Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно–інформаційних систем і програмної інженерії
(назва факультету)
Комп’ютерних наук
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

Магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Покращення безпекових характеристик мережі з використанням протоколу IPv6

Виконав: студент (ка) 6 курсу, групи САмз-61
спеціальності (напряму підготовки) 124
Системний аналіз
(шифр і назва спеціальності (напряму підготовки))

		Кукуруза А.О.
	(підпис)	(прізвище та ініціали)
Керівник		Щербак Л.М.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Мацюк О.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Гащин Н.Б.
	(підпис)	(прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Покращення безпекових характеристик мережі з використанням протоколу IPv6 // Дипломна робота ОР «Магістр» // Кукуруза Анатолій Олегович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САмз-61 // Тернопіль, 2019 // С. – , рис. – , табл. – , додат. – , бібл. – .

Ключові слова: MAC, IANA, CAM, TCAM, DoS, CVSS, NAT, ARP.

У першому розділі задача зводиться до аналізу специфікації мережевого протоколу IPv6, пошуку можливих проблем та загроз, їх дослідження на базі тестової лабораторії. По результатам досліджень необхідно здійснити пошук можливих методів усунення небезпек та вразливостей і здійснити порівняльний аналіз для обладнання двох виробників.

У другому розділі розглянуто специфікацію мережевого протоколу IPv6. Сюди входять такі основні аспекти, як розширення простору адрес, новий заголовок мережевого рівня, а також основні функції (такі, як авто налаштування, та використання протоколу ICMPv6). Окрім цього, наведено коротку порівняльну характеристику протоколів IPv4 та IPv6.

У третьому розділі розглянуто питання розгортання протоколу IPv6 яке відбувається одночасно із появою нових загроз безпеки кінцевих користувачів та їхніх даних. Загалом, проблеми безпеки пов'язані з протоколом IPv6 можна розділити на дві категорії: ті, що успадковані від його попередника – протоколу IPv4 та нові проблеми, пов'язані із новими можливостями, що були додані до протоколу. Деякі вразливості протоколу не враховані його

специфікацією. Такі недоліки неможливо усунути, при цьому не змінюючи сам протокол. Вирішення подібних проблем зазвичай лягає на плечі розробників.

У четвертому розділі розглянуто етапи проектування мережі, при яких можуть використовуватися різні методи аналізу захищеності і визначення загального рівня захищеності, які, базуються на кількісних і якісних методиках аналізу ризику. Графи атак забезпечують ефективний спосіб моделювання сценаріїв мережевих атак, а «Загальна система оцінки вразливостей» CVSS дає числові оцінки кожної уразливості. У комплексі, ці підходи можуть дати оцінку рівня захищеності комп'ютерної мережі.

У п’ятому розділі розглянута методика підвищення рівня безпеки локальної мережі.

У спеціальній частині наведено організацію мережевої безпеки комп’ютерної мережі та засоби моніторингу та діагностики комп’ютерної мережі.

ANNOTATION

Network safety characteristics improvement using IPv6 protocol // Diploma work degree “Master” // Kukuruza Anatolii // Ternopil Ivan Pul`uj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Computer Science // Ternopil, 2019 // P. , Fig – , Table – .

In the first section, the task is to analyze IPv6 network protocol specification, to search for possible problems and threats, and to research them on the basis of a test laboratory. According to the results of research it is necessary to search for possible methods of elimination of hazards and vulnerabilities and to carry out a comparative analysis for the equipment of two manufacturers.

The second section discusses the specification of the IPv6 network protocol. These include such basic aspects as expanding address space, the new network layer header, and basic functions (such as auto-configuration and protocol, ICMPv6). In addition, a brief comparison of IPv4 and IPv6 protocols is given.

The third chapter addresses the issue of deploying the IPv6 protocol, which occurs simultaneously with the emergence of new threats to the security of end users and their data. In general, security issues related to IPv6 protocol can be divided into two categories: those that are inherited from its predecessor - the IPv4 protocol and new problems associated with the new features that have been added to the protocol. Some vulnerabilities in the protocol are not taken into account by its specification. Such shortcomings can not be eliminated, without changing the protocol itself. Solving such problems usually falls on the shoulders of developers.

The fourth section deals with the stages of network design, which can be used with different techniques of security analysis and determining the overall level of security, which are based on quantitative and qualitative methods of risk analysis.

Attack graphs provide an effective way to simulate network attack scenarios, and the "Common Vulnerability Assessment System" CVSS provides numerical estimates of each vulnerability. In the complex, these approaches can assess the level of security of the computer network.

The fifth section deals with the methodology for increasing the level of security of the local network.

In the special part the organization of network security of the computer network and means of monitoring and diagnostics of the computer network are presented.

The process of implementing the new generation IPv6 network protocol has been gradually taking place over the past few years (the launch of which was June 6, 2012). However, the pace of development of the World Wide Web is much higher, which stimulates the acceleration of the transition to IPv6.

But what is still stopping the implementation of the protocol of the new version? One of the obstacles is the fear of the unknown, since reconfiguring the hardware to work with the new protocol can lead to unpredictable consequences, in particular when working with IPv4 at the same time. In addition, to ensure the robust deployment of the IPv6 network protocol, you need to focus on security issues. When developing the IPv4 protocol, this was far from the main criterion, so it had many vulnerabilities. Given that the IPv4 protocol has been used for many years, most of the shortcomings that he inherited have been eliminated as they are detected, and these practices have proven themselves well. Yes, at the time of IPv4 implementation, the networks were fairly small and it was not so critical, given the scale of modern networks, such mistakes could lead to more serious consequences.

Therefore, the topic of work was the study of the level of security of the network protocol IPv6. The main objective of the research is to increase the level of security of computer networks operating with the IPv6 network protocol. The paper considers the implementation of IPv6 security, based on the experience gained

through the use of IPv4; threat and vulnerability of the protocol, based on Cisco and juniper hardware.

The results of the work can be used in the process of implementing an IPv6 network layer protocol on the above-mentioned manufacturers to improve security.

Keywords: MAC, IANA, CAM, TCAM, DoS, CVSS, NAT, ARP.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

IPv4 – (англ. «Internet Protocol version 4») Інтернет протокол версії 4.

IPv6 – (англ. «Internet Protocol version 6») Інтернет протокол версії 6.

MAC – (англ. «Media Access Control») управління доступом до носія.

EUI-64 – (англ. «Extended Unique Identifier») розширений унікальний ідентифікатор.

IANA – (англ. «Internet Assigned Numbers Authority») «Адміністрація адресного простору Інтернет».

RIR – (англ. «Regional Internet Register») регіональний Інтернет реєстратор.

RFC – (англ. «Request for Comments») запит коментарів.

MTU – (англ. «Maximum Transmission Unit») максимальний розмір блоку корисного навантаження.

ICMPv4 – (англ. «Internet Control Message Protocol for the Internet Protocol

Version 4») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 4.

ICMPv6 – (англ. «Internet Control Message Protocol for the Internet Protocol

Version 6») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 6.

ARP – (англ. «Address Resolution Protocol») протокол визначення адрес.

ND – (англ. «Neighbor Discovery») пошук сусіда.

CAM – (англ. «Content-addressable Memory») асоціативна пам’ять.

TCAM – (англ. «Ternary Content-addressable Memory») трійкова асоціативна пам’ять

NA – (англ. «Neighbor Advertisement») представлення сусіда.

RA – (англ. «Router Advertisement») представлення сусіднього маршрутизатору.

RD – (англ. «Router Discovery») пошук сусіднього маршрутизатора.

NAT – (англ. «Network Address Translation») перетворення мережевих адрес.

ЦП – центральний процесор.

MitM – (англ. «Man in the Middle») атака «людина посередині».

DoS – (англ. «Denial of Service») атака «Відмова у доступі.

CVSS – (англ. «Common Vulnerability Scoring System») Система загальної оцінки вразливостей.

ВСТУП

Процес впровадження мережевого протоколу нового покоління IPv6 відбувається поступово протягом останніх років (Всесвітній запуск якого відбувся 6 червня 2012 року). Але, темпи розвитку всесвітньої мережі Інтернет, значно вищі, що стимулює прискорення переходу на IPv6.

Та, що ж все-таки зупиняє призупиняє впровадження протоколу нової версії? Одна із перешкод, це страх перед невідомим, так як переналаштування обладнання для роботи з новим протоколом може призвести до непередбачуваних наслідків, зокрема при одночасній роботі з IPv4. Окрім цього, для забезпечення надійного розгортання мережевого протоколу IPv6 необхідно акцентувати увагу на проблемах безпеки. При розробці протоколу IPv4 це був далеко не основний критерій, тому він мав багато вразливостей. З огляду на те, що протокол IPv4 використовувався протягом багатьох років, більшість недоліків, що йому притаманні усувались по мірі їх виявлення, і ці практики добре себе зарекомендували. Та, на час впровадження IPv4, мережі були досить невеликі, і це було не так критично, враховуючи масштаби сучасних мереж, подібні помилки можуть призвести до серйозніших наслідків.

Тому, темою роботи стало дослідження рівня безпеки мережевого протоколу IPv6. Основна мета досліджень – підвищення рівня безпеки комп’ютерних мереж, що працюють із мережевим протоколом IPv6. У роботі розглянуто реалізацію безпеки протоколу IPv6, що спирається на досвід, накопичений через використання IPv4; загрози та вразливості протоколу, на базі обладнання cisco та juniper.

Результати роботи можуть використовуватись в процесі впровадження протоколу мережевого рівня IPv6 на обладнані вищезгаданих виробників для підвищення рівня безпеки.

1 НАУКОВО ТЕХНІЧНА ПРОБЛЕМА

Дослідження проведені співробітниками Arbor Networks разом із Університетом Мічиган, Міжнародним Інститутом Комп'ютерних Наук, Verisign Labs та Університетом Іллінойс свідчать про те, що за останні роки все-таки здійснено прорив у впровадженні протоколу IPv6 [1]. Для оцінки ситуації вибрано сім основних показників, що представлені на рис. 1.1.

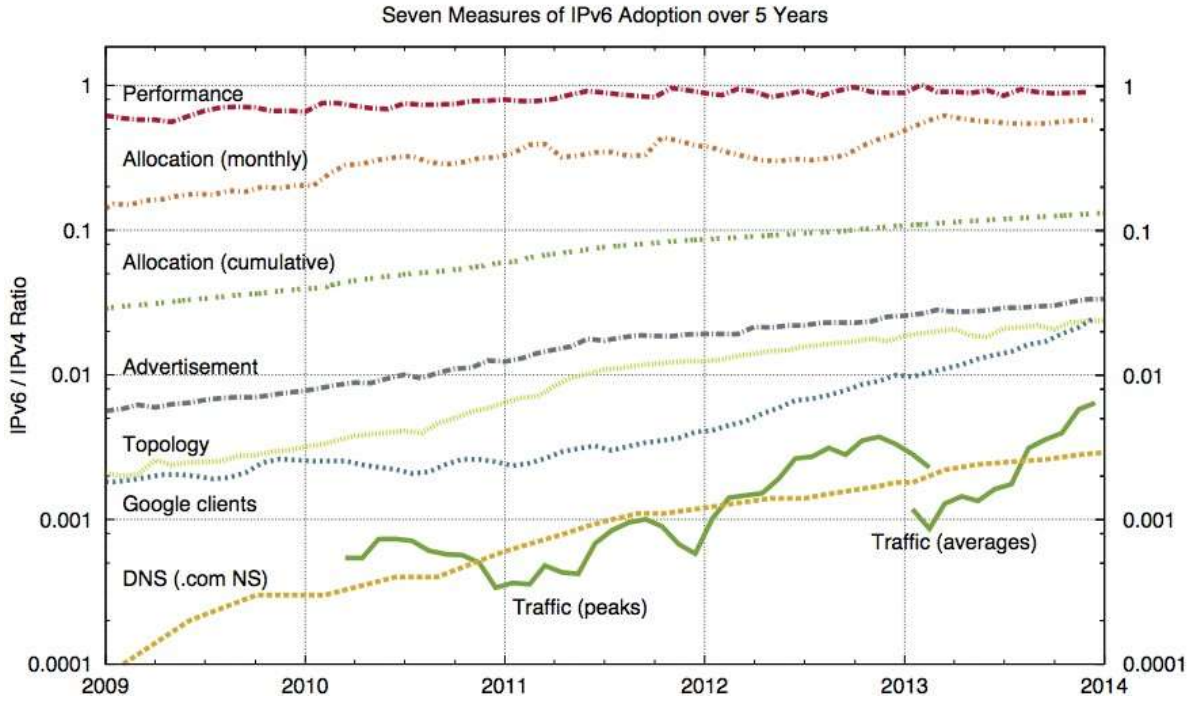


Рисунок 1.1 – Сім показників адаптації до протоколу IPv6

Та не зважаючи на це, протокол мережевого рівня IPv6 є не досить розповсюдженим, про що свідчать статистичні дані. Лише 14% сервіс провайдерів закінчили впровадження IPv6 у своїх мережах, в той час як лише 4% почали пропонувати IPv6 своїм кінцевим користувачам [2].

Про стовідсоткову готовність до роботи з новим мережевим протоколом заявляє компанія Google. Як відомо, її пошукова система та сервіси найпопулярніші серед кінцевих користувачів, тому компанія Google

збирає і свою статистику. За її даними, станом на закінчення 2014 року, відсоток користувачів, що використовують сервіси Google через IPv6 складає 4.24% [3]. На рис. 1.2 видно, що тенденція використання IPv6 щороку збільшується.

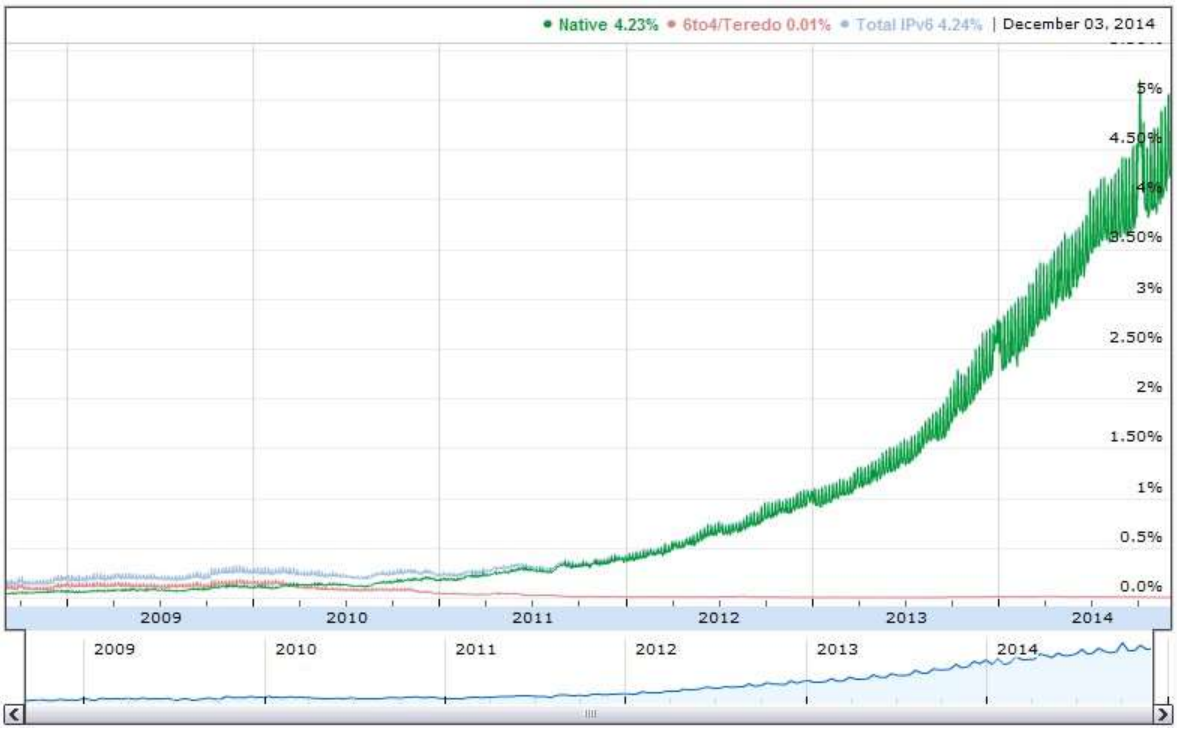


Рисунок 1.2 – Статистичні дані компанії Google з використання IPv6

Нещодавно для стимулювання впровадження IPv6 вступив у силу спеціальний протокол для регіональних реєстраторів. Тепер новий блок адрес IPv4 буде надаватись лише у тому випадку, коли компанія доведе, що вже впровадила протокол IPv6 у своїй мережі. Тобто, якщо з'явиться необхідність у публічних адресах IPv4, доведеться впровадити IPv6.

Всі ці дані свідчать про те, що впровадження протоколу поступово відбувається, і використовуються всі можливості для прискорення цього процесу.

На сьогодні безпека протоколу IPv6 є однією з основних проблем, що гальмують його поширення . Так як на даний момент цей протокол не

використовується в мережах за замовчуванням (відбувається поступова міграція з IPv4 на IPv6), немає ні найкращих практик та рекомендацій для мережевих адміністраторів, ні будь-яких гарантій, що реалізовані стеки протоколів IPv6 і методи забезпечення безпеки не мають помилок [4].

Задача зводиться до аналізу специфікації мережевого протоколу IPv6, пошуку можливих проблем та загроз, їх дослідження на базі тестової лабораторії. По результатам досліджень необхідно здійснити пошук можливих методів усунення небезпек та вразливостей і здійснити порівняльний аналіз для обладнання двох виробників.

2 АНАЛІЗ СПЕЦИФІКАЦІЙ ПРОТОКОЛУ IPV6

IPv6, який іноді називають IP наступного покоління, – це нова версія протоколу IPv4, яка визначає числові адреси пристроїв у мережі та дозволяє спілкуватися між ними. Потреба в новій версії протоколу IP виникла з деяких питань, пов'язаних із мережами на базі IPv4 та зростаючою кількістю мереж, які потребують доступу до Інтернету, що створило дефіцит IPv4-адрес. У першому триместрі 2011 року ICANN оголосила, що останній доступний блок IPv4-адрес був виданий. Незважаючи на те, що користувачі можуть і не потребувати публічної IP-адреси для підключення до Інтернету, цей дефіцит є проблемою для компаній та великих мереж, які потребують публічних IPv4-адрес. IPv6 вирішує цю проблему, надаючи теоретичний максимум 2 ^ 128 адрес [5].

2.1 Адресація IPv6

Адреси IPv6 мають 128 біт, тоді як адреси IPv4 – лише 32 біти.

IPv6 full address	IPv6 short form
2001:0db8:3c4d:0004:0213:72ff:fe7b:3cde	2001:db8:3c4d:4:213:72ff:fe7b:3cde
2001:0db8:85a3:0000:0000:8a2e:0370:7334	2001:db8:85a3:0:0:8a2e:370:7334
	2001:db8:85a3::8a2e:370:7334
ff01:0000:0000:0000:0000:0000:0000:0001	ff01:0:0:0:0:0:0:1
	ff01::1
0000:0000:0000:0000:0000:0000:0000:0001	0:0:0:0:0:0:0:1
	::1

Рисунок 2.1 – Приклад IPv6-адрес

Кожна IPv6-адреса записується, використовуючи усього 32 шістнадцяткових числа, згрупованих у набори з чотирьох шістнадцяткових чисел, розділених двокрапками (полями). Типова IPv6-адреса наведена нижче.

2001: 0db8: 3c4d: 0004: 0213: 72ff: fe7b: 3cde

Зважаючи на те, що адреси IPv6 довгі, є два способи зменшити розмір їх представлення: (1) «провідні 0» опускаючи послідовні нулі послідовно у кожному полі, і (2) "All-0s" робиться замінивши одну групу послідовних полів, що містять лише нулі двома двокрапками (: :). На рисунку 2.1 представлений приклад IPv6-адрес [5].

2.2 Префікс IPv6

IP-префікси адрес розділяють адреси на розділ мережі та розділ інтерфейсу. IPv6 робить не використовуйте слово хост для опису частини адреси IPv6, призначеної для хостів, але інтерфейс, оскільки пристрій (хост) може мати більше одного інтерфейсу. Стандартний префікс в IPv6 розбиває адреси на дві половини по 64 біти кожна. Ліва половина – це мережева частина, а частина – увімкнена праворуч – частина інтерфейсу. Префікс може змінюватися, щоб призначити більше бітів мережевій частині і менше до частини інтерфейсу [4].

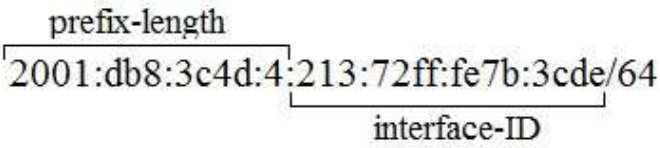


Рисунок 2.2 – Префікс IPv6

Однак опис частини інтерфейсу зберігається в 64 біт, що дозволяє зберігати достатньо місця для автоматичного генерування IPv6-адрес, і

використовує модифікований EUI-64 процес, що вимагає розмір 64 біт в частині інтерфейсу.

2.3 Типи адрес IPv6

Протокол IPv6 визначає три основні типи IP-адрес, серед яких Unicast, Multicast та Anycast. Трансляції IPv4, які використовуються для деяких функцій мережі, були замінені спеціальними типами багатоадресної IPv6 адреси. IANA зарезервувала префікс для кожного типу адреси IPv6.

First 12 bits	IPV6 Prefix	Allocation	Type
0000 0000 0000 0000	::/8	Unspecified and loopback	Unicast
0010 0000 0000 0000	2000::/3	Global unicast addresses	Unicast/Anycast
1111 1110 1000 0000	FE80::/10	Link-local unicast addresses	Unicast
1111 1110 0000 0000	FEC0::/7	Unique local unicast addresses	Unicast
1111 1111 0000 0000	FF00::/8	Multicast addresses	Multicast

Рисунок 2.3 – Типові адреси IPv6 та їх префікси

Це також дозволяє легко визначити тип адреси IPv6 за його префіксом. На рисунку 2.3 описуються деякі типові адреси IPv6 та їх префікси [5].

2.3.1 Однонаправлена адреса

Адреса Global Unicast – це унікальні глобальні IP-адреси, які можна перенаправляти через Інтернет.

Глобальні унікальні адреси еквівалентні IPv4-загальнодоступним адресам. Як описано в таблиці 2, адресам Global Unicast присвоюється діапазон 2000 :: / 3. Формат глобальної індивідуальної адреси дозволяє агрегувати префікс маршрутизації, що сприяє зменшенню розміру таблиць маршрутизації.

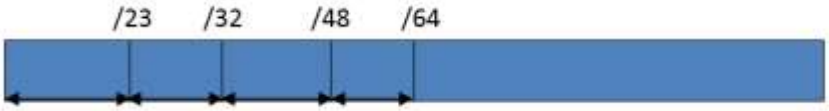


Рисунок 2.4 – Формат глобального префіксу однонаправлених адрес

Навіть незважаючи на те, що IETF не вказав довжину префікса для мереж різних розмірів, тоді використовується RIR, як ARIN, при призначенні глобальних однонаправлених адрес [6]:

- Префікс реєстру: перші 23 біти (/ 23) визначають регіональні Інтернет-регістри (RIR) до якої належить адреса. Всього існує 5 RIR у світі, а IANA призначає простір IP-адреси для кожної з них за допомогою 23 Register Prefix.
- Префікс провайдера: Наступні 9 біт (/ 32) будуть використані відповідним RIR для присвоєння блоку IP-адрес до провайдерів. Призначена IP-адреса включає 23-бітний префікс RIR та наступні 9 біт в свою чергу ідентифікують провайдера. Інтернет-провайдери, що спілкуються з іншими провайдерами можуть просто обміняти свій префікс на маршрутний трафік.
- Префікс сайту: Інтернет-провайдер використовує наступні 16 біт (/ 48) для виділення префікса сайту, що робить його 48-бітовим префіксом з унікальним ідентифікатором.
- Підмережа: Нарешті, користувачі можуть використовувати наступні 16 біт для створення підмереж у межах організацій. 16 біт дозволяють створити до 65535 підмереж.

Цей тип IP-адрес унікальний і дійсний лише в межах посилання. Трафік від цього IP до іншої адреси не можна перенаправити в Інтернет. Ці адреси часто самостійно присвоюються IPv6 коли увімкнено пристрій, що використовує процес автоматичної конфігурації, але його також можна налаштувати вручну. Усі інтерфейси IPv6 повинні мати принаймні локальну

однонаправлену IP-адресу. Маршрутизатори IPv6 перенаправляють свої локальні IP-адреси і посилають повідомлення маршрутизатора NDP.

2.3.2 Multicast addresses

Ці адреси призначені для адреси інтерфейсів у межах всієї приватної мережі і вважаються еквівалентом приватних адрес IPv4. Ці IP-адреси не можуть бути маршрутизовані до Інтернету, але, як очікується, вони будуть унікальними для кожної організації, оскільки їх достатньо IPv6 адрес для цього.

Вбудовані IPv4 (кодовані NSAP адреси) Ці адреси були розроблені для забезпечення сумісності з IPv4, IPX та мережевою службою для доступу під час переходу до IPv6 [7].

Багатоадресні адреси ідентифікують групи інтерфейсів, тому вони використовуються для доставки пакетів одночасно на декілька інтерфейсів, подібні до адрес багатоадресної передачі в IPv4. Багатоадресна адреса є Інтерфейс один до багатьох та IPv6 можуть належати до багатьох груп багатоадресної передачі. Основна відмінність між IPv4 Multicast та IPv6 Multicast адресами є те, що останні використовують мережеві ресурси більш ефективно. Також багатоадресна адреса в IPv6 замінює деякі функції мережі, в свою чергу IPv4 використовує широкомовну адресу. На рисунку 2.4 перераховано деякі адреси для групової передачі, які визначаються IETF та їх сферами застосування.

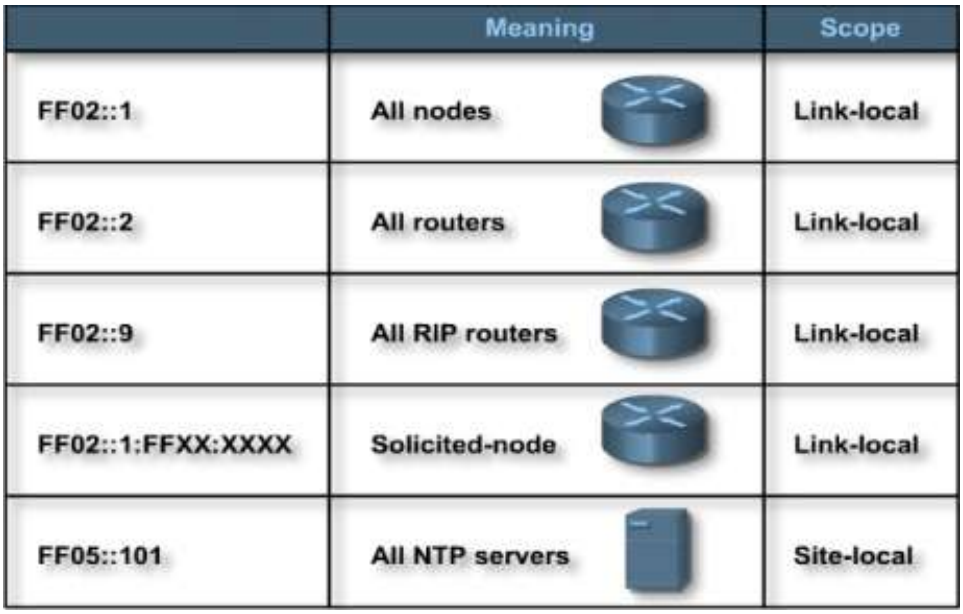


Рисунок 2.4 – Групова передача

Групова передача важлива для IPv6, оскільки вона є ядром багатьох функцій IPv6, щоб встановити автоматичну конфігурацію. IPv6 адресам групової передачі присвоюється префікс “FF00 :: / 8”. Перший і другий параметр встановлюються на всі 1; третій параметр – це прапор, який визначає тип адреси групової передачі (0 для постійної або 1 для непостійної); а четвертий параметр встановлює обсяг адреси. Область може бути встановлена одним із наступних значень [7]:

- 1 для області інтерфейсу;
- 2 для області посилання;
- 3 для локальної підмережі, де підмережі можуть охоплювати декілька посилань;
- 4 для локальної адміністративної сфери;
- 5 для різних типів сайту;
- 8 для організаційної сфери (кілька сайтів однієї організації);
- E для глобальної сфери.

Наприклад, адреса групової адреси, що починається з FF02 :: / 16, є постійною адресою групової передачі (0) зі зв'язково-локальним розмахом (2). І решта 112 біт у групової адреси є груповий ідентифікатор.

IANA не призначає конкретний блок IPv6 адрес для адрес Anycast. IPv6 будь-які адреси реалізуються за допомогою глобальних одноадресних адрес шляхом їх присвоєння більше ніж один інтерфейс. Коли пакет надсилається на адресу Anycast, він спрямовується до найближчого інтерфейсу. У межах WAN відстань, обчислена маршрутизацією використовується для визначення найближчого інтерфейсу. У локальній мережі найближчим інтерфейсом є перший сусід який «спілкується» з інтерфейсом відправника. Деякі характеристики адрес Anycast [7]:

- Адреси Anycast виділяються з адресного простору Unicast, тому вони є відмінні від одноадресної адреси. При призначенні інтерфейсу він повинен знати що IP-адреса – це адреса Anycast.
- У IPv6 Anycast визначається як спосіб надіслати пакет до найближчого інтерфейсу, який є член групи Anycast.
- Присвоєння декілька адрес Anycast: маршрутизатор-підмережа Anycast та Mobile домашній агент IPv6 Anycast.
- Адреса Anycast не повинна використовуватися в якості адреси джерела пакета IPv6.
- Адреси Anycast рідко використовуються, і досвіду їх використання не існує.

2.4. Механізми автоматичної конфігурації IPv6

IPv6 визначає два механізми автоматичної конфігурації IP-адреси: стан та стан без стану. Механізм без стану (SLAAC) дозволяє хостам генерувати власні IP-адреси. Цей механізм використовує мережеву інформацію,

рекламовану маршрутизаторами в пакетах, які називаються «NDP Router Advertisements», які включають префікс підмережі для посилання. Хости отримують цю інформацію та генерують IPv6 адресу, що поєднує префікс і автоматично створений ідентифікатор інтерфейсу. За відсутності маршрутизаторів, хост може генерувати лише свої локальні адреси посилань. Однак локальні адреси є лише локальними і цього достатньо для спілкування між вузлами у тому самому посиланні [8].

Механізм стану допомагає хостам отримувати інформацію про конфігурацію мережі з сервера (Сервер DHCPv6). Різниця між конфігурацією без стану і станом полягає в тому, що Сервер DHCPv6, який надає службові послуги, запам'ятовує стан клієнта від одного запиту до іншого.

Служба без хоста не зберігає жодної державної інформації. DHCPv6 також може використовуватися для дозволу хостів використовуючи конфігурацію без стану для отримання додаткової мережевої інформації. Для цього документу він визначає, що механізм без хоста використовується, коли сайт не особливо стосується точності адреси хостів, які використовуються, якщо вони унікальні та правильно маршрутизовані. Використовується сервер DHCPv6 коли сайт вимагає більш жорсткого контролю за точним визначенням адреси.

2.5 Процес автоматичної конфігурації

Важливо зрозуміти процес, який хост виконує для автоконфігурування IPv6-адрес. ORACLE / Sun Microsystems в посібнику з адміністрування IPv6, описує процес автоматичної конфігурації наступним чином [9]:

Автоконфігурація починається, коли ввімкнено інтерфейс, сумісний з багатоадресною передачею, наприклад, під час запуску системи. Вузли, як хости, так і маршрутизатори, починають автоматичну конфігурацію,

генеруючи локальну адресу для інтерфейсу. Локальна адреса посилання формується додаванням ідентифікатора інтерфейсу до відомого префікса локального зв’язку.

Вузол повинен спробувати перевірити, що «орієнтовна» локальна адреса посилання ще не використовується іншим вузлом по посиланню. Після перевірки може бути призначена локальна адреса посилання інтерфейсу. Зокрема, вузол надсилає сусідові запити повідомлення, які містить адреса посилання. Якщо інший вузол вже використовує цю адресу, вузол повертає повідомлення сусіда, вказуючи, що він використовує цю адресу. Якщо інший вузол намагається використати ту саму адресу, вузол також надсилає сусідові запит для визначення адреси. Кількість передач чи повторних передач сусідніх запитів та затримка між послідовними запитами, є специфічними для зв'язку.

Якщо вузол визначає, що його орієнтовна локальна адреса посилання не є унікальною, автоконфігурування зупиняється, і тоді необхідна ручна конфігурація інтерфейсу. Щоб спростити процедуру наприклад, адміністратор може надати альтернативний ідентифікатор інтерфейсу, який переосмислює ідентифікатор за замовчуванням. Тоді механізм автоматичної конфігурації можна застосувати за допомогою нового унікального ідентифікатора інтерфейсу. Як альтернатива, локальні посилання та інші адреси потрібно налаштувати вручну.

Після того, як вузол визначить, що його орієнтовна локальна адреса посилання є унікальною, вузол призначає адресу інтерфейсу. У цей момент вузол має підключення на рівні IP сусідніх вузлів. Решта етапів автоматичної конфігурації виконуються лише хостами.

Наступна фаза автоматичної конфігурації включає отримання доступу маршрутизатора або визначає відсутність маршрутизаторів. Якщо маршрутизатори є, тоді надсилається повідомлення, яке визначає тип автоматичної конфігурації хоста. Якщо маршрутизатори присутні, викликається «DHCPv6».

Маршрутизатори періодично надсилають пакети. Однак затримка між послідовними пакетами, як правило, довші, ніж хост, який виконує автоматичну конфігурацію.

Щоб швидко отримати пакет, хост надсилає один або кілька маршрутизованих запити на багатоадресні маршрутизатори. Повідомлення маршрутизатора містить два прапори, які вказують на тип автоматичної конфігурації. Конфігурація керованої адреси вказує, чи повинні хости використовувати «DHCPv6» для отримання адрес. Інший вказівник конфігурації стану вказує, чи повинні хости використовувати DHCPv6, виключаючи адреси. Повідомлення з маршрутизаторів містять префікс та [довжина префікса] інформація [використовується під час].

Після того, як визначено IP-адресу, вона повинна бути перевірена на унікальність перед призначенням інтерфейсу. Унікальність адреси визначається насамперед символом ідентифікатора інтерфейсу. Таким чином, якщо вузол вже перевірив унікальність link-local адреса, додаткові адреси не потрібно перевіряти окремо [якщо такі є створено з того ж ідентифікатора інтерфейсу]. На відміну від усіх адрес, які були отримані вручну слід перевіряти індивідуально. Щоб прискорити автоматичну конфігурацію, хост може генерувати свою локальну адресу посилання та перевірити його унікальність, в той час як хост чекає повідомлення з маршрутизатора. Маршрутизатор може затримати відповідь на маршрутизатор на кілька секунд. Отже, загальний час, необхідний для завершення автоконфігурації, може бути значно довшим, якщо два кроки виконуються послідовно [10].

2.6 Безпека IPv6

Перш ніж вивчити безпеку в IPv6, ми наведемо короткий опис загального мережевого рівня безпеки.

Атака відмови в обслуговуванні (DOS): У цій формі атаки зловмисник намагається заблокувати авторизованих користувачів, які мають доступ до певного комп'ютера чи послуги. Трансляція повідомлень, також відомі як атака «Смурфа», є прикладом атаки DOS.

Напад «Людина в середині» (MITM): У цій атаці зловмисник розміщує себе в середині між двома користувачами, які спілкуються. Зловмисник гарантує, що весь трафік між користувачами проходять через нього і здатний бачити весь трафік. Через відсутність належного механізмами аутентифікації в IPv4 ці атаки можна легко здійснити.

Атаки фрагментації: Ці атаки використовують спосіб обробки певних систем з великим розміром IP-пакетів. Пінг «death attack» – приклад такого типу нападу, в якому використовується багато малих фрагментів пакетів ICMP, які при повторному зібранні в пункті призначення перевищують максимально дозволений розмір для IP-дейтаграми. Це може спричинити збій системи [10].

Розвідувальна атака: у цій атаці нападник намагається дізнатися якомога більше про мережу цілі. Сканування – це техніка, яка використовується для цієї мети, і яка виявляє відкриті порти та іншу мережеву інформацію. Оскільки адресний простір IPv4 невеликий, він є простіший для сканування всього адресного простіру.

ARP poisoning and ICMP redirect: підробка ARP – це техніка підробки фальшивих ARP повідомлень в мережі. Зловмисник оновлює кеш ARP хоста з неправдивою інформацією через підроблені відповіді ARP. Ця методика відома як отруєння ARP (Fewer, 2007). Перенаправлення ICMP повідомляє системі використовувати альтернативний шлях. Це зазвичай використовується маршрутизаторами для хосту, коли він надсилає пакети до іншого шлюзу неправильні пакети на маршрутизатор. Підробляючи повідомлення про переадресацію ICMP, зловмисник може змінити таблицю маршрутизації в хост-системі.

2.6.1 Огляд безпеки IPv6 і IPv4

Відомі проблеми безпеки IPv4 були враховані під час проектування IPv6. Розглянемо враховані зауваження в IPv6 [11]:

Проміжні пристрої не дозволяють фрагментувати пакети та забороняють перекриття фрагментами пакетів, гарантується, що фрагменти можуть виконувати лише пристрої джерела. Причому, якщо повторно зібрані пакети були менше 1280 октетів, тоді пристрої, як передбачається, скидають їх, оскільки будь-який рівень зв'язку даних, що передає дані IPv6, повинен бути здатний доставляти IP пакет, що містить 1280 байт або менше, без необхідності викликати кінцеву фрагментацію на рівні IP. Ці рекомендації забезпечують краще пом’якшення атаки фрагментації.

«The broadcast storms», які впливали на IPv4, були видалені. Натомість Multicast та Anycast замість їх. Щоб пом'якшити широкомовні атаки, RFC2463 вказує це «Повідомлення ICPMv6 не повинні генеруватися, як відповідь на пакет з IPv6 адреси призначення багатоадресної передачі, зокрема адреса багатоадресної передачі на рівні каналів зв'язку або широкомовна трансляція рівня адреси.»

Усі повністю сумісні пристрої IPv6 мають право підтримувати IPSec. Протокол IPv4 повинен був модернізувати заголовки IPSec в оригінальний кадр IPv4, але IPv6 має можливість підтримувати IPSec за допомогою заголовків розширень (Kaeo, 2006).

2.6.2 Проблеми безпеки IPv6

Незважаючи на зусилля дизайнерів щодо створення інтернет-протоколу із вбудованою безпекою, IPv6 має деякі проблеми безпеки. Важливо пам’ятати, що IPv6 не є панацеєю безпеки [11].

Розвідувальні атаки

Великий пул адреси IPv6 утрудняє перевірку пінгу та сканування портів. Однак, нові широкополосні адреси в IPv6 дозволяють противнику знаходити певний набір ключових систем (маршрутизаторів) легше. Більше того, якщо адміністратори призначають легко запам’ятовуванні адреси ключовим системам, атака стає набагато легшою.

Атаки через автоматичну конфігурацію

Як описано вище, у режимі автоматичної конфігурації адреси без стану (SLAAC), маршрутизатор транслює 64-бітну глобальну адресу, а вузол генерує решта 64 біт для його інтерфейсу. Вузли (хости та маршрутизатори) використовують Neighbor Discovery для декількох функцій, таких як знаходження сусідніх маршрутизаторів для переадресації пакетів та відстеження доступних сусідів (Нарте, Nordmark & Simpson, 1998). Зловмисник може використовувати цю функцію, щоб показувати себе як маршрутизатор і отримувати весь трафік від цілі.

Одним із кроків процесу автоматичної конфігурації в IPv6 є те, що інтерфейс виконує DAD (Виявлення дублікатів адреси), щоб переконатися, що жоден інший вузол не має тієї ж IP-адреси. Зловмисник у посиланні може надіслати пакет відповідей із повідомленням, що він має довірену IP-адресу.

Інтерфейс генерує ще одну IP-адресу та повторює процес DAD. Якщо зловмисник продовжує надсилати відповіді на кожного DAD, система врешті-решт відмовляється і чекатиме інструкції конфігурацій. Це являє собою тип атаки DOS [6].

Ще одним недоліком автоматичної конфігурації є те, що шахрайський маршрутизатор може рекламувати глобальний префікс за посиланням, який має вузли в цій частині мережі, налаштовують свої IP адреси з глобальним префіксом IPv6. Тепер мережа стає відкритою для зловмисника.

Атака «людина в середині»

При такому нападі зловмисник за тим же посиланням, що і його ціль, може відповідати на багатоадресну передачу повідомлення, надіслане

цільовою адресою всім вузлам багатоадресної адреси із запитом MAC-адреси. Після отримання багатоадресного повідомлення зловмисник надсилає підроблену відповідь і приймає на себе передбачуваний транспортний потік між A і B (Caicedo, Joshi & Tuladhar, 2009). На рисунку 2.5 показано діаграму повідомлень, що надсилаються під час атаки такого типу [7].

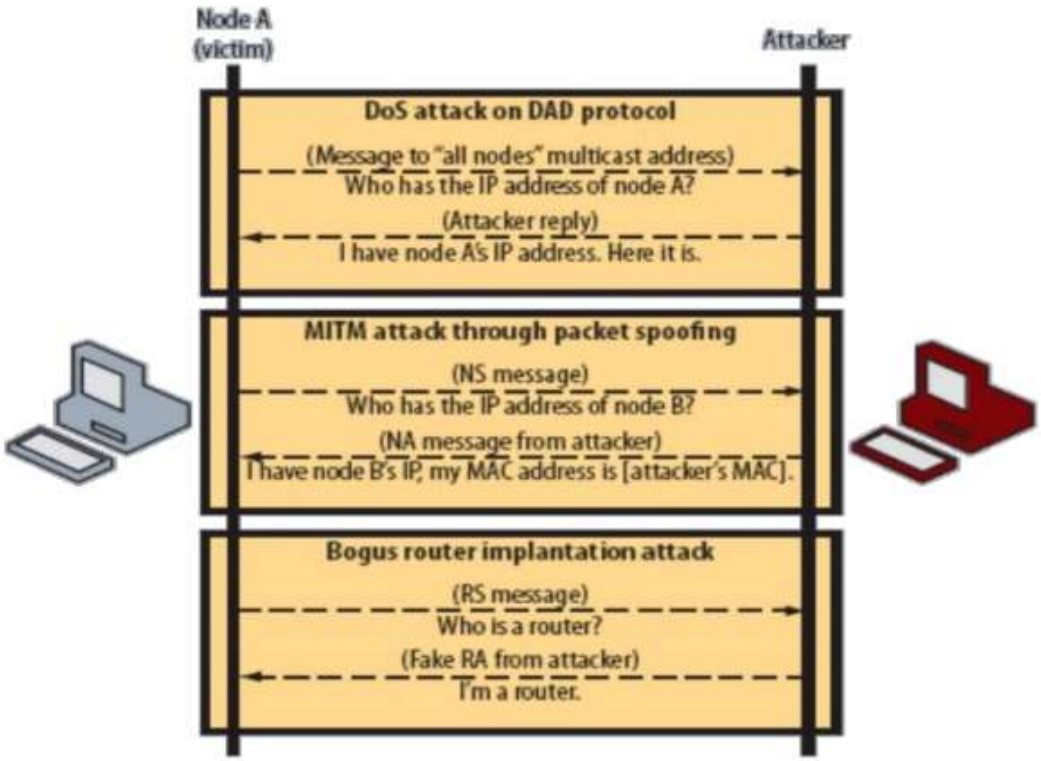


Рисунок 2.5 – Атаки на IPv6, пов'язані з процесом автоматичної конфігурації

Атака зловмисника на маршрутизатор

Ця функція IPv6 дозволяє зловмиснику змінювати заголовок IPv6 і вказувати шлях пакету до місця призначення. Трафік може бути спрямований через велику кількість вузлів на шляху до пункту призначення. Таким чином, це відкриває спосіб створення DoS-атаки. Зловмисник може використовувати цю функцію атакуючи певну частину мережі.

Проблеми, пов'язані з подвійним стеком

Сьогодні більшість мереж користувачів використовують IPv4. Існує три типи тунелів IPv6 – IPv4, які включають Teredo, 6to4 та протокол автоматичного тунельного адресації внутрішньомістового сайту (ISATAP). Ці тунелі дозволяють пакетам IPv6 інкапсулюватись всередині IPv4 та надсилати через підтримку IPv4 брандмауери або пристрої трансляції мережевих адрес (NAT) (Marshan, 2009). Таким чином, якщо брандмауери не є налагоджені для перевірки IPv6 трафіку всередині пакетів IPv4, зловмисники можуть скористатися тунелюванням, механізмом запуску атак в мережі.

ICMP та багатоадресна адресація

Мережевий адміністратор може фільтрувати весь ICMP і багатоадресний трафік в IPv4, щоб запобігти деяким атакам.

Однак ICMP і багатоадресна передача є невід'ємною частиною функціонування IPv6. Цю відповідальність адміністратори мережі вирішують, які ICMP та багатоадресними повідомленнями.

Інструменти, пов'язані з безпекою для IPv6

THC-IPv6 – це повний набір інструментів, який може бути використаний для перевірки властивих слабкостей протоколу в IPv6 та ICMPv6. Він включає такі інструменти [10]:

- parasite6: підробляння / супровід реклами ICMP. Це ставить зловмисника як «manin-the middle», такий же, як ARP «man-in-mid» (паразит).
- live6: ефективний інструмент сканування системи.
- fake_router6: Він оголошує зловмисника маршрутизатором в мережі з найвищим рівнем пріоритету.
- redir6: Він інтелектуально перенаправляє трафік до зловмисника (людина-посередині) за допомогою ICMP перенаправлення.
- toobig6: Це зменшує MTU з тимпринципом, що і redir6.

- detect-new-ip6: Він виявляє нові пристрої IPv6, які приєднуються до мережі. Він може запустити сценарій до автоматичного сканувати цієї системи.
- dos-new-ip6: Він виявляє нові пристрої IPv6 і повідомляє їм, що вибраний IP-файл забезпечує механізм з'єднання з мережею.
- fake_mld6: Він повідомляє про зловмисника у групі, що вибирає багатоадресну передачу.
- fake_mipv6: Він краде мобільну IP-адресу зловмиснику, якщо IPSEC не потрібен для аутентифікації.
- fake_advertiser6: Він надсилає підроблені повідомлення про зловмисника в мережі.
- smurf6: Локальний генератор атаки smurf.
- rsmurf6: Віддалений сніфер.

sendpees6: Він генерує запити на сусідів з великою кількістю криптографічних запитів генерованих адрес. Це тримає процесор зайнятим.

Серед інших інструментів, які використовуються для тестування функцій захисту протоколу, мережі або аналізу трафіку [7]:

- Інструменти пакетів: Snort, TCPdump, Sun Solaris snoop, Wireshark, Windump, WinPcap, NetPeek, SnifferPro, ngrep.
- Сканери: Halfscan6, Nmap, Netcat.
- Інструменти DOS: 6tunneldos, 4to6ddos.
- Підробники пакетів: Scapy6, SendIP, Packit.
- Інструменти моніторингу локальних мереж IPv6: Nagios, Argus, MRTG.
- Загальні засоби діагностики для Linux: tracepath6, traceroute6, ping6.

2.7 Тестовий режим захисту IPv6: напади та аналіз

Тепер, коли обговорення переходить на тестову планку IPv6, головна мета в цій роботі – переглянути IPv6 загрози безпеці та зрозуміння, як їх запобігти. Тестовий шар був налаштований за допомогою Cisco комутатора, концентратора, та п'яти настільних ПК та два ноутбуки [7].

Налаштування лабораторної мережі

У цьому тестовому шарі реалізовано три різних мережі. Перша мережа потребувала двох ПК з ОС Linux, які діяли, як маршрутизатори IPv6 та два ПК клієнта. Комп'ютери маршрутизатора надали маршрутизатор клієнтам для автоматичної конфігурації. На ПК, що використовуються як маршрутизатор, запускається Fedora Core 10 і кожен має два мережевих інтерфейси. Відомості про конфігурацію та команди для усунення несправностей перелічено в Додатку А: Конфігурація обладнання лабораторії. залежно від тесту, який слід виконати – ноутбук буде доданий до концентратора для здійснення атак.

Друга та третя мережі були реалізовані за допомогою комутаторів Cisco 3750, двох клієнтських ПК, і двох ноутбуків. Перед кожним тестом подається схема реалізованої мережі. Жодна з реалізованої мережі не підключені до Інтернету чи іншої зовнішньої мережі.

2.8 Фальшиві атака на маршрутизатор

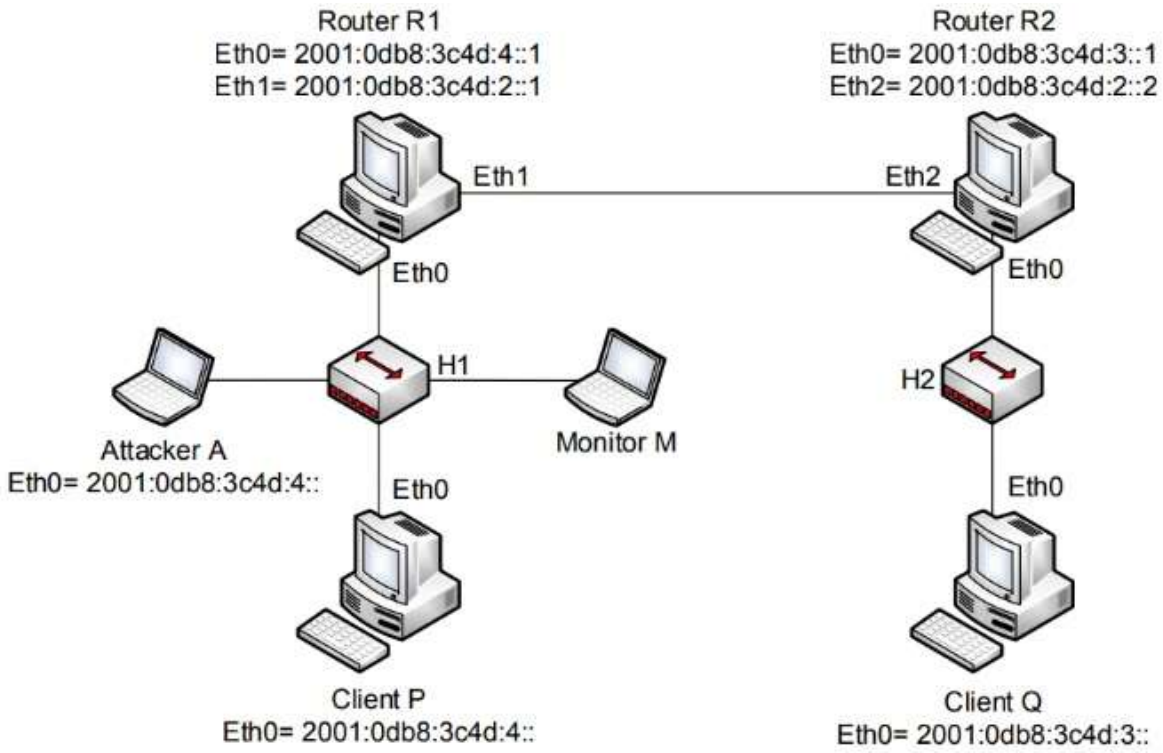


Рисунок 2.6 – Налаштування мережі для фальшивої атаки маршрутизатора

Цей експеримент виконується за допомогою інструментарію THC-IPv6. На рисунку 2.64 описано налаштування, де «P» робочий стіл – це цільовий клієнт, «Q» – робочий стіл – жертва, маршрутні пакети «R1 і R2», «H1» – концентратор, з'єднаний між "P" і "R1", "H2" – це концентратор, з'єднаний між "R2" і "Q", "A" – це зловмисник, а "M" – ноутбук для моніторингу [11].

Нормальна робота мережі IPv6

- Попередні умови
- Усі ПК вимкнено.
- Маршрутизатори вмикаються. Усі концентратори ввімкнено, а M підключений до H1.
- M не має жодних мережевих служб, таких як DHCP або DNS.
- M увімкнено і фіксує мережевий трафік на H1.

Експеримент

– Увімкніть комп'ютер "P" і "Q".

– Зачекайте, поки P і Q стабілізуються.

– P надсилає 10 пінгів до Q.

– Збережіть Capture як звичайний1_mmddyyyy_attempt # .cap.

Спостереження

На рисунку 2.7 показана інформація про пакет маршрутизатора, що висилається R1.

No.	Time	Source	Destination	Protocol Info
1	0.000000	fe80::213:72ff:fe7d:5419	ff02::1	ICMPv6 Router advertisement

Рисунок 2.7 – Інформація про пакет на маршрутизаторі з R1

Лістинг 2.1 – Frame 1 (110 bytes on wire, 110 bytes captured)

```
Ethernet II, Src: Dell_7d:54:19 (00:13:72:7d:54:19), Dst:
IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6
    0110 .... = Version: 6
        [0110 .... = This field makes the filter "ip.version==6" possible: 6]
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 56
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source: fe80::213:72ff:fe7d:5419 (fe80::213:72ff:fe7d:5419)
    Destination: ff02::1 (ff02::1)
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x3725 [correct]
    Cur hop limit: 64
    Flags: 0x00
        0... .... = Not managed
        .0.. .... = Not other
        ..0. .... = Not Home Agent
        ...0 0... = Router preference: Medium
    Router lifetime: 15
    Reachable time: 0
```

```
Retrans timer: 0
ICMPv6 Option (Prefix information)
    Type: Prefix information (3)
    Length: 32
    Prefix length: 64
    Flags: 0xc0
        1... .... = Onlink
        .1.. .... = Auto
        ..0. .... = Not router address
        ...0 .... = Not site prefix
    Valid lifetime: 2592000
    Preferred lifetime: 604800
    Prefix: 2001:db8:3c4d:4::
ICMPv6 Option (Source link-layer address)
    Type: Source link-layer address (1)
    Length: 8
    Link-layer address: 00:13:72:7d:54:19
```

No.	Time	Source	Destination	Protocol	Info
118	446.985111	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
119	451.036728	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
120	455.122211	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
121	458.848941	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
122	460.780681	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
123	460.783129	fe80::213:72ff:fe7d:5	ff02::1:ffdc:7d7b	ICMPv6	Neighbor solicitation
124	460.783300	2001:db8:3c4d:4:208:7	fe80::213:72ff:fe7d:5	ICMPv6	Neighbor advertisement
125	460.783307	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
126	461.782330	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
127	461.782630	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
128	462.783756	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
129	462.783775	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
130	463.781937	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
131	463.782247	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
132	463.822173	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
133	464.781850	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
134	464.782156	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
135	465.781736	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
136	465.782003	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
137	466.781665	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
138	466.781972	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
139	467.781584	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
140	467.781897	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
141	468.643870	fe80::213:72ff:fe7d:5	ff02::1	ICMPv6	Router advertisement
142	468.781479	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
143	468.781777	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply
144	469.781407	2001:db8:3c4d:4:208:7	2001:db8:3c4d:3:213:7	ICMPv6	Echo request
145	469.781723	2001:db8:3c4d:3:213:7	2001:db8:3c4d:4:208:7	ICMPv6	Echo reply

Рисунок 2.8 – Пінг, надісланий з P до Q

Фальшива атака на маршрутизатор

Попередні умови:

- Усі ПК вимкнено.
- Маршрутизатори вмикаються. Усі концентратори ввімкнено, а M підключений до H1.
- M не має жодних мережевих служб, таких як DHCP або DNS.
- M увімкнено і фіксує мережевий трафік на H1.

– Зловмисник "A" вимкнено та підключений до H1.

Експеримент [9]:

– Увімкніть комп'ютери "P" і "Q".
– Зачекайте, поки P і Q стабілізуються.
– Пінг від P до Q 10 разів.
– Увімкніть A і дочекайтеся його стабілізації.
– Запустіть фальшиву атаку маршрутизатора.
– Надішліть 10 пінгерів на Q від P
– Збережіть захоплення як Fakerouterattack1_mmddyyyy_count # .txt

No.	Time	Source	Destination	Protocol Info
1	0.000000	fe80::213:72ff:fe7d:5419	ff02::1	ICMPv6 Router advertisement

Рисунок 2.9 – Пакет розсилки першого маршрутизатора, розісланий R1

Лістинг 2.2 – Frame 1 (110 bytes on wire, 110 bytes captured)

```
Ethernet II, Src: Dell_7d:54:19 (00:13:72:7d:54:19), Dst:
IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 56
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source: fe80::213:72ff:fe7d:5419 (fe80::213:72ff:fe7d:5419)
    Destination: ff02::1 (ff02::1)
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x36e9 [correct]
    Cur hop limit: 64
    Flags: 0x00
        0... .... = Not managed
        .0.. .... = Not other
        ..0. .... = Not Home Agent
        ...0 0... = Router preference: Medium
    Router lifetime: 75
    Reachable time: 0
    Retrans timer: 0
    ICMPv6 Option (Prefix information)
        Type: Prefix information (3)
        Length: 32
        Prefix length: 64
        Flags: 0xc0
            1... .... = Onlink
            .1.. .... = Auto
```

3 ДОСЛІДЖЕННЯ РІВНЯ І ФОРМУВАННЯ МЕТОДИКИ РІВНЯ БЕЗПЕКИ ПРОТОКОЛУ

При проектування комп’ютерної мережі виникають питання безпеки нашої мережі, тому для нам потрібно провести аналіз безпеки і визначити вразливість нашої мережі, а також провести аналіз вразливостей мережі. За допомогою графів атак можна змоделювати сценарії можливих атак на мережу, і зокрема дати оцінку вразливості об’єкта дослідження. У сукупності ці підходи дозволяють оцінити рівень безпеки мережі [10].

Щоб зробити перевірку рівня безпеки комп’ютерної мережі потрібно:

- виконати побудову графа;
- виявити вразливості «вузьких місць» в захисті;
- розрахувати показники;

– привести отримані метрики до вимог для посилення безпеки.

Для аналізу захищеності мережі, потрібно провести аналіз безпеки проектованої комп'ютерної мережі. Дані аналізу, в свою чергу дадуть розробити рекомендації по підвищенню безпеки.

3.1 Розгортання в тестовій лабораторії

Для того, щоб провести тестування нашої мережі потрібно розгорнути тестову лабораторію. Моделювання проведемо за допомогою програмного забезпечення під управлінням Unix операційних систем. Тестування проведемо наближено де реальних умов.

Наведемо типи пристроїв і операційних систем, які були використані для моделювання віртуальної мережі (таблиця 3.1).

Таблиця 3.1 – Типи пристроїв і операційних систем

Тип пристрою	Назва пристрою (hostname)	Операційна система
Маршрутизатор	R1cisco, R2cisco	IOS 15.4S
	R1jun, R2jun	Virtual JunOS 12.0
Комутатор	SWcisco	CatOS 12.2
	SWjun	Virtual JunOS 12.0
ПК (Кінцеві пристрої)	PC1–c, PC1–j	Windows 7
	PC2–c, PC2–j	Windows 8
	PC3–c, PC3–j	Ubuntu

Щоб провести тестування нашої мережі, проведемо віртуальну емуляцію, за допомогою «IOS Cisco Juniper і OS Vjun». Віртуальна емуляція

була проведена за допомогою VMware під керівництвом операційних систем Ubuntu і Windows (7-8).

За допомогою утиліти «Scapy» було проведено моделювання атаки на мережу, вона в свою чергу дає можливість подивитись звіти, які в свою чергу дають можливість провести аналіз атак. Для того щоб відстежити повідомлення було використано утиліту «tcpdump».

При моделюванні нашої комп'ютерної мережі, було використано мережеві інтерфейси «Ethernet», які в свою чергу дають обмеження на використання віртуально обладнання. Зокрема всі пристрої знаходяться в одній віртуальній мережі. Атака яка проводилась зображена схематично на рисунку 3.1.

При моделюванні внутрішньої і зовнішньої атаки ми використали програмне забезпечення «Cisco і Juniper». Було використано технологію тунелювання з використанням протоколу IPv4.

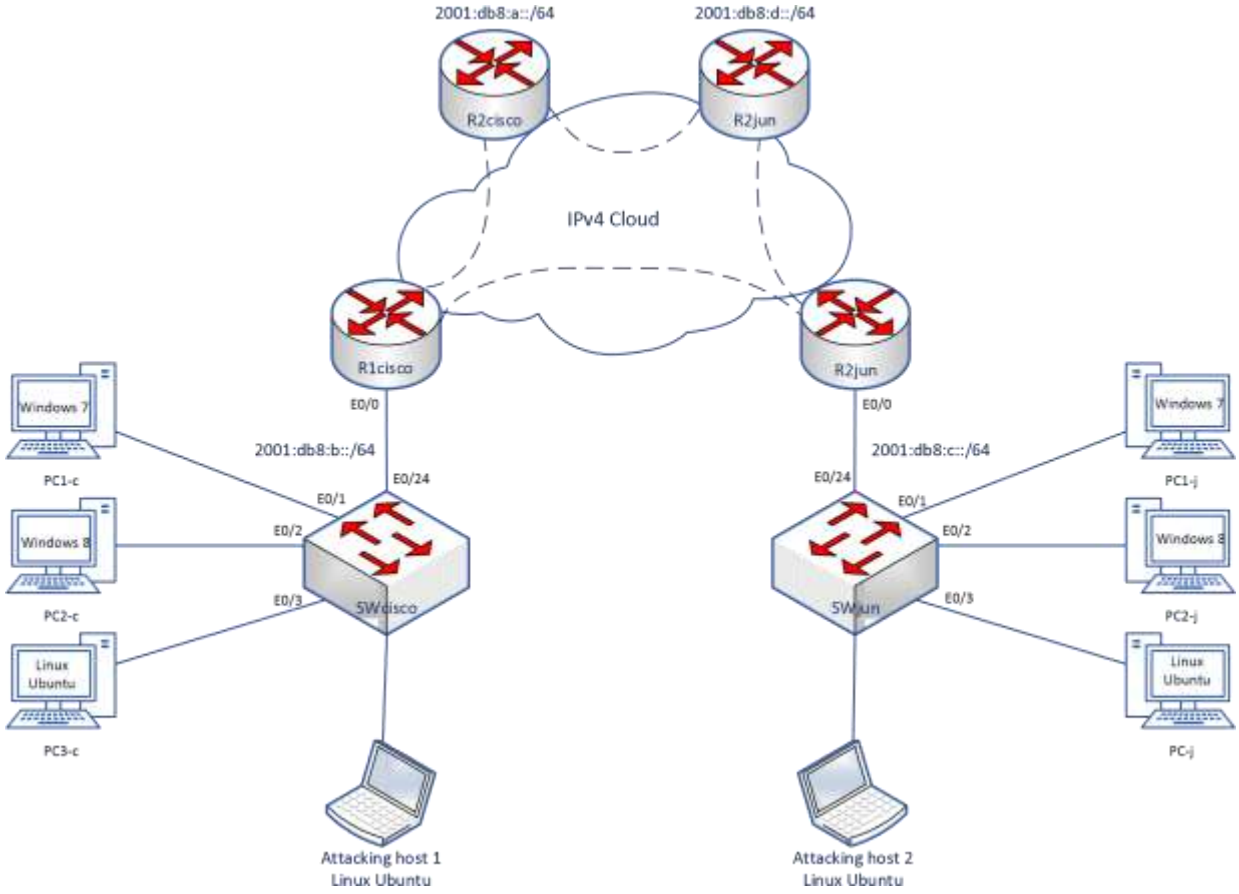


Рисунок 3.1 – Топологія віртуальної мережі

В таблиці 3.2 наведено адресна схема з’єднань.

Саме тестування нашої мережі ми провели за допомогою двох етапів, які включали в себе виконання тестів без використання заходів безпеки і з використанням заходів безпеки. Це дасть змогу перевірити надійність і коректність роботи комп’ютерної мережі [11].

Таблиця 3.2 – Адресна схема з'єднань в локальних сегментах

Пристрій (hostname)	Інт–с	Фізична адреса	IPv6 адреса	Опис
R1cisco	Eth 0/0	aabb.cc00.6e00	fe80::a8bb:ccff:fe00:6e00	router to switch
			2001:db8:a::a8bb:ccff:fe00:6e00	
PC1-c		0030 0000 0201	fe80::2824:c9b8:895f:f78f	Link-local
			2001:db8::a:2824:c9b8:895f:f78f	Unicast global
PC2-c		0030 0000 0202	fe80::3834:c9b8:895f:f78f	Link-local
			2001:db8:a::3834:c9b8:895f:f78f	Unicast global
PC3-c		0030 0000 0203	fe80::0230:00ff:fe00:0203	Link-local
			2001:db8:a::0230:00ff:fe00:0203	Unicast global
R1jun	Eth 0/0	b0:a8:6e:aa:bb:cc	fe80::b2a8:6eff:feaa:bbcc	router to switch
			2001:db8:b:: b2a8:6eff:feaa:bbcc	
PC1-j		0030 0000 0204	fe80::4844:c9b8:895f:f78f	Link-local
			2001:db8:a::4844:c9b8:895f:f78f	Unicast global
PC2-j		0030 0000 0205	fe80::5854:c9b8:895f:f78f	Link-local
			2001:db8:a::5854:c9b8:895f:f78f	Unicast global
PC3-j		0030 0000 0206	fe80::0230:00ff:fe00:0206	Link-local
			2001:db8:a::0230:00ff:fe00:0206	Unicast global
Attacking host 1		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:a::105c:0fff:fe92:89c5	Unicast global
Attacking host 2		12:5c:0f:92:89:c5	fe80::105c:0fff:fe92:89c5	Link-local
			2001:db8:b::105c:0fff:fe92:89c5	Unicast global

Тестування.

За допомогою інтелектуальних методів в мережі IPv4 при пошуку наявних адрес унеможливлює ефективне використання, порівнюючи з

мережею IPv6, тому, що кількість загальних комбінацій може збільшитись до 264.

Утиліти alive6 яка використовувалась при дослідження в IPv6 проявила себе найбільш ефективніше. За допомогою цих методів ми створили сценарій повідомлення який зображено на рисунку 3.2.

```
src_ip = 'fe80::105c:0fff:fe92:89c5'

Packet1 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest()

Packet2 = IPv6(src=src_ip, dst="ff02::1") \
/ICMPv6EchoRequest(data=RandString(10))
```

Рисунок 3.2 – «Набір повідомлень для IPv6 Intelligence»

При виконання цього сценарію ми отримали результати:

– згідно «RFC 4443» у «Windows 7-8» в першому повідомленні немає відповіді, а в другому – відповідь про помилку;

– згідно «RFC 4443» ОС Ubuntu не задовольняє вимогам, і тому має вразливість на два повідомлення.

В зв'язку з цим тестуванням ми отримали адреси наших пристроїв, які зображені на рисунках 3.3-3.4.

Потрібно сказати, що за допомогою пасивного прослуховування можуть бути визначені кінцеві адреси наших пристроїв [12].

```
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=1 ttl=64 time=0.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=1 ttl=64 time=1.2 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=12.0 ms
(DUP!)
64 bytes from fe80::105c:0fff:fe92:89c5: icmp_seq=2 ttl=64 time=0.5 ms
64 bytes from fe80::2824:c9b8:895f:f78f: icmp_seq=2 ttl=64 time=11.0 ms
(DUP!)
```

Рисунок 3.3 – «Результат аналізу IPv6 (ОС Cisco)»

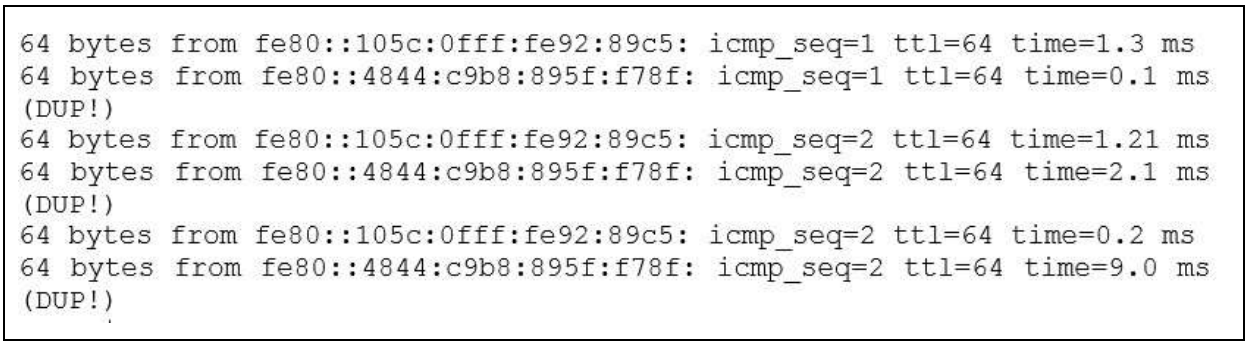


Рисунок 3.4 – «Результат аналізу IPv6 (ОС Juniper)»

На даний момент не має достатніх методів для запобігання

Не існує ефективних методів запобігання дослідження мережі, які не впливали б на роботу мережі. Заборона багатоадресних повідомлень не призведе до автоматичної настройки кінцевих пристроїв і пов'язаних з ними процедур; фільтрація повідомлень ICMPv6.

Smurf атака

Smurf – це мережевий рівень розподіленої атаки відмови в обслуговуванні (DDoS), названий на честь зловмисного програмного забезпечення DDoS.Smurf, що дозволяє виконувати його.

Атаки Smurf дещо схожі на пінг, оскільки обидва здійснюються шляхом надсилання пакетів запитів ICMP Echo.

Однак, на відміну від регулярного потоку пінг, Smurf є вектором атаки посилення, який збільшує свій потенціал збитку, використовуючи характеристики мереж мовлення. На рисунку 3.3 зображено типи «Smurf-атак» [12].

Таблиця 3.3 – Типи Smurf-атак

Назва	Адреса відправника	Адреса приймача
Smurf атака	Адреса жертви	*all-nodes* мультикаст
Зворотна Smurf атака	*all-nodes* мультикаст	Адреса жертви
Smurf затоплення	*all-nodes* мультикаст	*all-nodes* мультикаст

У стандартному сценарії хост А надсилає запит ICMP Echo (ping) на хост В, викликаючи автоматичну відповідь. Час, необхідний для отримання відповіді, використовується як міра віртуальної відстані між двома хостами.

У мережі широкомовної передачі даних IP-запит надсилається кожному хосту, що вимагає відповіді від кожного з одержувачів. Під час атак Smurf-атакуючі скористаються цією функцією, щоб посилити їхній атакуючий трафік.

На рисунку 3.5 показаний сценарій повідомлення.

```
Packet = IPv6(src=src_pc1, dst="ff02::1") \
/ICMPv6EchoRequest()
```

Рисунок 3.5 – Сценарій повідомлення для атаки Smurf

Сценарій атаки Смурфа може бути розбитий наступним чином:

- Зловмисне програмне забезпечення Smurf використовується для генерування підроблених запитів Echo, що містять підроблений IP-код джерела, який фактично є цільовим сервером.
- Запит надсилається до проміжної мережі широкомовної IP-адреси.
- Запит передається всім хостам в мережі.

– Кожен хост надсилає відповідь ICMP на адресу підробленого джерела.
– При достатній кількості відповідей ICMP пересилається цільовий сервер.

Коефіцієнт посилення атаки Смурфа корелює з кількістю хостів у проміжній мережі. Наприклад, мережа IP-трансляцій із 500 хостами створить 500 відповідей на кожен підроблений запит Echo. Зазвичай кожна з посилань має той самий розмір, що і вихідний запит ping.

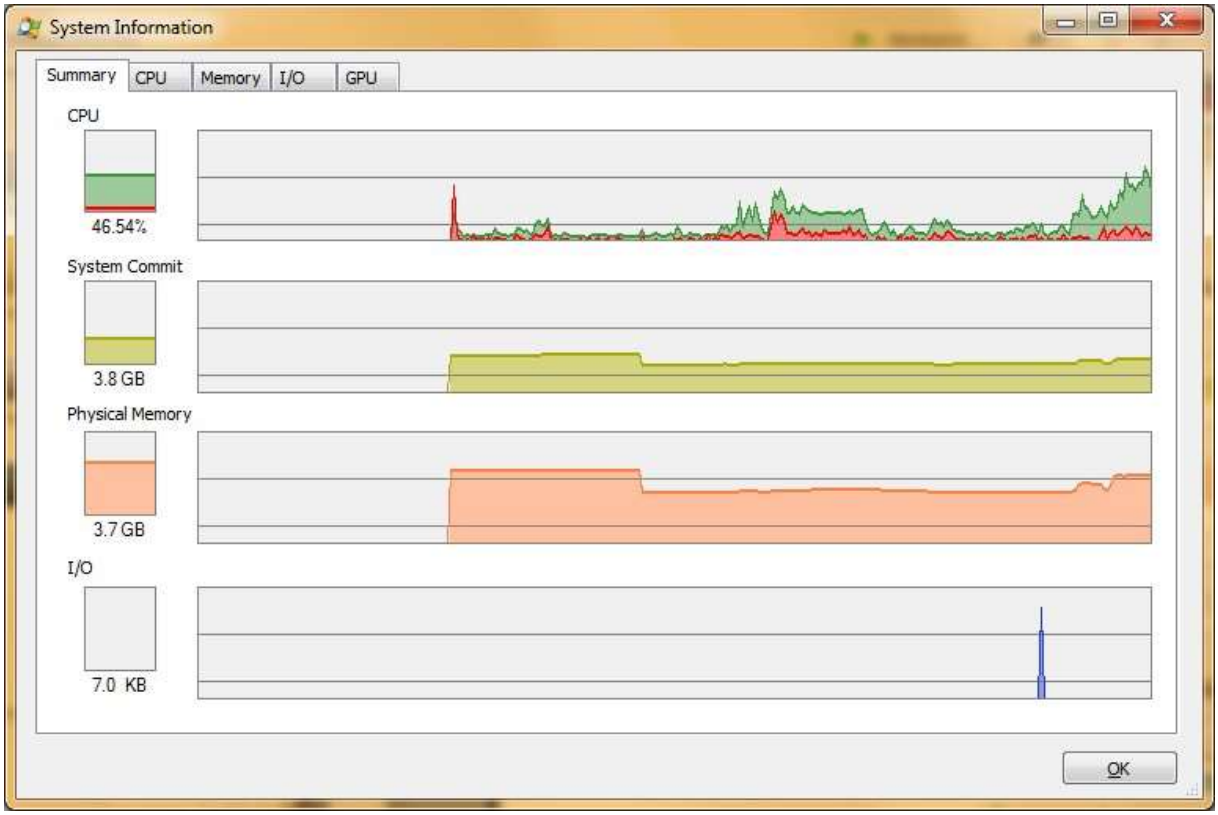


Рисунок 3.6 – Продуктивність завантаження Windows 7 при атаці Smurf

Слід зазначити, що під час нападу служба в проміжній мережі, ймовірно, буде зашумлена [11].

Окрім демонстрації в Інтернеті, це повинно стимулювати операторів забороняти їхнім мережам бути невідомими учасниками атаки Смурфа.

Для цього потрібно зробити:

- Вимкніти передачі, спрямовані на IP-адресу, на маршрутизаторі.
- Переконфігурувати свою операційну систему, щоб заборонити відповіді ICMP на запити IP-трансляції.
- Переконфігурувати брандмауер по прикладу, щоб заборонив пінг-файли, що виходять за межі вашої мережі.

На даний час ми не можемо унеможливити атаки Smurf, які впливають на роботу мережевої системи, через те що повідомлення, які фільтруються ICMPv6, унеможливлять діагностику мережі.

Використання розширених заголовків

Транспорт «Hop-by-Hop» – це принцип управління потоком даних у мережі. За допомогою «Hop-by-Hop» -транспорту частинки даних передаються з вузла в вузол способом «пересування вперед».

Оскільки транспорт «Hop-by-Hop» є не тільки вузол джерела та пункту призначення, а й є деяким або всіма проміжними вузлами, він дозволяє пересилати дані, навіть якщо шлях між джерелом та пунктом призначення не є постійно з'єднаним під час спілкування.

Однак принцип «Hop-by-Hop» «говорить», що контроль за транспортом повинен здійснюватися в «Hop-by-Hop», якщо впровадження транспорту з переїздом не досягає значно кращих показників. Більше того, для перенесення стрибку за хопом потрібна інформація про стан потоку на проміжних вузлах, що обмежує його масштабованість. Це одна з причин того, що майже вся комунікація сьогодні керується транспортними протоколами, такими як TCP.

Поточні дослідження в галузі розрдільних мобільних мереж розглядають транспорт «Hop-by-Hop» для прикладних сценаріїв, коли підключення від кінця до кінця доступне лише з періодичністю, оскільки за таких умов перевезення за допомогою переходу може досягти значного підвищення продуктивності [12].

На рисунку 3.7 показано перевірку на вразливість за допомогою генерування повідомлень «Scapy». Саме повідомлення складається з 102000 символів «A» і 150000 символів «B».

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*120) \
/PadN(optdata='\102'*150) \
/ICMPv6EchoRequest()
```

Рисунок 3.7 – Повідомлення з прихованим текстом

Саме повідомлення після цього виявилось неушкодженим (рисунок 3.8)

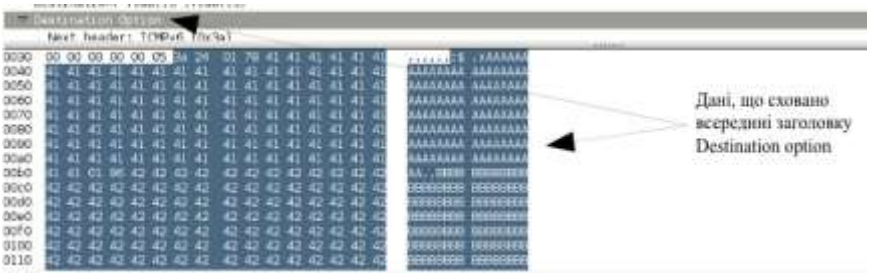


Рисунок 3.8 – Приховане повідомлення

RouterAlert

У MPLS мітка зі значенням 1 представляє мітку попередження маршрутизатора. Це значення мітки є законним в будь-якому місці стека міток, крім внизу. Коли отриманий пакет містить це значення мітки у верхній частині стека міток, він доставляється в локальний програмний модуль для обробки. Фактичне переадресація пакета визначається міткою під ним у стеці. Однак, якщо пакет передається далі, ярлик маршрутизатора слід натиснути назад на стек мітки перед переадресацією. Використання цієї мітки аналогічно використанню «Опція сигналізації маршрутизатора» в IP-пакетах. Оскільки ця мітка не може виникнути внизу стеку, вона не пов'язана з конкретним протоколом мережевого рівня.

На рисунку 3.9 показано сценарій аовідомлення RouterAlert

```
packetRouterAlert = IPv6(dst=dst_r1) /
IPv6ExtHdrHopByHop(options=RouterAlert(value=0))
/TCP(sport=RandShort(),dport=80)/
```

Рисунок 3.9 – Використання параметра RouterAlert

Коли ми відправимо «20000» повідомлень, навантаження на процесор збільшиться. На рисунках 3.10-3-11 зображено навантаження процесора з часом дискретизації 5 хвилин на вісі абсцис, а на вісі ординат показано завантаження маршрутизаторів «Cisco і Juniper».

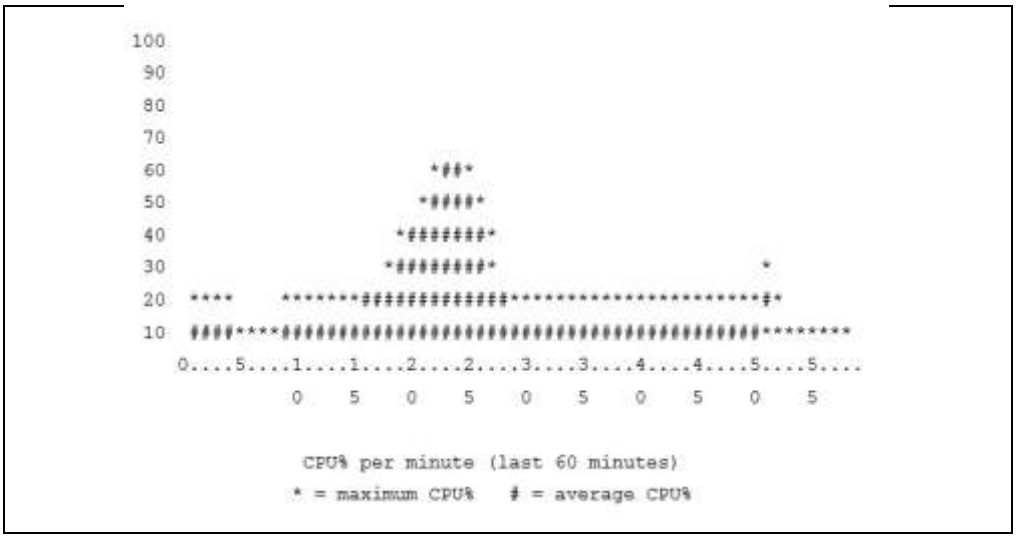


Рисунок 3.10 – Навантаження процесора з часом дискретизації 5 хвилин на маршрутизаторі «Cisco»

При аналізі DoS-атаки ми бачимо, що навантаження маршрутизатора Cisco – 60 відсотків, а навантаження маршрутизатора Juniper – 50 відсотків.

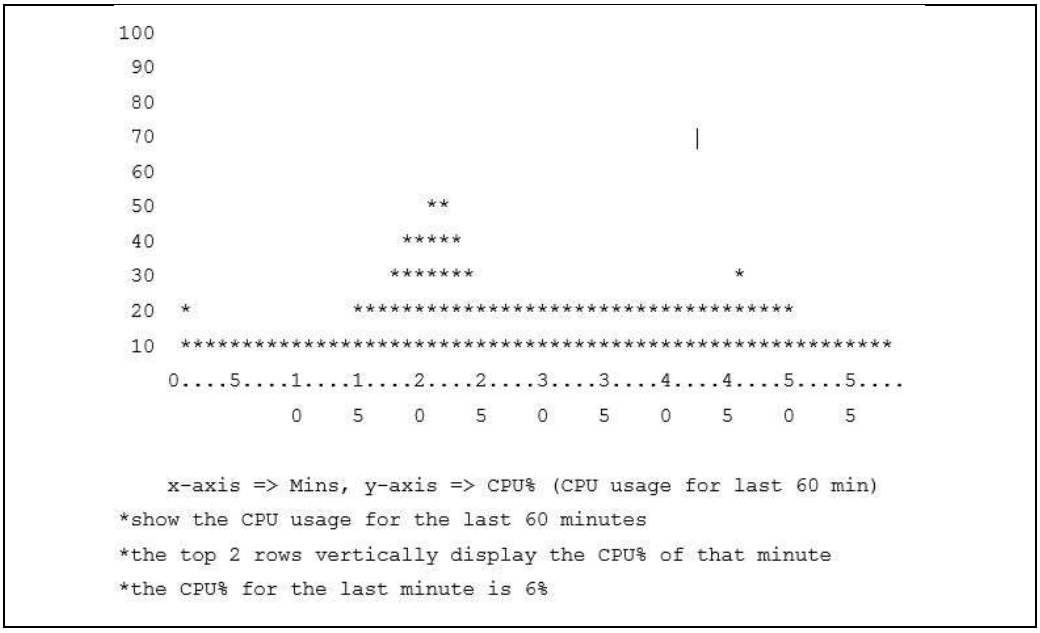


Рисунок 3.11 – Навантаження процесора з часом дискретизації 5 хвилин маршрутизаторі «Juniper»

Для протоколу IPv6 характерна ознака для заголовків розширення [10]:

– немає;
– 1 або більше.

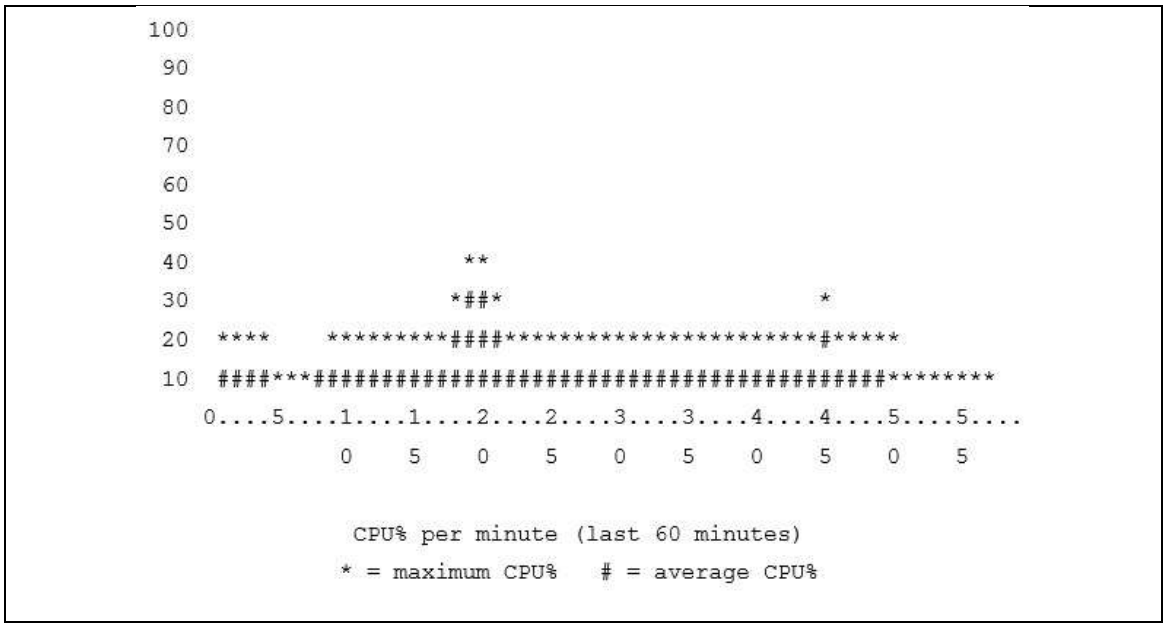
На рисунку 3.12 показано сценарій повідомлення заголовків.

```
packet = IPv6(src=src_ip, dst=dst_ip) \
/IPv6ExtHdrHbyHOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrDestOpt(options=PadN(optdata='\101'*10) \
/IPv6ExtHdrRouting(addresses=["2001:78::1","2001:20::385"])\
/ICMPv6EchoRequest()\
/TCP_SYN=TCP(sport=1500, dport=80, flags="S", seq=100)\
/TCP_SYNACK=sr1(ip/TCP_SYN)
send(packet)
```

Рисунок 3.12 – Сценарій повідомлення з послідовністю заголовків

При відправці «20000» повідомлень збільшилася завантаження процесора на маршрутизаторах. На рисунках 3.13-3-14 зображено

навантаження процесора з часом дискретизації 5 хвилин на вісі абсцис, а на вісі ординат показано завантаження маршрутизаторів «Cisco і Juniper».



Малюнок 3.13 – Навантаження процесора з часом дискретизації 5 хвилин на маршрутизаторі «Cisco»

Провівши аналіз DoS-атаки ми можемо зробити висновок, що подріблене повідомлення не можуть виявити ОС даних виробників.

Відсіювання повідомлень при наявності розширених заголовків може завдати шкоди для користувача трафіку [12].

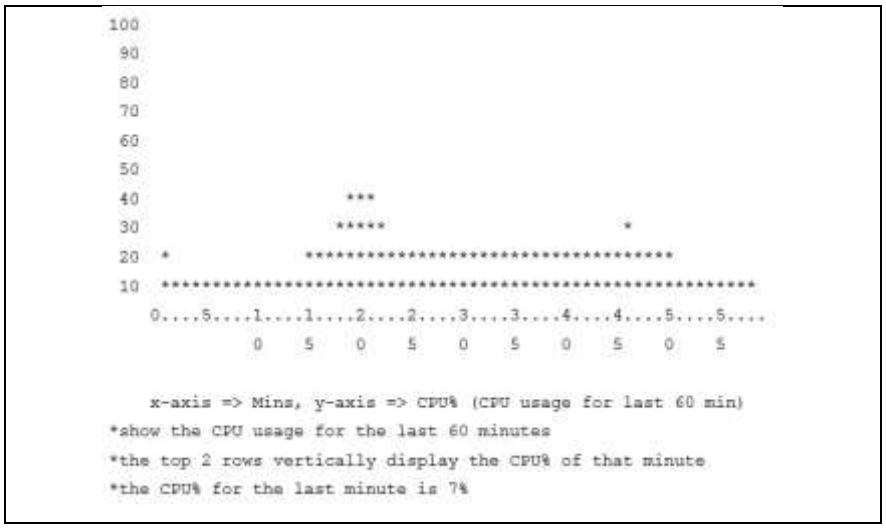


Рисунок 3.14 – Навантаження процесора з часом дискретизації 5 хвилин маршрутизаторі «Juniper»

IPv6 Fragmentation

Фрагментація – це нормальний процес у мережах з комутацією пакетів. Це відбувається, коли приймається великий пакет і розмір MTU відповідного вихідного інтерфейсу занадто малий. Фрагментація розбирає IP-пакет на менші пакети перед передачею. Приймаючий хост виконує перекомпонування фрагмента і передає повний IP-пакет до стеку протоколів. Фрагментація – це процес IP, TCP та інші шари вище IP не беруть участі.

Сценарій повідомлення зображено на рисунку 3.15.

На рисунку 3.16 показано як повідомлення передається отримувачу без налаштувань безпеки.

```
payload = '\101'*10
pkt = IPv6(src= src_ip, dst= dst_ip, plen=16)
icmpv6 = ICMPv6EchoRequest(cksum=csum)
frag1 = IPv6ExtHdrFragment(offset=0, m=1, id=502, nh=58)
frag2 = IPv6ExtHdrFragment(offset=1, m=0, id=502, nh=58)
packet1 = pkt/frag1/icmpv6
packet2 = pkt/frag2/payload
```

Рисунок 3.15 – Повідомлення, яке є першим і останнім фрагментом

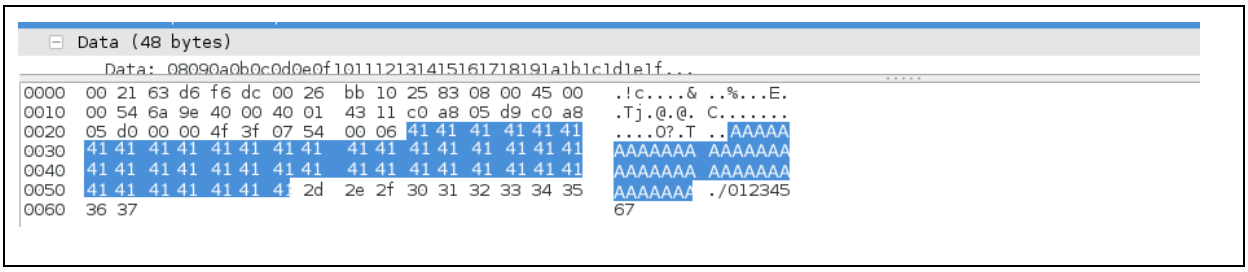


Рисунок 3.16 – Повідомлення передане отримувачу без налаштувань безпеки

Графи атак моделюють, як для атаки можуть поєднуватися кілька вразливих місць. Вони представляють стани системи, використовуючи сукупність умов, пов'язаних із безпекою, наприклад, наявність вразливості на певному хості або зв'язок між різними хостами. Експлуатація вразливості моделюється як перехід між системними станами [10].

3.2 Розробка системи безпеки, для підвищення захисту мережі

Для того щоб підвищити систему безпеки потрібно використовувати різні методи фільтрації повідомлень, які в свою чергу характеризуються за різними ознаками. Зокрема в таблиці 3.4 показано ймовірні методи налаштувань, які в свою чергу можна використати для ефективного використання при досліджені атак [11].

В свою чергу варто звернути увагу на фільтрацію з заголовками розширення, які ми досліджували на інтерфейсах комп’ютерної мережі.

Таблиця 3.4 – Налаштування пристроїв для «Cisco і Juniper»

Cisco	Juniper
Фільтрація за заголовками розширення	
ipv6 access-list BLK-EXT-HDR deny ipv6 any any fragments deny ipv6 any any dst-option deny ipv6 any any hbh deny ipv6 any any routing permit ipv6 any any	family inet6 { filter blk-ext-hdr { term t1 { from { extension-headers fragment; extension-headers destination; extension-headers hop-by-hop; extension-headers routing; } then discard; } term default { then accept; } } }
Налаштування фільтрації RA повідомлень (комутатор)	
	family ethernet-switching { filter block-router-advert { term t1 { from { icmp-type router-advertisement; } then discard; } term default { then accept; } } }

Налаштування обмежень DHCPv6 SOLICIT повідомлень	
class-map match-all DHCPv6_SOLICIT_CL match protocol ipv6 match access-group name DHCPv6_SOLICIT ! policy-map INGRESS class DHCPv6_SOLICIT_CL police rate 8000 bps conform-action transmit exceed-action drop violate-action drop ! interface Ethernet0/0 load-interval 30 ipv6 dhcp relay destination FF02::1:2 service-policy input INGRESS ! ipv6 access-list DHCPv6_SOLICIT permit udp any eq 546 any eq 547	system services{ dhcp-local-server{ dhcpv6{ overrides { interface-client-limit 3 } } } }
Налаштування фільтрації DHCPv6 повідомлень	
ipv6 access-list CLIENT_PORT deny udp any eq 547 any permit ipv6 any any	family ethernet-switching { filter rouge-dhcp { term t1 { from { dhcp-type advertise; dhcp-type reply; } then discard; } term default { then accept; } } }

Для попередження атак варто звернути увагу на підміну RA повідомлень. Для того щоб використати обладнання Cisco, необхідно доставляти додаткове обладнання.

Також необхідно виділити атаки, які використовують прихований канал, що в свою чергу не мають достатнього впливу на наше обладнання, але можуть призвести до втрати конференційної інформації. При створені політики мережі потрібно врахувати можливість відслідковування пакетів, зокрема з розширенням заголовків «Hop-byHop та Destination».

Для налаштування обмежень з роботою DHCPv6 сервера потрібно налаштувати фільтрації DHCPv6.

4 СПЕЦІАЛЬНА ЧАСТИНА

4.1 Організація мережевої безпеки комп'ютерної мережі

Мережева безпека – це комплексне поняття, це і обмеження небажаного доступу, та збереженість інформації, і роботоздатність самої мережі.

Мережева безпека в мережах забезпечується адміністраторами мереж. У підприємстві цю функцію виконує вчитель інформатики. При цьому перед ними стоять наступні завдання:

- забезпечення стабільного функціонування локальної мережі;
- адміністрування мережних принтерів;
- встановлення дозволів доступу до мережевих ресурсів;
- встановлення дозволів доступу до локальних ресурсів;
- забезпечення збереження інформації користувачів.

Для забезпечення стійкого функціонування мережі проводиться аналіз її складу. В мережі навчального закладу є досить велика кількість персональних комп'ютерів і вони розподілені по навчальних аудиторіях та класах, які поділені на окремі робочі групи. Робочі станції робочих груп мають різні однотипні назви. На мережу виділено окремий діапазон IP- адрес для робочих груп, які чітко використовуються і не повторюються на окремих ПК.

Головні комутатори та сервер розміщені в спеціальних шафах, до яких обмежений доступ. Головні комутатори контролюють MAC-адреси пакетів, що дозволяє блокувати порт, якщо виявлено пакети з невідомими MAC-адресами, а також виявляти випадки підключення однієї і тієї ж MAC-адреси до різних портів. Також комутатори роблять постійний моніторинг широкомовних запитів, що є однією з складових частин системи безпеки

локальної мережі, тим більше що такий моніторинг не породжує додаткового трафіку.

Захист мережі від зовнішніх вторгнень забезпечується апаратним Firewall'ом. Також функції захисту виконують головні комутатори мережі. Ці пристрої входять до серії NetDefend. NetDefend представляє собою рішення в області безпеки, що включає вбудовану підтримку брандмауера, балансування навантаження, функції відмовостійкості, механізм Zone-Defense, фільтрацію вмісту, авторизацію користувачів, блокування «миттєвих» повідомлень та програм P2P, захист від атак «відмова в обслуговуванні» DoS і підтримку віртуальних локальних мереж VPN. Пристрої NetDefend також містять у собі набір функцій для моніторингу та підтримання стану і безпеки мережі, у тому числі відправлення повідомлень електронною поштою, ведення журналу системних подій і надання статистики в режимі реального часу. Ці функції, поряд з можливістю оновлення програмного забезпечення, гарантують, що міжмережевий екран зможе надати максимальну продуктивність і безпеку для мережі.

Для створення засобів захисту інформації необхідно визначити природу погроз, форми й шляхи їх можливого прояву й здійснення в автоматизованій системі.

Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем говорять про те, що інформація в процесі введення, зберігання, обробки й передачі зазнає різним випадковим впливам. Причинами таких впливів можуть бути:

- відмови й збої апаратури;
- перешкоди на лінії зв'язку від впливів зовнішнього середовища;
- помилки людини як ланки системи;
- системні й системотехнічні помилки розроблювання;
- структурні, алгоритмічні й програмні помилки;

– аварійні ситуації;

– інші впливи.

Немає жодних сумнівів, що будуть відбуватись навмисні спроби злому мережі ззовні. У зв'язку із цією обставиною потрібно ретельно передбачити захисні заходи.

Для обчислювальних систем характерні наступні штатні канали доступу до інформації:

– термінали користувачів, самі доступні з яких це робочі станції в комп'ютерних класах;

– термінал адміністратора системи;

– термінал оператора функціонального контролю;

– засобу відображення інформації;

– засобу завантаження програмного забезпечення;

– засобу документування інформації;

– зовнішні канали зв'язку.

Прийнято розрізняти п'ять основних засобів захисту інформації:

– технічні;

– програмні;

– криптографічні;

– організаційні;

– законодавчі.

4.2 Засоби моніторингу та діагностики комп’ютерної мережі

Моніторинг та мережеметрія – це безперервний контроль інформаційних та комунікаційних процесів у системі, збирання оперативних (моніторинг) та статистичних (мережеметрія) даних про якість функціонування мережі, використання її ресурсів тощо. Результати

моніторингу попередньо опрацьовують та зберігають у попередніх функціях моніторингу. На підставі цих даних за запитом адміністратора в будь-який час можна сформувати звіти.

Є такі форми звітів:

– звіт про термінали (активність терміналу, ім'я прикладної програми, яка працює на ньому, час активності);

– звіт про лінії (які станції зв'язані лінією, активність, статистика трафіку, відомості про повторення передавань, збої);

– звіт про прикладні програми (приєднання, статистика використання, з якими терміналами працює).

Статистичні дані про використання мережі обчислюють на підставі узагальнення оперативних. Тут є можливість оцінити ступінь використання ресурсів мережі, ефективність її роботи.

Моніторинг дає можливість відслідковувати діяльність окремих користувачів з метою дотримання безпеки даних. Сама процедура моніторингу виконується на багатьох рівнях мережі з використання спеціального технічного забезпечення, протоколів, баз даних, служб.

Розглянемо загальну характеристику способів організації моніторингу в КМ. Зрозуміло, що якщо вести моніторинг лише на одному з рівнів протоколу, то про ефективність таких процедур говорити не доводиться. Саме тому моніторинг доцільно проводити на різних рівнях:

– на фізичному рівні досліджуються параметри кабельної системи;

– на канальному та мережевому рівнях аналізуючи трафік, декодують та перехоплюють кадри і пакети;

– на верхніх рівнях проводиться вивчення взаємодії станцій з використанням конкретних протоколів та властивостей їх параметрів;

– на рівні застосувань можливий аналіз взаємодії застосувань (напрямку клієнта і сервера, бази даних).

Адміністратору передусім слід відслідковувати параметри взаємодії на рівні застосувань. Однак, як показує досвід, причини неефективності роботи слід шукати і у функціонуванні протоколів нижчих рівнів.

Розглянемо особливості моніторингу на деяких рівнях.

На фізичному рівні найважливіше місце займає аналіз кабельної системи. В кабелях можуть виникати наступні несправності:

- обрив;
- коротке замикання;
- затиснення кабелю;
- погане навантаження;
- інші дефекти (згини, петлі тощо).

На вищих рівнях застосовують аналіз роботи сегмента, використовуючи аналізатор протоколу, що являє собою програмно-апаратний блок, який переймає весь потік інформаційного сегменту, аналізує, декодує та інтерпретує його.

Тут можлива реалізація найважливіших функцій:

- фільтрування;
- ініціалізація;
- генерування тестових даних.

Фільтрування – в загальному потоці виділяється пакет з певними ознаками.

Ініціалізація – відбувається зв'язок між режимами перехоплення і відображення з конкретними подіями. В даному випадку визначена подія (надходження кадру, визначення протоколу певної довжини чи звертання до вказаного сервера) запускає перехоплення протоколу.

Генерування тестових даних – в мережі створюється тестовий потік вказаного типу пакетів заданої інтенсивності.

Можливість використання розподіленої системи керувань мережею із застосуванням агентів моніторингу та аналізу, бази даних параметрів стандарту MIB, протоколів SNMP та RMON, систем моніторингу та аналізу дає змогу значно підвищити ефективність збору інформації про функціонування окремих вузлів ЛКМ із врахуванням часових затрат.

RMON – це розширення SNMP, в основі якого, як і в основі SNMP, лежить збір і аналіз інформації про характер інформації, переданої по мережі. Як і в SNMP, збір інформації здійснюється апаратно-програмними агентами, дані від яких надходять на комп'ютер, де встановлено додаток управління мережею. Відмінність RMON від свого попередника полягає, в першу чергу, в характері інформації, що збирається – якщо в SNMP ця інформація характеризує тільки події, що відбуваються на тому пристрої, де встановлений агент, то RMON вимагає, щоб одержувані дані характеризували трафік між мережевими пристроями, а адже саме це, як правило, і цікавить адміністратора мережі найбільше.

Використовувані комутатори підтримують 4 групи даних:

- statistics;
- history;
- alarms;
- events.

Перша група носить назву групи статистики (statistics). У ній збирається загальна інформація про трафік в даному сегменті і ступінь використання пропускної здатності мережі – кількості переданих байтів і мережевих пакетів, число помилок і колізій і т.д.

Група історії (history) відповідає за збір інформації, визначеної в групі статистики, протягом певного часу (від однієї секунди до однієї години) (рисунок 4.1). У результаті виявляється можливим проаналізувати поточні тенденції в роботі мережі і порівняти поточний стан з базовим – це дозволить

виявити небажані явища в роботі мережі раніше, ніж вони перетворяться на серйозну проблему (наприклад, поки збої в роботі обладнання не привели до його повної відмови).

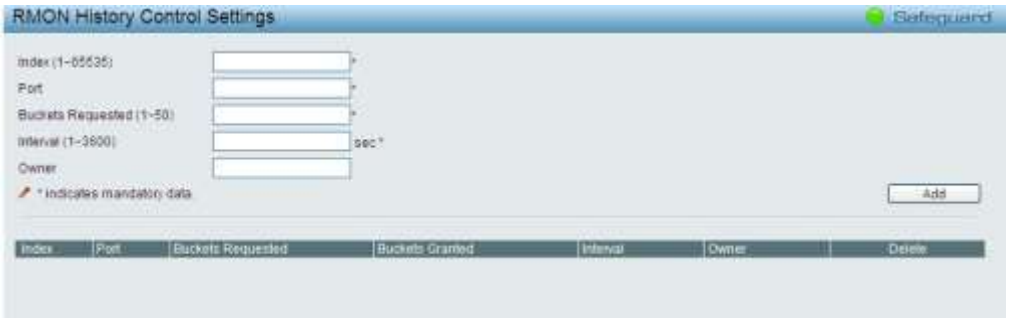


Рисунок 4.1 – Налаштування групи історії

Група аварійних сигналів (alarms) дозволяє користувачеві визначити ряд порогових рівнів (ці пороги можуть ставитися до самих різних речей – будь-якому параметру з групи статистики, амплітуді або швидкості його зміни і багато чому іншому), по перевищенні яких генерується аварійний сигнал. Користувач може також визначити, за яких умов перевищення порогового значення має супроводжуватися аварійним сигналом – це дозволить уникнути генерації сигналу через дрібниці, що погано, по-перше, тому, що на постійно палаючу червону лампочку ніхто не звертає уваги, а по-друге, тому, що передача непотрібних аварійних сигналів по мережі призводить до зайвої завантаженні ліній зв'язку. Аварійний сигнал, як правило, передається у групу подій, де і визначається, що з ним робити далі.

У групі подій (events) визначається, коли слід відправляти аварійний сигнал додаткові керування, коли – перехоплювати пакети, і взагалі – як реагувати на ті чи інші події, що відбуваються в мережі, наприклад, на перевищення заданих в групі alarms порогових значень: чи слід ставити до відома додаток керування, чи треба просто запротоколювати дану подію і

продовжувати працювати. Події можуть і не бути пов'язані з передачею аварійних сигналів (рисунок 4.2).

Рисунок 4.2 – Вікно налаштування групи подій

Керовані комутатори D-link дають можливість без додаткового обладнання проводити моніторинг мережі на фізичному рівні. Вони ведуть статистику по кожному порту (рисунок 4.5), і дають можливість визначити появу на них проблем. З їх допомогою можна визначити пошкодження на кабелі (розрив, коротке замикання) (рисунок 4.3). Також вони ведуть системний журнал усіх спроб підключення, що дає можливість виявити спроби не санкціонованого доступу до мережі (рисунок 4.4).

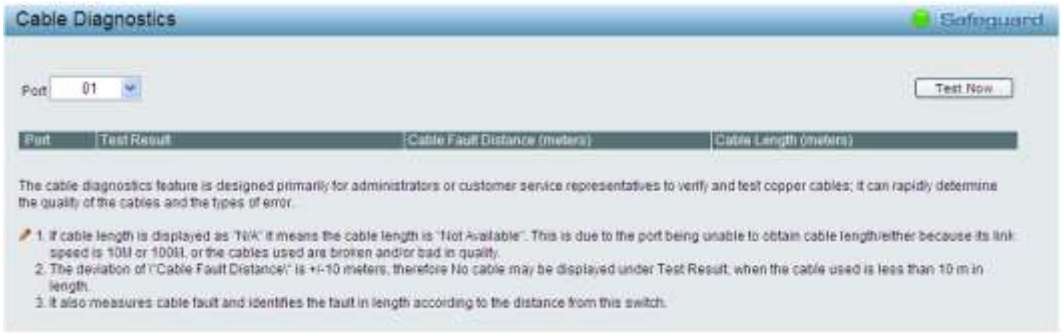


Рисунок 4.3 – Діагностика кабелю

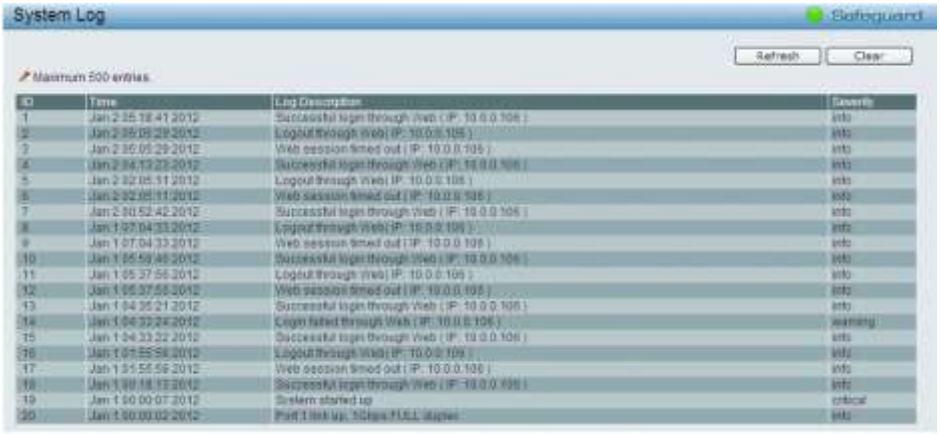


Рисунок 4.4 – Системний журнал комутатора

Рисунок 4.5 – Статистика на 1 порті

Щоб детальніше протестувати мережу підприємства використано команду ping командного рядка Windows. Ping – це службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP. Отже, було виконано пінгування з одного комп’ютера на інший, результат виконання команди показаний на рисунку 4.6.

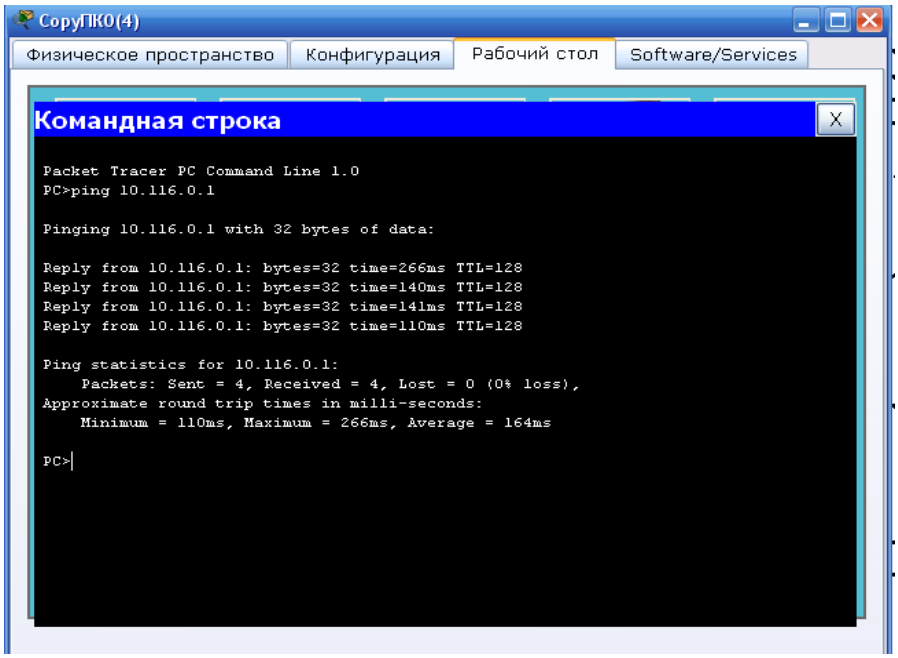


Рисунок 4.6 – Результат виконання команди ping до віддаленого комп’ютера

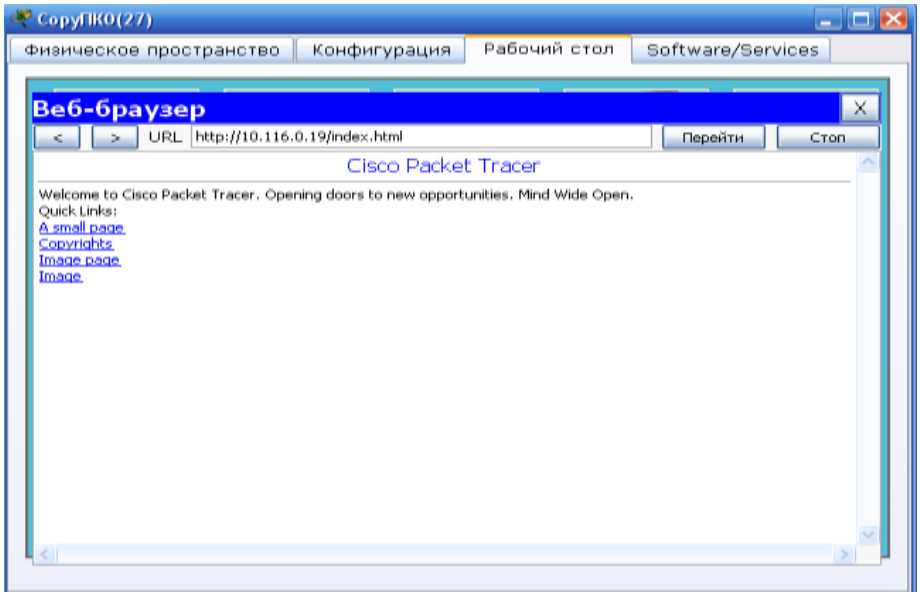


Рисунок 4.7 – Результат виконання команди ping до сервера

Також виконано команду ping до серверу, який буде обслуговувати користувачів і є невід’ємною часткою мережі. Результат виконання команди показаний на рисунку 4.7.

5 ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Головною метою розділу є обґрунтування економічної ефективності впровадження даної розробки і визначення терміну окупності капітальних вкладень. Для цього необхідно здійснити розрахунок норм часу, визначити витрати на оплату праці та відрахувань на соціальні заходи, розрахувати матеріальні витрати, витрати на електроенергію, суму амортизаційних відрахувань, скласти кошторис витрат та визначити собівартість науково-дослідницької роботи, розрахувати ціну програмного продукту.

5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу є важливим критерієм, тому що коефіцієнт корисної дії залежить від оптимального використання часу.

Розробка системи поділена на декілька основних етапів, а саме:

– підготовка опису задачі;

– збір необхідної інформації для аналізу існуючих методів збору інформації у туристичній сфері;

– вибір технологій для розробки системи;

– збір необхідних даних для розробки системи;

– розробка системи;

– тестування системи.

Нормативи часу застосовуються для того, щоб здійснити оцінку тривалості виконання.

Інженер є виконавцем на усіх етапах створення системи.

Витрати часу по окремих операціях технологічного процесу наведені в таблиці 7.1.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовка опису задачі	Інженер	7
2.	Збір необхідної інформації для аналізу існуючих методів збору інформації у туристичній сфері	Інженер	10
3.	Вибір технологій для розробки системи	Інженер	16
4.	Збір необхідних даних для розробки системи	Інженер	7
5.	Розробка системи	Інженер	25
6.	Тестування системи	Інженер	5
Разом			70

На реалізацію системи витрачено 70 годин, серед яких майже третину часу на стадію розробки.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Заробітна плата – це грошова винагорода, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу. Розмір заробітної плати залежить від таких показників: професійно-ділових якостей працівника, складності, результату, умов виконуваної роботи.

Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за

фактично відпрацьований час. Показники, що впливають на нарахування додаткової заробітної плати: кваліфікація, досягнуті і заплановані показники.

Тривалість робочого дня становить 8 годин, а середня кількість робочих днів – 24,5 дні/міс. Або 196 год./міс. Такі показники потрібно приймати при розрахунку заробітної плати.

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно із законодавством України мінімальна заробітна плата становить 22, 41 грн/год.

Рекомендовані тарифні ставки: керівник дипломної роботи – 30,00...50,00 грн./год., інженер – 22,41...30,00 грн./год., консультант – 22,41...30,00 грн./год., технік – 22,41...30,00 грн./год., лаборант – 22,41...25,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \, , \tag{5.1}$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 22{,}41 \cdot 70 = 1568{,}7 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \tag{5.2}$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, становить 0,1–0,15.

$$З_{дод} = 1568,7 \cdot 0,15 = 235,305 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 1568,7 + 235,305 = 1804,005 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ – 22%;
- військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0,235 , \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

Звідси, сума відрахувань становить:

$$В_{с.з.} = 1804,005 \cdot 0,235 = 423,94 \text{ грн.}$$

Отже, для створення системи для оплати праці необхідно 2227,95 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених

матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i \,, \tag{5.5}$$

де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} \,. \tag{5.6}$$

Проведені розрахунки занесемо у таблицю 5.2.

Таблиця 5.2 – Зведені розрахунки матеріальних витрат

Найменув. матеріальних ресурсів	**Один. виміру**	**Норма витрат**	**Ціна за один., грн.**	**Затрати матер., грн.**	**Загальна сума витрат на матер., грн.**
1 Основні матеріали					
Площадка для розміщення результату розробки	штук	1	100	–	100
2 Допоміжні витрати					
Використання мережі Internet	місяч. абон-та	–	105	105	105
Разом:					205

Загальні матеріальні витрати становлять 205 грн. В перспективі розширення функціональних можливостей програмного продукту може виникнути ряд додаткових витрат.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S\,, \qquad (5.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (2,42 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютера для створення роботи – 400 Вт, кількість годин роботи обладнання згідно таблиці 7.1 – 70 години.

Тоді,

$$З_в = 0{,}4 \cdot 70 \cdot 2{,}42 = 67{,}76 \text{ грн.}$$

Затрати на електроенергію становлять 67,76 грн

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

З одного боку, амортизаційні відрахування – це витрати підприємства, тому що їхню суму, нараховану на виробничі необоротні активи, включають у собівартість продукції, робіт, послуг. Водночас, у складі доходу від реалізації продукції суму амортизаційних відрахувань розглядають як цільовий фонд, складову фінансових ресурсів, призначених для відтворення зношених у процесі виробництва необоротних матеріальних і матеріальних активів.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Отже, використовуючи в роботі 1 комп'ютер балансовою вартістю 18900 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 18900 \cdot 5\% / 100\% = 945 \text{ грн.}$$

Оскільки робота виконувалась 70 години, то амортизаційні відрахування будуть становити:

$$A = 945 \cdot 70 / 70 = 945 \text{ грн.}$$

Амортизаційні відрахування становлять 945 грн.

5.6 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведемо у таблицю 5.3.

Таблиця 5.3 – Кошторис витрат на НДР

Зміст витрат	**Сума, грн.**	**В % до загальної суми**
1	2	3
Витрати на оплату праці (основну і додаткову заробітну плату)	1804,005	52,36
Відрахування на соціальні заходи	423,94	12,30
Матеріальні витрати	205	5,95
Витрати на електроенергію	67,76	1,97
Амортизаційні відрахування	945	27,4
Собівартість	3445,709	100,00

Таким чином найбільшою сумою для собівартості системи є витрати на оплату праці, які становлять 52,36 % від загальної суми собівартості системи та амортизаційні відрахування, які становлять 27,4.

Собівартість ($С_в$) програмного продукту розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А. \quad (5.9)$$

Отже, собівартість програмного продукту дорівнює:

$$С_в = 1804{,}005 + 423{,}94 + 205 + 67{,}76 + 945 = 3445{,}709 \text{ грн.}$$

Собівартість програмного продукту становить 3445,709 грн.

5.7 Розрахунок ціни програмного продукту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ), \quad (5.10)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

K – кількість замовлень;

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

$ПДВ$ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти K та $B_{н.і.}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.11)$$

Звідси ціна складе:

$$Ц = 3445{,}709 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 5375{,}3 \text{ грн.}$$

Розрахована ціна на створення системи, становить 5375,3 грн.

5.8 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_В}, \tag{5.12}$$

де $П$ – прибуток;

$C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в . \tag{5.13}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 5375{,}3 - 3445{,}709 = 1929{,}591 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{C_в}. \tag{5.14}$$

Тоді,

$$E_р = 1929.591 / 3445{,}709 = 0\ ,56 .$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}\ , \qquad (5.15)$$

Термін окупності дорівнює:

$$T_p = 1 / 0{,}56 = 1{,}8 \text{ роки}$$

Термін окупності капітальних вкладень становить 1,8 роки

5.9 Висновок до сьомого розділу

В економічній частині роботи розраховано основні техніко-економічні показники створення системи (див. таблицю 5.4).

Значення економічної ефективності становить 0,56. Розвиток вважається доцільним та економічно вигідним, якщо період окупності становить значення у межах від 1 до 3 років. Для створення системи цей показник 1,8.

Таблиця 5.4 – Техніко–економічні показники НДР

№ п/п	Показник	Значення
1	Собівартість, грн.	3445,709
2	Плановий прибуток, грн.	1929,591
3	Ціна, грн.	5375,3
4	Економічна ефективність	0,56
5	Термін окупності, рік	1,8

Отже, створення системи є економічно вигідним проектом за всіма основними техніко-економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

6.1.1 Професійні захворювання користувачів комп'ютерів

Професійні хвороби (професійна патологія) – це галузь медицини, що вивчає причини, характер порушень у різних системах організму, викликаних дією несприятливих факторів виробничого середовища, їх клінічну картину, діагностику, способи лікування і профілактики. Профзахворювання діляться на два основних види: гострі і хронічні.

Гострі професійні захворювання на увазі недуга, що виник в результаті короткого (протягом не більше однієї робочої зміни або робочого дня) впливу отруйними речовинами або шкідливими чинниками.

Якщо якийсь фактор впливав протягом довгого часу, ефект від нього накопичувався протягом тривалого терміну, і тут говорять про хронічний професійному захворюванні. Професійні хвороби тісно пов'язані з іншими галузями медицини, а також з гігієною праці. Саме гігієна праці дає чітке уявлення про причину захворювання – один або комплекс несприятливих факторів виробничого процесу, що впливають на людину. Кожному з них гігієністи праці дають якісну і кількісну оцінку, визначають часові показники їх дії. Для правильної діагностики професійного захворювання особливо важливо ретельне вивчення санітарно-гігієнічних умов праці, його «професійного маршруту», що включає всі види робіт, які нею з початку праці.

Праця є основою діяльності людини, сприятливо впливає на її здоров'я і забезпечує добробут суспільства. Але за певних умов деякі види праці можуть стати причиною дезорганізації в діяльності нервової, ендокринної, серцево-судинної систем, шлунково-кишкового тракту, опорно-рухового апарату. Недостатнє технічне оснащення виробничого процесу, недодержання чітко регламентованих санітарно-гігієнічних норм призводить до «поломки» в

одній чи кількох з перерахованих систем організму людини, виникає патологічний процес, який і назвали професійною патологією, професійними хворобами.

У клініках профзахворювань перелічених медичних установ працюючі різних підприємств України, в яких виникла підозра на професійне захворювання, проходять поглиблене обстеження та лікування. Крім клініки професійних захворювань, у НДІ є консультативні поліклініки, в яких щодня проводиться прийом осіб з підозрою на професійне захворювання.

Амбулаторний прийом передбачає обстеження у лікарів основних медичних спеціальностей (терапевта, невропатолога, окуліста, отоларинголога, дерматолога, ортопеда, стоматолога, алерголога, гінеколога, рентгенолога). Із застосуванням електрофізіологічних, біохімічних, гематологічних, алергологічних, рентгенологічних та інших методів у кабінетах відділення функціональної діагностики проводиться поглиблене дослідження окремих органів і систем організму, що дає змогу або підтвердити, або зняти, або змінити клінічний діагноз.

Додаткові методи досліджень мають винятково важливе значення під час встановлення точного діагнозу і вирішення питання про подальшу працездатність пацієнта. Деякі дослідження проводяться двічі – до і після курсу відновлювального лікування, що допомагає в об’єктивній оцінці ефективності проведеного відновлювального лікування.

Основне завдання клінік профзахворювань – не тільки поглиблено обстежити хворого, поставити йому точний діагноз, але й провести ефективний курс відновлювального лікування з використанням медикаментозних, фізіотерапевтичних методів, спрямованих на збереження працездатності пацієнта за своєю професією (професійна реабілітація).

Електрофтальмія – це гостре ураження кон’юнктиви і рогівки ока, викликане ультрафіолетовим випромінюванням. В умовах виробництва, де

використовується електрозварювання, електрофтальмія становить 2% від загальної кількості пошкоджень очей тільки з втратою працездатності. Легкі випадки електроофтальмії, що протікають переважно без втрати працездатності, набагато перевищують цю цифру: 26% усіх електрофтальмій припадає на зварників, а решта – на робітників інших професій (збирачі, слюсарі, кранівники, підсобні робітники та інше), які за умовами праці перебувають у зоні виконання електрозварювальних робіт.

Електроофтальмією можуть страждати також працівники, які обслуговують дугові електропечі, і ті, хто має справу з дуговими прожекторами. Причиною електроофтальмії є вплив ультрафіолетового випромінювання з середньою довжиною хвилі (UV-B від 290 до 320 нм) і короткою (UV-C від 100 до 290 нм). Промені з такою довжиною хвилі випромінюють штучні джерела УФО – кварцові лампи, електроди апарату для електрозварювання; UV-C повністю поглинається епітелієм кон'юнктиви і рогівки.

Ультрафіолетовий опік кон'юнктиви і рогівки спостерігається у осіб, які зазнали опромінення бактерицидними лампами (персонал операційних, процедурних, фізіотерапевтичних кабінетів, соляріїв), у недосвідчених електрозварників або у людей, що спостерігають за електрозварювальними роботами. Ультрафіолетовий опік має кумулятивну дію, тому реакція уражених тканин проявляється через 6-8 годин після експозиції. Через 6-8 годин після опромінення у потерпілих з'являються перші скарги на відчуття «піску» в очах, потім відчуття дискомфорту в очах швидко наростає і через 1-2 години розвивається різко виражений синдром рогівки: гострий біль в очах, світлобоязнь, блефароспазм, сльозотеча. Зір зазвичай не страждає, однак перевірити це складно через судорожно стислі повіки. Пацієнти вкрай неспокійні.

Об'єктивне дослідження очей можливо тільки після інстиляції місцевого анестетика, що усуває на 20-25 хвилин синдром рогівки.

Спостерігається помірний набряк і гіперемія повік (фотодерматит), кон'юнктивна або змішана ін'єкція, набряк кон'юнктиви. Рогівка в основному прозора, блискуча, хоча при високій індивідуальній чутливості до УФО або після тривалої експозиції може бути набряк, поодинокі бульбашки підведеного епітелію або точкові ерозії, які фарбуються флюоресцеїном. Діагноз встановлюється на підставі типового анамнезу (вплив УФО, поява перших симптомів ураження рогівки через 6-8 годин після експозиції), характерної клінічної картини (поєднання суб'єктивно різко вираженого синдрому рогівки і досить мізерних об'єктивних змін з боку кон'юнктиви і рогівки), результатів дослідження зору, зовнішнього огляду і біомікроскопії з фарбуванням рогівки флюоресцеїном.

Лікування спрямоване на ослаблення симптомів синдрому рогівки, стимуляцію епітелізації і профілактику інфікування мікроерозій рогівки. Рекомендується носіння світлозахисних окуляр. У більшості випадків симптоми фотоофтальмії безслідно проходять за 2-3 дні; якщо зберігається легка світлобоязнь, слід продовжувати інстиляції актовегина і ще 2-3 тижні носити окуляри зі світлофільтрами. Інфрачервоні промені при постійному впливі викликають у працівників гарячих цехів (плавильників, сталеварів, ковалів) розвиток теплової катаракти. Тільки на початку свого розвитку теплова катаракта має особливості, що вказують на професійний характер захворювання кришталика (ранні нашарування на зонулярній платівці передньої капсули кришталика, коли ще може і не бути помутніння його волокон).

Інфрачервоне випромінювання має виражений тепловий вплив на повіки, кон'юнктиву і деякі структури, особливо в передньому відділі ока. Для внутрішньоочних структур особливо небезпечне випромінювання з довжиною хвилі 900-1000 нм. Максимальне підвищення температури відзначається в задній камері ока, що пов'язано з поглинанням теплової радіації пігментним

епітелієм райдужної оболонки. Меншою мірою підвищується температура також у кришталику і волозі передньої камери.

Професійна теплова катаракта (катаракта склодувів, металургів) у початковій стадії розвитку має характерні клінічні особливості. Помутніння виникають спочатку в задньому кортикальному шарі кришталика. Після формування повного коркового помутніння диференціальна діагностика теплової та вікової (або ускладненої) катаракти стає неможливою.

Створення фізіологічних умов праці – єдиний правильний і радикальний спосіб ліквідації виробничих травм та професійних хвороб очей. Профілактика професійних ушкоджень очей в сучасних умовах – це комплекс організаційних, інженерно-технічних та санітарно-гігієнічних заходів, здійснюваних за такими основними напрямками:

– раціоналізація виробничих процесів передбачає їх комплексну механізацію та автоматизацію, а на підприємствах хімічної промисловості – і герметизацію всіх технологічних процесів. Особливу увагу слід приділяти поліпшенню технології виробничих процесів, що дають високий відсоток ушкоджень очей, заміні цих процесів більш досконалими і безпечними. Необхідний постійний технічний контроль за станом верстатів, агрегатів, якістю ручного інструменту, дотримання вимог техніки безпеки;

– забезпечення санітарно-гігієнічних норм виробничих приміщень. Освітленість робочого місця повинна забезпечувати достатню яскравість робочих поверхонь, штучне освітлення не повинно давати ні прямого, ні відображеного відблиску;

– впровадження і вдосконалення методів індивідуального і колективного захисту очей. Індивідуальний захист очей здійснюється за допомогою захисних окулярів, масок, світлофільтрів. Окуляри повинні бути легкими, зручними, прозорими, не перекручувати представлені предмети, не обмежувати поле зору, не пітніти, легко дезінфікуватись. Захист очей від

променевої енергії повинен здійснюватися за допомогою світлофільтрів, які вибірково поглинають одні промені і пропускають інші. При роботі в гарячих цехах для захисту очей від теплових випромінювань (інфрачервоних променів) застосовують світлофільтри із синього скла, що володіють здатністю поглинати інфрачервоні промені. Для захисту очей від сліпучого світла застосовують так звані сонцезахисні окуляри зі світлофільтрами з жовто-зеленого або темного скла. Для захисту очей від ультрафіолетових променів при електрозварювальних роботах служать світлофільтри з темного жовто-зеленого скла. Колективний захист очей здійснюється: огорожею металорізальних верстатів, робочих місць для слюсарних, абразивних робіт металевими сітками на висоту людського зросту і спеціальними щитками при електрозварювальних роботах; установкою на верстатах захисних щитків, екранів, кожухів різної конструкції. Кращими захисними екранами є автоблокування, тобто екрани з автоматизованим пристроєм, завдяки якому при неробочому (відкинутому) положенні екрану верстат вимикається; забезпечення металорізальних верстатів потужними витяжними установками для уловлювання та відведення металевої стружки;

– професійний відбір при прийомі на роботу, при виборі професії та диспансерне спостереження за працівниками з боку лікарів медико-санітарних частин, у тому числі окулістами, мають велике значення у профілактиці пошкоджень очей. Оцінка стану органу зору і його функцій проводиться з урахуванням вимог професії і пов’язаних з нею трудових процесів. Ретельно проведені дослідження під час попереднього огляду виключають прийом людей з дефектами органів зору. Періодичні огляди працюючих в порядку диспансерного спостереження лікарями дозволяють:

– своєчасно діагностувати і лікувати професійні та інші захворювання очей, а також вживати заходів щодо попередження подальшого їх прогресування;

– виявити акомодаційні і рефракційні зміни і своєчасно призначити або змінити коригувальні окуляри.

При проведенні періодичних медичних оглядів працюючих у шкідливих умовах праці в контакті з фізичними факторами, які призводять до змін з боку органу зору, необхідна обов'язкова участь лікаря-офтальмолога.

При очних захворюваннях може бути протипоказана робота в таких умовах:

– робота при значній запиленості виробничих приміщень і постійному контакті з подразнюючими речовинами;

– робота в умовах теплового або ультрафіолетового випромінювання (робота ливарника, коваля, сталевара, склодува).

Надійність системи «людина–комп'ютер» значною мірою визначається функціональним станом людини. Психофізіологічні та емоційні перенапруження, втома людини-оператора можуть призвести в комп'ютеризованих системах керування до помилок і як наслідок – до значних економічних втрат. Проте, незадовільний функціональний стан користувачів комп'ютерів може викликати небажані наслідки (професійні та професійно зумовлені захворювання), що також пов'язано зі значними соціальними та економічними втратами враховуючи стрімке зростання кількості комп'ютеризованих робочих місць.

Визначення та вивчення факторів, що впливають на функціональний стан користувачів комп'ютерів дозволить виділити основні причини виникнення станів напруженості, стомлення, стресу і здійснити відповідні профілактичні заходи.

Трудова діяльність користувачів комп'ютерів відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі – фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля,

шум, параметри мікроклімату та ціла низка світлотехнічних показників. Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів – значно менший.

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями.

Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях.

Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів.

Оскільки робота користувачів комп'ютерів частіше за все проходить за активної взаємодії з іншими людьми, то виникають питання раціоналізації міжособових відносин. Цей комплекс питань порушує як психологічні, так і соціально-психологічні аспекти трудових взаємовідносин, які також є факторами «ризику», що відчутно впливають на функціональний стан користувачів комп'ютерів.

Таким чином, на користувача комп'ютера впливає комплекс факторів. Врахування ступеня та якості впливу цих факторів на функціональний стан

дозволяють розробити заходи та засоби щодо забезпечення безпеки, підвищення працездатності та збереження здоров'я користувачів комп'ютерів.

Отже, до основних факторів, що впливають на функціональний стан користувачів комп'ютера належать:

1. Виробниче середовище характеризується такими шкідливими факторами:

– фізичні: електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників;

– хімічні: пил, шкідливі хімічні речовини, які виділяються при роботі принтера і копіювальної техніки;

– біологічні: підвищений вміст в повітрі патогенних мікроорганізмів, особливо в приміщенні з великою кількістю працюючих, при недостатній вентиляції, особливо в період епідемій;

– психофізіологічні: напруження зору та уваги, інтелектуальні та емоційні навантаження, тривалі статичні навантаження і монотонність праці.

2. Трудовий процес – характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями;

3. Внутрішні засоби діяльності – це професійні якості та виробничий досвід, які обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи розв'язання виробничих завдань навіть у нестандартних ситуаціях;

4. Зовнішні засоби діяльності – визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його

елементів, просторового розташування основного і допоміжного устаткуванні, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів;

5. Соціально-психологічні фактори трудових взаємовідносин.

Таким чином, на користувача комп'ютера впливає комплекс факторів. Урахування ступеня та якості впливу цих факторів на функціональний стан дозволяють розробити заходи та засоби щодо забезпечення безпеки, підвищення працездатності та збереження здоров'я користувачів комп'ютерів.

6.2 Безпека в надзвичайних ситуаціях

6.2.1 Створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території

На сьогодні стан навколишнього природного середовища є загальнодержавною проблемою, комплексне вирішення якої залежить не лише від міністерств чи органів місцевого самоврядування окремих адміністративно-територіальних регіонів, але й від кожного громадянина.

З метою оцінки стану навколишнього середовища, забезпечення конституційного права людини на безпечне для його життя та здоров'я довкілля в Україні створена і функціонує державна система моніторингу довкілля. Державна система моніторингу довкілля – це система спостережень, збирання, оброблення, передавання, збереження та аналізу інформації про стан довкілля, прогнозування його змін і розроблення науково-обґрунтованих рекомендацій для прийняття рішень про запобігання негативним змінам стану довкілля та дотримання вимог екологічної безпеки.

Система моніторингу є складовою частиною національної інформаційної інфраструктури, сумісної з аналогічними системами інших

країн. Система моніторингу – це відкрита інформаційна система, пріоритетами функціонування якої є захист життєво важливих екологічних інтересів людини і суспільства; збереження природних екосистем; відвернення кризових змін екологічного стану довкілля і запобігання надзвичайним екологічним ситуаціям.

Державна система моніторингу довкілля – це система спостережень, збирання, оброблення, передачі, зберігання й аналізу інформації про стан навколишнього природного середовища, прогнозування його змін і розроблення науково обґрунтованих рекомендацій для прийняття управлінських рішень про запобігання негативним змінам довкілля та дотримання вимог екологічної безпеки. Вона створюється з дотриманням міжнародних вимог і є сумісною з аналогічними міжнародними системами.

Структура та рівні державної системи моніторингу довкілля передбачають розбудову таких видів моніторингу навколишнього природного середовища (НПС) в Україні:

– загальний (стандартний) моніторинг НПС – це оптимальні за кількістю параметрів спостереження в пунктах, об’єднаних в єдину інформаційно-технологічну мережу, що дають змогу розробляти управлінські рішення на всіх рівнях;

– оперативний (кризовий), сутність якого полягає у спостереженнях за спеціальними показниками на цільовій мережі пунктів у реальному масштабі часу за окремими об’єктами та джерелами підвищеного екологічного ризику в окремих регіонах, котрі визначено як зони надзвичайної екологічної ситуації, а також у районах аварій із шкідливими екологічними наслідками з метою забезпечення оперативного реагування на кризові ситуації та прийняття рішень щодо їх ліквідації, створення безпечних умов життєдіяльності;

– фоновий (науковий) моніторинг НПС – спеціальні високоточні спостереження за всіма компонентами природного довкілля, а також за

характером, складом, кругообігом та міграцією забруднювальних речовин, за реакціями організмів на забруднення на рівні окремих популяцій, геосистем і біосфери в цілому. Так моніторинг здійснюється у природних та біосферних заповідниках і на інших територіях, що охороняються.

В Україні є розвинута нормативно-правова база для проведення геоекологічного моніторингу. Постановою Кабінету Міністрів затверджене «Положення про державну систему моніторингу довкілля» від 30 березня 1998 р., яке визначає порядок створення та функціонування Державної служби моніторингу довкілля (ДСМД). ДСМД – це система установ, які збирають, аналізують, зберігають і поширюють інформацію про стан довкілля, прогнозують його зміни та надають науково обґрунтовані рекомендації для прийняття відповідних рішень ДСМД – складова національної інформаційної інфраструктури, що є відкритою інформаційною системою. Пріоритет її функціонування – захист життєдіяльності громадян і суспільства загалом, збереження природних екосистем, запобігання кризовим змінам у довкіллі та виникненню надзвичайних екологічних ситуацій антропогенно-техногенного походження.

Система державного моніторингу довкілля контролює об’єкти трьох масштабних рівнів:

– локального – територію окремих об’єктів (підприємств, міст, ландшафтів та їх складових);

– регіонального – територію економічних і природних регіонів та адміністративно-територіальних одиниць;

– національного – територію країни загалом.

Створення і функціонування системи моніторингу з метою інтеграції екологічних інформаційних систем, що охоплюють певні території, ґрунтується на принципах:

– узгодженості нормативно-правового та організаційно-методичного забезпечення, сумісності технічного, інформаційного і програмного забезпечення її складових;

– систематичності спостережень за станом довкілля та техногенними об’єктами, що впливають на нього;

– своєчасності отримання, комплексності оброблення та використання екологічної інформації, що надходить та зберігається в системі моніторингу;

– об’єктивності первинної, аналітичної і прогнозної екологічної інформації та оперативності її доведення до органів державної влади, органів місцевого самоврядування, громадських організацій, засобів масової інформації, населення України, зацікавлених міжнародних установ та світового співтовариства.

Фінансуються роботи зі створення і функціонування ДСМД та її частин за рахунок коштів, передбачених у державному та місцевих бюджетах згідно з чинним законодавством

Система моніторингу спрямована на:

– підвищення рівня вивчення і знань про екологічний стан довкілля;

– підвищення оперативності та якості інформаційного обслуговування користувачів на всіх рівнях;

– підвищення якості обґрунтування природоохоронних заходів та ефективності їх здійснення;

– сприяння розвитку міжнародного співробітництва у галузі охорони довкілля, раціонального використання природних ресурсів та екологічної безпеки.

Основними завданнями суб’єктів системи моніторингу є:

– довгострокові систематичні спостереження за станом довкілля;

– аналіз екологічного стану довкілля та прогнозування його змін;

– інформаційно-аналітична підтримка прийняття рішень у галузі охорони довкілля, раціонального використання природних ресурсів та екологічної безпеки;

– інформаційне обслуговування органів державної влади, органів місцевого самоврядування, а також забезпечення екологічною інформацією населення країни і міжнародних організацій.

Також суб'єкти моніторингу забезпечують:

– удосконалення підпорядкованих їм мереж спостережень за станом довкілля;

– уніфікацію методик спостережень і лабораторних аналізів, приладів та систем контролю;

– створення банків даних для наступного їх багатоцільового колективного використання за допомогою єдиної комп'ютерної мережі, що забезпечує автономне і спільне функціонування складових цієї системи та її зв'язок з іншими інформаційними системами, котрі діють в Україні та за кордоном.

Отже, створення і функціонування Державної системи моніторингу довкілля має сприяти здійсненню державної екологічної політики, що передбачає:

– екологічно раціональне використання природного та соціально-економічного потенціалу держави, збереження сприятливого середовища життєдіяльності суспільства;

– соціально-екологічне й економічно раціональне розв'язання проблем, що виникають унаслідок забруднення довкілля, небезпечних природних явищ, техногенних аварій та катастроф;

– розвиток міжнародного співробітництва щодо збереження біорізноманіття природи, охорони озонового шару атмосфери, запобігання

антропогенній зміні клімату, захисту лісів і лісовідновлення, транскордонного забруднення довкілля, відновлення природного стану річок.

6.3 Висновок до восьмого розділу

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» дипломної роботи магістра було розглянуто професійні захворювання користувачів комп’ютерів, а також створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території.

7 ЕКОЛОГІЯ

7.1 Сталий розвиток як парадигма суспільного зростання

Усвідомлення людством реальної небезпеки екологічної катастрофи, яка загрожує існуванню цивілізації, стало причиною початку розробки концепції сталого розвитку. Новою парадигмою розвитку суспільства розглядається парадигма сталого розвитку, яку доцільно розуміти не лише в контексті зміни стосунків людини і природи задля розширення можливостей економічного зростання, а як скоординовану глобальну стратегію виживання людства, орієнтовану на збереження і відновлення природних спільнот у масштабах, необхідних для повернення до меж господарської місткості біосфери.

Об’єктом дослідження є поняття «сталого розвитку» та концепція сталого розвитку.

Предметом дослідження є історія виникнення терміну «сталий розвиток» та його суть, історія розробки концепції сталого розвитку, основні її аспекти, рівні та принципи.

Мета дослідження полягає у визначенні суті поняття «сталий розвиток» та концепції сталого розвитку.

Методами дослідження виступають загальнонаукові прийоми й методи: порівняльний, історичний, діалектичний, системний аналіз.

Робота складається із плану, вступу, трьох розділів, висновків, списку використаних джерел.

Практичне значення дослідження полягає у отриманні важливих висновків, які можуть бути застосовані при подальшій науковій роботі (написання статей, рефератів, диплому тощо); при розробці стратегії сталого розвитку України, визначення місця та ролі екологічної складової в системі

чинників, які впливають на сталий розвиток країни та її національної безпеки; при дослідженні природно-ресурсного потенціалу в умовах сталого розвитку; при дослідженні екологічної безпеки тощо.

Появу терміну «сталий розвиток» (СР) (sustainable development) пов'язують з ім'ям прем'єр-міністра Норвегії Гру Харлем Брундланд, яка сформулювала його в звіті «Наше спільне майбутнє», що було підготовлено для ООН і опубліковано у 1987 р. Міжнародною комісією з навколишнього середовища і розвитку. Вона визначала його як розвиток, який задовольняє потреби теперішнього часу, проте не ставить під загрозу здатність майбутніх поколінь задовольняти свої власні потреби.

Загалом після опублікування в 1987 р. доповіді Комісії по економічному розвитку ООН «Наше спільне майбутнє» вчені та аналітики запропонували понад 70 визначень поняття сталого розвитку. Спроби визначити зміст цього процесу науковим товариством не мали позитивного результату, навпаки – з’явилися нові терміни: зрівноважений, стійкий, збалансований, екорозвиток та ін. Наведемо кілька зарубіжних і вітчизняних визначень цього терміну. Так, Інститут світових ресурсів (1996 р.) визначає СР як розвиток, при якому природні ресурси, людство і фінанси управляються і використовуються таким чином, щоби збільшити багатство і благоустрій людей без погіршення умов їх життєдіяльності у майбутньому. СР у формулюванні Світового банку – управління сукупним капіталом суспільства в інтересах збереження і збільшення людських можливостей.

Б.М. Данилишин визначає СР як систему відносин суспільного виробництва, при якій досягається оптимальне співвідношення між економічним ростом, нормалізацією якісного стану природного середовища, ростом матеріальних і духовних потреб населення. На думку С. Дорогунцова, О. Ральчука, СР – це певна траєкторія довготермінового збільшення загального блага людства, яка поділяється на такі складові: соціально-економічну та техногенно-екологічну безпеки. В. Трегобчук СР визначає як

економічне зростання, за якого ефективно розв’язуються найважливіші проблеми життєзабезпечення суспільства без виснаження, деградації і забруднення довкілля. Як бачимо із наведених визначень, спільною ознакою СР є збалансування, врівноваження потреб з ресурсними й екологічними можливостями територій, а також такий розвиток людства та характер використання ним ресурсів планети, який дає змогу задовольняти потреби сьогодення та не підриває потенційні можливості забезпечення потреб наступних поколінь.

Найточніший, на мою думку, підхід до систематизації вищенаведених термінів, визначила З. В. Герасимчук, яка визначила сталий розвиток як процес забезпечення функціонування територіальної системи із заданими параметрами в певних умовах, протягом необхідного проміжку часу, що веде до гармонізації факторів виробництва та підвищення якості життя сучасних і наступних поколінь за умови збереження і поетапного відтворення цілісності навколишнього середовища.

Сталий розвиток – багаторівневе поняття. Його індивідуальний рівень виходить з того, що будь-які зміни довкілля спричинені діяльністю окремої людини. Потрібні радикальні зміни індивідуальної свідомості кожної людини щодо можливих наслідків своєї особистої діяльності. Будь-яка глобальна проблема людства обов'язково має і свій «індивідуальний вимір».

Життєва сталість залежить від прийняття людьми зобов'язань пошуку балансу у відносинах з іншими людьми і з природою, керуючись правилами такі, що люди повинні ділитися один з одним життєвими благами і піклуватися про Землю. Людство повинне брати від природи не більш того, що вона може створити. Це означає прийняття такого життєвого стилю і такого шляху розвитку, що поважають природу і діють у рамках її обмежень. Це може бути зроблене без відмови від численних вигод, що приносить сучасна технології, забезпечуючи функціонування технологій в рамках зазначених обмежень.

Принципи сталого розвитку взаємозалежні і взаємопідтримувані. З представлених нижче принципів, перший – основний, як той, що забезпечує етичну базу для інших.

Основними принципами сталого розвитку є:

- повага і турбота до всіх живих співтовариств;
- поліпшення якості людського життя;
- збереження життєздатності і розмаїтості Землі;
- забезпечення сталого використання відновлюваних ресурсів;
- мінімізація виснаження невідновлюваних ресурсів;
- зміна індивідуальних позицій і діяльності.

Отже, можна зробити висновок, що для того, щоб дотримуватися принципів концепції сталого розвитку, реалізувати її, необхідно розпочати з найскладнішого, на мою думку, рівня, а саме – індивідуального. Кожній людині необхідно змінити «споживацьке» ставлення, почати думати про навколишнє середовище, людей навколо та майбутні покоління. Адже досягти спільної мети можна лише за умови об’єднання зусиль всіх людей, які мають усвідомити загрозу для подальшого життя на Землі, а відтак докорінно змінити, перш за все, свій світогляд та свої дії.

7.2 Джерела теплового забруднення атмосфери і методи його зменшення

Теплове забруднення визначається впливом теплових полів на повітряне й водне середовище. Негативний вплив тепла на повітряне середовище виявляється шляхом підвищення теплових градієнтів температури над міськими, сільськими агломераціями в порівнянні із природними природними екосистемами, що спричиняє зміну енергетичних процесів в атмо- і гідросфері в сільській і особливо міській місцевості. Так, тепловий

вплив проявляється в погіршенні режиму земної поверхні (термокарст, соліфлюкція, полою й ін.) і умов життя людей.

У промислових центрах і великих містах атмосфера піддається тепловому забрудненню в зв'язку з тим, що в атмосферу надходять речовини з більш високою температурою, ніж навколишнє повітря. Температура викидів зазвичай вище середньої багаторічної температури приземного шару повітря. З труб промислових підприємств, вихлопних труб двигунів внутрішнього згоряння, при опаленні будинків, лісових пожежах виділяються речовини, нагріті до 60° С і більше. Середньорічна температура атмосферного повітря над великими містами і промисловими центрами на 6-7°С вище температури повітря прилеглих територій. Фахівці відзначають, що в останні 25 років середня температура тропосфери піднялася на 0,7° С.

Основними джерелами теплового забруднення:

- гарячі цехи і підземні газоходи металургійних підприємств;
- теплотраси;
- збірні колектори;
- комунікаційні тунелі;
- тунелі метрополітену;
- обігріваються підземні споруди;
- підземні сховища зрідженого газу.

Одним із наслідків теплового забруднення атмосфери являється парниковий ефект. Парниковий ефект – підвищення температури нижніх шарів атмосфери планети в порівнянні з ефективною температурою, тобто температурою теплового випромінювання планети, що спостерігається з космосу.

На сьогоднішній день основною світовою угодою про протидію глобальному потеплінню є Кіотський протокол (узгоджений в 1997, вступив в

силу в 2005). Протокол включає більше 160 країн світу і покриває близько 55% загальносвітових викидів парникових газів.

Кіотський протокол передбачає систему квот на викиди тепличних газів. Суть його полягає в тому, що кожна з країн отримує дозвіл на викид певної кількості тепличних газів. При цьому передбачається, що якісь країни чи компанії перевищать квоту викидів. В таких випадках ці країни або компанії зможуть придбати право на додаткові викиди у тих країн чи компаній, викиди яких менше виділеної квоти. Таким чином передбачається, що головна мета – скорочення викидів тепличних газів в наступні 15 років на 5% – буде виконана.

7.3 Висновок до дев’ятого розділу

В розділі екологія було розглянуто питання сталого розвитку, як парадигми суспільного зростання і джерела теплового забруднення атмосфери і методи його зменшення.

ВИСНОВКИ

При проектування комп’ютерної мережі виникають питання безпеки нашої мережі, тому для того нам потрібно провести аналіз безпеки і визначити вразливість нашої мережі, а також провести аналіз вразливостей мережі. За допомогою графів атак можна змоделювати сценарії можливих атак на мережу, і зокрема дати оцінку вразливості об’єкта дослідження. У сукупності ці підходи дозволяють оцінити рівень безпеки мережі.

Для того, щоб зробити перевірку рівня безпеки комп’ютерної мережі нами було виконано:

- побудову графа можливих дій;
- виявлено вразливості «вузьких місць» в захисті;
- розраховано показники захищеності;
- приведено отримані метрики до вимог для посилення безпеки.

Для попередження атак варто звернути увагу на підміну RA повідомлень. Для того, щоб використовувати обладнання Cisco, необхідно доставляти додаткове обладнання.

Також необхідно виділити атаки, які використовують прихований канал, що в свою чергу не мають достатнього впливу на наше обладнання, але можуть призвести до втрат конференційної інформації. При створені політики мережі потрібно врахувати можливість відслідковування пакетів, зокрема з розширенням заголовків «Hop-byHop та Destination».

Для налаштування обмежень з роботою DHCPv6 сервера потрібно налаштувати фільтрації DHCPv6.

В розділі «Обґрунтування економічної ефективності» проведено розрахунок доцільності нашої розробки і пораховано економічний ефект.

В розділі «Екологія» розглянуто питання поверхневих вод і проведено опис первинного оброблення статистичних даних.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» наведено вимоги до клавіатурних пристроїв та зроблено опис осіб які підлягають обов’язковому страхуванню від нещасних випадків. Також було проведено розрахунок освітлення для виробничих приміщень.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Arbor Networks. Стаття Marc Eisenbarth [Електронний ресурс]: Режим доступу: http://www.arbornetworks.com/asert/2014/08/ipv4–is–not–enough/ – Назва з екрану. Дата перегляду – 3.12.2019 р.

2. IPv6 Readiness in the Communication Service Provider Industry. An Incognito Software Report, April 2014, 18 p.

3. Santosh Naidu P1, Amulya Patcha, IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures. IOSR Journal of Computer Engineering (IOSR–JCE), Nov. – Dec. 2013, 66–75 p.

4. Google Official Blog. Під ред. Lorenzo Colitti IPv6 Statistics [Блог]: Режим доступу: http://www.google.com/intl/en/ipv6/statistics/— Назва з екрану. Дата перегляду – 3.12.2019 р.

5. Diane Teare. Implementing Cisco IP Routing (ROUTE) Foundation

Learning Guide Foundation learning for the ROUTE 642–902 Exam– Индианаполис: Cisco Press, 2004. 765 с.

6. RFC 2460 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc2460 – Назва з екрану. Дата перегляду – 23.12.2019 р.

7. RFC 4443 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4443 – Назва з екрану. Дата перегляду – 9.01.2019 р.

8. RFC 4861 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4861 – Назва з екрану. Дата перегляду – 10.01.2019 р.

9. RFC 4429 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html/rfc4429 – Назва з екрану. Дата перегляду – 10.01.2019 р.

10. Google Official Blog. Під ред. Lorenzo Colitti Access Google services over IPv6 [Блог] : Режим доступу: www.google.com/intl/en/ipv6/ — Назва з екрану. Дата перегляду – 4.10.2019 р.

11. *Gabi Nakibly Michael Arov* "Routing Loop Attacks using IPv6 Tunnels"– 7 USENIX Association Berkeley, CA, USA, 2009, 7 p.

12. *Sander Degen, Arjen Holtzer* Testing the security of IPv6 implementations – Nederland's, March 2014, 42 p.

13. Модели, построенные с использованием теории графов [Електронний ресурс].– Режим доступу: http://inf–bez.ru/?p=762 – Назва з екрану. Дата перегляду – 12.12.2019 р.

14. ДСанПіН 3.3.2–007–98. Гігієнічні вимоги до організації роботи з візуальними дісплейними терміналами електронно–обчислювальних машин\МОЗ України–К.:1998.18с.

15. ДСН 3.3.6.042–99 Санітарні норми мікроклімату виробничих приміщень – Київ, 2000.

16. ДБН–В.2.5–28–2006–Природне і штучне освітлення.

17. ДСН 3.3.6.037–99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

18. Правила улаштування електроустановок ПУЕ–2009.

19. НАПБ Б.03.002–2007. Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности.

20. НПАОП 0.00–1.28–10 Правила охорони праці під час експлуатації електронно–обчислювальних машин.