



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) UA (11) 107617 (13) U

(51) МПК (2016.01)

H04L 12/00

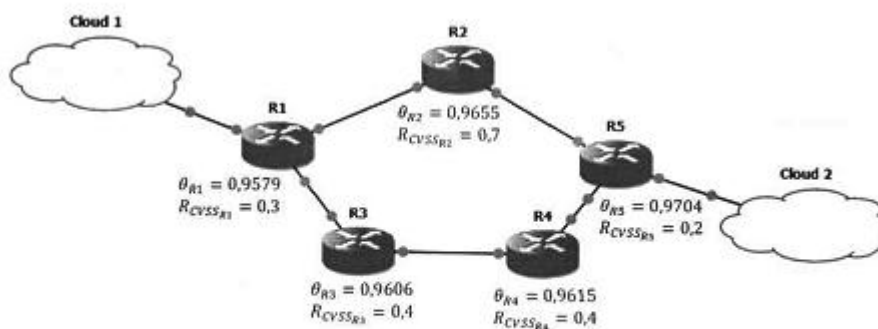
(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки:	u 2016 00667	(72) Винахідник(и):	Снігуров Аркадій Владиславович (UA), Чакрян Вадим Хазарович (UA)
(22) Дата подання заявки:	27.01.2016	(73) Власник(и):	ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ, пр. Науки, 14, м. Харків, 61166 (UA)
(24) Дата, з якої є чинними права на корисну модель:	10.06.2016		
(46) Публікація відомостей про видачу патенту:	10.06.2016, Бюл.№ 11		

(54) СПОСІБ МАРШРУТИЗАЦІЇ ТРАФІКУ ЗА ДОПОМОГОЮ ПРОТОКОЛУ EIGRP З УРАХУВАННЯМ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(57) Реферат:

Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки здійснює динамічну маршрутизацію трафіку на основі математичної моделі протоколу EIGRP. Додаткового введено параметр ризику інформаційної безпеки маршруту при передачі трафіку між вузлом-відправником та вузлом-отримувачем змінюється метрика протоколу EIGRP з урахуванням вимог інформаційної безпеки та забезпечується вибір найбільш безпечного, як для даних так і для мережі, маршруту передачі трафіку в заданій мережі між вузлами.



топология мережі, що використовується для проведення
експериментів

Фиг. 1

UA 107617 U

Корисна модель належить до електрозв'язку і є технологією маршрутизації трафіку, і може знайти застосування на прикордонних вузлах (маршрутизаторах і комутаторах третього рівня) транспортної телекомунікаційної мережі (ТКМ) при розв'язанні задач маршрутизації для забезпечення вибору найбільш безпечного маршруту передачі трафіка в заданій ТКМ.

Відомий, вибраний за прототип, спосіб динамічної маршрутизації в ТКМ (див. Enhanced Interior Gateway Routing Protocol. RFC draft ver. 4 / D. Savage, J. Ng, S. Moore, та ін. 2015 [Електронний ресурс].

<https://tools.ietf.org/html/draft-savage-eigrp-04>), в якому розв'язується задача динамічної маршрутизації трафіку без петель в ТКМ між вузлом-відправником і та вузлом-отримувачем і з урахуванням таких параметрів мережі як: пропускна здатність каналів зв'язку, затримка передачі пакету в каналах зв'язку, завантаженість каналів зв'язку та надійність передачі даних в каналах зв'язку заданої ТКМ. Задача динамічної маршрутизації формалізується як знаходження маршруту передачі трафіку між вузлами i, j з найменшою метрикою $\min_{p \in P_{i,j}} M_{p,i,j}$, де $M_{p,i,j}$ - найменша метрика одного з маршрутів $p_{i,j}$ між вузлами i, j ; $M_{p,i,j}$ - набір метрик усіх можливих метрик між вузлами i, j ; за умови, що $p \in P_{i,j}$, де $p_{i,j}$ - це маршрут p між вузлами i, j , а $P_{i,j}$ - набір усіх можливих маршрутів між вузлами i, j .

В цьому способі для розрахунку метрики маршрутів використовуються наступна формула:

$$M_p = \left[\left(K_1 \cdot B_{\min}^p + \frac{K_2 \cdot B_{\min}^p}{256 - L_{\max}^p} + K_3 \cdot D_{\text{sum}}^p \right) \cdot \frac{K_5}{K_4 + R_{\text{sum}}^p} \right] \cdot 256, \quad (1)$$

де $B_{\min}^p$ - найменше значення зваженого показника пропускної здатності в маршруті p ; $L_{\max}^p$ - найбільша загрузка одного з каналів зв'язку в маршруті p ; D_{sum}^p - сумарна затримка пакетів в маршруті p [мкс]; $R_{\min}^p$ - найменша надійність одного з каналів зв'язку в маршруті p ; $p \in P_{i,j}$, $P_{i,j}$ - усі можливі маршрути в заданій мережі при передачі інформації між вузлами i, j , при $i \neq j$. Коефіцієнти K_1, K_2, K_3, K_4, K_5 дозволяють враховувати в метриці вищевказані параметри.

Стандартно в алгоритмі протоколу EIGRP коефіцієнти K_1 та K_3 дорівнюють 1, а K_2, K_4, K_5 дорівнюють 0.

Розрахунок зваженої пропускної здатності виконується наступним чином:

$$B_{\min}^p = \left\lfloor \frac{10^7}{\min(B_{i,j}^{l,p})} \right\rfloor \left\lceil \frac{\text{Кбит}}{c} \right\rceil, \quad (2)$$

де $\min(B_{i,j}^{l,p})$ - найменша пропускна здатність одного з каналів зв'язку 1 в маршруті p при передачі інформації між i - вузлом-відправником та j - вузлом-отримувачем.

Для розрахунку сумарної затримки маршруту використовується наступна формула:

$$D_{\text{sum}}^p = \sum_{i \neq j} D_{i,j}^p, \quad (3)$$

де $\sum_{i \neq j} D_{i,j}^p$ - сума затримок пакетів кожного каналу зв'язку, які входять в маршрут p при передачі інформації між i - вузлом-відправником та j - вузлом-отримувачем.

У наведеному способі протокол динамічної маршрутизації EIGRP ніяк не враховує ризики інформаційної безпеки при виборі маршруту передачі трафіку.

В основу корисної моделі поставлена задача вибору оптимального маршруту передачі даних в ТКМ між вузлами i, j з урахуванням вимог інформаційної безпеки як для трафіку, так і для мережі, що дозволить вибирати найбільш безпечний шлях транспортування трафіку в заданій мережі.

Поставлена задача вирішується тим, що в способі динамічної маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки, що здійснює динамічну маршрутизацію трафіку на основі математичної моделі протоколу EIGRP, згідно з

винаходом, завдяки введенню додаткового параметру ризику інформаційної безпеки R_s^p маршруту p при передачі трафіку між вузлом-відправником і та вузлом-отримувачем j

змінюється метрика протоколу EIGRP з урахуванням вимог інформаційної безпеки та забезпечується вибір найбільш безпечного, як для даних так і для мережі, маршруту передачі трафіку в заданій мережі між вузлами i, j , при цьому формула розрахунку метрики приймає наступний вигляд:

$$M_p = \left[\left(K_1 \cdot B_{\min}^p + \frac{K_2 \cdot B_{\min}^p}{256 - L_{\text{sum}}^p} + K_3 \cdot \frac{D_{\text{sum}}^p}{10} \right) \cdot \frac{K_5}{K_4 + R_{\text{sum}}^p} \right] \cdot 16^{(2 - (1 - R_s^p))},$$

де $B_{\min}^p$ - найменше значення зваженого показника пропускної здатності в маршруті p ; L_{max}^p - найбільша загрузка одного з каналів зв'язку в маршруті p ; D_{sum}^p - сумарна затримка пакетів в маршруті p [мкс]; $R_{\min}^p$ - найменша надійність одного з каналів зв'язку в маршруті p ; $p \in P_{i,j}$, $P_{i,j}$ - усі можливі маршрути в заданій мережі при передачі інформації між вузлами i, j , при $i \neq j$; K_1, K_2, K_3, K_4, K_5 - коефіцієнти, що дозволяють враховувати в метриці вищевказані параметри, при $K_1, K_3 = 1$ та $K_2, K_4, K_5 = 0$; R_s^p - показник ризику, який розраховується як просте математичне середнє ризику усіх вузлів в маршруті p , при $R_s^p \in [0;1]$.

Суть корисної моделі пояснюється кресленнями, де зображені:

на фіг. 1 - топологія мережі, де R_1, R_2, R_3, R_4, R_5 - є маршрутизаторами, Cloud 1 - є відправником пакетів, Cloud 2 - є приймачем пакетів. Як вказано у формулі (4) метрика враховує параметр інформаційної безпеки маршрутів, який розраховується на основі параметрів маршрутизаторів, які наведено на фіг. 1, де $\theta_{R1}, \theta_{R2}, \theta_{R3}, \theta_{R4}, \theta_{R5}$ - це показник вразливості мережі при видаленні вузла R_1, R_2, R_3, R_4 або R_5 відповідно та всіх його каналів зв'язку,

$R_{\text{CVSS}_{R1}}, R_{\text{CVSS}_{R2}}, R_{\text{CVSS}_{R3}}, R_{\text{CVSS}_{R4}}, R_{\text{CVSS}_{R5}}$ - показники ризику вузлів R_1, R_2, R_3, R_4 або R_5 відповідно що розраховуються на основі методології NIST CVSS v2;

на фіг. 2 - наведено графік, що відображає затримку пакетів при передачі інформації за оптимальним маршрутом в топології, що наведено на фіг. 1, у наступних випадках: коли в мережі відсутня DoS атака, коли в мережі присутня DoS атака, але відсутній механізм захисту, коли в мережі присутня DoS атака, та присутній механізм захисту;

на фіг. 3 - наведено графік середньої затримки пакетів при передачі за оптимальним маршрутом в топології, що приведена на фіг. 1, в тих самих випадках що перераховані для фіг. 2.

В даному випадку DoS (англ. "Denial of Service") атака означає атаку відмови в обслуговуванні та реалізується за допомогою програми Torch (t50), як передача великої кількості пакетів з Cloud 1 до Cloud 2, що призводить до значних витрат системних ресурсів проміжних маршрутизаторів, через які проходять пакети, що, в свою чергу, збільшує затримку пакетів в маршруті.

Заявлений спосіб реалізується таким чином.

В формулу розрахунку метрики вводиться додатковий параметр, який відображає ризик інформаційної безпеки маршруту p при передачі інформації в ТКМ між вузлами i, j , так, що формула розрахунку метрики прийме наступний вигляд:

$$M_p = \left[\left(K_1 \cdot B_{\min}^p + \frac{K_2 \cdot B_{\min}^p}{256 - L_{\text{sum}}^p} + K_3 \cdot \frac{D_{\text{sum}}^p}{10} \right) \cdot \frac{K_5}{K_4 + R_{\text{sum}}^p} \right] \cdot 16^{(2 - (1 - R_s^p))}, \quad (4)$$

і буде відрізнятися від формули (1) тим, що константа масштабування приймає значення 16 замість 256 та возводиться у ступінь $(2 - (1 - R_s^p))$, де R_s^p - показник ризику, який розраховується як просте математичне середнє ризику усіх вузлів в маршруті p , при $R_s^p \in [0;1]$.

В такому випадку ступінь константної величини лежить в межах $(2 - (1 - R_s^p)) \in [1;2]$, а сама константна величина може коливатися в межах $16^{(2 - (1 - R_s^p))} \in [16;256]$. По суті, вираз $(1 - R_s^p)$ є рейтингом безпеки заданого маршруту p , тобто є величиною зворотною до ризику.

Розрахунок показника ризику пропонується виконувати за наступною формулою:

$$R_S^P = 1 - \left(1 - K_{CVSS} \cdot \frac{\sum_{i \in p} R_{CVSS_i}}{n_p} \right) \cdot \left(1 - K_{\theta} \cdot \left(1 - \frac{\sum_{i \in p} \theta_i}{n_p} \right) \right), (5)$$

де R_S^P - ризик інформаційної безпеки маршруту p ; K_{CVSS} - коефіцієнт важливості показника ризику, $K_{CVSS} \in [0;1]$; $\sum_{i \in p} R_{CVSS_i}$ - сума показників ризиків кожного з вузлів в маршруті p , що розраховуються на основі методології NIST CVSS v2; K_{θ} - коефіцієнт важливості показника ризику, $K_{\theta} \in [0;1]$; $\sum_{i \in p} \theta_i$ - сума показників вразливості кожного з вузлів в маршруті p , що розраховуються на основі формули вразливості вузла з математичного апарату теорії живучості інформаційних систем; n_p - загальна кількість вузлів, що входять у маршрут p .

Коефіцієнти важливості K_{CVSS} та K_{θ} дозволяють варіювати вплив відповідних показників, на основі яких виконується розрахунок стогового показника ризику. Слід зазначити, що для коректної роботи представленого методу, дані коефіцієнти мають бути однакові на всіх вузлах мережі.

Живучість мережі розраховується за наступною формулою:

$$\theta_i = \frac{\varepsilon - \varepsilon_i}{\varepsilon}, (6)$$

де θ_i - вразливість мережі при видаленні вузла i та всіх його каналів зв'язку, $\theta_i \in (0;1]$; ε - глобальна ефективність мережі; ε_i - глобальна ефективність в мережі, в разі видалення i -го вузла та всіх його каналів зв'язку.

При вирахуванні ефективності мережі, на відміну від стандартного підходу теорії живучості, використовується не відстань між вузлами, а метрика, яка враховує різноманітні показники сучасних ТКС та розраховується за наступною формулою:

$$\varepsilon = \frac{1}{n \cdot (n-1)} \cdot \sum_{i \neq j, i, j \in [1, n]} \frac{1}{\min_{p \in P_{i,j}} \mu_p}, (7)$$

де $\min_{p \in P_{i,j}} \mu_p$ - мінімальна метрика одного з маршрутів p між вузлами i, j ; при умові $i \neq j$ розрахунок виконується між кожною парою вузлів мережі, що досліджується; n - кількість вузлів в заданій мережі;

$$\mu_p = \sum_{m \in p} \mu_m, (8)$$

де $\sum_{m \in p} \mu_m$ - сума метрик кожного з каналів зв'язку m , які входять в маршрут p ; μ_m розраховується на основі формули (1), з тими ж параметрами та значеннями коефіцієнтів, що і для розрахунку стандартної метрики протоколу EIGRP на заданому вузлі.

Коефіцієнти важливості є бінарними змінними $K_{CVSS} \in \{0;1\}$, $K_{\theta} \in \{0;1\}$. Існує чотири комбінації, при яких активуються чи деактивуються показники, на основі яких розраховується остаточний показник ризику інформаційної безпеки. Різні комбінації коефіцієнтів важливості мають свої унікальні властивості і використовуються в наступних випадках:

1. $K_{CVSS} = 0$, $K_{\theta} = 0$ - у випадку, якщо показник ризику інформаційної безпеки не використовується. У такому випадку, формула (4) приймає вигляд формули (1). Стандартно активований даний варіант комбінації коефіцієнтів важливості.

2. $K_{CVSS} = 1$, $K_{\theta} = 0$ - у випадку, коли максимальний пріоритет віддається забезпеченню конфіденційності та цілісності транзитного трафіку.

3. $K_{CVSS} = 0$, $K_{\theta} = 1$ - у випадку, коли максимальний пріоритет віддається забезпеченню захисту вузлів від атак типу відмова в обслуговуванні та збереженню структурної цілісності мережі.

4. $K_{CVSS} = 1$, $K_{\theta} = 1$ - враховує параметри конфіденційності, цілісності та доступності трафіку, а також захисту структурної цілісності мережі.

Значення коефіцієнтів важливості змінюються адміністратором в ручному режимі. Комбінація коефіцієнтів важливості $K_{CVSS} = 1$, $K_{\theta} = 1$ може викликати нестабільність за рахунок внесення незбалансованості в формулу оцінки ризику інформаційної безпеки та не рекомендується до застосування.

5 Як захисний алгоритм для збереження структурної цілісності мережі пропонується використовувати перемаршрутизацію трафіку за наступними правилами:

1. Пріоритетний та довірчий трафік пропускати по маршруту з найкращою метрикою.

2. Весь інший трафік передавати по іншому(их) маршруту(ах). Пріоритетність та довірчість трафіку може визначатися на основі

10 корпоративної політики безпеки, в якій прописані довірчі IP адреси та додаткові параметри, що визначають пріоритетність трафіку. Для контролю трафіку пропонується використовувати листи доступу.

Приклад 1

15 В топології на фіг. 1 всі канали зв'язку мають однакову пропускну здатність 100 [Мбіт/с] та однакову стандартну затримку на всіх інтерфейсах. Мережа використовується як транзитна між Cloud 1 – вузлом-відправником та Cloud 2 – вузлом-отримувачем. В заданій мережі розглядаються два найкоротших маршрути між Cloud 1 та Cloud 2: $p1 \in [R1; R2; R5; WAN]$, $p2 \in [R1; R3; R4; R5; WAN]$. Маршрут $p1$ без врахування показника ризику інформаційної безпеки є оптимальним.

20 У випадку, коли коефіцієнти $K_{CVSS} = 0$ та $K_{\theta} = 0$, метрики маршрутів $p1$ та $p2$ відповідно мають наступні значення: $M_{p1} = 2880$, $M_{p2} = 2240$.

У першому випадку розглядається комбінація коефіцієнтів важливості $K_{CVSS} = 0$, $K_{\theta} = 1$. На фіг. 2, 3 наведені результати використання алгоритму перемаршрутизації трафіку. З них видно, що перемаршрутизація трафіку визволяє ресурси оптимального маршруту $p1$, що дозволяє майже в 4 рази зменшити затримку передачі пакетів за цим маршрутом (затримка пакетів вимірювалась як час між ring-запитом від вузла, що знаходиться в Cloud 1 до вузла, що знаходиться у Cloud 2). Тим самим цей спосіб дозволяє підвищити якість та надійність передачі пріоритетного та довірчого трафіку та зменшити ризик виходу зі строю найбільш продуктивного маршруту в заданій мережі.

30 У другому випадку розглядається комбінація коефіцієнтів важливості $K_{CVSS} = 1$; $K_{\theta} = 0$ та рівні уразливостей вузлів R_{CVSSi} , які наведено на фіг. 1, метрики маршрутів $p1$ та $p2$ відповідно приймають наступні значення: $M_{p1} = 6305$, $M_{p2} = 5516$. В такому випадку маршрут $p1$ більше не буде оптимальним, а пакети передаватимуться по маршруту $p2$, тим самим зменшуючи ризик порушення інформаційної безпеки транзитних даних.

35 Наведений приклад підтверджує досягнення технічного результату при здійсненні заявленого способу.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

40 Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки, що здійснює динамічну маршрутизацію трафіку на основі математичної моделі протоколу EIGRP, який відрізняється тим, що завдяки введенню додаткового параметру ризику інформаційної безпеки R_s^p маршруту p при передачі трафіку між вузлом-відправником i та вузлом-отримувачем j змінюється метрика протоколу EIGRP з урахуванням вимог інформаційної безпеки та забезпечується вибір найбільш безпечного, як для даних так і для мережі, маршруту передачі трафіку в заданій мережі між вузлами i, j , при цьому формула розрахунку метрики приймає наступний вигляд:

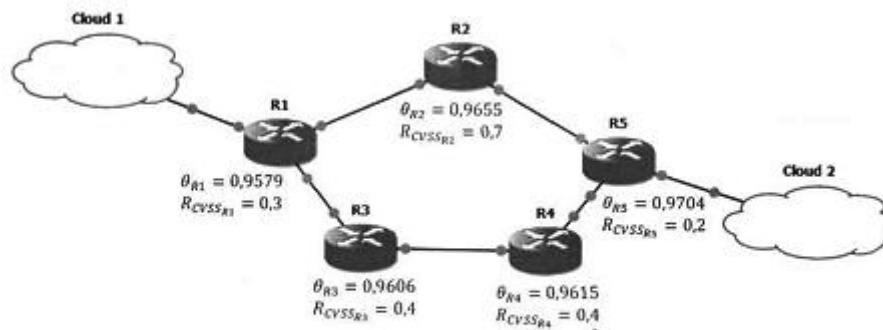
$$M_p = \left[\left(K_1 \cdot B_{\min}^p + \frac{K_2 \cdot B_{\min}^p}{256 - L_{\text{sum}}^p} + K_3 \cdot \frac{D_{\text{sum}}^p}{10} \right) \cdot \frac{K_5}{K_4 + R_{\text{sum}}^p} \right] \cdot 16^{(2 - (1 - R_s^p))},$$

де $B_{\min}^p$ - найменше значення зваженого показника пропускну здатності в маршруті p ; $L_{\max}^p$ -

50 найбільше завантаження одного з каналів зв'язку в маршруті p ; D_{sum}^p - сумарна затримка

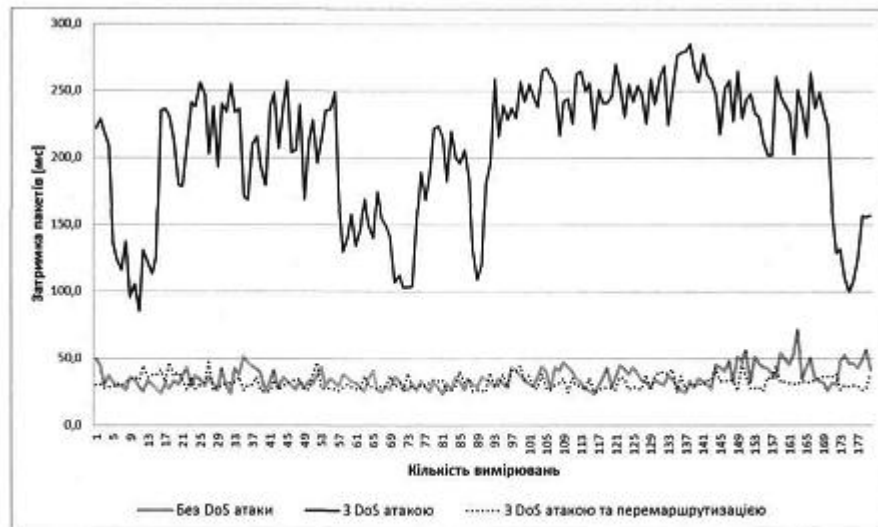
пакетів в маршруті p [мкс]; $R_{\min}^p$ - найменша надійність одного з каналів зв'язку в маршруті p ; $p \in P_{i,j}$, $P_{i,j}$ - усі можливі маршрути в заданій мережі при передачі інформації між вузлами i, j , при $i \neq j$; K_1, K_2, K_3, K_4, K_5 - коефіцієнти, що дозволяють враховувати в метриці вищевказані параметри, при $K_1, K_3 = 1$ та $K_2, K_4, K_5 = 0$; R_s^p - показник ризику, який розраховується як

5 просте математичне середнє ризику усіх вузлів в маршруті p , при $R_s^p \in [0; 1]$.



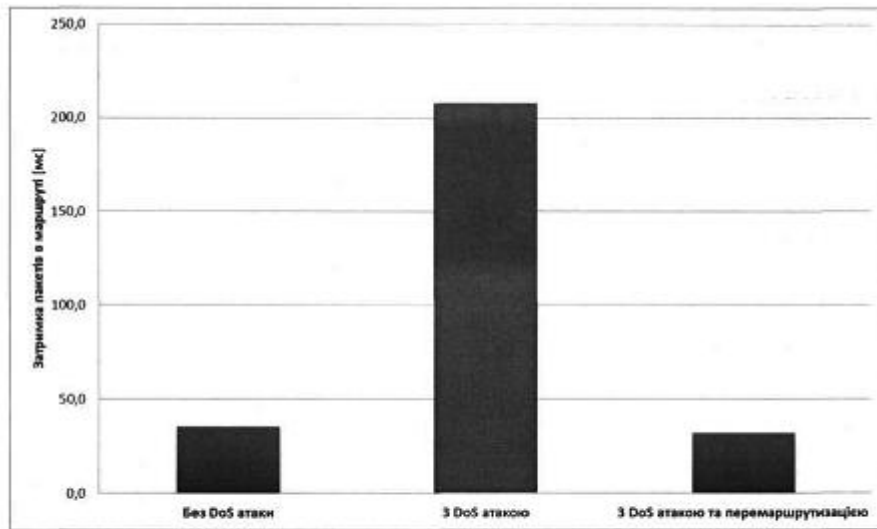
топологія мережі, що використовується для проведення експериментів

Фіг. 1



затримка пакетів при передачі за оптимальним маршрутом при наявності/відсутності атаки/захисних заходів

Фіг. 2



середня затримка пакетів в маршруті при наявності/відсутності
атаки/захисних заходів

Fig. 3

Комп'ютерна верстка Г. Паяльніков

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601