МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ
І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КУКУРУЗА АНАТОЛІЙ ОЛЕГОВИЧ

УДК 004.04

ПОКРАЩЕННЯ БЕЗПЕКОВИХ ХАРАКТЕРИСТИК МЕРЕЖІ З ВИКОРИСТАННЯМ ПРОТОКОЛУ IPV6

124 «Системний аналіз»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, професор кафедри комп'ютерних наук
Щербак Леонід Миколайович
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри інформатики і математичного моделювання
Гащин Надія Богданівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 28 грудня 2019 р. о 9-00 годині на засіданні екзаменаційної комісії №29 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська 56, навчальний корпус №1, ауд. 702

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи є те що процес впровадження мережевого протоколу нового покоління IPv6 відбувається поступово протягом останніх років. Але, темпи розвитку всесвітньої мережі Інтернет, значно вищі, що стимулює прискорення переходу на IPv6.

Мета роботи: є підвищення рівня безпеки комп'ютерних мереж, що працюють із мережевим протоколом IPv6.

Об'єкт, методи та джерела дослідження. протокол IPv6.

Наукова новизна отриманих результатів: розроблена методика, що вказує на доцільність використання додаткових налаштувань безпеки в мережі IPv6 та рекомендації щодо використання додаткових заходів безпеки.

Завдання дослідження:

- здійснити порівняльний аналіз для обладнання двох виробників;
- розглянути специфікацію мережевого протоколу IPv6;
- розглянути питання розгортання протоколу IPv6;
- здійснити пошук можливих методів усунення небезпек та вразливостей;
- розглянути етапи проектування мережі, при яких можуть використовуватися різні методи аналізу захищеності і визначення загального рівня захищеності;
- розглянути методику підвищення рівня безпеки локальної мережі;
- виконати техніко-економічне обґрунтування прийнятих рішень;
- виконати додаткові розділи з охорони праці, безпеки в надзвичайних ситуаціях та екології.

Практичне значення отриманих результатів. Графи атак забезпечують ефективний спосіб моделювання сценаріїв мережевих атак, а «Загальна система оцінки вразливостей» CVSS дає числові оцінки кожної уразливості..

Апробація. Окремі результати роботи доповідались на VIII Міжнародній науково-технічній конференції молодих учених та студентів „Актуальні задачі сучасних технологій", Тернопіль, ТНТУ, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 9 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 100 арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено аналіз процесу впровадження мережевого протоколу нового покоління IPv6.

В першому розділі описано науково технічну проблему.

В другому розділі проведено аналіз специфікації протоколу IPv6. В основі специфікації протоколу IPv6 лежить попередня версія мережевого протоколу. Звичайно ж, є суттєві відмінності, але основні функції залишаються тими ж самими.

Основна мета розробки нового протоколу – розширення простору адрес, що й спричинило зміни. Основний заголовок містить поля, використання яких є необхідним. Додаткові функції, такі як фрагментація, передача повідомлення через певні вузли реалізуються за допомогою заголовків розширення, що робить довжину основного заголовку постійною. Окрім цього, в заголовку взагалі відсутнє поле контрольної суми, так як вважається надлишковим. Такий підхід спрощує процес обробки повідомлення.

За використання IPv6 заборонена транзитна фрагментація. Тобто ця процедура повинна виконуватись лише кінцевими пристроями.

Протокол ICMPv6, необхідний для повноцінного функціонування IPv6 теж зазнав деяких змін в порівнянні із попередньою версією, що використовувалася із IPv4. Завдяки ньому, в комп’ютерних мережах, що використовують IPv6 стає можливим автоматичне налаштування, пошук сусідів, перевірка унікальності адреси та ін.. Для цьому використовуються механізми описані протоколом ND та повідомлення ICMPv6. Таким чином, більше немає необхідності в протоколах ARP та DHCP.

В третьому розділі проведено аналіз атак. Вказані атаки можуть складати не весь список можливих небезпек, що можуть мати місце при використанні нового мережевого протоколу. Жертвами атак можуть бути як кінцеві користувачі, так і проміжне обладнання (маршрутизатори та комутатори).

При виконанні аналізу уразливостей, можна віднести їх до різних категорій і врахувати приналежність одразу до декількох із них.

Виділено такі категорії: внутрішні – проблеми безпеки, що стосуються локальної мережі; зовнішні – проблеми безпеки, що стосуються глобальної (зовнішньої мережі); DoS – проблеми безпеки, які можуть призвести до відмови в обслуговуванні; Firewall – проблеми безпеки, пов'язані з мережевим екраном або іншими фільтруючими пристроями; Приховані – проблеми безпеки, які дають можливість створення прихованого каналу зв'язку; Розвідка – проблеми безпеки, пов'язані з виявленням адресної інформації кінцевих пристроїв; MitM – проблеми безпеки, які можуть бути використані для підключення до каналу передачі даних між його учасниками з метою перехвату, видалення або зміни інформації.

В спеціальній частині описано організацію мережевої безпеки комп’ютерної мережі.

В частині «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» опрацьовано наступні питання: професійні захворювання користувачів комп'ютерів, а також створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території.

В частині «Екологія» розглянуто питання сталого розвитку, як парадигми суспільного зростання і джерела теплового забруднення атмосфери і методи його зменшення.

У загальних висновках щодо дипломної роботи наведено отримані технічні рішення і запропоновано організаційно-технічні заходи, які забезпечують виконання поставленого завдання.

ВИСНОВКИ

В ході виконання завдань дипломної роботи було виконано ряд наступних завдань:

1. здійснено порівняльний аналіз для обладнання двох виробників;
2. розглянуто специфікацію мережевого протоколу IPv6;
3. розглянуто питання розгортання протоколу IPv6;
4. здійснено пошук можливих методів усунення небезпек та вразливостей;
5. розглянуто етапи проектування мережі, при яких можуть використовуватися різні методи аналізу захищеності і визначення загального рівня захищеності;
6. розглянуто методику підвищення рівня безпеки локальної мережі.

Також було здійснено економічні розрахунки, спрямовані на визначення економічної ефективності від від дослідження збіжності мережі на базі динамічних протоколів маршрутизації, а також прийнято рішення щодо подальшого розвитку.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Кукуруза А.О. Методи оптимізації програми / А.О. Кукуруза // Матеріали VIII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

АНОТАЦІЯ

В дипломній роботі виконано дослідження рівня безпеки мережевого протоколу IPv6 для виявлення можливих недоліків та вразливостей. На основі аналізу рівня безпеки протоколу IPv6 виявлено ряд недоліків, частина з яких успадкована від попередньої версії – IPv4.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, ПРОТОКОЛ, КАНАЛ, ДОС-АТАКА, ТУНЕЛЬ.

ANNOTATION

In the dissertation, IPv6 network protocol security research was conducted to identify possible deficiencies and vulnerabilities. On the basis of analysis of the security level of the IPv6 protocol, a number of shortcomings were identified, some of which were inherited from the previous version - IPv4.

Key words: COMPUTER NETWORK, PROTOCOL, CHANNEL, DOS-ATTACK, TUNNEL.