- *Вдосконалення захисту мережі.* Використання методів фільтрації трафіку та інших засобів безпеки, щоб забезпечити ефективний захист мережі від потенційних загроз.
- *Запобігання вторгненням та аналіз вразливостей.* Використання систем виявлення та запобігання вторгнень для вчасного виявлення та запобігання вразливостям, які можуть бути використані зловмисниками.
- *Боротьба з атаками DDoS.* Використання фільтрації трафіку для відсіювання шкідливого трафіку, що допомагає у запобіганні атак DDoS та забезпеченні нормальної роботи мережі.
- *Забезпечення безпеки сполучень з віддаленими пунктами.* Використання VPN та шифрування трафіку для захисту конфіденційності та цілісності даних під час обміну інформацією з віддаленими пунктами.
- *Моніторинг та аналіз загроз.* Аналіз та моніторинг трафіку дозволяє вчасно виявляти аномальні активності та потенційні загрози для мережі.

- *Управління доступом та політиками безпеки.* Використання Access Control Lists (ACLs) для обмеження доступу до ресурсів та встановлення політик безпеки для забезпечення відповідності стандартам безпеки.
- *Безпека веб-додатків та даних.* Використання Web Application Firewalls (WAFs) для захисту веб-додатків та запобігання атак на дані.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ЗОВНІШНІ ЗАГРОЗИ БЕЗПЕЦІ ТА МЕТОДИ ПРОТИДІЇ

Під зовнішніми загрозами розуміють такі загрози безпеці інформації, ініціатором (виконавцем) яких є зовнішній по відношенню до ресурсів інформаційної системи суб'єкт (зловмисник), який не має авторизованого доступу до ІС. Найчастіше загрози такого виду надходять із мережі Інтернет, тобто, з інших інформаційних систем, зі звичайних персональних комп'ютерів, але також можуть бути реалізовані за допомогою спеціалізованих технічних або програмно-технічних засобів, що не входять до самої глобальної мережі. Як найбільш відомі приклади таких загроз можна назвати атаки шкідливих програм, хакерів, шпигунське ПЗ і фішинг [1].

1.1. Види зовнішніх загроз

Загрози витоку акустичної (мовної) інформації. Виникнення загроз витоку акустичної (мовленнєвої) інформації, що міститься безпосередньо у вимовленій промові користувача ІС, під час опрацювання інформації в ІС, зумовлене наявністю функцій відтворення інформації акустичними засобами ІС або функцій голосового введення інформації в ІС, що стають дедалі більш поширеними на цей час.

Перехоплення акустичної (мовленнєвої) інформації в цих випадках можливе з використанням апаратури, що реєструє акустичні хвилі, а також електромагнітні (зокрема й оптичні) випромінювання та електричні сигнали, які виникають унаслідок перетворень у технічних засобах оброблення інформації, допоміжних технічних засобах і системах, та будівельних конструкціях під впливом акустичних хвиль.

Крім цього, перехоплення акустичної (мовної) інформації можливе з використанням спеціальних електронних пристроїв знімання мовної

інформації, впроваджених у технічні засоби оброблення інформації, допоміжні технічні засоби і системи та приміщення або під'єднаних до каналів зв'язку.

Загрози витоку видової інформації. Загрози витоку видової інформації реалізуються за рахунок перегляду інформації за допомогою оптичних засобів з екранів дисплеїв та інших засобів відображення засобів обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів оброблення графічної, відео- та літерно-цифрової інформації, що входять до складу ІС [1].

Крім цього, перегляд (реєстрація) інформації можливий з використанням спеціальних електронних пристроїв знімання, впроваджених у службових приміщеннях або приховано використовуваних фізичними особами під час відвідування ними службових приміщень.

Необхідною умовою здійснення перегляду (реєстрації) інформації є наявність прямої видимості між засобом спостереження та носієм інформації.

Загрози витоку інформації каналами побічних електромагнітних випромінювань і наведень (ПЕМВН). Виникнення загрози інформації каналами ПЕМВН можливе завдяки перехопленню технічними засобами побічних електромагнітних полів та електричних сигналів, що виникають під час опрацювання інформації технічними засобами ІС, які можуть нести корисну інформацію.

Генерація інформації, що циркулює в технічних засобах ІС у вигляді електричних ланцюгах технічних засобів ІС супроводжується побічними електромагнітними випромінюваннями, які можуть поширюватися за межі службових приміщень. Також до цього виду загрози належить використання незахищених бездротових каналів передавання інформації або слабкий їхній захист, що дає змогу перехоплювати інформацію безпосередньо з каналу зв'язку, оскільки такі випромінювання також часто поширюються за межі службових приміщень.

Загрози несанкціонованого доступу до інформації в інформаційному середовищі. Загрози несанкціонованого доступу (НСД) до ІС із застосуванням програмних і програмно-апаратних засобів реалізуються під час здійснення несанкціонованого, зокрема випадкового, доступу, унаслідок якого здійснюється порушення конфіденційності (копіювання, несанкціоноване розповсюдження), цілісності (знищення, модифікація) і доступності (створення ситуації, за якої читання або зміна стає неможливим) інформації, та містять у собі [2]:

- загрози доступу (проникнення) в операційне середовище комп'ютера з використанням штатного програмного забезпечення (засобів операційної системи або прикладних програм загального застосування);
- загрози створення позаштатних режимів роботи програмних (програмно-апаратних) засобів за рахунок навмисних змін службових даних, ігнорування передбачених у штатних умовах обмежень на склад і характеристики оброблюваної інформації, спотворення (модифікації) самих даних тощо. - загрози типу "відмова в обслуговуванні" (DDoS-атаки);
- загрози впровадження шкідливих програм: троянів, шпигунського програмного забезпечення, програм-вимагачів тощо.

Під час розроблення системи захисту інформації зазвичай виокремлюють і розглядають саме цей вид загроз, оскільки від решти видів

існує досить мало специфічних способів захисту (що реалізуються безпосередньо в рамках інформаційної системи, не вдаючись до застосування додаткових засобів). Зовнішні загрози НСД найчастіше надходять різними каналами зв'язку ІС із зовнішнім світом і, відповідно, саме від таких загроз здатні захистити різні програмні засоби, такі, як системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), фільтри трафіку, антивірусне ПЗ, системи резервного копіювання даних та інші.

1.2. Принципи дії зовнішніх загроз НСД

Усі зовнішні загрози несанкціонованого доступу до даних поділяються на дві основні групи - активні та пасивні. У першому випадку загроза виникає в результаті активних дій зловмисника, який отримує доступ до даних безпосередньо, а в другому - сама загроза реалізується зловмисником, але виникає в результаті дій користувача (наприклад, запуск програми, неправильне налаштування системи тощо). Тим не менш, для реалізації пасивної загрози безпеки необхідні подальші дії з боку зловмисника, від яких можна створити ефективний захист [3].

Загрози НСД в ІС підрозділяють на 3 основні типи загроз: загрози доступу до операційного середовища комп'ютера, загрози створення позаштатних режимів роботи та загрози впровадження шкідливих програм.

Загрози доступу (проникнення) в операційне середовище комп'ютера. Загрози такого типу реалізуються з використанням штатного програмного забезпечення (засобів ОС або прикладних програм). Зовнішні загрози доступу до ОС реалізуються з використанням протоколів мережевого адміністрування (віддалений доступ, віддалена конфігурація). Ці загрози застосовні як до ІС на базі робочого місця (персональні комп'ютери), так і до всіх ІС, що мають під'єднання до мереж загального користування та глобальних мереж (сервери).

Унаслідок реалізації такої загрози зловмисник може як отримати доступ до даних, що зберігаються в ІС, так і повністю вплинути на робочий процес підприємства, що може призвести до повного виведення ІС з ладу.

Загрози створення нештатних режимів роботи. Такі загрози також називаються загрозами типу "відмова в обслуговуванні" або DDoS. Як правило, вони розглядаються стосовно ІС на базі локальних і розподілених ІС незалежно від призначення. Їхня реалізація зумовлена тим, що під час розроблення системного або прикладного програмного забезпечення не враховується можливість навмисних дій щодо цілеспрямованої зміни:

- змісту службової інформації в пакетах повідомлень, що передаються мережею;
- умов обробки даних (наприклад, ігнорування обмеження на довжину повідомлення);
- форматів подання даних;
- програмного забезпечення обробки даних.

Унаслідок реалізації такої загрози відбувається переповнення буферів, блокування та зациклення процедур обробки, що призводить до зависання комп'ютера та призупинення роботи ІС (а це може призвести до збитків) або до того, що ІС починає передавати дані, які не повинна була передавати, і зловмисник може перехопити ці дані.

Загрози впровадження шкідливих програм. Кількість шкідливих програм у наші дні вже значно перевищує кілька сотень тисяч або навіть мільйонів. Усі вони мають різні способи дії і несуть різні наслідки, але більшість із них використовують або вразливості ПЗ, або помилки користувача. До цієї категорії належать усі програми-трояни, вимагачі, шпигунське ПЗ тощо.

Унаслідок реалізації такої загрози зловмисник може отримати доступ до даних, що зберігаються в ІС, а також до робочого процесу підприємства, призупинити працездатність ІС тощо.

РОЗДІЛ 2
ОЦІНКА ПОТЕНЦІЙНОЇ НЕБЕЗПЕКИ ЗОВНІШНІХ ЗАГРОЗ

2.1. Оцінка за збитками

Загрози несанкціонованого доступу до інформації сьогодні - реальна і серйозна небезпека інформаційній інфраструктурі, інтелектуальній та фізичній власності державних і комерційних об'єктів.

Доповідь Всесвітнього економічного форуму "Глобальні ризики 2023" розглядає кібератаки як одну з основних загроз світовій економіці. За ймовірністю настання, кібератаки входять до п'ятірки найімовірніших глобальних загроз на 2023 рік. У документі наводиться також графік зростання офіційно визнаних інцидентів кіберзлочинності із зазначенням значного збільшення втрат від таких злочинів на прикладі США (рис. 2.1):

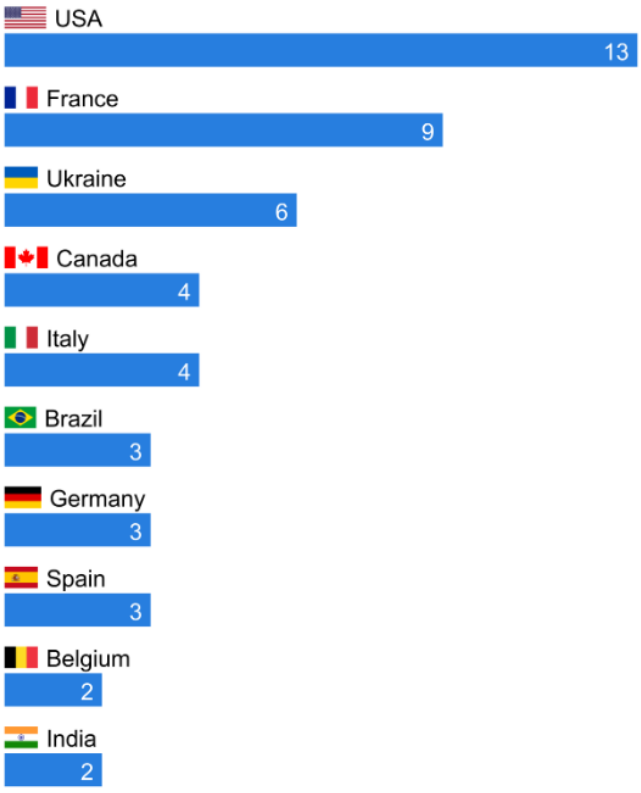

Рис. 2.1. Статистика кількості потужних кібератак за поточний рік

З настанням нового року важливо бути в курсі кібератак, які відбулися за останні 12 місяців. З розвитком технологій зростає і потреба в посиленні заходів кібербезпеки.

Ось найбільш значущі кібератаки з 2022 року до жовтня 2023 року та дії компаній для захисту даних від майбутніх загроз.

1. Rackspace. 06 грудня 2022 року компанія Rackspace Technology® повідомила про інцидент з вірусом-вимагачем, який вплинув на їхнє середовище хостингу Exchange. Це призвело до перебоїв у роботі деяких клієнтів.

Компанія швидко відреагувала, зібравши внутрішню команду безпеки та уклавши контракт з провідною фірмою з кіберзахисту. Вони розслідують інцидент і обмежують вплив потенційної втрати даних або доходів, а також будь-яких додаткових витрат.

Rackspace вжив проактивних заходів для ізоляції та локалізації інциденту, щоб захистити своїх клієнтів. Однак розслідування вважає, що програма-здирник була ізольована від інших продуктів, і що інші продукти продовжують працювати.

Rackspace розмістив попереджувальний банер, який оновлюється в режимі реального часу на своєму веб-сайті. Компанія активно вживає додаткових заходів безпеки для моніторингу будь-яких підозрілих повідомлень. Крім того, вони надають споживачам рекомендації щодо переходу від потенційно уражених сервісів. Це також включає допомогу в обмеженні впливу операцій клієнтів.

2. Окта LAPSUS$. 22 березня 2023 року LAPSUS$ опублікував в Інтернеті скріншоти, отримані від стороннього інженера служби підтримки клієнтів Okta. В результаті Okta опублікувала заяву, в якій пояснила ситуацію і запевнила, що сервіс Okta все ще безпечний. Вони заявили, що клієнтам не потрібно вживати жодних коригувальних дій.

Sitel - це підрядник співробітників Okta, який допомагає в організації підтримки клієнтів. Після невдалої спроби додати новий пароль до облікового запису одного з інженерів Sitel, з обережності, він був скинутий, і Sitel звернулася до криміналістичної фірми для подальшого розслідування.

Щоб зрозуміти потенційний вплив інциденту на безпеку, "Окта" проаналізувала дії співробітників Sitel у додатку SuperUser протягом п'яти днів. В результаті було встановлено, що близько 2,5% клієнтів отримали доступ до свого облікового запису "Окта" через Sitel.

Для прозорості клієнти отримають звіт про дії співробітників Sitel щодо їхнього орендаря Okta за цей період, щоб вони могли самостійно оцінити ситуацію.

Вихідний код на GitHub. Нещодавно Okta зазнала порушення безпеки, коли хтось викрав їхній вихідний код з репозиторіїв GitHub. Керівник служби безпеки Okta Девід Бредбері (David Bradbury) надіслав повідомлення про те, що сталося, своїм контактам зі служби безпеки електронною поштою.

Зловмисник не отримав доступу до жодних даних клієнтів або сервісів. Користувачі різних сервісів Okta не постраждали від інциденту.

3. Crypto. Криптовалютна біржа Crypto зазнала хакерської атаки на початку цього року. Це призвело до несанкціонованого виведення біткоїнів та ефіру на суму близько $35 млн (спочатку оцінювалося в $15 млн).

Для розслідування та вирішення проблеми Crypto призупинила виведення коштів на 14 годин. В цілому, жоден клієнт не втратив кошти, оскільки Crypto запобігла майже всім несанкціонованим зняттям коштів. Всі інші випадки були відшкодовані.

Вони також впровадили свою Всесвітню програму захисту облікових записів (WAPP), яка обіцяє відновити кошти до $250 000 для відповідних користувачів.

4. Дрібниці порівняно з 620 мільйонами доларів, вкраденими у Axie Infinity. Компанія Chainalysis, криптоаналітична фірма, нещодавно допомогла уряду США повернути близько 30 мільйонів доларів з викрадених коштів, виведених з онлайн-гри Axie Infinity. Відповідальними за крадіжку є північнокорейські хакери, відомі як Lazarus Group, пов'язані з численними крадіжками криптовалют за останні роки.

Завдяки Chainalysis та правоохоронним органам вдалося повернути частину викрадених коштів, що стало першим випадком, коли США вилучили криптовалюту, викрадену північнокорейськими хакерами.

Загальна сума викрадених коштів перевищила 600 мільйонів доларів, але з їхньою допомогою вдалося повернути принаймні частину з них, увійшовши в історію.

5. Вторгнення росії в Україну та IT-армія. Група хакерів в Україні порушує роботу російських веб-сервісів у відповідь на російське вторгнення 24 лютого 2022 року. Група під назвою "IT-армія України" успішно вивела з ладу сайти кремля, державної думи, державних ЗМІ, кількох банків та енергетичного гіганта "Газпром", росія намагалася зупинити кібератаки, фільтруючи доступ до певних веб-сайтів, але це призвело лише до ще більших збоїв у роботі.

6. Кібератаки на Чорногорію: Винна росія. Експерти з кількох країн кинулися розслідувати і відновлювати комп'ютерну систему уряду Чорногорії після скоординованих кібератак, що почалися приблизно 20 серпня 2022 року і поставили під загрозу державну інфраструктуру. Атака була частково здійснена російськомовною бандою вимагачів, відомою як Cuba ransomware під назвою Zerodate.

Дехто підозрює, що за цим стоїть кремль або навіть державні спецслужби. І це може бути пов'язано з тим, що Чорногорія вступила до НАТО, незважаючи на російський спротив, і взяла участь у західних санкціях проти москви щодо України, що змусило країну терористку назвати їх ворогам.

7. Log4j. Log4j - це стандартизована утиліта Java, яка існує вже 20 років. Однак у грудні 2022 року було виявлено критичну вразливість під назвою Log4Shell, яка дозволяла неавторизованим і непідготовленим суб'єктам загроз отримати контроль над додатками, що призводило до вартісних порушень.

Незважаючи на численні спроби вирішити проблему, багато організацій залишаються вразливими до ризику Log4Shell: станом на жовтень 2023 року 2,5% активів залишаються вразливими. Крім того, 29% активів показали рецидиви, незважаючи на те, що раніше було досягнуто повного усунення.

8. LAPSUS$. Вперше LAPSUS$ потрапив у заголовки новин у грудні 2021 року через атаку на Міністерство охорони здоров'я Бразилії, а в березні наступного року привернув увагу світової спільноти завдяки масштабним кібератакам на такі компанії, як "Окта", Microsoft, Samsung і Vodafone.

Після цього у квітні 2022 року влада заарештувала і висунула звинувачення двом підліткам до 18 років у зв'язках з LAPSUS$. Незважаючи на те, що їм було пред'явлено кілька звинувачень, діяльність групи продовжилася, і незабаром після цього

хакери опублікували зламані вихідні коди додатків таких великих компаній, як Facebook і DHL.

Хоча невідомо, чи LAPSUS$ також стоїть за витоком даних Uber і зломом Rockstar Games, дехто занепокоєний відсутністю протоколів кібербезпеки у цих великих компаній і тим, що ці молоді люди можуть стати мішенню для цих величезних корпорацій.

9. X (Твіттер): 5,4 мільйона акаунтів користувачів викрадено в результаті атаки соціальної інженерії 5 серпня 2023 року X (Twitter) повідомив, що хакер під псевдонімом "Диявол" скористався помилкою нульового дня, щоб прив'язати особисті ідентифікатори, такі як номери телефонів та електронні адреси, до акаунтів користувачів на платформі соціальних мереж.

Вступаючи в 2024 рік, ми повинні знати про найбільш критичні кібератаки попереднього року і про те, чого ми можемо навчитися на їхньому прикладі. Rackspace, Okta та Crypto.com були важливими цілями у 2023 році, і кожна з них пропонує уроки для бізнесу будь-якого розміру.

Злом Axie Infinity був одним з найбільших в історії, а участь росії в кібератаках на Чорногорію показує, що жодна країна не застрахована від цих загроз країни спонсора тероризму. Крім того, витік Log4j підкреслює важливість постійного оновлення всього програмного забезпечення, а злам X (Twitter) демонструє силу атак соціальної інженерії [4].

2.2. Оцінка за кількістю кібератак

Згідно з дослідженням проєкту SecurityLab, кількість кіберзлочинів у третьому кварталі 2023 року зросла на 89,3%, а питома вага таких діянь сягнула 19,9% від загальної кількості правопорушень (рис. 2.3).

Рис. 2.2. Статистика кількості кібератак на інфраструктуру України за 2023 рік

При цьому розкриття таких злочинів зберігається на рівні не більше 23%, а частка в загальній кількості злочинів по країні становить 19-22%. Таким чином, правоохоронні органи вже зараз не справляються з розслідуваннями кіберзлочинів, а в разі збереження такої тенденції існує ризик, що кібератаки стануть основною загрозою діяльності підприємств і без вжиття необхідних заходів захисту можуть стати основною причиною припинення діяльності великої кількості підприємств

2.3. Фільтрація мережевого трафіку як спосіб захисту від зовнішніх загроз

Фільтрація трафіку - це один зі способів обмеження доступу користувачів або інформаційних систем до певної інформації (ресурсів мережі). Застосування систем фільтрації трафіку дає змогу отримати [5]:

- захист від шпигунських програм, DDoS-атак, троянів та інших атак;
- неможливість відвідування потенційно небезпечних, небажаних і відомих заражених інтернет-сайтів;
- виявлення засобів стеження за активністю користувачів (телеметрії).

Фільтрація трафіку застосовується в дуже широкому діапазоні масштабів і рівнів значущості інформаційних систем - від захисту домашньої мережі від однієї популярної загрози до великих критично важливих об'єктів. Наприклад, відповідно до Вимог щодо забезпечення безпеки значущих об'єктів критичної інформаційної інфраструктури України, контроль і аналіз мережевого трафіку входить до переліку заходів із забезпечення безпеки для об'єктів 1 категорії значущості.

Також система фільтрації трафіку, як і будь-яка інша система забезпечення інформаційної безпеки, має забезпечувати виконання основних вимог:

- запобігання несанкціонованому доступу до інформації та (або) передачі її особам, які не мають права на доступ до інформації;
- своєчасне виявлення фактів несанкціонованого доступу до інформації;
- попередження можливості несприятливих наслідків порушення порядку доступу до інформації;
- недопущення впливу на технічні засоби обробки інформації, внаслідок якого порушується їхнє функціонування;
- постійний контроль за забезпеченням рівня захищеності інформації.

Для того, щоб зрозуміти, на якому етапі передавання інформації відбувається фільтрація трафіку, необхідно розглянути мережеву модель за моделлю OSI, яку застосовують на сьогодні (рис. 2.3). Ця модель визначає 7 рівнів взаємодії систем - від фізичного (фізичне середовище передавання даних) до прикладного (взаємодія між конкретними додатками) [5].

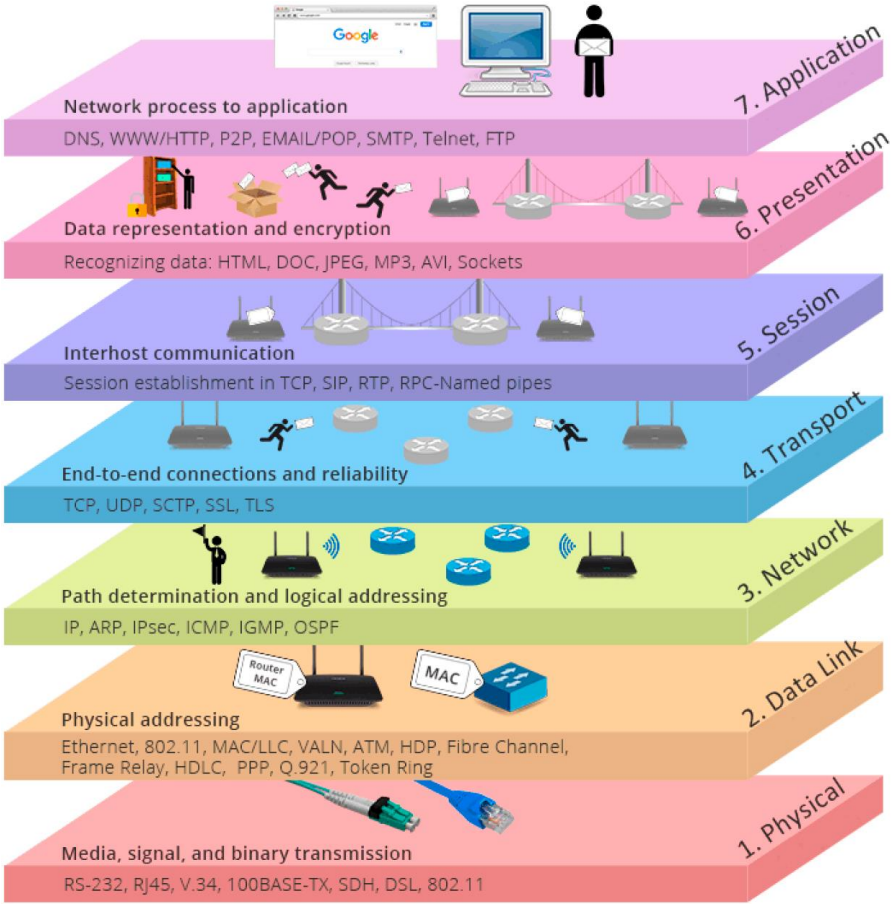

Рис. 2.3. Мережева модель OSI

Фільтрація трафіку, як правило, реалізується на мережевому та/або транспортному рівні в моделі OSI, саме ці рівні забезпечують глобальну адресацію переданих мережею Інтернет пакетів даних. Це пов'язано з тим, що нижчі рівні мережі (фізичний, канальний) не мають способів глобальної адресації, або їхня адресація ефективна лише в невеликих масштабах, а вищі рівні найчастіше недоступні, тому що більше ніж 70% трафіку в мережі на сьогоднішній день складається із зашифрованих даних з використанням протоколів шифрування, реалізованих на вищих рівнях мережевої моделі [5].

Проте варто зазначити, що нижчий рівень у мережевій моделі, то вищий рівень захисту, що забезпечується фільтром, і то вища швидкість його роботи, і для кожної конкретної ситуації можлива реалізація фільтра на потрібному в даному випадку рівні. Наприклад, фільтр на фізичному рівні не виконує функцію фільтрації безпосередньо переданих даних, але може захистити мережу від перепадів напруги, природних катаклізмів і загроз витоку інформації каналами зв'язку.

Така фільтрація трафіку зазвичай називається URL-фільтрацією (оскільки оперує IP-адресами і пов'язаними з ними доменними іменами) або контент-фільтрацією (оскільки фільтрує трафік за конкретним його вмістом, а не за набором властивостей або відмінних ознак). Умовно такі системи фільтрації можна оцінювати за чотирма основними показниками:

1. Точність - успішність фільтрації (чи блокує система весь небажаний трафік і чи пропускає весь корисний);
2. Прозорість - чіткість параметрів, що дають змогу віднести трафік до забороненого;
3. Відкритість - користувач або системний адміністратор отримують достовірну інформацію про те, що ресурс, до якого він намагається отримати доступ, віднесений до заборонених;
4. Підзвітність - ступінь участі населення в політиці фільтрації контенту (може бути застосовано до глобальних фільтрів на рівні країн і міст).

2.4. Класифікація методів фільтрації трафіку

Системи фільтрації трафіку можна розділити на чотири групи за методом їх встановлення (розміщення) [6]:

1. Міжнародний рівень. Фільтрація DNS-запитів здійснюється централізовано на державному рівні, забезпечуючи в такий спосіб максимальний контроль держави над обмеженими ресурсами. Недоліком такого методу є складність його реалізації та великі витрати на це, оскільки Інтернет - мережа децентралізована, і в ній неможливо без серйозних модифікацій знайти одну точку входу всіх зовнішніх ресурсів.
2. Рівень інтернет-провайдера. Найбільш використовуваний метод на сьогоднішній день, визнаний досить надійним для обмеження доступу до ресурсів на підставі переліків заборонених сайтів та інших державних документів на рівні країни. Цей рівень зручний тим, що, з одного боку, на ньому нескладно організувати кілька єди-

них точок маршрутизації трафіку, через які будуть під'єднані всі споживачі, а з іншого, є відносно глобальним і дає змогу централізовано регулювати доступ до ресурсів з боку держави.

3. Рівень інтернет-шлюзу. Використовується в локальних мережах приватними установами та користувачами. На цьому рівні фільтрація трафіку найчастіше доступна за замовчуванням, але вимагає налаштування фахівцем і не вимагає великих вкладень.

4. Рівень комп'ютера користувача. Метод використовує програмне забезпечення, встановлене на ПК користувача, і, відповідно, забезпечує фільтрацію тільки на тому ПК, де було встановлено ПЗ. Такий метод ефективний для домашнього використання.

Із цієї класифікації можна дійти висновку, що система фільтрації являє собою програмний або програмно-апаратний комплекс, що перехоплює весь мережевий трафік, який проходить на заданому рівні, аналізує його вміст і ухвалює рішення про пропуск трафіку у внутрішню мережу на підставі реєстру обмежувальних ресурсів, який зберігають у якомусь вигляді в базі даних (рис. 2.4).

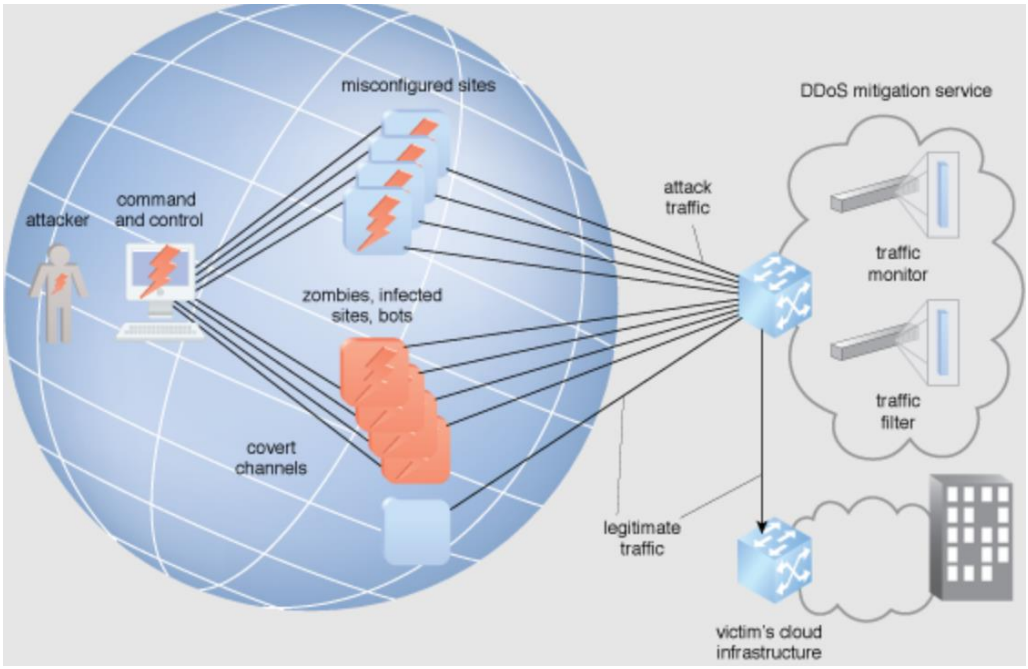

Рис. 2.4. Структура системи фільтрації трафіку

2.5. Глибокий аналіз трафіку (DPI)

На додаток до URL-фільтрів або контент-фільтрів іноді може застосовуватися технологія, звана глибоким аналізом трафіку (Deep Packet Inspection, DPI). DPI - це технологія перевірки та фільтрації пакетів за їхнім вмістом на основі накопичення статистичних даних. Система DPI, крім здійснення фільтрації за URL та ідентифікації протоколів і застосунків, присікає спроби проникнення і поширення шкідливого програмного забезпечення, аналізуючи передані дані. Система DPI здатна також і розшифровувати захищений мережевий трафік, встановлюючи проміжне захищене підключення до мережевого ресурсу (рис. 2.5) [7].

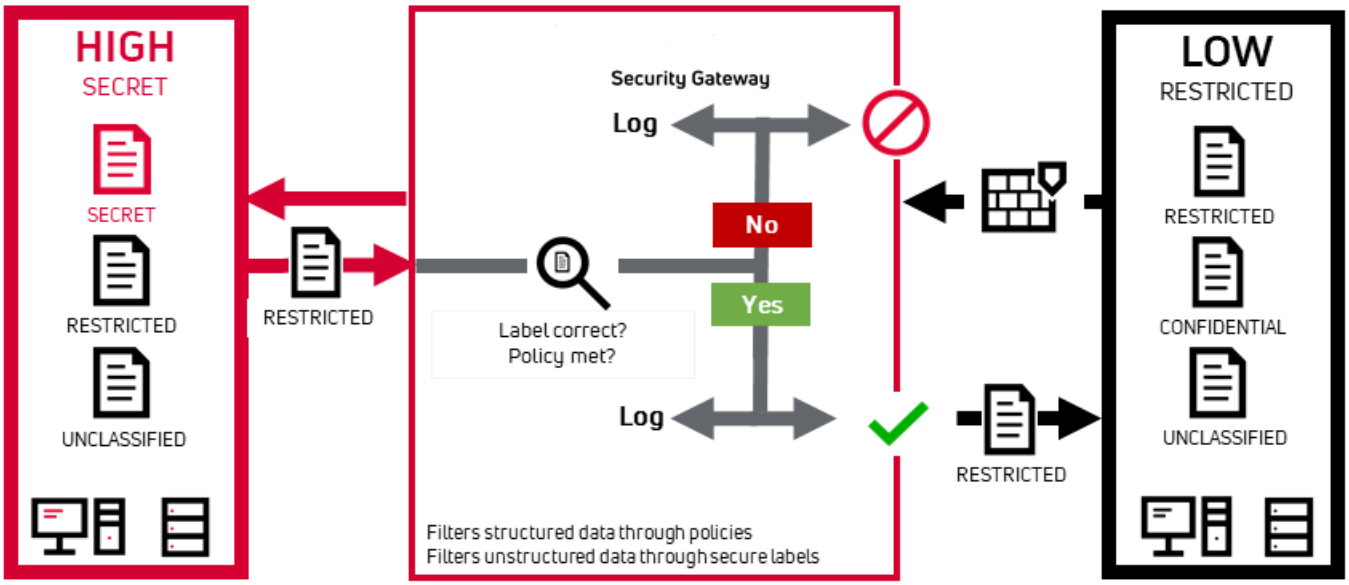

Рис. 2.5. Схема роботи системи DPI у захищеному з'єднанні на прикладі шлюзу Ideco Selecta

Основна відмінність системи DPI від звичайного фільтра трафіку полягає в тому, що DPI працює на всіх верхніх рівнях моделі OSI, починаючи з мережевого (рис. 2.6), що робить ці системи значно гнучкішими й точнішими.

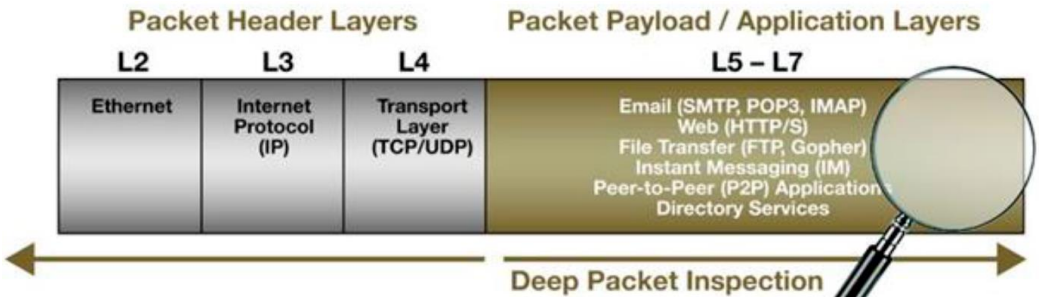

Рис. 2.6. DPI в моделі OSI

Принцип роботи системи DPI близький до принципу роботи антивірусного програмного забезпечення: для ідентифікації небажаного трафіку використовують сигнатурний аналіз, що передбачає дослідження трафіку за допомогою "підписів" і складається з п'яти етапів:

1. Аналіз зразка (Pattern analysis);
2. Числовий аналіз (Numerical analysis);
3. Поведінковий аналіз (Behavioral analysis);
4. Евристичний аналіз (Heuristic analysis);
5. Аналіз протоколу/стану (Protocol/state analysis).

Основним недоліком систем DPI є їхня складність роботи та налаштування, а також значне уповільнення мережі. Для того, щоб система забезпечувала той рівень захисту мережі, коли недостатньо звичайного контент-фільтра, потрібне тривале та складне її налаштування, що має значно більше кроків і параметрів. А оскільки система має аналізувати весь трафік, що проходить, повністю, а не тільки заголовки або метадані, відповідно, потрібні великі апаратні ресурси, а за великих обсягів трафіку, що проходить, можуть спостерігатися великі затримки, оскільки система може не впоратися зі збільшеним навантаженням.

РОЗДІЛ 3
ПРИНЦИП РОБОТИ СИСТЕМИ ФІЛЬТРАЦІЇ ТРАФІКУ

3.1. Фільтрація трафіку за IP-адресами

Система фільтрації трафіку зазвичай працює на основі так званих наборів правил - наборів записів (URL-адрес, IP-адрес, TCP-портів тощо), які необхідно блокувати ("чорний список") або які необхідно дозволяти, блокуючи всі інші ("білий список"). Під час надходження чергового пакета із зовнішньої мережі система фільтрації перехоплює цей пакет, перевіряє його метадані та вміст на збіг з одним із записів набору правил і, якщо виявлено збіг, або пропускає пакет у локальну мережу, або відкидає його - локальна мережа навіть не дізнається про існування такого пакета. Водночас для того, щоб користувач міг розуміти, що трафік було заблоковано, система фільтрації може передати в локальну мережу, наприклад, веб-сторінку з інформацією про причину блокування (якщо заблокували веб-сайт, який запитували) [8].

У найпростішому випадку набір правил являє собою один послідовний список (або по одному списку на кожен тип фільтрації), що складається з шаблонів і ключових слів адрес, і система фільтрації після розбору пакету просто зчитує файл порядково, застосовуючи до записів методи обробки регулярних виразів і порівнюючи запис з адресою в пакеті. Більш сучасні та ефективні системи фільтрації на додаток до простих списків можуть використовувати методи машинного навчання і великих даних для визначення потенційно небажаного трафіку, але такі системи схильні до частих помилкових спрацьовувань.

У цій роботі буде розглянуто принцип роботи трьох основних компонентів системи фільтрації: IP-адрес, TCP-портів і URL-адрес.

IP-адресація, як 4, так і 6 версії, має ієрархічну структуру, тобто адреса вузла записується блоками чисел, які адміністратор кожної конкретної мережі може використовувати для групування вузлів за логічними або фізичними критеріями. Підмережа IP-адрес - це набір IP-адрес, що починаються із заданих чисел. Наприклад, запис

"10.0.0.0.0/8" вказує на всі хости, у яких перші 8 біт (одне число) дорівнюють зазначеним, тобто "10". Схожий принцип застосовний і для IPv6, однак, використовується рідше через відсутність стандартизації на глобальному рівні.

Так само і мережевий фільтр може бути налаштований на фільтрацію не тільки конкретного вузла, а великої кількості вузлів за допомогою вказівки тільки на співпадаючу частину їхніх адрес. Це корисно, наприклад, коли веб-сайт для збільшення продуктивності розміщується на декількох серверах з різними IP-адресами, а обмежити доступ до нього за URL з якої-небудь причини немає можливості [9].

Для фільтрації трафіку за IP-адресою система фільтрації насамперед отримує пакет і читає дані із заголовка IP-пакета (рис. 3.1). У цьому заголовку завжди вказано в незашифрованому вигляді IP-адресу джерела (Source address) та IP-адресу призначення (Destination address), які завжди вказують на початкове джерело пакету (за винятком випадків, коли використовується VPN або інше тунелювання - у цьому разі фільтрація трафіку стандартними засобами неможлива, і єдиний спосіб обмежити доступ до хостів у цьому разі - обмежувати доступ до самих VPN-серверів).

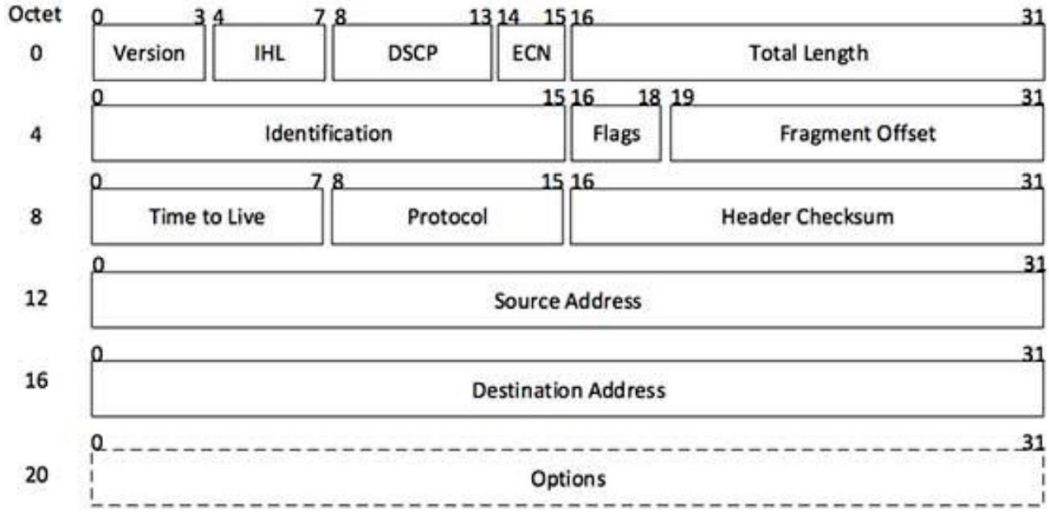

Рис. 3.1. Склад заголовка IP-пакета

Для ефективного пошуку отриманої IP-адреси джерела в наборі правил бажано, щоб список адрес було відсортовано від найбільшої підмережі до найдрібнішої, отже, у разі збігу знайденої адреси із записом великої підмережі не доведеться порівнювати

запис із більш точними значеннями, і цей пакет можна буде відфільтрувати набагато раніше.

IP-адреса в наборі правил може бути записана різними способами. Це можуть бути як описані вище конкретні хости або підмережі, так і регулярний вираз, якщо якийсь ресурс має кілька IP-адрес, вони не входять в одну підмережу, але мають загальні параметри. Наприклад, для IPv4-адрес можуть бути коректними такі записи:

- 125.13.255.1
- 125.13.0.0/16
- 125.13.255.*

* (режим обмеження доступу до всіх IP-адрес).

3.2. Фільтрація трафіку за TCP-портами

Принцип фільтрації за TCP-портами схожий на фільтрацію за IP-адресами з тією різницею, що для визначення трафіку використовуються TCP-порти - ідентифікатори додатків, реалізовані на транспортному рівні мережевої моделі. Відповідно, для цього система фільтрації трафіку повинна також зчитати порт призначення (Destination port) із заголовка TCP-пакета (рис. 3.2), вкладеного в IP-пакет. TCP-пакети також передаються мережею в незашифрованому вигляді, що забезпечує надійність такого способу фільтрації [10].

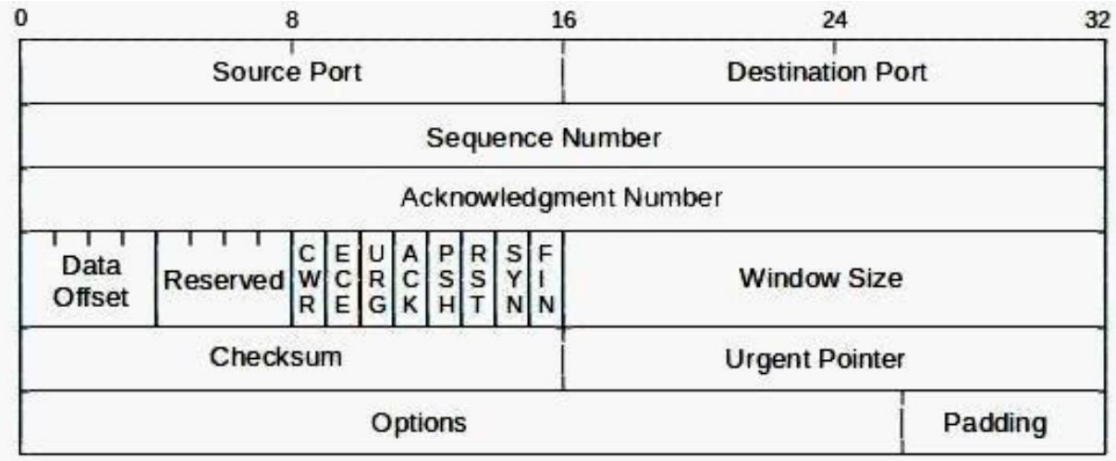

Рис. 3.2. Склад заголовка TCP-пакета

Такий спосіб фільтрації забезпечує обмеження доступу до конкретних застосунків, оскільки для кожного застосунку використовується свій номер порту. Також існує багато зумовлених портів (наприклад, 80 - веб-сторінки, HTTP, 3389 - підключення до віддаленого робочого столу, RDP тощо) [11].

Спосіб визначення трафіку для фільтрації практично ідентичний описаному вище для IP-адресації: достатньо списку фільтрованих портів. Однак у наборах правил, суміщених із правилами для IP-адрес, допустимо також вказувати конкретну IP-адресу джерела для заданого протоколу. Приклади допустимих записів:

Для ізольованого списку:

- 80
- 22-23
- 445,446,447

Для суміщеного списку:

- *:80
- *:[22-23]
- *:[445,446,447]
- 115.19.126.7:2334

3.3. Фільтрація трафіку за URL-адресами

Для реалізації цього компонента необхідно, щоб пристрій, на якому розміщений фільтр трафіку, мав доступ до DNS-сервера - сервера перетворення доменних імен на IP-адреси, або був встановлений безпосередньо на DNS-сервері. Це пов'язано з тим, що пакети в мережі Інтернет ідентифікуються тільки за IP-адресами, а URL-адреси мають однозначне перетворення на такі адреси і створені тільки для зручності користувача.

Відповідно, під час отримання пакета мережевий фільтр повинен визначити доменне ім'я за IP-адресою джерела пакета.

Після отримання доменного імені система може продовжувати свою роботу, порівнюючи отриманий домен зі списком правил.

Однак принцип роботи URL-фільтрації загалом набагато складніший за попередні. Це пов'язано з тим, що IP-адреси не завжди відповідають реальним доменним іменам і навпаки. Існують так звані віртуальні сервери, які під час запиту веб-сайту перенаправляють користувача на інший сервер з іншим доменним ім'ям. Зазвичай це робиться для балансування навантаження, але ускладнює роботу фільтра трафіку [12].

Як приклад можна навести пошуковий сервіс Google. Як видно на рис. 3.3, доменному імені google.com відповідає відразу кілька IP-адрес. При цьому під час спроби визначити доменне ім'я однієї з цих адрес, воно виявляється зовсім іншим - у реальності сервери пошукової системи Google розташовані на серверах *.1e100.net.

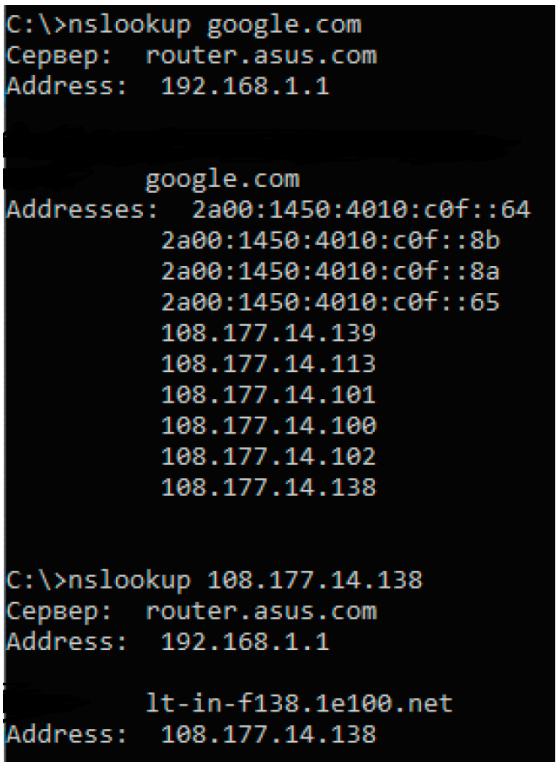

Рис. 3.3. Приклад множинної відповідності IP-адрес і доменних імен

Виходячи з цього, можна зробити висновок, що система фільтрації трафіку за URL-адресами повинна, щонайменше, створювати і підтримувати актуальну таблицю зв'язків IP-адрес і доменів, оскільки навіть статичні домени можуть змінювати своє розташування. Під час отримання пакета система повинна перевіряти URL на відповідність не тільки безпосередньо списку правил, а й іншим доменам, пов'язаним із цією IP-адресою або URL [14].

Сам же список правил нічим не відрізняється від попередніх і може містити як прості URL-адреси, так і регулярні вирази:

- google.com
- nau.edu.ua
- *.microsoft.com
- *.net

* (режим обмеження доступу до всіх доменів).

3.4. Огляд систем-аналогів

Інтернет Контроль Сервер (ІКС). ІКС - це програмне рішення для контентної фільтрації трафіку на основі наборів правил. ІКС здебільшого працює з наперед визначеними наборами правил - наприклад, зі списку SkyDNS або вбудованим реєстром безпечних сайтів. Проте, в ІКС можна створювати і власні заборонні та дозвільні правила [15].

ІКС розрахований на середні та великі організації (ще більше - на освітні установи), пропонуючи ліцензії, починаючи від 10 користувачів. Як і попередні аналоги.

До недоліків ІКС можна віднести низький рівень документованості, незрозумілість опису функціоналу системи, застарілий інтерфейс і реалізацію тільки на програмному рівні на одному ПК.

Вбудовані фільтри трафіку. Також варто зазначити, що крім окремих спеціалізованих рішень, функції фільтрації мережевого трафіку часто входять до складу антивірусних пакетів або систем управління домашніх маршрутизаторів. Такі системи фільтрації розраховані здебільшого на кінцевих користувачів, не надають особливої гнучкості їхнього налаштування і часто сильно обмежені. Наприклад, хоча в складі ПЗ маршрутизаторів така функція присутня часто, проте, вона присутня далеко не завжди, і її здібності сильно різняться від пристрою до пристрою. Наприклад, на одному з маршрутизаторів компанії Asus (рис. 3.4) є можливість налаштування списку фільтрації URL-адрес, ключових слів (DPI без можливості аналізу зашифрованого трафіку) і мережевих служб [16].

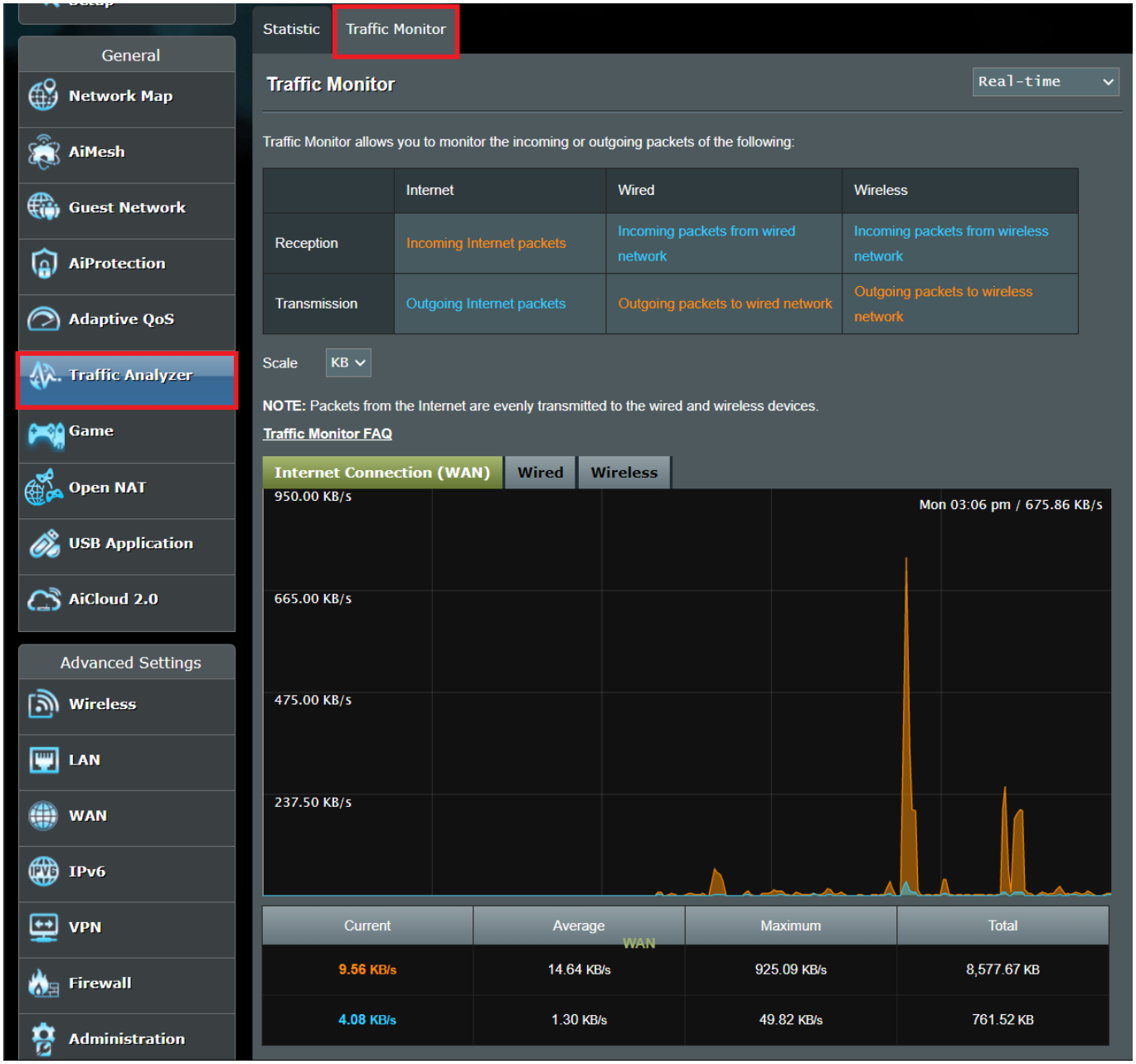

Рис. 3.4. Фільтр трафіку в складі ПЗ маршрутизатора Asus

Однак такий широкий набір функцій зазвичай доступний лише у високій цінової категорії пристроїв і часто функціонал такого вбудованого фільтра обмежується коротким набором правил за URL-адресами. Проте основними перевагами фільтрів такого класу є простота їхнього налаштування і доступність, але під час використання в межах організації необхідно застосовувати спеціалізовані рішення [17].

РОЗДІЛ 4
МЕТОД ФІЛЬТРАЦІЇ ТРАФІКУ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ МЕРЕЖІ ВІД ЗОВНІШНІХ ЗАГРОЗ

4.1. Проєктування прототипу системи фільтрації трафіку

Для проведення первинної оцінки ефективності роботи системи фільтрації трафіку було прийнято рішення створити так званий "візуальний" прототип системи, оскільки для реалізації системи, яка б перехоплювала весь трафік і передавала його на мережевий адаптер користувача, тільки пропускаючи його через фільтр, потрібне або спеціалізоване обладнання, або більш низькорівневий доступ до операційної системи. Розроблюваний прототип дасть змогу лише побачити, який трафік у принципі проходить через мережевий інтерфейс ПК, і візуально відобразити на екранній формі, який трафік був би відфільтрований на підставі заданих користувачем правил.

Прототип має реалізовувати три основні функції [18]:

1. Введення користувачем правил для фільтрації, формат яких було описано в розділі 3;
2. Читання пакетів, що проходить через мережевий інтерфейс ПК, і їх розшифровка;
3. Порівняння даних (адрес джерела і призначення) з кожного пакета з наданим користувачем списком (тобто перевірка знаходження отриманої адреси в списку правил) і відображення мітки про збіг адрес на екранній формі.

Для введення користувачем правил достатньо будь-якого джерела - текстового файлу, введення з консолі або вікно введення тексту на екранній формі, які під час запуску програми мають збережуться в її робочій пам'яті та використовуватися надалі під час відображення даних. Для цього прототипу було обрано варіант екранної форми з вікном введення тексту, реалізованих засобами бібліотеки Windows Forms мовою програмування C#.

Зчитування пакетів з мережевого інтерфейсу в стандартному призначеному для користувача застосунку можна реалізувати двома основними способами - це використання мережевих сокетів, вбудованих в API Windows, або застосування сторонньої бібліотеки роботи з трафіком, наприклад, SharpPcap, що ґрунтується на популярній програмі NPcap та її API, що надає великі можливості для отримання й аналізу мережевого трафіку. Для цього прототипу було обрано другий варіант, оскільки мережеві сокети в ОС Windows є вже доволі застарілою технологією, не вирізняються швидкодією, схильні до виникнення помилок і проблем у роботі, і незабаром їх може бути виключено з API. Бібліотека SharpPcap має у своєму складі вже велику кількість методів роботи з перехопленими мережевими пакетами, що спрощує подальшу роботу і зменшує ймовірність виникнення помилок [19].

Для визначення IP-адрес джерела і призначення, щоб потім порівнювати їх зі списком зумовлених правил, їх необхідно витягти з переданого пакета. Пакети в мережі Інтернет мають вкладену структуру, тому необхідно насамперед отримати вміст Ethernet-пакета, який є обгорткою для всіх інших даних, а потім, якщо всередині міститься IP-пакет (третій рівень за моделлю OSI), то зчитати дані заголовків і отримати адреси звідти (рис. 4.1). Якщо отриманий пакет не є IP-пакетом, то він має бути відкинутий і в аналізі участі не бере.

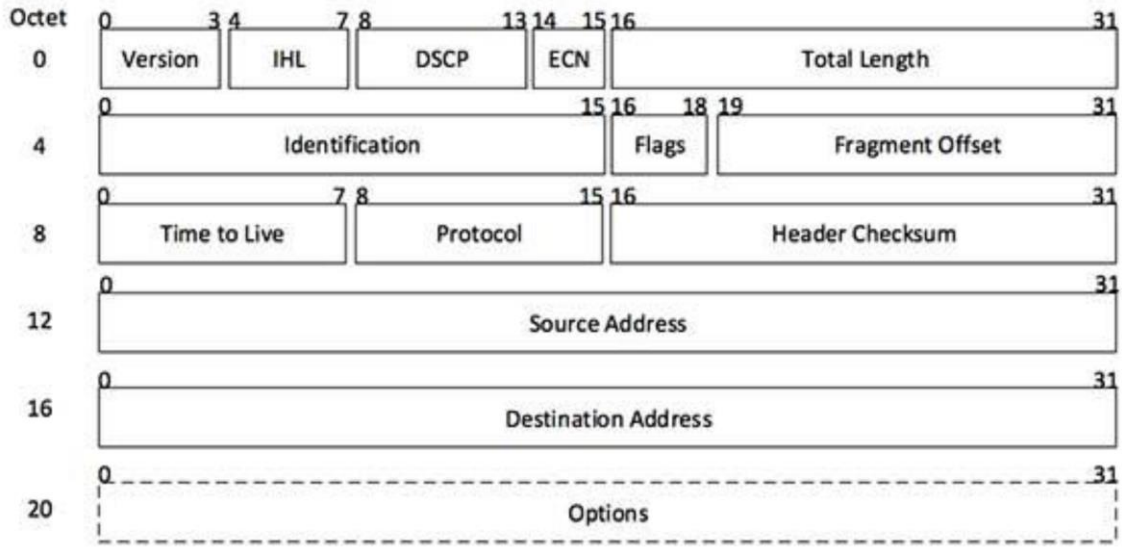

Рис. 4.1. Структура IP-пакета

4.2. Реалізація робочого прототипу

Візуальний прототип. Для реалізації спроєктованого в попередньому розділі візуального прототипу було створено проєкт Windows Forms у середовищі розроблення Microsoft Visual Studio, який складається з двох екранних форм - форми вибору пристрою для захоплення, що відкривається під час запуску застосунку, та основної форми застосунку, в якій виводиться список отриманих пакетів та вводиться список користувацьких правил. Під час запуску програми бібліотека SharpPcap отримує всі доступні мережеві інтерфейси ПК (рис. 4.2) і виводить їх у створену форму (рис. 4.3).

```
private void DeviceListForm_Load(object sender, EventArgs e)
{
    foreach (var dev :ILiveDevice in CaptureDeviceList.Instance)
    {
        var str :string = String.Format("{0} {1}", dev.Name, dev.Description);
        deviceList.Items.Add(str);
    }
}
```

Рис. 4.2. Метод отримання списку мережевих інтерфейсів ПК

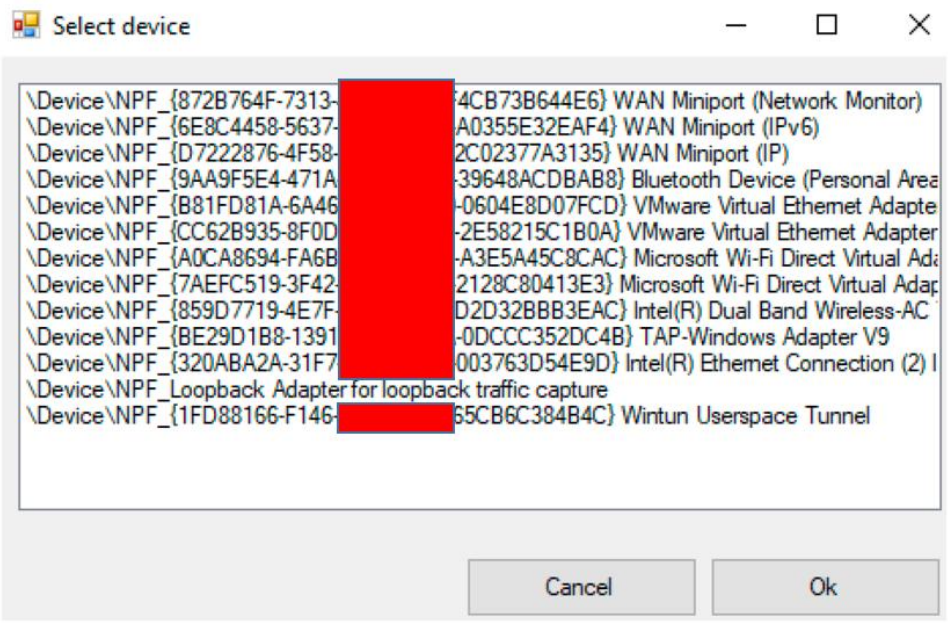

Рис. 4.3. Форма вибору мережевого інтерфейсу

Після цього було створено основну форму застосунку: на ній розміщено деревоподібний список отриманих пакетів (елемент інтерфейсу TreeView), вікно введення

правил (елемент RichTextBox) і кнопки збереження списку правил і запуску перехоплення пакетів.

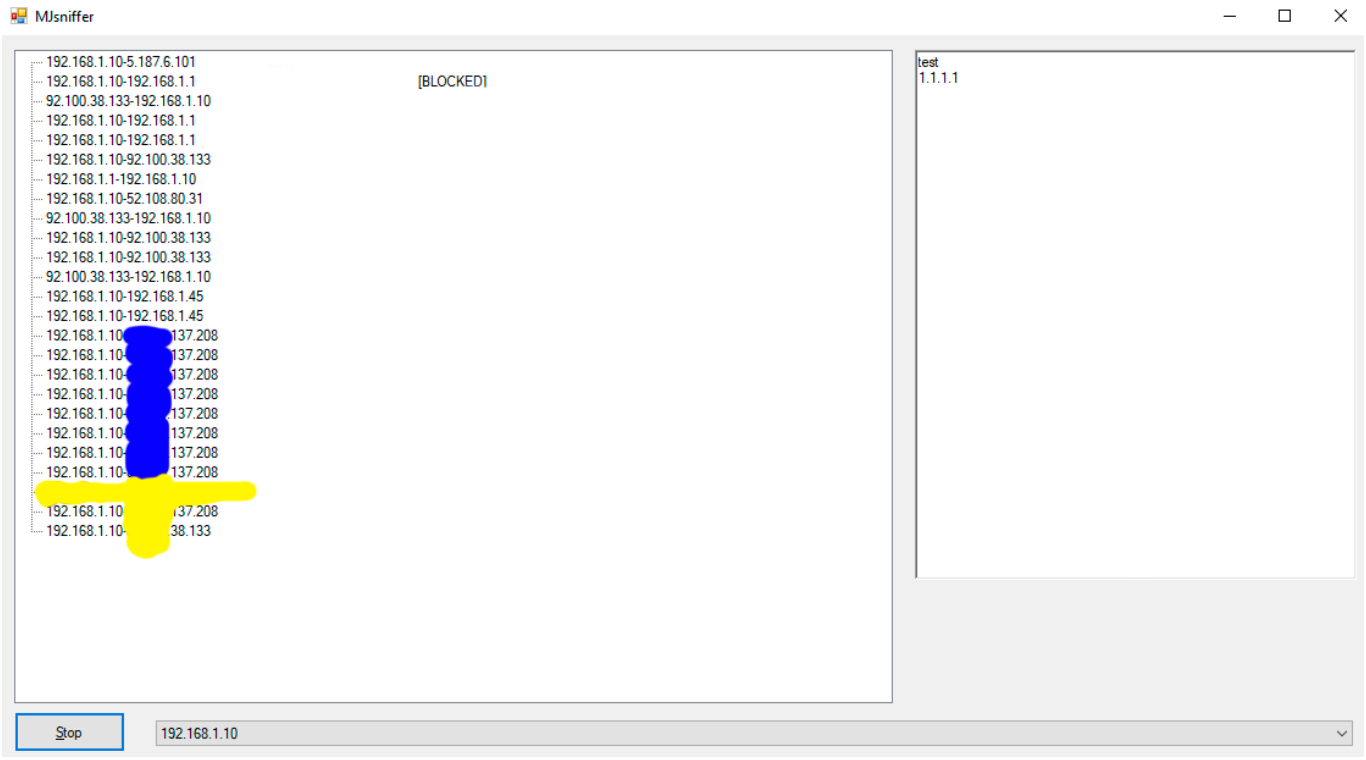

Рис. 4.4. Основна форма додатка

При отриманні нового пакета на мережевий інтерфейс викликається метод ParseData основної форми, який, використовуючи функції бібліотеки SharpPcap, на основі отриманих даних у вигляді масиву байт розбиває їх на складові. У нашому випадку, для роботи прототипу необхідний тільки заголовок IP-пакета, який витягується з даних. Після цього відбувається перевірка на збіг адреси джерела або призначення (як IP-адреси, так і доменного імені) з будь-яким значенням зі списку правил. Якщо таке знаходиться, то до тексту виведеного заголовка пакета додається мітка "[BLOCKED]", що означає, що такий трафік буде відфільтровано за правилами чорного списку. Після цього формується текст для виведення на форму і додається в загальне дерево (рис. 4.5).

```
private void ParseData(byte[] byteData, int nReceived)
{
    TreeNode rootNode = new TreeNode();
    IPHeader ipHeader = new IPHeader(byteData, nReceived);

    AddTreeNode addTreeNode = new AddTreeNode(OnAddTreeNode);
    var forbiddenText = "";
    foreach (var address in forbiddenAddresses)
    {
        if (ipHeader.SourceAddress.ToString().Contains(address) ||
            ipHeader.DestinationAddress.ToString().Contains(address) || ipHeader.SourceUrl.Contains(address) ||
            ipHeader.DestinationUrl.Contains(address))
            forbiddenText = "[BLOCKED]";
    }
    rootNode.Text = ipHeader.SourceAddress.ToString() + "~" +
        ipHeader.DestinationAddress.ToString() + "~(" + ipHeader.SourceUrl + "~-~" + ipHeader.DestinationUrl + ")" + "~" + forbiddenText;
    treeView.Invoke(addTreeNode, new object[] {rootNode});
}
```

Рис. 4.5. Метод отримання пакета і виведення його на форму

Під час проведення кожної перевірки на збіг IP-адресу з пакета та IP-адресу зі списку правил перетворюють на доменне ім'я за допомогою методу Dns.GetHostEntry(ipAddress), що входить до бібліотеки System.Net, щоб перевірити кожну комбінацію адрес (рис. 4.6). При цьому не всі IP-адреси можуть бути дозволені в домени, тому необхідно додати перевірку на існування доменного імені, і якщо його не знайдено, то виводити інформацію про те, що доменне ім'я дозволити не вдалося.

```
public string SourceUrl
{
    get
    {
        try
        {
            return Dns.GetHostEntry(SourceAddress).HostName;
        }
        catch (Exception e)
        {
            return "<unknown>";
        }
    }
}
```

Рис. 4.6. Метод перетворення IP-адреси в доменне ім'я

4.3. Оцінювання ефективності роботи першого прототипу

Для проведення тестування в програму було додано кілька тестових правил (URL-адрес), які, найімовірніше, можуть зустрітися під час роботи фільтра.

Після цього було запущено захоплення пакетів із мережевого інтерфейсу на кілька хвилин і паралельно було виконано запити до кількох веб-сайтів і відкрито кі-

лька програм, що використовують інтернет-з'єднання. Адреси джерела або призначення яких містили адреси зі списку, було додано позначку [BLOCKED], що означає, що цей трафік справді було б відфільтровано.

Виходячи з отриманих результатів, можна зробити висновки, що:

- був успішно відфільтрований трафік, спрямований безпосередньо на вузол, зазначений у списку правил, зокрема, написаний у вигляді доменного імені;
- не було відфільтровано трафік до вузлів, доменні імена яких не збігаються з реальними, незважаючи на збіг IP-адреси (віртуальні адреси або проксі-сервери, наприклад, amazonaws.com, cloudflare.net). Для усунення цього недоліку надалі можна буде спробувати під час додавання адреси перетворювати доменні адреси на IP-адресу і потім назад, щоб отримати всі віртуальні адреси, які надалі необхідно буде блокувати;
- найімовірніше, було перехоплено далеко не всі реальні пакети, спрямовані на віддалені сервери у зв'язку з тим, що ПК, на якому виконували тестування, розташовано в локальній мережі маршрутизатора за перетворенням NAT, а також більшість трафіку передають по захищеному HTTPS-з'єднанню. Для вирішення цієї проблеми в наступній версії прототипу необхідно передбачити можливість проведення тестування на ПК, під'єднаному безпосередньо до мережі Інтернет, а також застосувати інші технології перехоплення пакетів, які дають змогу зчитувати зашифроване з'єднання.

4.4. Проєктування нової версії прототипу в режимі проксі-сервера

У першій, "візуальній" версії робочого прототипу читання переданих каналом зв'язку пакетів здійснювалося безпосередньо з мережевого інтерфейсу за допомогою API бібліотеки SharpPcap (додаток NPcap). Такий підхід має значні переваги - приміг-

ром, він практично не уповільнює роботу мережі, ніяк не втручаючись у процес передавання даних, сама бібліотека надає великі можливості з читання й аналізу перехоплених пакетів, що зручно для побудови демонстраційного застосунку. Однак у реальному застосуванні такий підхід має кілька недоліків: по-перше, пакети з мережевого інтерфейсу за допомогою цієї бібліотеки можна тільки зчитувати, але не можна якимось чином вплинути на їхній вміст або напрямок. По-друге, зважаючи на устрій IPv4-мереж (локальні мережі часто розміщені за маршрутизатором, що виконує трансляцію мережевих адрес - NAT), цей спосіб не завжди коректно визначає адреси джерела і призначення пакетів, і не може визначити деякі метадані зашифрованих пакетів, хоча вони і передаються у відкритому вигляді.

Тому було прийнято рішення змінити підхід і реалізувати так званий проксі-сервер. Проксі-сервер - це програма, що виконує роль посередника між клієнтом і цільовим сервером, тобто розташовується в проміжку між комп'ютером і зовнішньою мережею (рис. 4.7). Такий сервер, по суті, перехоплює весь трафік, що передається комп'ютером у зовнішню мережу і навпаки, і надалі може його або передати як є, або якимось чином змінити, або повністю відхилити запит [19-21].

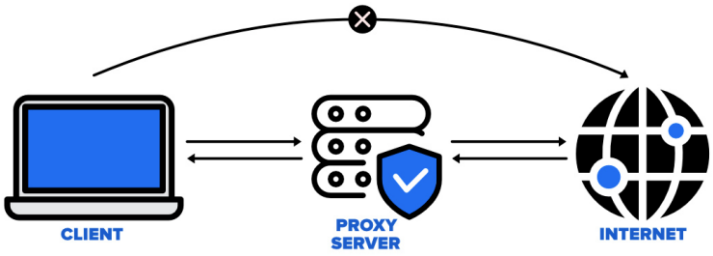

Рис. 4.7. Розташування проксі-сервера в схемі обміну даними

До недоліків використання проксі-сервера можна зарахувати його більш обмежену сферу впливу: найчастіше проксі-сервер працює тільки з HTTP-трафіком, тобто із запитами на Інтернет-сайти з веб-браузерів, а також із додатковими маршрутами передання даних між призначеними для користувача додатками. Такий сервер не здатний обробляти і фільтрувати трафік інших застосунків без внесення модифікацій вручну, але в більшості випадків цей недолік можна вважати незначним, оскільки для

блокування застосунків зазвичай використовується міжмережевий екран (брандмауер) або стандартні засоби захисту ОС, а фільтр мережевого трафіку частіше корисний саме під час роботи на Інтернет-сайтах.

Реалізувати прототип проксі-сервера можна також мовою програмування C#, для цього можна використовувати "прослуховувач" HttpListener (застарілий підхід, що спричинятиме проблеми під час роботи із захищеними з'єднаннями) або готові сторонні бібліотеки, наприклад, Titanium Web Proxy. Ця бібліотека дає змогу в кілька рядків коду під'єднати проксі-сервер до потрібного порту, налаштувати його як глобальний для всієї системи або ж тільки на конкретний застосунок. Після призначення потрібних обробників подій доступна робота з усіма стандартними і розширеними властивостями і методами класу HttpRequest мови C# в асинхронному режимі, є підтримка сертифікатів SSL і TLS, робота в "прозорому" режимі та багатьох інших можливостей.

4.5. Реалізація нової версії прототипу

Для створення поліпшеної версії прототипу було створено консольний застосунок у середовищі розроблення Microsoft Visual Studio, до якого було додано NuGet-пакет Titanium.Web.Proxy (рис. 4.8). Консольний застосунок було використано замість графічного для значного прискорення роботи сервера з огляду на зниження витрат ресурсів на відмальовування екранних форм, а оскільки нова версія фільтра трафіку працює повноцінно в операційній системі, то немає необхідності наочно відстежувати поведінку застосунку застосунку.

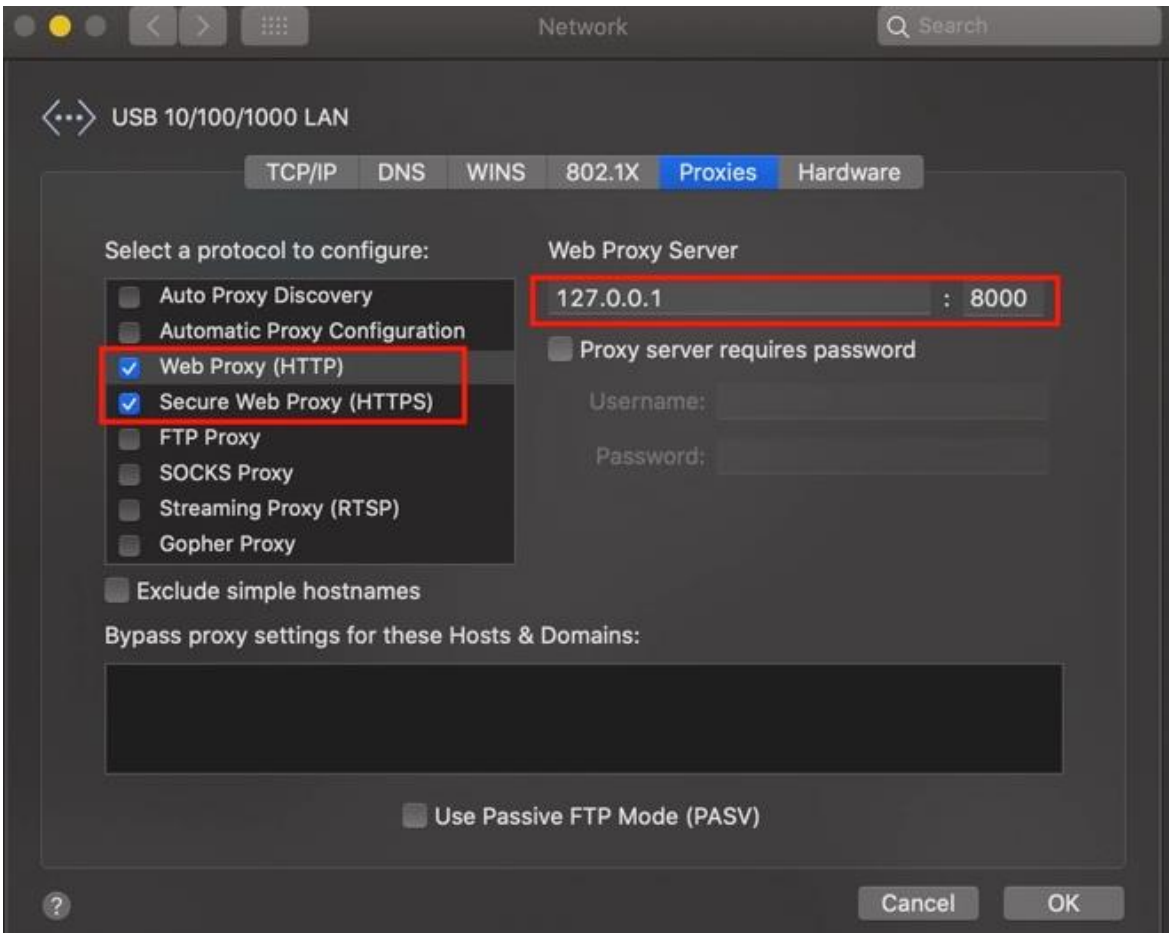

Рис. 4.8. Встановлення пакета Titanium.Web.Proxy в рішення

Алгоритм роботи програми залишається тим самим: на початку роботи користувач наповнює список правил, після чого запускається безпосередньо фільтр трафіку. При цьому під час введення кожного правила автоматично додаються до списку IP-адреси та доменні імена, які можуть бути знайдені від введеного (рис. 4.9). Наприклад, якщо користувач вводить домен сайту google.com, то до чорного списку, крім цього домену, додаються всі IP-адреси, що визначаються за цим доменом, а також домени, що визначаються за отриманими IP-адресами, наприклад, 1e100.net (рис. 4.10). У разі, якщо за ланцюжком доменів або адрес не знайдено, до чорного списку додається тільки введене значення.

```
if (!blockedUrls.Contains(enteredValue))
    blockedUrls.Add(enteredValue);
try
{
    var ips :IPAddress[] = Dns.GetHostAddresses(enteredValue);
    foreach (var ipAddress in ips)
    {
        if (!blockedIps.Contains(ipAddress.ToString()))
            blockedIps.Add(ipAddress.ToString());
        try
        {
            var host :string = Dns.GetHostEntry(ipAddress).HostName;
            if (!blockedUrls.Contains(host))
                blockedUrls.Add(host);
        }
        catch (Exception e)
        {
        }
    }
}
catch (Exception e)
{
}
```

Рис. 4.9. Метод додавання до чорного списку введеної користувачем URL-адреси

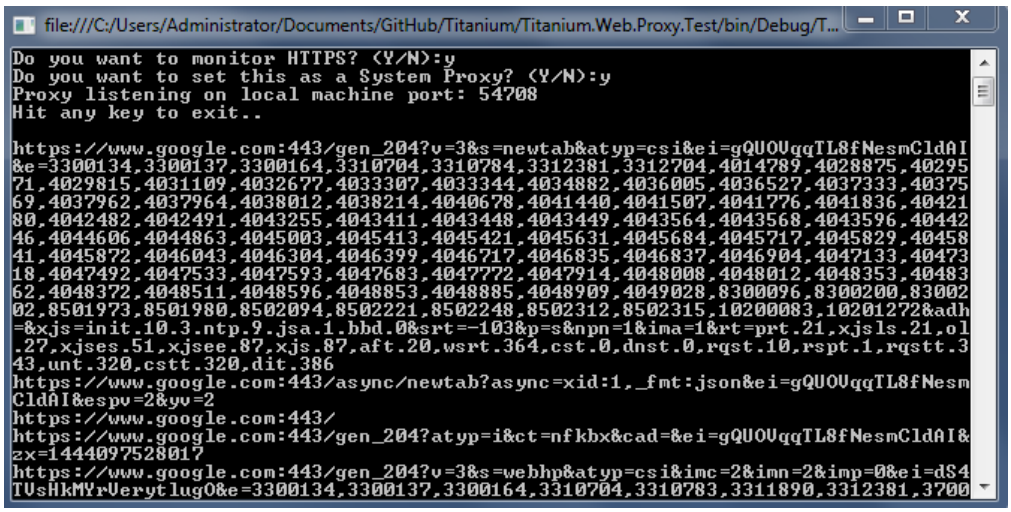

Рис. 4.10. Приклад введення правила та отриманого в результаті списку

Після цього запускається безпосередньо проксі-сервер із потрібними параметрами (наприклад, глобально на всю операційну систему або для конкретних застосунків) і налаштовуються обробники подій отримання HTTP-запитів і відповідей.

Для реалізації фільтрації трафіку в обробнику події OnRequest (під час отримання HTTP-запиту від клієнта) проводиться читання URL запиту, доменного імені та пошук пов'язаних із ним IP-адрес. Потім за стандартним алгоритмом мережевого фільтра перевіряється наявність отриманих даних у списках блокованих доменів або IP-адрес (рис. 4.11). Якщо результат негативний, то проксі-сервер має передати запит без змін. У разі отримання позитивного результату можна або просто вивести інформацію про це на консоль, або перенаправити запит, наприклад, на сторінку з інформацією про блокування.

```
var requestUrl :string = e.HttpClient.Request.RequestUri.AbsoluteUri;
var requestIps = new IPAddress[0];
try
{
    requestIps = await Dns.GetHostAddressesAsync(e.HttpClient.Request.Host);
}
catch (Exception ex)
{
}

var isResourceBlocked = blockedUrls.Contains(requestUrl) ||
                        blockedUrls.Contains(e.HttpClient.Request.Host) ||
                        requestIps.Any(ip => blockedIps.Contains(ip.ToString()));
```

Рис. 4.11. Метод пошуку адрес у списку заборонених

4.6. Тестування роботи прототипу

Для тестування фільтра інтернет-трафіку доцільно застосувати два види тестування - модульне та системне. Модульне тестування (так звані unit-тести) дає змогу перевірити мінімальні функції програми окремо, які можна ізолювати одна від одної, не виконуючи повний цикл робіт програми. Функціональне тестування, зі свого боку, дає змогу перевірити роботу прототипу загалом, використовуючи реальні приклади роботи та інструменти, але виключаючи взаємодію з користувачем. Такий вид тестування дає змогу покрити набагато більше функцій програми - наприклад, формат виведення, швидкість реальної роботи тощо, ніж модульні тести.

Модульне тестування виконується шляхом написання тестових сценаріїв тією самою мовою програмування, що й сам застосунок (тобто, по суті, застосунок запускає сам себе і тестує свої методи). Базова функціональність тестування підтримується в середовищі розроблення Microsoft Visual Studio, але для створення складніших сценаріїв і спрощення їхнього налагодження часто використовуються тестові адаптери. В даному випадку в рішення було додано адаптер NUnit - популярний фреймворк для модульного тестування коду мовою C#.

Модульні тести найчастіше створюють в окремому проєкті, але допускається їхній опис і в окремому файлі поточного проєкту, що й було зроблено в цій роботі для підвищення читабельності та скорочення розміру отриманого застосунку. У проєкт було додано новий файл FilterTests, до якого було під'єднано бібліотеку NUnit.Framework, після чого файл було наповнено тестами. Сам процес опису модульних тестів складається з чотирьох основних етапів:

- опис глобальних змінних - сутностей, які зберігатимуться протягом усіх запусків тестів. У цьому випадку це набір правил фільтрації, екземпляр прототипу мережевого фільтра, шлях до каталогу для збереження результатів і код, що повертається фільтром;
- дії до запуску всіх тестів - виконуються одноразово, в даному випадку, генерується випадковий код, з яким надалі порівнюється текст, що повертається фільтром;
- модульні тести - набір методів і/або тестових сценаріїв, однозначно іменованих відповідно до описуваних ними сценаріїв, які безпосередньо виконують тестування конкретних функцій;
- дія після завершення всіх тестів - виконується одноразово, в даному випадку, зупиняються всі створені в рамках модульних тестів екземпляри фільтрів трафіку.

У рамках тестування цього прототипу було розроблено і виконано 9 сценаріїв:

- фільтрація трафіку за списком правил, заданих у тексті програми, в режимі "чорний список", з проходом за базовим списком правил і за робочим списком;

- фільтрація трафіку за списком правил, заданих у тексті програми, в режимі "білий список", з проходом базовим списком правил і робочим списком - у цьому разі жоден запит не має бути заблоковано;
- фільтрація трафіку за списком правил, заданих у конфігураційному файлі filter.config з урахуванням зазначеного у файлі режиму роботи фільтра, з проходом за базовим списком правил і за робочим списком;
- фільтрація трафіку за списками правил, заданих у тексті програми (в обох режимах - "чорний список" і "білий список") або в конфігураційному файлі, з проходом за списком випадкових адрес. Список випадкових адрес для цього тесту отримується зчитуванням журналів роботи фільтра трафіку на попередньому звичайному запуску, під час якого було виконано відвідування безлічі різних веб-сайтів.

Кожен модульний тест має схожу структуру (приклад наведено на рис. 4.12) - перед початком виконання виконується зчитування списку правил (на прикладі - задано явно в тексті тесту), потім створюється новий екземпляр мережевого фільтра, водночас, якщо попередній уже існував, то він зупиняється. Після цього виконується прохід за потрібним списком адрес для перевірки, виконується HTTP-запит на кожну адресу і перевіряється, чи містить відповідь випадковий код, згенерований перед запуском усіх тестів. Залежно від режиму роботи і входження адреси в список правил визначається, чи має бути заблокована адреса чи ні, і в разі розбіжності тест вважається непройденим.

```
public static void TestBaseAllowConfig()
{
    baseConfig = new FilterConfig(FilterMode.AllowList)
    {
        Urls = new List<string> { "stackoverflow.com", "microsoft.com", "github.com", "stackexchange.net", "linustechtips.com" },
        IpAddresses = new List<string> { "1.1.1.1", "8.8.8.8" }
    };
    filter?.Stop();
    filter = new NetworkFilter(new ExplicitProxyEndPoint(IPAddress.Any, 80, true),
        ConfigBuilder.FromConfig(baseConfig), returnCode);
    filter.Start();
    foreach (var url :string in baseConfig.Urls.Where(u :string => !u.Contains("*")))
    {
        TestSingleAddress(AddressType.Url, url.StartsWith("http://") ? url : "http://" + url);
    }
    foreach (var ip :string in baseConfig.IpAddresses.Where(i :string => !i.Contains("*")))
    {
        TestSingleAddress(AddressType.IP, "http://" + ip);
    }
}
```

Рис. 4.12. Приклад модульного тесту

Для перегляду результатів модульного тестування існує безліч варіантів як схожих адаптерів, так і цілих інструментаріїв для експорту та візуалізації результатів. Найчастіше це може бути застосовано для великих програмних продуктів і розглядається можливість застосування таких інструментів у майбутньому, але для таких невеликих модульних тестів цілком достатньо вбудованого в MS Visual Studio оглядача тестів, який дозволяє розробнику переглядати результати тестування (рис. 4.13).

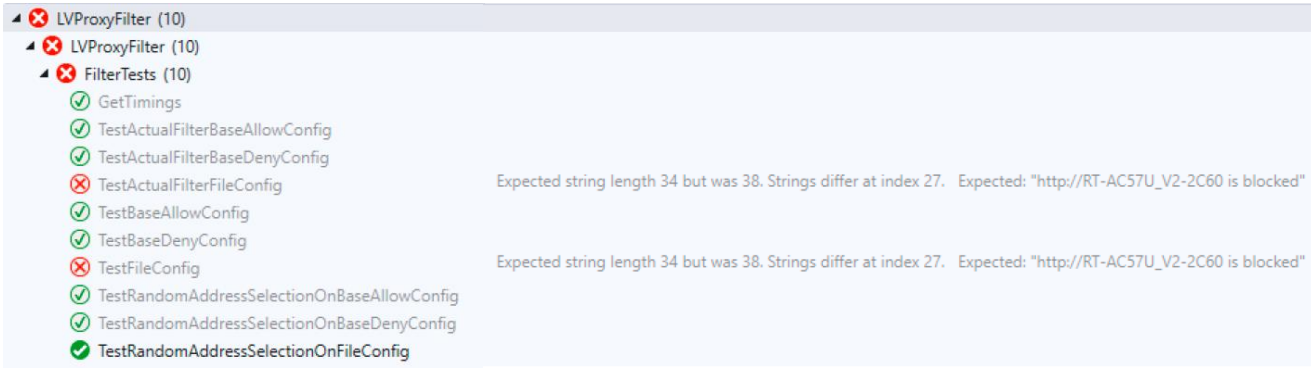

Рис. 4.13. Результати виконання модульних тестів

Як видно з наведеного вище списку результатів, майже всі створені тести були виконані без помилок. Виникли помилки на локальних адресах, які, найімовірніше, в принципі не є робочими, тому надалі достатньо виключити ці адреси з робочого набору правил, які включаються до нього. Однак модульне тестування не завжди однозначно визначає якість роботи продукту, оскільки виконується на досить вузьких вибірках даних, а також не дає змоги перевірити роботу системи загалом. Найкращим способом вважається системне тестування, що виконується із залученням кінцевих користувачів або тестувальників, але такий спосіб є доволі трудомістким, і в межах цієї роботи його переваги, найімовірніше, мінімальні. Тому було прийнято рішення як другий вид тестування виконати функціональне, поєднане з тестуванням продуктивності.

Для виконання функціонального тестування додатків, пов'язаних із роботою в браузері, часто використовується популярний інструмент автоматизації дій веб-браузера - Selenium. До його переваг належать наявність адаптерів і фреймворків для роботи на мові C#, підтримка новітніх версій браузера і велика гнучкість налаштування.

Як приклад такого виду тестування були проведені заміри часу завантаження веб-сторінок за вимкненого і ввімкненого фільтра трафіку. Як вибірку URL-адрес для перевірки було використано ті самі випадкові адреси, зібрані з журналу роботи фільтра за деякий період. Оскільки драйвер завжди очікує завантаження сторінки до кінця, то досить увімкнути секундомір перед переходом на сторінку та зупинити його після переходу, у результаті чого буде отримано час завантаження сторінки в мілісекундах (рис. 4.14).

```
public static void GetRandomAddressSelectionTimingsOnFileConfig()
{
    var fileConfig = ConfigBuilder.FromFile(baseFolder + "filter.config");
    var allowedUrls = File.ReadAllText(resultFolder + "allowedurls.txt").Split("\n");
    filter?.Stop();
    filter = new NetworkFilter(new ExplicitProxyEndPoint(IPAddress.Any, 80, true),
        fileConfig, returnCode);
    filter.Start();

    var driver = new ChromeDriver();
    foreach (var url :string in allowedUrls)
    {
        var sw = new Stopwatch();
        sw.Start();
        try
        {
            driver.Navigate().GoToUrl(url);
        }
        catch
        {
            sw.Stop();
            sw.Reset();
        }
        if (sw.IsRunning)
            sw.Stop();
        Logger.UnfilteredTimings.Add(sw.ElapsedMilliseconds.ToString());
    }

    driver.Close();
}
```

Рис. 4.13. Реалізація замірів часу завантаження сторінок

4.7. Результати тестування роботи системи фільтрації трафіку

Модульне тестування. Як було описано в попередньому підрозділі, на заданому наборі правил було успішно виконано 7 із 9 тестів, тобто, ефективність (вірніше, якість роботи) фільтра склала 77%. Тому в алгоритм роботи прототипу фільтра було

внесено зміни відповідно до виявлених недоліків - зокрема, було враховано ігнорування некоректних URL-адрес під час виконання перевірки на коректність виконання блокування. Після внесення змін вдалося домогтися 100%-го проходження всіх модульних тестів (рис. 4.14).

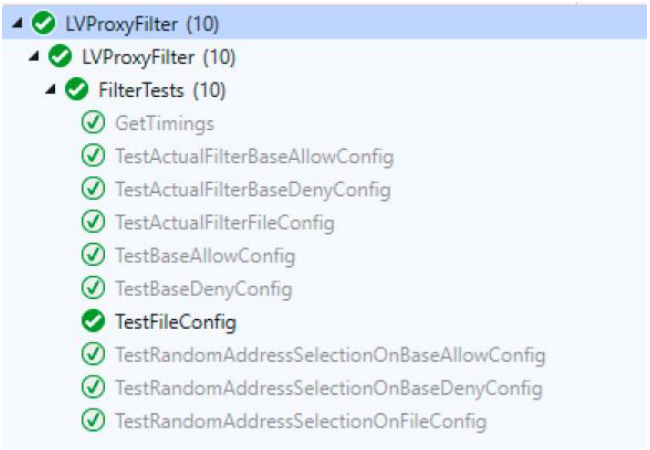

Рис. 4.14. Результати повторного модульного тестування

За результатами цього тестування можна зробити висновок, що кожна окрема функція алгоритму роботи мережевого фільтра на даний момент відпрацьовує коректно. Однак надалі при зміні або розширенні функціональності програми необхідно підтримувати її покриття модульними тестами і збільшувати вибірку тестових даних.

4.8. Функціональне тестування

Під час виконання функціонального тестування було виконано завантаження 345 веб-сторінок у стандартному браузері та оцінювання швидкості їхнього завантаження без під'єднання фільтра трафіку і з його використанням. Насамперед було перевірено, що відповідь від розробленого прототипу збігається та містить як явну інформацію про блокування, так і заданий псевдовипадковий код, що повертається.

Результати замірів часу були зведені в таблицю Excel, за допомогою якої було розраховано необхідні значення і побудовано стовпчасту діаграму, на якій можна наочно побачити різницю у швидкості завантаження сторінок (рис. 4.15).

Рис. 4.15. Діаграма зміни часу завантаження сторінки після ввімкнення мережевого фільтра

Мінімальна затримка завантаження веб-сторінки, пов'язана з роботою прототипу мережевого фільтра, становила 0 мс, максимальна - 99 мс, і в середньому затримка становила близько 20 мс. Отримана різниця в часі зумовлена тим, що під час надходження запиту на вхід фільтра трафіку відбувається пошук пов'язаних із запитуваною URL-адресою IP-адрес для того, щоб забезпечити блокування за будь-якою з пов'язаних IP-адрес. При цьому частина таких зв'язків уже були закешовані локально, оскільки виконувалися не вперше, а частина - виконувалися вперше з початку сесії й отримували безліч адрес.

Проте навіть 20 мілісекунд - результат не найкращий для фільтра трафіку, оскільки зі збільшенням розмірів бази правил фільтрації та збільшенням кількості запитів така затримка буде дедалі помітнішою. Одним із варіантів зменшення такої затримки може бути використання динамічних списків правил, коли перевірка за пов'язаними IP-адресами виконуватиметься тільки в разі, якщо запит на поточну адресу виконується вперше, а після цього - зберігатиметься у списку правил як дозволений або як заборонений. Ця функціональність не входить у рамки реалізації простого прототипу, але має бути обов'язково застосована до уваги під час розроблення промислової версії програми.

Як наочний приклад ефективності роботи системи фільтрації трафіку можна навести її використання для блокування небажаного вмісту веб-сторінок, наприклад, реклами.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

Незалежно від виду професійної діяльності питання охорони праці людини повинні вирішуватися на всіх стадіях трудового процесу.

Оцінка небезпечних і шкідливих виробничих факторів в значній мірі залежить від забезпечення безпечних і здорових умов праці. Зміни, які відбуваються в організмі людини, можуть бути викликані різними джерелами. Це може бути результатом робочого середовища, надмірного фізичного та розумового навантаження, нервово-емоційного стресу або кількох цих факторів разом.

Відповідно, інженер відділу моніторингу стану транспортної IP-мережі є суб'єктом охорони праці. Він відповідає за розробку програмного комплексу, призначеного для контролю мережевого ПЗ на наявність дефектів і збоїв, діагностики та ідентифікації дефектів мережевого устаткування за допомогою дослідження спектральних характеристик сигналу.

Інженер працює в відділі моніторингу транспортних IP-мереж у центральному корпусі підприємства.

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера відділу моніторингу транспортних мереж

Оформлення робочого місця програміста. Приміщення програміста завдовжки 8 метрів, завширшки 5 метрів, має загальну площу 40 метрів квадратних і висоту стелі 3,5 метрів. У приміщенні є шість робочих місць з комп'ютерами. Кожне робоче місце має робочий стол площею 1.44 м2, стілець і персональний комп'ютер із монітором, системним блоком, клавіатурою та мишею. Згідно з [36], одне робоче місце має мати площу не менше 6,0 кв. м і об'єм не менше 20,0 куб. м. Отже, цього приміщення достатньо для розміщення шести робочих місць операторів ПК.

Термін «небезпечний» використовується для опису факторів, які негайно погіршують здоров'я працівника. Чинники, які безпосередньо або побічно призводять до порушення працездатності або здоров'я працівників, називають шкідливими факторами виробничого середовища.

На програміста впливають наступні небезпечні та шкідливі фактори [37]: мікроклімат, недостатнє освітлення та статична електрика.

Мікроклімат місця роботи програміста Роботи програмістів належать до категорії ІА або ІА, тому вони повинні відповідати наступним вимогам [38]:

Таблиця 5.1

Оптимальні величини температури, відносної вологості та швидкості руху повітря в робочій зоні виробничих приміщень

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 ІТ-відділі температура та вологість, виміряні приладом, відомим як психрометр Августа, відповідають показникам теплого періоду року. Розташовані в приміщенні 6 ПК є джерелами тепловиділення, а нагріті поверхні опалювальної системи використовуються для створення ідеального мікроклімату в приміщенні в холодний період року. Гранично допустима густина потоку енергії є нормованим показником ІЧВ $I_{г.д}$, Вт/м^2, яка встановлюється в залежності від площі опромінюваної поверхні тіла людини ($S_{опр}$). Нормовані рівні складають: $I_{г.д}$ =35 Вт/м^2 при $S_{опр}$ > 50%; $I_{г.д}$=70 Вт/м^2 при $S_{опр}$ ~ 25-50%; $I_{г.д}$=100 Вт/м^2 при $S_{опр}$ < 25%

Штучне та природне освітлення. Коефіцієнт природного освітлення (КПО) є стандартним параметром природного освітлення, згідно з [39]. КПО визначаються за типом зорових робіт, які виконуються. Роботи програміста відносяться до середньої точності (IV розряд зорових робіт із мінімальним розміром об'єкта розрізнення 0,5–1,0 мм) з КПО=1,5% при використанні бокового освітлення. Для штучного освітлення стандартними параметрами є Емін, мінімальний рівень освітленості, і КП, коефіцієнт пульсації світлового потоку, який не повинен перевищувати 20%. Розділ зорових робіт визначає мінімальну освітленість. Відповідно до IV розряду зорових робіт вона становить 300-500 лк.

Генератори випромінювання Таблиця 4.2 показує допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітора комп'ютера. Потужність експозиційної дози є нормованим параметром невикористаного рентгенівського випромінювання. Рівень чутливості монітора не повинен перевищувати 100 мкР/год на відстані 5 см від його поверхні. Зазвичай на робочому місці програміста рівень рентгенівського випромінювання не перевищує 20 мкР/год.

Таблиця 5.2

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні монітора ПК	10 Вт/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні монітора ПК	0.3 А/м
Напруженість для операторів ПК не повинна перевищувати	20 кВ/м

Напруженість електричної складової може досягати 6 В/м на відстані 5-10 см від екрана та корпуса монітора, що не перевищує допустимі значення.

Безпека електроенергії. Електрична індукція Приміщення IT-відділу відноситься до 1 класу небезпеки ураження електричним струмом, якщо воно не є підвищеною небезпекою (сухе, без пилу, нормальна температура повітря, ізольовані підлоги та мало заземлених приладів).

На робочому місці програміста є лише стандартний корпус системного блоку комп'ютера IBM. Для знешкодження статичної електрики на системному блоці повинно бути встановлене заземлення відповідно до [40]: пункт 5 «Заходи по захисту від статичної електрики». Системний блок не відповідає вищевказаним нормам, оскільки на ньому відсутнє заземлення.

Основні фактори, які можуть призвести до ураження людини електричним струмом на робочому місці, включають: дотик до металевих неструмоведучих частин, таких як корпус комп'ютера, які можуть бути під напругою через ушкодження ізоляції; нерегламентоване використання електричних приладів; і відсутність навчання співробітників правилам електробезпеки.

5.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів на інженера відділу моніторингу транспортних мереж

Нормалізація повітря на робочому місці. Для створення та автоматичної підтримки в IT-відділі необхідно дотримуватися ідеальних температур, вологості, чистоти та швидкості руху повітря незалежно від зовнішніх умов. У холодні роки використовується водяне опалення, а в теплі роки використовується кондиціонування повітря [41].

Технічне освітлення. Під час аналізу освітлення робочого міста програміста було виявлено, що воно не відповідає встановленим нормам. Тому, щоб покращити умови праці, ми рекомендуємо встановити п'ять додаткових світильників і збільшити загальну кількість лам до 36 світлодіодних ламп. Крім того, необхідно планувати очищення віконних блоків і світильників щорічно не менше двох разів [39].

Безпека електроенергії. Пропоную наступні технічні заходи та засоби захисту для забезпечення електробезпеки в ІТ-відділі: зволожувачі та нейтралізатори, антистатичне покриття підлоги; зменшення накопичення статичної електрики; забезпечити приєднання металевих корпусів устаткування до жили, що заземлюється. Заземлення корпусу комп'ютера дозволяє підвести жилу, що заземлює, до розеток. Для електроустановок з напругою до 1000 В стандартний опір заземлення становить 4 Ом. Крім того, необхідно дотримуватися організаційних процедур, таких як своєчасне проведення інструктажів з техніки безпеки [42].

Ергономіка та управління робочим місцем. Після оцінки робочого місця програміста в ІТ-відділі було встановлено, що воно відповідає вимогам.

Виходячи з результатів аналізу важкості та напруженості праці, пропоную скоротити час роботи за комп'ютером до п'ятдесяти хвилин протягом восьми годин робочого дня [43].

5.2.1. Розрахунок освітленості робочого місця інженера на відповідність розряду зорової роботи

За даними вимірювань (люксметр Ю-116), рівень природної освітленості поверхні, де розташований комп'ютер програміста, складає 200 лк у порівнянні з освітленістю відкритого небосхилу 20000 лк. Отже, КПО = 1%, що не відповідає нормативному КПО.

Світлодіодні лампи T8 G13 використовуються для штучного освітлення у приміщенні. Вони мають багато переваг порівняно з люмінесцентними та лампами розжарювання, включаючи більшу світлову віддачу (у 2-5 разів більшу, ніж у ламп розжарювання) і триваліший термін служби (до 10 000 годин) [24].

Проведемо розрахунок штучного освітлення для кімнати площею 40 квадратних метрів, яка має ширину 5 метрів, довжину 8 метрів і висоту 3,5 метрів, використовуючи метод коефіцієнта використання світлового потоку.

Для визначення кількості світильників, які повинні забезпечити нормований рівень освітленості, використовуємо формулу:

$$F=E*S*K*Z/n \quad (5.1)$$

(де **F** – світловий потік, що розраховується, Лм; **E** – нормована мінімальна освітленість, Лк; E = 300 Лк; **S** – площа освітлюваного приміщення (у нашому випадку S=40 м^2); **Z** – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1...1,2, в нашому випадку Z=1,1); **K** – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку К=1,5); **n** – коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, і обчислюється в долях одиниці;) залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{ст.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{ст}$ = 40% і $\rho_{стелі}$=60%.

Обчислимо індекс приміщення за формулою:

$$i=S/h(A+B) \qquad (5.2)$$

(де **S** – площа приміщення, S=40 м^2; **h** – розрахункова висота підвісу, h = 3.3 м; **A** – ширина приміщення, A = 5 м; **B** – довжина приміщення, B = 8 м.)

Підставивши значення отримаємо: **i=40/3.3(5+8)=0.93**. Знаючи індекс приміщення, знаходимо **n=0.22**. Підставимо всі значення у формулу для визначення світлового потоку **F**:

F=(300*1.5*40*1.1)/0.22=90000 Лм.

Для освітлення використані світлодіодні лампи з матовим покриттям типу LRC-T8-S1500G13-220-22,0W, світловий потік яких $\mathbf{F_л = 2500}$ Лм.

$$N=F/F_л \quad (4.3)$$

(де **N** – визначуване число ламп; **F** – світловий потік, **F=90000 Лм**; **Fл** – світловий потік однієї лампи, $\mathbf{F_л = 2500}$ **Лм**.)

N=90000/2500=36

Світильники ЛПО використовуються в приміщенні. Кожен світильник складається з чотирьох ламп. Таким чином, необхідно використовувати дев'ять світильників із 36 лампами, які працюють.

У ІТ-відділі авіапідприємства, де проводився аналіз робочого місця програміста, є п’ять світильників із двадцять лампами, тому рівень штучного освітлення не відповідає санітарним нормам.

5.3. Пожежна безпека на підприємстві

Згідно з [44], приміщення ІТ-відділу центрального офісу авіапідприємства відноситься до категорії Д «Негорючі речовини та матеріали в холодному стані». місця, де знаходяться ГР систем машин, охолодження та гідроприводу, устаткування з масою не більше 60 кг при тиску не більше 0,2 мПа, кабелі електропроводки до устаткування, окремі меблі на місцях

Центральний офіс ІТ-відділу по пожежній небезпеці будівельних конструкцій відноситься до категорії К1 (малопожежонебезпечні), оскільки тут знаходяться займисті речовини (книги, документи, меблі, оргтехніка тощо) і важкогорючі речовини (сейфи, різне устаткування тощо), які можуть горіти без вибуху, якщо вони стикаються з вогнем.

Будинки можна класифікувати за конструктивними характеристиками як будинки з несучими та огороджуючими конструкціями, виготовленими з природних або штучних каменів, бетону або залізобетону; для перекриттів допускається використання дерев’яних конструкцій, захищених штукатуркою або важкогорючими листовими, а також плитних матеріалів.

Таким чином, будинок Центрального офісу має третю ступінь вогнестійкості (III).

Приміщення ІТ-відділу авіапідприємства має клас пожежної небезпеки Ф 4.2.

Причини пожежі. Пожежа в ІТ-відділі може спричинити жахливі наслідки, такі як смерть людей, втрата цінної інформації та шкода майну, тому необхідно: виявити та усунути всі фактори, які можуть спричинити пожежу; розробити план ліквідації пожежі; і розробити план евакуації людей.

На пожежі можуть впливати такі фактори, як блискавка в будинку або зовнішні джерела тепла; несправності електропроводки, розеток і вимикачів, які можуть призвести до короткого замикання або пробою ізоляції; використання ушкоджених або несправних електроприладів; або необережне поводження з вогнем і недотримання правил безпеки.

Засоби для гасіння пожеж і пожежно-охоронної сигналізації.

Як сказано в [44]: «3.3. На кожному підприємстві повинен бути встановлений відповідний протипожежний режим з урахуванням його пожежної небезпеки. Цей режим повинен включати: порядок експлуатації та обслуговування наявних технічних засобів протипожежного захисту (протипожежного водопроводу, насосних станцій, установок пожежної сигналізації, автоматичного пожежогасіння, димовидалення, вогнегасників тощо). В приміщенні встановлено один переносний вуглекислотний вогнегасник ВВК-5, якого достатньо для цього типу приміщення та площі. Крім того, на стелі встановлено два бездротові ІЧ-датчики диму Страж М-501, розраховані на площу 40 квадратних метрів.

Якщо виникне пожежа, спрацює протипожежна сигналізація, необхідно відключити електроживлення, викликати пожежну команду за номером 101, вивести людей із приміщення відповідно до плану евакуації, представленого на рисунку 4.1, і використовувати вогнегасники для ліквідації пожежі. Коли горить невеликий вогонь, можна скористатися підручними засобами, щоб перешкодити доступу повітря до вогнища.

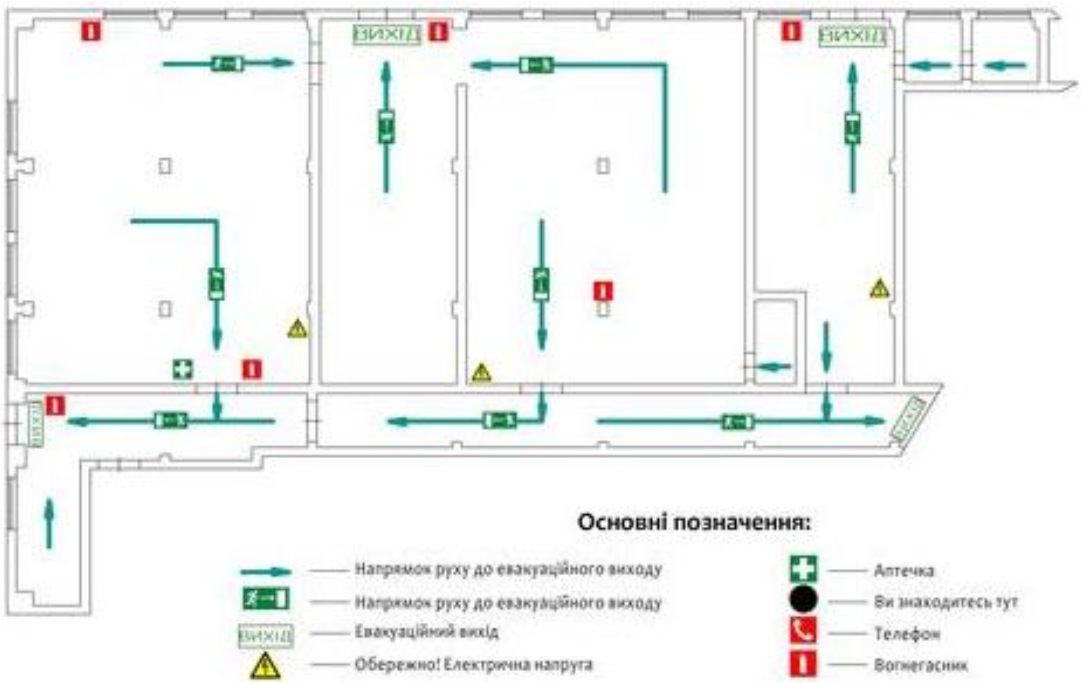

Рис. 5.1. План евакуації з приміщення відділу моніторингу транспортних мереж

5.4. Інструкція з охорони праці при роботі на персональних робочих станціях

Попередні заходи безпеки перед початком роботи:

- Перед початком роботи працівник повинен перевірити цілісність корпусу системного блоку, принтера, клавіатури та відео монітора.
- Перевірте цілісність кабелів живлення та місць їх підключення, включаючи розетки, продовжувачі, розгалужувачі та штепсельні вилки.
- Підготувати робоче місце, прибравши все, що заважає вам виконувати завдання.
- Включити живлення ПК.
- Працівник повинен повідомити керівника або спеціаліста відділу інформаційних технологій, якщо комп'ютер не завантажується або не виходить на робочий режим після ввімкнення.
- Повідомте безпосереднього керівника про будь-які проблеми. Зверніться до нього, перш ніж розпочати роботу.

Правила безпеки на робочому місці:

- Всі компоненти столу, включаючи клавіатуру, повинні бути стійко розташовані. Крім того, необхідно передбачити можливість переміщення клавіатури. Її розміщення та кут нахилу повинні відповідати потребам користувача ПК. Якщо в конструкції клавіатури немає місця для опору долонь, клавіатура повинна бути розташована на відстані не менше 100 мм від краю столу, щоб забезпечити оптимальну відстань для моніторного поля. Коли ви працюєте на клавіатурі, вам слід сидіти прямо, не напружуючись.
- Для зменшення несприятливого впливу на користувача пристроїв типу «миша» (вимушена поза, постійний контроль за якістю дій) слід забезпечити більшу площу поверхні столу, щоб «миша» могла переміщатися і мати зручний упор для ліктьового суглоба.
- Не дозволяється розмовляти сторонніми речами, створювати шуми тощо.
- Кожного разу, коли комп'ютер не працює, хлопко-паперова салфетка слід мити з мильним розчином. Екран і захисний екран протирають спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби для очищення поверхонь комп'ютерних технік.
- Забороняється: - самостійно ремонтувати апаратуру, в якій кінескоп та інші частини можуть бути під високою напругою (до 25 кВ0); - класти будь-які предмети на клавіатуру ПК, включаючи бутерброди та напої; - торкатися до клавіатури або близько до неї. Це може вивести її з ладу; - затуляти вентиляційні отвори в пристрої, що може призвести до перегріву та виходу з ладу.
- Щоб зменшити негативний вплив факторів ризику, пов'язаних із роботою на комп'ютерах, на стан здоров'я працівників, передбачаються додаткові регламентовані перерви для відпочинку користувачів комп'ютерів: 10 хвилин під час безперервної роботи та 15 хвилин під час кожної другої години роботи.
- Якщо це можливо, слід змінити діяльність на іншу, яка не пов'язана з роботою на ПК.
- Чергування операцій введення тексту та введення даних (зміна змісту та темпу роботи) може зменшити негативний вплив монотонності.

- При роботі з лазерными принтерами слід переконатися, що принтер розташований поруч із системним блоком, щоб з'єднувальні шнури не натягнулися. Не можна встановлювати принтер на системний блок.
- Перш ніж розпочати програмування принтера, переконайтеся, що він знаходиться в режимі зв'язку з системним блоком.
- Щоб уникнути пошкодження апарату, потрібно використовувати папір, марка якого вказана в інструкції до принтера. Це найчастіше папір вагою 60-135 г/м2, типу Canon або Xerox 4024.
- Щоб зменшити ймовірність загинання паперу, обрізайте краї паперу гострим лезом ножа, який не має заусенців.
- Бажано вимикати живлення відео монітора під час роботи (більше 20 хвилин), коли втручання користувача в програму не потрібне.
- Під час перерв необхідно виконувати рекомендовані вправи для очей, хребта та рук, щоб підтримувати загальний тонус м'язів і запобігти кістково-м'язовим проблемам, зоровому дискомфорту та іншим несприятливим суб'єктивним почуттям.
- Кількість мікропауз (від 1 до 2 хвилин) має бути індивідуальною. Перерви можуть мати різний характер і включати виконання допоміжних робіт, не пов'язаних із роботою ПК, прийом їжі та виконання рекомендованих вправ.
- Залежно від того, наскільки ви втомилися, рекомендується виконувати фізичні вправи протягом дня. Гімнастика повинна сприяти корекції вимушеної пози, покращити кровообіг, частково компенсувати та скоротити рухову активність.
- Якщо ви помітите будь-яку несправність, таку як іскри, пробоїв, запах гару або ознаки горіння, негайно припиніть роботу, відключіть все обладнання від електромережі та негайно повідомте безпосереднього керівника або спеціаліста по ремонту комп'ютерів.
- Правила безпеки для завершення роботи на персональному комп'ютері
- Закінчити та зберегти файли, які знаходяться в роботі в пам'яті комп'ютера (ПК). Виконати всі необхідні дії, щоб забезпечити коректне завершення роботи операційної системи.

- Вимкнути системний блок і принтер, а також інші периферійні пристрої. Вимкнути живлення пристрою безперебійного живлення (ПБЖ).
- Вимкнути комп’ютер кнопкою «POWER» (ЖИВЛЕННЯ) і вийняти штепсельну вилку з кабелю живлення.Накрийте клавіатуру кришкою, щоб уникнути попадання пилу.
- Порядок на робочому місці.

Висновки. У цьому розділі розглядаються способи, за допомогою яких небезпечні та шкідливі виробничі фактори можуть впливати на технічний персонал відділу ІТ. Розраховано освітленість робочої зони. Ми отримали дев’ять світильників із 36 світлодіодними лампами, які є ідеальним варіантом для освітленості робочої зони та не порушують стандарти освітленості 300-500 лк. Було розроблено інструкцію з охорони праці при роботі з персональними комп’ютерами, а також рекомендації щодо пожежної безпеки для ІТ-відділу..

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1. Аналіз впливу техногенних чинників на навколишнє природне середовище

У результаті діяльності людини в середовищі існування воно поступово змінювало свій вигляд, що призвело до руйнування біосфери та створення штучного середовища, відомого як техносфера. Науковці стверджують, що сьогодні майже все середовище, в якому живе людина, є техногенним. Техносфера, яку людина створила, охоплює майже всю планету і навіть вийшла за межі Землі.

Техногенне середовище, також відоме як техносфера, складається з наслідків діяльності людини.

Люди постійно виконують два основні завдання, коли вони працюють у техногенному середовищі: створювати та використовувати системи, які захищають їх від шкідливих факторів.

Вплив негативних факторів техносфери на організм людини та навколишнє середовище може бути прямим або непрямим [45].

6.2. Принцип роботи базових станцій і стільникових пристроїв та їх негативний вплив на довкілля

У сучасному світі практично неможливо уникнути впливу ЕМП через стрімке зростання технологій і приладів.

ЕМП стільникового зв’язку походить від телефонних трубок і базових станцій супроводу стільникового зв’язку. Ці джерела ЕМП працюють по-різному на кожного. Стільниковий телефон як джерело ЕМП має можливість максимально наближатися до голови користувача на відстань від двох до п’яти сантиметрів у неконтрольованих

умовах. Головний мозок, периферичні рецепторні зони вестибулярного апарату, слухові аналізатори та сітківка очей піддаються впливу ЕМП. Крім того, люди, з якими споживач розмовляє по телефону, також піддаються впливу випромінювання стільникового телефону.

Електромагнітні поля створюються на базових станціях імпульсно. Це залежить від часу доби, насиченості покриття базових станцій і кількості базових станцій, розташованих у певній зоні. Саме базові станції генерують техногенне електромагнітне поле, яке покриває всю область дії стільникового зв'язку. Базові станції мають низькоінтенсивне електромагнітне поле радіочастотного діапазону, яке впливає на людей щодня.

За даними екологів і лікарів-гігієністів, добре відомо, що будь-який діапазон електромагнітного випромінювання має серйозні наслідки для здоров'я людини та її здатності працювати. Поширеність електромагнітних полів робить їх більш небезпечними для людини, ніж радіація. Електропроводка, освітлення, побутові електроприлади, лінії електропередач тощо створюють електричні поля промислової частоти, які оточують людей щодня.

У зв'язку зі стрімким розширенням мережі джерел фізичних полів електромагнітної природи та збільшенням їх потужностей енергетичне навантаження від електромагнітних випромінювань як у промисловості, так і в побуті постійно зростає. Хоча людина фізично не може відчувати електромагнітне поле, воно знижує адаптивні резерви, імунітет, працездатність, викликає синдром хронічної втоми та підвищує ризик захворювань. Діти, підлітки, вагітні жінки та люди з ослабленим здоров'ям особливо уразливі до електромагнітних випромінювань.

Вплив електромагнітного поля на клітину. Електромагнітне поле впливає на заряджені частинки та стрими, перетворюючи енергію поля на рівні клітини в інші форми енергії.

Цетогенетичні (вихід хромосомних аберацій) дослідження показали, що клітини в експериментальній групі з порушеннями були більші, ніж клітини в контроль-

ній групі. Опромінення ЕМП повітряно-сухого насіння і проростків салату також призвело до збільшення хромосомних аберацій. У клітинах крові корів з ферми виявили більше генетичних ушкоджень і аномальних гематопоезу [46].

Вплив електромагнітного поля на тканини. На зміни в живій тканині також впливають слабкі електромагнітні поля з меншим порогом теплового ефекту. Були проведені дослідження щодо впливу стільникового телефону, комп'ютерного блоку та інших електронних пристроїв на організм людини. В результаті цих досліджень було виявлено, що вплив цих джерел проявляється в тому, що регенерація тканин погіршується.

В електричному полі атоми та молекули поляризуються, а полярні молекули орієнтуються в напрямку розповсюдження магнітного поля. У результаті змінної поляризації діелектрика (сухожиль, хрящів, кісток) і струмів провідності змінне електричне поле нагріває тканини живих організмів.

Вплив електромагнітного поля на нервову систему. Проводились перші експерименти щодо впливу електромагнітного поля на нервову систему. Електромагнітне поле впливає на мембрани нейронів, пам'ять, умовно-рефлекторну діяльність і мозок. У моделях показано, як слабкі електромагнітні поля можуть впливати на процеси синтезу в нервових клітинах. Коркові нейрони демонструють значні зміни імпульсації, що призводить до порушення переданої інформації в більш складні структури мозку. Виявлено, що порушення короткочасної пам'яті можуть виникнути в результаті дії електромагнітного поля в надвисокочастотному діапазоні..

Вплив електромагнітного випромінювання на імунну систему. Наразі є достатньо інформації про те, що електромагнітне поле порушує процеси імуногенезу. Електромагнітне поле змінює характер інфекційного процесу, порушує білковий обмін, зменшує вміст альбумінів і збільшує гамма-глобуліни в крові. Крім того, електромагнітне поле може виступати як пусковий фактор або алерген, що викликає сильні реакції у алергіків, коли вони контактують з ним.

Вплив електромагнітного поля на статеву систему. Електромагнітне випромінювання призводить до зниження функції сперматогенезу, зміни менструального циклу, уповільнення ембріонального розвитку, вроджених каліцтв у новонароджених дітей і зниження лактації у годуючих матерів.

Вплив електромагнітного поля на рослини. Численні дослідження показали, що електромагнітні хвилі мають значний вплив на біологічні об'єкти через низку індукованих ефектів. Як слабкі, так і сильні ЕМП впливають на морфологію, фізіологію, біохімію та біофізичні характеристики рослин. Вони впливають на зростання, розвиток і розмноження рослин.

Рівень електричного поля, реєстрованого поблизу повітряних ліній (ПЛ), теоретично достатній для пошкодження листя рослин. Експерименти та спостереження, проведені щодо впливу ЕМП ліній електропередачі на рослини, показали, що в порівнянні з контролем суха маса надземної маси рослин вівса та соняшника, зростаючих під ПЛ, була нижчою. ЕМП має негативний вплив на потенційну нітрогенезну активність різосферної популяції та довжину проростків рослин.

Вплив слабких електромагнітних полів на живі організми. На зміни в живій тканині також впливають слабкі електромагнітні поля з меншим порогом теплового ефекту. Ряд наукових установ проводить дослідження біологічного впливу стільникових телефонів, комп'ютерних блоків та інших електронних пристроїв. Здатність електронних пристроїв завдавати шкоди досліджувалася як у робочому, так і у вимкненому стані, а також без джерела живлення [47].

Результати досліджень, які вивчали вплив стільникового телефону, комп'ютера та інших сучасних радіоелектронних засобів на різні організми як у робочому, так і у вимкненому стані, виявилися невтішними і показали, що вони негативно впливають на стан біологічних об'єктів. Це призвело до зменшення рухової активності та виживання мікроорганізмів, збільшення смертності мікроорганізмів, погіршення регенерації тканин, порушення ембріонів.

6.3. Методи та засоби захисту навколишнього середовища від впливу техногенних чинників

Захист від електромагнітних випромінювань. Потрібно вжити низку заходів, щоб захистити працівників і людей, які проживають у зоні дії радіоелектронних засобів, від впливу ЕМВ. Це можуть бути організаційні, інженерно-технічні та лікарсько-профілактичні дії.

Органи санітарного нагляду відповідають за організацію та інженерно-технічну роботу. Санітарні лабораторії підприємств і установ, які використовують джерела електромагнітного випромінювання, повинні брати участь у гігієнічних оцінках нового будівництва та реконструкції об'єктів, які виробляють і використовують радіозасоби, а також нових технологічних процесів і обладнання з використанням ЕМП. Вони також повинні проводити поточний санітарний нагляд за об'єктами, які використовують джерела електромагнітного випромінювання, виконувати організаційно-методич

Необхідно забезпечити, щоб опромінюючі та опромінюючі об'єкти розташовувалися таким чином, щоб зменшити інтенсивність опромінення, ще на етапі проєктування. У зв'язку з тим, що повністю уникнути опромінення неможливо, необхідно зменшити ймовірність проникнення людей у місця з високою інтенсивністю ЕМП, щоб зменшити час, який люди проводять під опроміненням.

Колективні (група будинків, район, населений пункт) і локальні (окремі будівлі, приміщення) і інженерно-технічні методи та засоби захисту мають вирішальне значення. Розрахунок поширення радіохвиль у конкретній місцевості є основою колективного захисту. Природні екрани, такі як складки місцевості, лісонасадження та нежитлові будівлі, є найбільш економічно ефективними.

Встановлення антени на горі може значно зменшити інтенсивність поля, яке опромінює населений пункт. Наприклад, для високоспрямованих антен, орієнтація діаграми спрямованості змінюється відповідно, збільшуючи висоту антени. Але висока антена менш стійка, складніша та дорожча. Крім того, цей захист погано працює з відстані.

Затухання хвилі, яка проходить через екран (наприклад, через лісову смугу), має бути враховано при захисті екрана від випромінювання. Рослинність може служити екраном. Відбивні та радіопоглинальні щити, які використовуються як спеціальні екрани, дорогі та неефективні.

Локальний захист використовується часто, оскільки він дуже ефективний. Використання радіозахисних матеріалів забезпечує високе поглинання енергії випромінювання у матеріалі та віддзеркалення його поверхні. Екранування шляхом віддзеркалення використовується за допомогою металевих листів і сіток з хорошою провідністю. Металізовані стіни можна обклеювати металізованими шпалерами, віковими сітками та шторами [47].

Хоча в цьому місці немає багато випромінювання, віддзеркалене екранами випромінювання поширюється по простору та потрапляє на інші предмети.

Персонал, який працює на невеликій відстані, повинен бути захищений шляхом екранування апаратури.

Поруч із віддзеркалюючими є екрани, виготовлені з матеріалів, що поглинають випромінювання. Існує широкий спектр радіопоглинальних матеріалів, як однорідних, так і композиційних, які складаються з різноманітних діелектричних і магнітних речовин. Поглинальна поверхня екрана виготовляється шорсткою, ребристою або у вигляді шипів, щоб підвищити продуктивність. Радіопоглинаючі матеріали можуть захистити навколишнє середовище від ЕМП, який виробляє джерело в екранованому об’єкті.

Засоби індивідуального захисту використовуються лише тоді, коли інші засоби захисту недоступні або недостатньо ефективні: під час переходу через зони збільшеної інтенсивності випромінювання, під час ремонту та налагодження в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливості виконання операцій і погіршують умови гігієни.

Тіло захищається одягом, виготовленим із металізованих тканин і радіопоглинаючих матеріалів. Металева тканина, схожа на металеву сітку, послаблює випромінювання на 20-30 дБ, оскільки вона складається з бавовняних чи капронових ниток,

спірально обвитих металевим дротом. Забезпечте контакт ізольованих провідників під час зшивання компонентів захисного одягу. Таким чином, електрогерметизація швів проводиться за допомогою електропровідних розчинів або клеїв, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок між неконтактними проводами.

Спеціальні окуляри зі скла з провідною плівкою двоокису олова на внутрішній стороні захищають очі. Гумова оправа окулярів послаблює випромінювання НВЧ на 20-30 дБ завдяки використанню металізованої тканини або запресованої металевої сітки.

Оскільки допустима щільність потоку енергії для ніг і рук у багато разів вища, ніж для тіла, рукавички та бахіли зараз вважаються непотрібними.

Засоби колективного та індивідуального захисту можуть гарантувати безпеку працівників протягом тривалого часу на радіооб'єктах [47].

Колективний та індивідуальний захист від шуму. Протидія шуму є джерелом його виникнення. Це найефективніший метод боротьби з шумом. Розробляються малошумні механічні передачі, вентилятори та підшипникові вузли.

Зниження шуму звукопоглинанням. Об'єкт, який випромінює шум, міститься в кожусі, внутрішні стінки якого покриті звукопоглинальним матріалом. Кожух повинен мати достатню звукопоглинальну здатність, щоб він не заважав роботі іншого обладнання та не пошкоджував інтер'єр цеху. Цей метод схожий на кабіну, де знаходиться найбільш гучний об'єкт і де працює працівник. Використовуючи звукопоглинальний матеріал, який покриває кабіну зсередини, він замість того, щоб просто ізолювати джерело шуму від решти виробничого приміщення, використовує його для зменшення рівня шуму всередині кабіни.

Зниження шуму звукоізоляцією. Цей метод полягає в тому, що шумовипромінювальний об'єкт або декілька найбільш шумних об'єктів розташовуються окремо, ізольовано від основного, менш шумного приміщення звукоізолювальною стіною або перегородкою. Розташування найбільш шумного предмета в окремій кабіні також допомагає зменшити шум. При цьому кількість людей, які відчувають шум, буде менше,

але рівень шуму не зменшиться. Розташування оператора в спеціальній кабіні дозволяє йому спостерігати та контролювати технологічні процеси, щоб забезпечити звукоізоляцію. Установка екранів і ковпаків також забезпечує звукоізоляцію. Вони не знижують шум в приміщенні, але захищають робоче місце та людину від прямого впливу звуку.

Зниження шуму акустичною обробкою приміщення. Акустична обробка приміщення передбачає використання звукопоглинальних матеріалів для покриття стелі та верхніх стін. Як наслідок цього, інтенсивність відбитих звукових хвиль зменшується. Стелі можуть мати звукопоглинальні щити, конуси, куби або резонаторні екрани (штучні поглиначі). Застосовувані матеріали та конструкції, місце розташування, розмір, геометрія та розташування джерел шуму впливають на ефективність акустичної обробки приміщень. Витягнута форма має більший ефект у низьких приміщеннях, де висота стелі не перевищує 6 м. Зниження шуму на 8 дБА можна досягти за допомогою акустики [49].

У процесі проєктування промислових об’єктів і обладнання необхідно враховувати заходи щодо зниження шуму. Особливу увагу слід приділити переміщенню шумного обладнання в окреме приміщення, щоб зменшити кількість працівників, які працюють у приміщеннях з високим рівнем шуму, а також здійсненню заходів, спрямованих на зниження шуму при мінімальних витратах коштів, обладнання та матеріалів. Зниження шуму залежить від знешумлення всього обладнання з високим рівнем шуму.

Створення шумових карт і спектрів шуму обладнання та виробничих приміщень є першим кроком до знешумлення робочого обладнання в приміщенні. За допомогою цих карт визначається напрямок роботи.

Висновок. Розвиток електроніки та радіотехніки призвів до забруднення природного середовища електромагнітними випромінюваннями, також відомими як поля. Радио-, телевізійні та радіолокаційні станції є їхніми основними джерелами. Те-

левізійні центри або ретранслятори, радіоцентри та засоби радіозв'язку різного призначення розташовані поблизу кожного обласного центру, багатьох районних центрів і великих міст.

Для захисту людей, які знаходяться в зоні дії деяких радіоелектронних засобів від електромагнітних полів, необхідні організаційні, інженерно-технічні та лікувально-профілактичні заходи.

Санітарні норми та правила для радіотехнічних і електротехнічних об'єктів розроблені на основі медико-біологічних досліджень. Вони контролюють умови їхньої експлуатації, щоб захистити людей від шкідливих електромагнітних випромінювань.

Таким чином, на етапі проєктування об'єкти мають бути розташовані таким чином, щоб інтенсивність опромінення була мінімальною. Крім того, необхідно заздалегідь забезпечити зменшення кількості часу, протягом якого персонал залишається в зоні опромінення. Джерела випромінювання повинні мати мінімальну потужність. Крім того, державні органи повинні дотримуватися державних правил України та не порушувати їх.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було вивчено основні види зовнішніх загроз і загроз несанкціонованого доступу до інформації як їхній основний різновид, дано оцінку їхній потенційній небезпеці, проведено аналіз принципу роботи системи фільтрації трафіку як способу захисту від цих загроз, а також спроєктовано і розроблено прототип такої системи.

Було дано визначення зовнішніх загроз інформаційній безпеці, розглянуто основні види зовнішніх загроз: загрози витоку акустичної та видової інформації, загрози витоку інформації каналами побічних електромагнітних випромінювань і наведень, загрози несанкціонованого доступу до інформації в інформаційному середовищі. Було вивчено основні принципи дії останнього виду загроз - способи їх виконання, небажані наслідки, режими виконання тощо.

Було дано оцінку потенційної небезпеки зовнішніх загроз безпеці з погляду отриманих унаслідок кіберзлочинів збитків і з погляду постійного зростання кількості загроз несанкціонованого доступу до інформації та відсутності механізму з їх розслідування. Було виявлено, що загрози цієї категорії останніми роками є одними з найбільш часто вживаних і приносять відносно великі збитки кінцевим користувачам і підприємствам, які потрапили під вплив тієї чи іншої зовнішньої загрози.

Було вивчено принцип роботи систем фільтрації трафіку, визначено основний алгоритм фільтрації, необхідні вхідні дані, вимоги до системи. Було з'ясовано, у якому сегменті мережі необхідно розміщувати ці системи, на яких рівнях інтернет-протоколів вони найефективніші, які існують додаткові способи аналізу інтернет-трафіку, а також виявлено основні вимоги до рівня захисту інформаційної системи з погляду законодавства.

Було проведено огляд систем-аналогів різного рівня - від рівня інтернет-провайдера до рівня комп'ютера користувача, що ґрунтуються на принципах фільтрації трафіку, зокрема, глибокого аналізу трафіку (DPI). Як основні системи фільтрації трафіку було розглянуто такі продукти, як Ideco UTM, Carbon Reductor DPI X, Інтернет

Контроль Сервер (ІКС) і один із прикладів системи, вбудованої в стороннє обладнання.

Було виконано проєктування простого прототипу системи фільтрації трафіку, якого достатньо для наочного розуміння принципу роботи системи. Для розробки такого прототипу було виконано аналіз способів перехоплення трафіку з мережевого інтерфейсу ПК, формату переданих за протоколом Ethernet даних і було реалізовано рішення для їхньої інтерпретації та подальшого опрацювання реалізованим фільтром.

Спроєктований прототип було реалізовано мовою програмування C# з використанням бібліотеки Windows Forms для відтворення графічного інтерфейсу та бібліотеки SharpPcap для перехоплення трафіку з мережевого інтерфейсу. Створений робочий прототип дав змогу наочно продемонструвати роботу системи фільтрації трафіку з погляду системного адміністратора та переконатися в ефективності рішення і необхідності продовження роботи, але не мав можливості здійснювати безпосередньо фільтрацію трафіку під час роботи.

Після цього було виконано доопрацювання прототипу, спрямоване на збільшення його швидкодії та точності роботи, а також систему було розширено з демонстраційної до інтегрованої в систему, яка здійснює реальну роботу. Для цього було змінено режим роботи системи з прямого перехоплення трафіку на роботу в режимі проксі-сервера і виконано його налаштування в ОС Windows 11.

Було виконано модульне та функціональне тестування розробленого прототипу системи фільтрації трафіку з прикладами правил фільтрації, під час якого було виявлено, що така система справді дає змогу виконувати реальну фільтрацію трафіку, причому зі значно меншим зниженням швидкодії, порівнюючи з початковим варіантом. Під час виконання тестування було коректно опрацьовано всі тестові запити, зокрема й ті, що розташовані на віртуальних веб-серверах.

Під час виконання тестування було дано оцінку точності роботи фільтра і його швидкодії. Було виявлено, що розроблений прототип здійснює фільтрацію з доволі високою ефективністю, близькою до 100% (у межах реалізованої функціональності),

і хоча й призводить до деяких затримок у роботі мережі, але ці затримки були очікуваними, і надалі можливе збільшення швидкодії системи завдяки застосуванню більш ефективних алгоритмів роботи.

Розроблений прототип системи фільтрації трафіку доволі сильно програє більшості розглянутих раніше систем-аналогів за набором функцій (наприклад, глибокий аналіз пакетів, підміна сертифіката і масштабованість), але значно виграє за легкістю налаштування і встановлення та за вартістю обслуговування. При цьому менший набір функцій не можна назвати критичним недоліком, оскільки, по-перше, системи подібного рівня найчастіше мають ще меншу кількість налаштувань, а по-друге, функції, яких немає в розробленій системі, складні в налаштуванні й застосовують досить рідко.

Отримані в результаті виконання цієї роботи висновки можуть надалі використовуватися під час формування рекомендацій щодо побудови інформаційних систем малого та середнього масштабу, а прототип системи фільтрації трафіку може бути розширено, доопрацьовано і застосовано в невеликих інформаційних системах для забезпечення базового рівня захисту від зовнішніх загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Y. Zhang, H. Xu and J. Wu, "An Automatic Background Filtering Method for Detection of Road Users in Heavy Traffics Using Roadside 3-D LiDAR Sensors With Noises," in IEEE Sensors Journal, vol. 20, no. 12, pp. 6596-6604, 15 June15, 2020.
2. S. S. P. Moka, S. M. Pilla and S. Radhika, "Real Time Density Based Traffic Surveillance System Integrated with Acoustic Based Emergency Vehicle Detection," 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 2020, pp. 1-7.
3. T. Seo, "Calibration-free traffic state estimation method using single detector and connected vehicles with Kalman filtering and RTS smoothing," 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 2020, pp. 1-5.
4. The Top 10 Biggest Cyberattacks of 2022, Agile IT, 2023 [link] https://www.agileit.com/news/biggest-cyberattacks-2022/.
5. L. He, Y. Wang, Q. Shi, Z. He, Y. Wei and M. Wang, "Multi-sensor Fusion Tracking Algorithm by Square Root Cubature Kalman Filter for Intelligent Vehicle," 2021 5th CAA International Conference on Vehicular Control and Intelligence (CVCI), Tianjin, China, 2021, pp. 1-4.
6. G. S. Rajaboevich, K. M. -X. Mirpulatovich and A. J. Tileubaevna, "Method for implementing traffic filtering in SDN networks," 2022 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2022, pp. 1-3.
7. L. Du, J. Zhang and W. Sun, "Design of Interacting Multiple Model with Unscented Kalman Filter for V2X Test," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2020, pp. 161-164.

8. H. Wang, Q. Miao, Y. Zhang and X. Wen, "Green Wave Zone Evaluation Method Based on Electronic Police Data," 2021 2nd International Conference on Big Data and Informatization Education (ICBDIE), Hangzhou, China, 2021, pp. 155-158.
9. E. E. Oma, J. Zhang and Z. Lv, "FPGA Based Traffic Sign Detection Using Support Vector Machine and Hybrid Filters," 2022 10th International Conference on Intelligent Computing and Wireless Optical Communications (ICWOC), Chongqing, China, 2022, pp. 45-49.
10. L. Zhang and Y. Lu, "Distributed Consensus-Based Boundary Observers for Freeway Traffic Estimation with Sensor Networks," 2020 American Control Conference (ACC), Denver, CO, USA, 2020, pp. 4497-4502.
11. N. F. Aminuddin, Z. Tukiran, A. Joret, M. N. Roslee, S. Yamaguchi and M. A. Ahmadon, "Hungarian-Particle Filtering Based Segmentation for On-Road Visual Vehicle Detection and Tracking," 2022 IEEE 4th Global Conference on Life Sciences and Technologies (LifeTech), Osaka, Japan, 2022, pp. 600-603.
12. M. Umarov, F. Muradov and T. Azamov, "Traffic Sign Recognition Method Based on Simplified Gabor Wavelets and CNNs," 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2021, pp. 1-5.
13. M. Umarov, J. Elov, S. Khalilov, I. Narzullayev and M. Karimov, "An algorithm for parallel processing of traffic signs video on a graphics processor," 2022 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2022, pp. 1-5.
14. S. A. Kashinath et al., "Review of Data Fusion Methods for Real-Time and Multi-Sensor Traffic Flow Analysis," in IEEE Access, vol. 9, pp. 51258-51276, 2021.
15. K. M. Malikovich, G. S. Rajaboevich, T. S. Sobirovna and E. Temurmalik, "Differentiated Services Code Point (DSCP) Traffic Filtering Method to Prevent Attacks," 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2021, pp. 1-4.

16. G. Yang et al., "A robust traffic scene recognition algorithm based on deep learning and Markov localization," 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), Shanghai, China, 2020, pp. 231-235.
17. X. Liang, "Research on Network Security Filtering Model and Key Algorithms Based on Network Abnormal Traffic Analysis," 2021 International Conference on Networking, Communications and Information Technology (NetCIT), Manchester, United Kingdom, 2021, pp. 226-229.
18. X. Liu, W. Gao, D. Feng and X. Gao, "Abnormal Traffic Congestion Recognition Based on Video Analysis," 2020 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), Shenzhen, China, 2020, pp. 39-42.
19. S. Luo, J. Zeng and J. Liu, "Research on Traffic Signal Light Recognition Method in Complex Scene," 2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2023, pp. 899-903.
20. D. Dan and X. Hao, "An Automatic Real-time Cable Modal Frequency Identification and Tracking Algorithm by Combining Recursive Band-pass Filter and Recursive Hilbert Transform," 2021 4th International Symposium on Traffic Transportation and Civil Architecture (ISTTCA), Suzhou, China, 2021, pp. 340-343.
21. Z. Chen, H. Xu, J. Zhao and H. Liu, "A Novel Background Filtering Method With Automatic Parameter Adjustment for Real-Time Roadside-LiDAR Sensing System," in IEEE Transactions on Instrumentation and Measurement, vol. 72, pp. 1-10.
22. X. Chen et al., "Sensing Data Supported Traffic Flow Prediction via Denoising Schemes and ANN: A Comparison," in IEEE Sensors Journal, vol. 20, no. 23, pp. 14317-14328.
23. W. Fang, W. Cai, B. Fan, J. Yan and T. Zhou, "Kalman-LSTM Model for Short-term Traffic Flow Forecasting," 2021 IEEE 5th Advanced Information

Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2021, pp. 1604-1608.

24. S. Taguchi and T. Yoshimura, "Online Estimation and Prediction of Large-Scale Network Traffic From Sparse Probe Vehicle Data," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 7233-7243.
25. D. N. Triwibowo, E. Utami, Sukoco and S. Raharjo, "Analysis of Classification and Calculation of Vehicle Type at APILL Intersection Using YOLO Method and Kalman Filter," 2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS), Makasar, Indonesia, 2021, pp. 1-6.
26. C. Ma, S. Gao, B. Liu and Y. Wang, "Resonant Cavity Backscattered Light Detection Method with Orthogonal Digital Lock-in Amplifier Combined with Kalman Filter," 2022 International Conference on Mechanical and Electronics Engineering (ICMEE), Xi'an, China, 2022, pp. 203-207.
27. X. Chen, J. Yin, K. Tang, Y. Tian and J. Sun, "Vehicle Trajectory Reconstruction at Signalized Intersections Under Connected and Automated Vehicle Environment," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 17986-18000.
28. V. Dahmen, A. Loder, G. Tilg, A. Kutsch and K. Bogenberger, "Traffic State Estimation with Loss Constraint," 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC), Macau, China, 2022, pp. 1907-1912.
29. J. Cheng and C. Li, "Design and Implementation of TLS Traffic Packet Filtering Technology Based on Netfilter Framework," 2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE), Brisbane, Australia, 2022, pp. 18-22.
30. H. Sun, H. -h. Chen, X. Cui and J. -x. Wang, "Vehicle Flow Statistics System in Video Surveillance based on Camshift and Kalman Filter," 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2021, pp. 362-366.

31. N. Zhang, X. Yang, H. Guo, H. Dong and W. Ma, "Approximate Inference of Traffic Flow State at Signalized Intersections Using a Bayesian Learning Framework," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 5, pp. 4765-4776.
32. T. G. Altundogan and M. Karakose, "A Noise Reduction Approach Using Dynamic Fuzzy Cognitive Maps for Vehicle Traffic Camera Images," 2020 Zooming Innovation in Consumer Technologies Conference (ZINC), Novi Sad, Serbia, 2020, pp. 15-20.
33. Y. Fang, A. Panah, J. Masoudi, B. Barzegar and S. Fatehi, "Adaptive Unscented Kalman Filter for Robot Navigation Problem (Adaptive Unscented Kalman Filter Using Incorporating Intuitionistic Fuzzy Logic for Concurrent Localization and Mapping)," in IEEE Access, vol. 10, pp. 101869-101879.
34. Z. He, R. Shao and J. Wang, "Estimation of urban arterial travel time based on dynamic bayesian network," 2021 China Automation Congress (CAC), Beijing, China, 2021, pp. 7939-7942.
35. J. Huo, X. Fu, Z. Liu and Q. Zhang, "Short-Term Estimation and Prediction of Pedestrian Density in Urban Hot Spots Based on Mobile Phone Data," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 10827-10838.
36. ДСанПіН 3.3.2-007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».
37. ГН 3.3.5-8-6.6.1-2002 «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».
38. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень».
39. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».
40. НПАОП 0.00-1.29-97 «Правила захисту від статичної електрики».

41. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».
42. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».
43. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».
44. НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні».
45. Прогнозування екологічних ризиків з використанням аналізу ієрархів і теорії нечітких множин: Міжнародна науково-практична конференція "І-й всеукраїнський з'їзд екологів": Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. Вінниця, 4-7 жовтня 2016 року. - 2016. - С.25.
46. Антипов В.В., Давидов Б.І., Тихончук В.С. Біологічна дія, нормування та захист від електромагнітних випромінювань. К.: Енергоатоміздат, 2002. - 177 с.
47. Філіппов Є.С. Вплив електромагнітних полів на біологічні об'єкти / Є.С. Філіппов, Є.Л. Ткачук. К. - 2018. -№1 - Том: 24. - С. 15-19.
48. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.
49. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.