

ISSN 1998-7927(print) ISSN 2664-6498 (online)

DOI: <https://doi.org/10.33216/1998-7927-2026-304-6-115-120>

УДК 004.7:004.056

МЕТОД ЗАБЕЗПЕЧЕННЯ ВІДМОВСТІЙКОСТІ БАГАТОКАНАЛЬНОЇ МЕРЕЖІ ШЛЯХОМ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА ДИНАМІЧНОГО ПЕРЕМИКАННЯ МАРШРУТІВ

Ваврічен В.О., Лобур Т.Б., Деркач М.В., Стадник М.А.

A METHOD FOR ENSURING FAULT TOLERANCE OF MULTI-HOMED NETWORK THROUGH LOAD BALANCING AND DYNAMIC ROUTE SWITCHING

Vavrichen V.O., Lobur T.B., Derkach M.V., Stadnyk M.A.

У статті розглянуто задачу забезпечення відмовостійкості багатоканальних мереж для підвищення доступності мережесервісів і безперервності функціонування інформаційної інфраструктури. Актуальність дослідження зумовлена зростанням вимог до надійності корпоративних мереж, у яких відмова окремих каналів зв'язку, перевантаження мережі або погіршення якості з'єднання можуть призвести до порушення роботи критично важливих інформаційних ресурсів. У роботі запропоновано метод забезпечення відмовостійкості багатоканальної мережі, у якій балансування мережесервісів між доступними WAN-каналами поєднано з динамічним перемиканням маршрутів залежно від їх доступності. Метод передбачає узгоджене використання маркування з'єднань і маршрутів, окремих таблиць маршрутизації та механізму автоматичного виключення недоступного каналу з подальшим перенаправленням трафіку через працездатні канали. Для проведення дослідження використано платформу VMware Workstation, у середовищі якої змодельовано віртуальну мережесервіс інфраструктуру з операційною системою MikroTik RouterOS Cloud Hosted Router. Побудована архітектура передбачає використання трьох незалежних WAN-каналів, технології Per Connection Classifier, засобів спеціалізованої підсистеми Mangle, окремих таблиць маршрутизації, механізмів трансляції мережесервіс адрес та автоматичного резервування каналів. Оцінку ефективності розробленого методу здійснено із застосуванням інструментів Ping, Tracert, SpeedTest та Wireshark, що дозволило дослідити коректність маршрутизації, стабільність передачі даних, пропускну здатність мережі, якість мережесервіс з'єднання. Результати проведеного моделювання продемонстрували відсутність втрат пакетів, рівномірний розподіл мережесервіс навантаження між доступними каналами зв'язку навіть за умов відмови одного з WAN-каналів завдяки автоматичному перенаправленню мережесервіс трафіку на резервні канали без необхідності ручного втручання адміністратора та з подальшим передаванням

нових мережесервіс з'єднань через доступні канали. Запропонований метод може бути впроваджений під час побудови корпоративних мереж та інших інформаційно-комунікаційних систем, для яких критичними є доступність сервісів, надійність функціонування, відмовостійкість та безперервність передачі даних.

Ключові слова: багатоканальна мережа, балансування навантаження, безперервність, відмовостійкість, динамічне перемикання маршрутів.

Вступ. Стрімкий розвиток інформаційно-комунікаційних технологій, поширення хмарних сервісів, віддаленої роботи та цифрових платформ зумовлюють підвищення вимог до надійності й безперервності функціонування мережесервіс інфраструктури. Для сучасних організацій стабільний доступ до мережесервіс ресурсів є необхідною умовою ефективного виконання бізнес-процесів, забезпечення інформаційної взаємодії та надання цифрових послуг. Навіть короточасне порушення мережесервіс з'єднання може призвести до простою інформаційних систем, втрати даних, зниження продуктивності та фінансових збитків. Особливо актуальною ця проблема є для корпоративних мереж, у яких одночасно використовуються хмарні сервіси, системи IP-телефонії, відеоконференцзв'язок та інші критично важливі інформаційні ресурси.

Одним із перспективних напрямів підвищення доступності мережесервіс є побудова багатоканальної архітектури доступу, що поєднує декілька незалежних каналів зв'язку. Такий підхід забезпечує рівномірний розподіл мережесервіс навантаження, автоматичне резервування каналів у разі виникнення відмов, а також підвищує стійкість

мережі до технічних несправностей і зовнішніх факторів. Особливої актуальності це набуває при одночасному використанні традиційних WAN-з'єднань, мобільних мереж LTE та супутникових систем зв'язку Starlink, які характеризуються різними параметрами пропускної здатності, затримки та доступності.

Разом із перевагами багатоканальна мережа потребує ефективних механізмів маршрутизації, балансування навантаження та автоматичного перемикавання між каналами. Крім того, така інфраструктура повинна враховувати можливі ризики, пов'язані з перевантаженням каналів, нестабільністю окремих типів з'єднань, помилками конфігурації та іншими чинниками, що можуть негативно впливати на доступність надання мережевих сервісів [1].

У зв'язку з цим актуальним є дослідження підходів до побудови відмовостійких багатоканальних мереж із застосуванням сучасних засобів маршрутизації, балансування навантаження та резервування каналів зв'язку.

Аналіз останніх досліджень і публікацій. Питання забезпечення відмовостійкості та ефективного використання ресурсів багатоканальних мереж останніми роками набуло особливої актуальності у зв'язку зі стрімким поширенням хмарних сервісів, периферійних обчислень (Edge Computing), технологій Інтернету речей та гібридних корпоративних мереж [2-4]. Традиційні архітектури WAN, що базуються на статичній маршрутизації або застосуванні одного каналу доступу, дедалі частіше не забезпечують необхідного рівня доступності, масштабованості та стійкості до відмов, особливо за умов змінного мережевого навантаження [5].

Сучасні дослідження переважно орієнтовані на розвиток концепції Software-Defined Wide Area Network (SD-WAN), яка забезпечує централізоване керування мережею, динамічне балансування трафіку, автоматичне резервування каналів зв'язку та адаптивну маршрутизацію.

У дослідженні [6] проаналізовано сучасний стан розвитку SD-WAN, класифіковано основні напрями досліджень, серед яких трафік-інжиніринг, оптимізація мережевих ресурсів, оркестрація сервісів і механізми забезпечення безпеки. Автори наголошують, що перспективними залишаються задачі інтелектуального балансування навантаження, забезпечення відмовостійкості та автоматичного відновлення після відмов каналів зв'язку.

Особливу увагу в роботі [7] приділено проблемам функціонування мереж у разі відмови контролерів, автори пропонують підходи до відновлення програмованості маршрутів, що дозволяють мінімізувати деградацію продуктивності мережі, та підкреслюють необхідність впровадження ефективних механізмів резервування й автоматичного переключення маршрутів, особливо для критично важливих інформаційних систем.

Подальший розвиток цього напрямку пов'язаний із реалізацією механізмів динамічного вибору маршрутів залежно від характеристик мережі. Підхід у роботі [5] демонструє, що адаптивний розподіл трафіку між декількома каналами дозволяє підвищити ефективність використання пропускної здатності та покращити якість обслуговування мережевих сервісів.

Окремим напрямом досліджень є впровадження інтелектуальних методів оптимізації балансування навантаження [8,9]. Зокрема, робота [10] демонструє перспективність алгоритмів глибокого навчання з підкріпленням (Deep Reinforcement Learning), які забезпечують адаптивний вибір маршрутів відповідно до поточного стану мережі та змін характеристик каналів зв'язку. Проте такі рішення потребують значних обчислювальних ресурсів, централізованої інфраструктури керування та складної інтеграції у вже існуючі корпоративні мережі.

Попри значний розвиток SD-WAN, питання практичної реалізації відмовостійкої багатоканальної маршрутизації на основі доступних засобів маршрутизації залишаються актуальними. Зокрема, потребує дослідження організація взаємодії механізмів балансування мережевих з'єднань, маркування маршрутів, окремих таблиць маршрутизації та автоматичного резервування каналів у разі зміни їх доступності. Такий підхід дозволяє розглядати не окремі механізми маршрутизації, а їх спільне використання для підтримання доступності мережевих сервісів за умов відмови одного з каналів зв'язку.

Мета статті. Розробити та дослідити метод забезпечення відмовостійкості багатоканальної мережі, який передбачає розподіл мережевих з'єднань між доступними WAN-каналами та автоматичне перемикавання маршрутів у разі зміни стану їх доступності.

Метод забезпечення відмовостійкості багатоканальної мережі. Основою

запропонованого методу є послідовна взаємодія механізмів розподілу з'єднань і динамічного керування маршрутами. Функціонування методу передбачає виконання таких основних етапів:

1. Визначення доступних WAN-каналів та формування відповідних маршрутів.
2. Класифікація нових мережевих з'єднань і призначення їм відповідних маршрутів.
3. Передавання трафіку через визначені WAN-канали відповідно до сформованого розподілу.
4. Контроль доступності каналів зв'язку.
5. У разі недоступності одного з каналів його виключення з маршрутизації та перенаправлення нових з'єднань через доступні канали.

Така послідовність забезпечує адаптацію маршрутизації до поточного стану WAN-з'єднань без необхідності ручної зміни конфігурації. Таким чином, балансування навантаження та резервування

каналів розглядаються як взаємопов'язані етапи функціонування одного методу.

Для проведення дослідження розробленого методу було сформовано віртуальне експериментальне середовище із застосуванням платформи VMware Workstation, що забезпечує можливість моделювання складних мережових архітектур без використання фізичного обладнання. Реалізація технології віртуалізації дозволяє створювати ізольовані мережові сегменти, конфігурувати віртуальні мережові адаптери та комутатори, а також відтворювати різні сценарії функціонування мережі за контрольованих умов. Такий підхід значно спрощує здійснення експериментальних досліджень, забезпечує відтворюваність отриманих результатів та мінімізує витрати на розгортання тестової інфраструктури.

Як програмну платформу маршрутизації використано операційну систему MikroTik RouterOS Cloud Hosted Router (CHR), що підтримує реалізацію сучасних механізмів маршрутизації, балансування навантаження, трансляції мережових адрес (NAT) та резервування каналів зв'язку. Використання MikroTik RouterOS CHR у віртуалізованому середовищі дозволило максимально наблизити експериментальні умови до реальної корпоративної мережової інфраструктури.

У процесі дослідження було змодельовано багатоканальну мережу (рис. 1), що включає три незалежні канали доступу до мережі Інтернет: основний WAN-канал, супутниковий канал Starlink та мобільний канал LTE, який застосовується як резервний. Для внутрішнього сегмента мережі було сформовано окремий LAN-інтерфейс, через який здійснювався обмін даними між маршрутизатором та клієнтською системою. Кожному інтерфейсу призначено статичні IP-адреси, що забезпечило незалежність функціонування окремих каналів та можливість їх подальшого тестування.

```
[admin@MikroTik] > /interface print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
# NAME TYPE ACTUAL-MTU MAC-ADDRESS
0 R lan ether 1500 00:0C:29:1B:E0:99
1 R wan1 ether 1500 00:0C:29:1B:E0:7B
2 R wan2 ether 1500 00:0C:29:1B:E0:85
3 R wan3 ether 1500 00:0C:29:1B:E0:8F
4 R lo loopback 65536 00:00:00:00:00:00
[admin@MikroTik] > _
```

Рис. 1. Архітектура багатоканальної мережі

Запропонована архітектура спрямована на забезпечення доступності інформаційних сервісів шляхом використання декількох незалежних каналів передачі даних. У разі виникнення відмови одного із зовнішніх каналів маршрутизатор автоматично перенаправляє мережний трафік через резервне підключення без необхідності ручного втручання адміністратора та з подальшим передаванням нових мережових з'єднань через доступні канали. Такий підхід дозволяє мінімізувати ризик втрати доступу до

інформаційних ресурсів та підвищує стійкість мережової інфраструктури до відмов.

На початковому етапі дослідження налаштовано базову конфігурацію MikroTik RouterOS CHR, яка передбачала налаштування мережових інтерфейсів, призначення IP-адрес, конфігурацію шлюзів за замовчуванням, DNS-серверів, локальної мережі та правил трансляції мережових адрес. Механізм NAT у режимі masquerade забезпечує коректне перетворення локальних IP-адрес у зовнішні під час передавання трафіку до мережі Інтернет [11], що дозволяє організувати одночасну роботу кількох WAN-інтерфейсів без конфліктів адресації та є необхідною умовою функціонування багатоканальної мережової архітектури. Для кожного каналу зв'язку створено окреме правило masquerade, яке забезпечує правильну трансляцію адрес відповідно до інтерфейсу виходу (рис. 2), що сприяє стабільній роботі методу забезпечення відмовостійкості багатоканальної мережі на основі балансування навантаження та динамічного перемикавання маршрутів.

```
[admin@MikroTik] > /ip firewall nat print terse
0 chain=srcnat action=masquerade out-interface=wan2
1 chain=srcnat action=masquerade out-interface=wan3
2 chain=srcnat action=masquerade out-interface=wan1
```

Рис. 2. Конфігурація NAT в MikroTik RouterOS CHR

Для впровадження механізму балансування навантаження застосовано технологію Per Connection Classifier (PCC), реалізовану засобами підсистеми Mangle операційної системи MikroTik RouterOS CHR. Принцип роботи алгоритму полягає у класифікації нових мережових з'єднань із подальшим рівномірним розподілом трафіку між декількома WAN-інтерфейсами. Для кожного сформованого з'єднання виконувалося маркування (connection marking), після чого відповідно до визначених правил здійснювалося маркування маршрутів (routing marking), що дозволило асоціювати трафік із відповідними таблицями маршрутизації. Такий підхід забезпечує збалансований розподіл навантаження між усіма доступними каналами зв'язку та підтримує цілісність мережових сесій під час передавання даних.

З метою забезпечення відмовостійкості мережової інфраструктури було сформовано окремі таблиці маршрутизації для кожного WAN-каналу (рис. 3).

```
[admin@MikroTik] > /ip route print where dst-address=0.0.0.0/0
Flags: D - DYNAMIC; I - INACTIVE; A - ACTIVE; S - STATIC; d - DHCP
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
# DST-ADDRESS GATEWAY ROUTING-TABLE DISTANCE
0 Dd 0.0.0.0/0 192.168.1.1 wan1 1
0 As 0.0.0.0/0 192.168.1.1 to_wan1 1
1 Is 0.0.0.0/0 192.168.2.1 to_wan2 1
2 Is 0.0.0.0/0 192.168.3.1 to_wan3 1
[admin@MikroTik] > _
```

Рис. 3. Таблиця маршрутизації в MikroTik RouterOS CHR

А також реалізовано механізм динамічного перемикавання маршрутів із використанням автоматичного резервування каналів шляхом

налаштування основного маршруту через три канали одночасно:

```
/ip route add dst-address=0.0.0.0/0
gateway=192.168.10.1,192.168.20.1,192.168.30.1
```

У разі втрати доступності одного з WAN-каналів маршрутизатор автоматично виключає його з процесу маршрутизації та перенаправляє трафік через інші працездатні канали без необхідності ручного втручання адміністратора, тим самим забезпечуючи оперативний розподіл мережевого трафіку відповідно до поточного стану доступності каналів зв'язку.

Розроблений метод забезпечує автоматичне перемикання маршрутизації у разі недоступності WAN-каналу та підтримує передавання мережевого трафіку через доступні канали.

Результати тестування розробленого методу. Після завершення конфігурації було проведено експериментальне дослідження функціонування запропонованої мережевої архітектури. Під час тестування аналізувалися основні показники якості мережевого з'єднання, зокрема затримка передавання пакетів, їх втрата, пропускна здатність каналів, рівень завантаження мережі та можливі помилки конфігурації. Це дозволило оцінити стабільність функціонування кожного каналу зв'язку, поведінку мережі за умов різного навантаження та особливості перемикання трафіку на резервні канали.

Для перевірки ефективності методу забезпечення відмовостійкості багатоканальних мереж було змодельовано сценарій відмови одного з WAN-каналів. Для цього відповідний інтерфейс було примусово відключено, після чого аналізувалися зміни маршрутів. Для моніторингу та аналізу мережевого трафіку використовувалися інструменти Ping, Tracert, SpeedTest та Wireshark [12]. За результатами аналізу мережевого трафіку не виявлено порушень маршрутизації чи некоректного розподілу з'єднань між активними WAN-каналами, це свідчить про успішне динамічне перемикання трафіку на резервний канал.

Експеримент показав працездатність реалізованого методу. Під час тестування було передано 20 ICMP-пакетів, усі з яких успішно отримали відповідь, втрати пакетів відсутні (0 %), значення TTL = 119 є стабільним для всіх відповідей, час відгуку змінюється в межах 21–35 мс, при цьому середній час становить 23,993 мс (рис. 4). Такі показники свідчать про низьку затримку передавання даних та відсутність істотних коливань часу відповіді, що є характерним для стабільного мережевого з'єднання.

Отримані результати підтверджують працездатність запропонованого методу розподілу та динамічного перемикання мережевого трафіку. Використання маркування з'єднань і маршрутів у поєднанні з окремими таблицями маршрутизації

забезпечило розподіл трафіку між доступними WAN-каналами (рис. 5).

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	119	34ms90us	
1	8.8.8.8	56	119	23ms682us	
2	8.8.8.8	56	119	22ms928us	
3	8.8.8.8	56	119	23ms244us	
4	8.8.8.8	56	119	24ms23us	
5	8.8.8.8	56	119	23ms285us	
6	8.8.8.8	56	119	27ms8us	
7	8.8.8.8	56	119	22ms849us	
...					
14	8.8.8.8	56	119	21ms665us	
15	8.8.8.8	56	119	22ms782us	
16	8.8.8.8	56	119	28ms288us	
17	8.8.8.8	56	119	22ms147us	
18	8.8.8.8	56	119	24ms297us	
19	8.8.8.8	56	119	22ms417us	
...tool-20 received=20 packet-loss=0% min-rtt=21ms665us avg-rtt=23ms993us max-rtt=34ms90us					
SEQ	HOST	SIZE	TTL	TIME	STATUS
20	8.8.8.8	56	119	25ms688us	
21	8.8.8.8	56	119	23ms546us	

Рис. 4. Результати тестування стабільності каналів зв'язку

```
[admin@Mikrotik] > /ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=prerouting action=mark-connection new-connection-mark=wan1_conn
  pass-through=yes dst-address-type=!local in-interface=lan
  per-connection-classifier=both-addresses:3/0
1 chain=prerouting action=mark-connection new-connection-mark=wan2_conn
  pass-through=yes dst-address-type=!local in-interface=lan
  per-connection-classifier=both-addresses:3/1
2 chain=prerouting action=mark-connection new-connection-mark=wan3_conn
  pass-through=yes dst-address-type=!local in-interface=lan
  per-connection-classifier=both-addresses:3/2
[admin@Mikrotik] >
```

Рис. 5. Конфігурація Mangle з використанням PCC

При відключенні одного з каналів маршрутизація продовжила функціонувати через доступні підключення, що підтверджує працездатність механізму автоматичного резервування. Таким чином, реалізація методу на основі балансування навантаження та динамічного перемикання маршрутів із застосуванням механізмів резервування каналів зв'язку забезпечує рівномірний розподіл мережевого навантаження між доступними каналами зв'язку, зберігаючи доступність мережі навіть у разі відмови одного з них. Розроблений метод може бути реалізований під час побудови корпоративних мереж, для яких критичними є висока доступність сервісів, безперервність передачі даних та ефективне використання пропускної здатності декількох незалежних каналів доступу до мережі Інтернет.

Висновок. У роботі розроблено та експериментально досліджено метод забезпечення відмовостійкості багатоканальної мережі на основі розподілу мережевих з'єднань між доступними WAN-каналами та динамічного перемикання маршрутів у разі зміни їх доступності. Це завдання є актуальним, оскільки може розглядатися як один із практичних механізмів забезпечення доступності інформаційних сервісів, що є однією з базових властивостей інформаційної безпеки сучасних інформаційно-комунікаційних систем.

Запропонований метод передбачає узгоджене використання механізмів PCC, Mangle, окремих таблиць маршрутизації та автоматичного резервування каналів. Науковий результат полягає у способі організації взаємодії зазначених механізмів, за якого зміна доступності одного з WAN-каналів призводить до його виключення з маршрутизації та

подальшого розподілу нових мережевих з'єднань між доступними каналами.

Експериментальне моделювання у середовищі VMware Workstation із використанням MikroTik RouterOS CHR підтвердило працездатність запропонованого методу. Під час тестування аналізувалися основні показники функціонування мережі, серед яких затримка передавання пакетів, рівень їх втрат, пропускна здатність каналів, стабільність маршрутизації та наявність можливих помилок конфігурації. Окрему увагу приділено оцінюванню поведінки системи за умов відмови одного із WAN-інтерфейсів, що дозволило визначити ефективність реалізованого механізму автоматичного резервування та оцінити його вплив на безперервність функціонування мережевих сервісів.

Практичне значення отриманих результатів полягає у можливості використання запропонованого методу під час побудови корпоративних мереж, інформаційно-комунікаційних систем та інших об'єктів критичної інфраструктури, для яких забезпечення доступності сервісів є одним із ключових завдань кібербезпеки.

Л і т е р а т у р а

27. Waqdan M., Louafi H., Mouhoub M. Security risk assessment in IoT environments: A taxonomy and survey // *Computers & Security*. 2025. Vol. 154.
28. Skarga-Bandurova I., Biloborodova T., Kjelstrup-Johnson K. R., Scheper T. V. O., Derkach M. Securing Tomorrow's Cities: Smart Infrastructure for Emergency Response, Crisis Management, and Defence // *Sustainable, Innovative, and Intelligent Industries and Societies*. Cham : Springer Nature Switzerland, 2026. P. 69–111.
29. Malyuta Y., Derkach M., Lobur T. Modeling a Fog Computing Network Architecture for Secure IoT Data Processing // *Security of Infocommunication Systems and Internet of Things*. 2025. Vol. 3, No. 2. Article 02017.
30. Petliak N., Klots Y., Karpinski M., Titova V., Tymoshchuk D. Hybrid system for detecting abnormal traffic in IoT // *CEUR Workshop Proceedings*. 2025. Vol. 4057. P. 21–36.
31. Ahmad S. K., Dixit M. Implementation of SD-WAN with Intelligent Traffic Steering and Load Balancing Based on SLA Metrics // *International Journal of Engineering and Management Research*. 2026. Vol. 16, No. 2. P. 98–105.
32. Fu C., Wang B., Wang W. Software-Defined Wide Area Networks (SD-WANs): A Survey // *Electronics*. 2024. Vol. 13, No. 15. Art. 3011.
33. Dou S., Guo Z. Path Programmability Recovery under Controller Failures for SD-WANs: Recent Advances and Future Research Challenges // *IEEE Communications Magazine*. 2024. Vol. 62, No. 11. P. 100–106.
34. Zagorodna N., Stadnyk M., Lypa B., Gavrylov M., Kozak R. Network Attack Detection Using Machine Learning Methods // *Challenges to National Defence in Contemporary Geopolitical Situation*. 2022. Vol. 1. P. 55–61.
35. Tymoshchuk D., Sverstiuk A., Klots Y., Petliak N., Titova V. An Explainable Artificial Intelligence Approach for Detecting Network Attacks // *CEUR Workshop Proceedings*. 2025. Vol. 4141. P. 38–51.
36. Cruvellier B., Jia D., Conan V., Jakllari G. Dynamic Load Balancing in SD-WAN with Deep Reinforcement Learning // *GLOBECOM 2025 – IEEE Global Communications Conference*. 2025. P. 4053–4058.
37. Mishko O., Matiuk D., Derkach M. Security of Remote IoT System Management by Integrating Firewall Configuration into Tunneled Traffic // *Scientific Journal of TNTU*. 2024. Vol. 115, No. 3. P. 122–129.
38. Lypa B., Horyn I., Zagorodna N., Tymoshchuk D., Lechachenko T. Comparison of Feature Extraction Tools for Network Traffic Data // *CEUR Workshop Proceedings*. 2024. Vol. 3896. P. 1–11.

Vavrichen V.O., Lobur T.B., Derkach M.V., Stadnyk M.A. A method for ensuring fault tolerance of multi-homed network through load balancing and dynamic route switching

The paper addresses the problem of ensuring fault tolerance of multi-homed networks to improve the availability of network services and the continuity of information infrastructure operation. The relevance of the study is determined by the increasing reliability requirements of corporate networks, where the failure of individual communication links, network congestion, or degradation of connection quality may disrupt the operation of critical information resources. The paper proposes a method for ensuring the fault tolerance of a multi-homed network, in which load balancing of network connections across available WAN links is combined with dynamic route switching depending on their availability. The method involves the coordinated use of connection and route marking, separate routing tables, and a mechanism for automatically excluding an unavailable link followed by traffic redirection through operational links. The study was conducted using the VMware Workstation platform, within which a virtual network infrastructure was modelled using the MikroTik RouterOS Cloud Hosted Router operating system. The developed architecture incorporates three independent WAN links, the Per Connection Classifier technology, the Mangle subsystem, separate routing tables, network address translation mechanisms, and automatic link redundancy. The effectiveness of the proposed method was evaluated using Ping, Tracert, SpeedTest, and Wireshark, which made it possible to investigate routing correctness, data transmission stability, network throughput, and connection quality. The simulation results demonstrated zero packet loss and a balanced distribution of network load among the available communication links, including under the failure of one of the WAN links, due to the automatic redirection of network traffic to redundant links without the need for manual administrator intervention, followed by the transmission of new network connections through the available links. The proposed method can be implemented in corporate networks and other information and communication systems where service availability, operational reliability, fault tolerance, and continuity of data transmission are critical requirements.

Keywords: multi-homed network, load balancing, continuity, fault tolerance, dynamic route switching.

Ваврічен Вікторія Олексіївна – здобувач вищої освіти кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя,

<https://orcid.org/0009-0004-8368-0327>.

e-mail: viktoriavavrichen@gmail.com,

Лобур Тарас Богданович – старший викладач кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя,

<https://orcid.org/0000-0001-8318-3815>.

e-mail: lobur_t@tntu.edu.ua,

Деркач Марина Володимирівна – к.т.н., доц., доцент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя,

<https://orcid.org/0000-0001-8977-2776>.

e-mail: m_derkach@tntu.edu.ua,

Стадник Марія Андріївна – к.т.н., доц., доцент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя,

<https://orcid.org/0000-0002-0287-2254>.

e-mail: stadnyk_m@tntu.edu.ua,

Дата першого надходження статті 16.07.2026.

Дата прийняття статті до друку після рецензування 26.08.2026.

Дата публікації 30.09.2026.



Стаття з відкритим доступом,
відповідно до умов ліцензії
[Creative Commons \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)