

Ярослав Вячеславович Мельник  
Віктор Євгенович Бобильов (кандидат військових наук, с.н.с.)

Національний університет оборони України імені Івана Черняхівського, Київ, Україна

## МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ІСНУЮЧИХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ПРОГРАМНИХ УТИЛІТ ДЛЯ ВИЗНАЧЕННЯ ТОПОЛОГІЇ ГЕТЕРОГЕННИХ МЕРЕЖ ДЛЯ ЗНАХОДЖЕННЯ АЛЬТЕРНАТИВНИХ ВАРІАНТІВ ПІДКЛЮЧЕННЯ

Сучасне інформаційне середовище постійно наражається на вплив зовнішніх або внутрішніх завад. У сучасний період постійного розвитку і удосконалення засобів радіоелектронної боротьби та методів впливу на телекомунікаційні системи їх захист стає дуже важливою та актуальною проблемою.

Існують програмне забезпечення та програмні утиліти, що представляють собою сукупність підходів, які надають можливість будувати телекомунікаційні мережі стійкими до впливу тих чи інших завад. Але більшість з них стосується технічних аспектів побудови мережі. Що стосується топології таких мереж, то при їх обґрунтуванні можна спиратися лише на їх невелику кількість.

Справа у тому, що гетерогенні мережі мають у своїй структурі велику кількість вузлів, що безпосередньо піддані впливу навмисних та ненавмисних завад. Тому, часом, виникає необхідність здійснювати заміну вузлів, через які проходить інформація, на інші, у зв'язку із впливом на них завад.

Заміна вузлів, або переключення проходження інформації через інші вузли, на які не впливають завади, породжує зміну топології гетерогенної мережі, що забезпечує альтернативні варіанти їх підключення.

На даний час не існує єдиних методичних підходів до реалізації дій щодо зміни топології мереж. Їх наявність надасть можливість обґрунтовано змінювати топологію гетерогенних мереж (ГМ) для забезпечення альтернативних варіантів їх підключення.

Тому, нижче наведена стаття присвячена наданню методичних рекомендацій щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж при пошуку альтернативних варіантів підключення.

**Ключові слова:** гетерогенна мережа; програмне забезпечення; програмні утиліти; топологія мереж; маршрутизація; структура гетерогенних мереж.

### Вступ

**Постановка проблеми.** У науково-технічних виданнях, що присвячені питанням побудови та використання сучасних телекомунікаційних мереж, описано декілька підходів до їх побудови та утримання у працездатному стані під час впливу на них навмисних та ненавмисних завад.

Структуру телекомунікаційної мережі загального користування (ТМЗК), у тому випадку, коли її неможливо одержати у якості вихідних даних від оператора зв'язку, виявляють шляхом аналізу ТМЗК спеціалізованим програмним (ПЗ). Наприклад, існуючі утиліти PathPing у сімействі операційних систем (ОС) MS Windows XP/2003/7/8/10 дозволяють визначити множину маршрутів у ТМЗК до необмеженої множини її кінцевих і транзитних елементів. Аналогічними утилітами є TracerPath та Tracerout у ОС Unix.

**Метою статті** є надання методичних рекомендацій щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж при пошуку альтернативних варіантів підключення.

### Виклад основного матеріалу дослідження

Алгоритм розкриття структури мережі систем загального користування носить ітеративний характер та складається із двох етапів: пошуку вузлів мережі та перевірки можливості встановити маршрут через наступний знайдений вузол.

Перед початком роботи алгоритму необхідно визначити вихідні дані. Для їх одержання, у першу чергу, знаходять перший маршрут шляхом трасування маршруту між вузлами зв'язку. При цьому для кожної пари вузлів  $A$  і  $B$  здійснюється як трасування  $A \rightarrow B$  так і  $B \rightarrow A$ , що часто дозволяє знаходити різні маршрути. Приклад реверсивного трасування наведений у таблиці 1.

Таблиця 1  
Приклад реверсивного трасування

	Маршрут $A \rightarrow B$	Маршрут $B \rightarrow A$
1.	217.76.205.218	188.213.165.186
2.	172.16.200.254	188.213.165.3
3.	172.16.200.1	62.149.185.51
4.	217.76.205.217	149.6.18.49
5.	149.6.190.78	130.117.48.113
6.	149.6.190.77	154.54.59.2
7.	130.117.48.93	154.54.60.113
8.	154.54.59.86	130.117.0.62
9.	154.54.58.5	154.54.59.181
10.	130.117.0.17	154.54.59.186
11.	154.54.38.102	154.54.36.234
12.	154.54.59.1	149.6.190.78
13.	130.117.48.114	217.76.205.217
14.	149.6.18.50	217.76.205.218
15.	62.149.185.60	
16.	188.213.165.186	

Одержання множини маршрутів з декількох точок до деякої кількості вузлів ТМЗК вже дозволяє отримати інформацію про її розгалуженість. Для більш детального вивчення структури ТМЗК можна виділити адресу будь-якого транзитного вузла, визначити по ньому адресу підмережі провайдера, до якої він належить, а потім здійснити пошук маршрутів до всіх вузлів, що входять у знайдені підмережі.

Алгоритм розкриття маршруту для одного варіанту підключення складається з наступних кроків (рис. 1):

1. Задається множина множин  $B = \{b^i\}$ ,  $\{b^j\} = \{e_b\}$ ,  $b \cap_j = \emptyset$  граничних вузлів (рис. 1, а).

2. Попарно визначаються усі маршрути  $r = \{e_r^j\}$ , з кожного вузла кожної множини границь до кожного вузла інших множин  $b$  (рис. 1, б).

3. Для усіх визначених в  $\{r\}$  вузлів  $\{e_r^j\}$  здійснюється виділення підсистеми провайдера, до якої належить вузол. Одержують множину  $e = \{e_r^j\}$ , яка містить у собі усі вузли підмереж провайдерів, через які проходять базові маршрути.

4. Кожний елемент  $\{e_r^j\}$  перевіряють на активність. Усі неактивні вузли видаляються з множини (рис. 1, в).

5. Здійснюють пошук маршруту з кожного вузла  $\{e_b\}$  в кожний вузол  $\{e_r^j\}$ . Отриману множину маршруту додають до  $\{r\}$ .

6. Отримують множину альтернативних маршрутів шляхом об'єднання всіх знайдених маршрутів у єдиний граф (рис. 1, г).

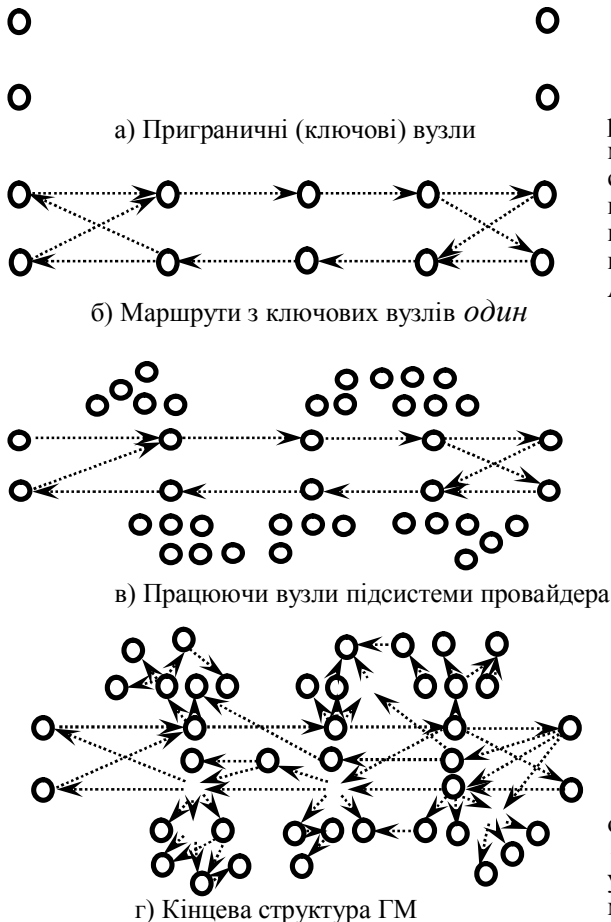


Рис. 1. Візуалізація алгоритмів розкриття ГМ

Даний алгоритм виконується для всіх варіантів підключення граничних вузлів до мережі Інтернет. Перевірка на активність знайдених вузлів здійснюється шляхом пересилання певних пакетів на різні (або усі) порти вузла.

Для автоматизації цих дій може бути використане спеціальне програмне забезпечення nmap, яке поширюється за вільною ліцензією.

Для апробації процедури було зроблено розкриття альтернативних варіантів підключення вузла  $A$  розміщеного у Києві до вузла  $B$ , розміщеного в Італії (місто Ареццо) (рис. 2).

У якості варіантів підключення вузла  $A$  розглядалося ADSL-підключення до локальної мережі. На рис. 3 і 4 показана візуалізація структури розкритої ГМ різних варіантів підключення, а також (рис. 5 і 6) графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів підключення через локальну мережу та ADSL.



Рис. 2. Географічне розташування вузла  $B$ .

У якості варіантів підключення вузла  $A$  розглядалося ADSL-підключення до локальної мережі. На рис. 3 і 4 показана візуалізація структури розкритої ГМ різних варіантів підключення, а також (рис. 5 і 6) графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів підключення через локальну мережу та ADSL.

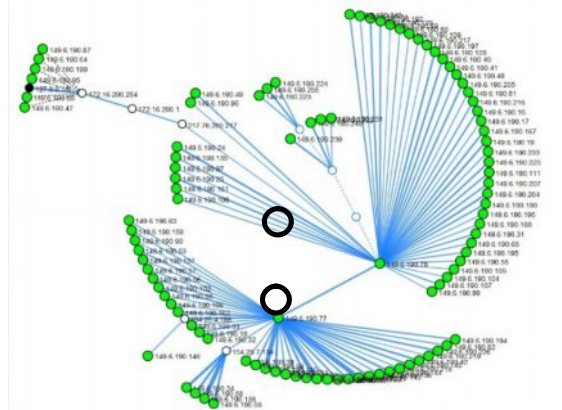


Рис. 3. Візуалізація розкритої структури ГМ з'єднання вузлів через локальну мережу

Покажемо виконання процедури на прикладі одного вузла з базових маршрутів  $B = \{217.76.205.218, 188.213.165.186\}$ . За допомогою утиліти TracerPath знайдемо перший базовий маршрут:

```
$ tracerpath 188.213.165.186
1: 172.16.200.254
2: 172.16.200.1
```

3: 217.76.205.217  
 4: 149.6.190.78  
 5: gi0-4-0-2.rcr21.kbp01.atlas.cogentco.com [149.6.190.77]  
 6: be2679.ccr21.bts01.atlas.cogentco.com [130.117.48.93]  
 7: be2988.ccr51.vie01.atlas.cogentco.com [154.54.59.86]  
 8: be2974.ccr21.muc03.atlas.cogentco.com [154.54.58.5]  
 9: be3072.ccr51.zrh02.atlas.cogentco.com [130.117.0.17]  
 10: be2043.rcr21.mil01.atlas.cogentco.com [154.54.38.102]  
 11: be3526.rcr51.vce01.atlas.cogentco.com [154.54.59.1]  
 12: be3137.rcr11.qzo03.atlas.cogentco.com [130.117.48.114]  
 13: 149.6.18.50  
 14: it1-is4-b.aruba.it [62.149.185.60]  
 15: host186-165-213-188.serverdedicati.aruba.it [188.213.165.186]

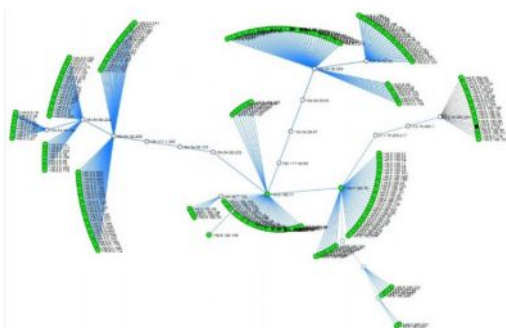


Рис. 4. Візуалізація розкритої структури ГМ з'єднання вузлів через локальну мережу

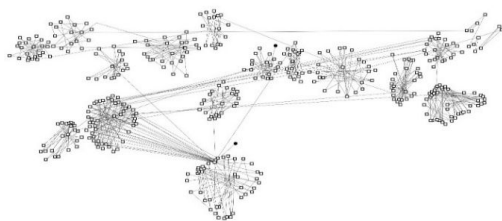


Рис. 5. Графічний спосіб візуалізації розкритої структури ГМ з'єднання вузлів через локальну мережу

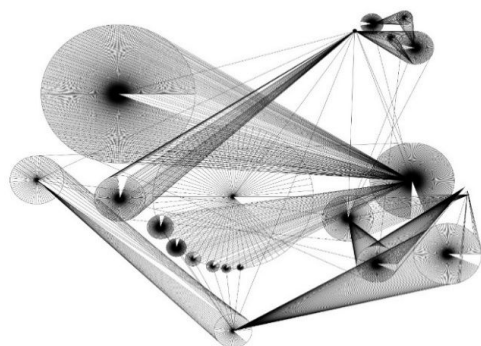


Рис. 6. Візуалізація розкритої структури ГМ з'єднання вузлів через ADSL – підключення

Визначимо підмережу провайдера першого зовнішнього вузла (149.6.190.78) за допомогою утиліти whois:  
 \$ whois 149.6.190.78

inetnum: 149.6.0.0 - 149.6.255.255  
 Діапазон вузлів 149.6.0.0 .... 149.6.255.255 додається в  $e_t$ . Перевіримо кожний вузол діапазону за допомогою утиліти nmap. Утиліта відправить певним чином сформовані запити на зазначені порти і для кожного працюючого вузла поверне наступну інформацію:  
 sudo nmap -sn -PE -PS22, 25, 80 -PA21, 23, 80, 3389 \

-PU -P0 --traceroute 149.6.0-255.0-255 149.6.190.78  
 Starting Nmap 7.70 ( <https://nmap.org> ) at 2018-05-15 10:55  
 Host 149.6.0.10 is up (0.047s latency).  
 TRACEROUTE (using port 22/tcp)  
 HOP RTT ADDRESS  
 - Hops 1-10 are the same as for 149.6.0.10  
 11 43.00 ms 149.6.0.0

Starting Nmap 7.70 at 2018-05-15 12:44 MSD  
 Host 93.157.123.0 is up (0.0021s latency).  
 MAC Address: FF:FF:FF:FF:FF:FF (Unknown)  
 Host novosm-user-gw.gtk.su (93.157.123.1) is up  
 MAC Address: 00:19:5B:F4:3B:81 (D-Link)  
 Здійснюється пошук маршруту для кожного виявленого вузла за допомогою утиліти tracerpath та всі маршрути запам'ятовуються, а далі поєднуються. Результат повного розкриття мережі наведено на рис. 2.

У випадку, коли немає можливості здійснювати пошук маршрутів з вузлів однієї з границь, можуть застосовуватися вузли-агенти. Нехай потрібно знайти всі доступні маршрути від вузла 172.16.200.254 (A), до 194.0.131.18 (B, один із серверів компанії МетаУА). Отримаємо за допомогою утиліти tracerpath маршрут A → B. Зімітуємо відсутність доступу до одного з вузлів, та задіємо вузол-агент.

1: 172.16.200.254  
 1: 172.16.205.1  
 2: 217.76.205.217  
 3: ctnet-10G-gw.ix.net.ua [185.1.50.23]  
 4: topnet2-10G-gw.ix.net.ua [185.1.50.234]  
 5: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.13]  
 6: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.14]  
 7: meta.ua [194.0.131.18]  
 Побудуємо маршрут з вузла-агента 31.172.139.22 до вузла, який аналізується 194.0.131.18:

1: v1089.nva1.kv.wnet.ua [31.172.139.22]  
 1: v3342.nval.kv.wnet.ua [217.20.162.34]  
 2: v3346.sh2.kh.wnet.ua [217.20.161.241]  
 3: v3346.sh2.kh.wnet.ua [217.20.161.241]  
 4: v3351.khar.kh.wnet.ua [217.20.161.85]  
 5: ea1.hostmsk.wnet.ua [217.20.161.85]  
 6: meta.br0-kiev-vlan823.top.net.ua [77.88.200.53]  
 7: meta-gw.top.net.ua [77.88.200.54]  
 8: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.13]  
 9: meta.ae10-822.lsr02-kiev.topnet.ua [77.88.206.14]  
 10: meta.ua [194.0.131.18]

Після цього здійснимо пошук з вихідного вузла 172.16.200.254 до вузлів з маршруту 31.172.139.22 → 194.0.131.18 і вилучимо частини маршрутів, які повторюються. У результаті було знайдено три маршрути, як наведено на рис. 7.

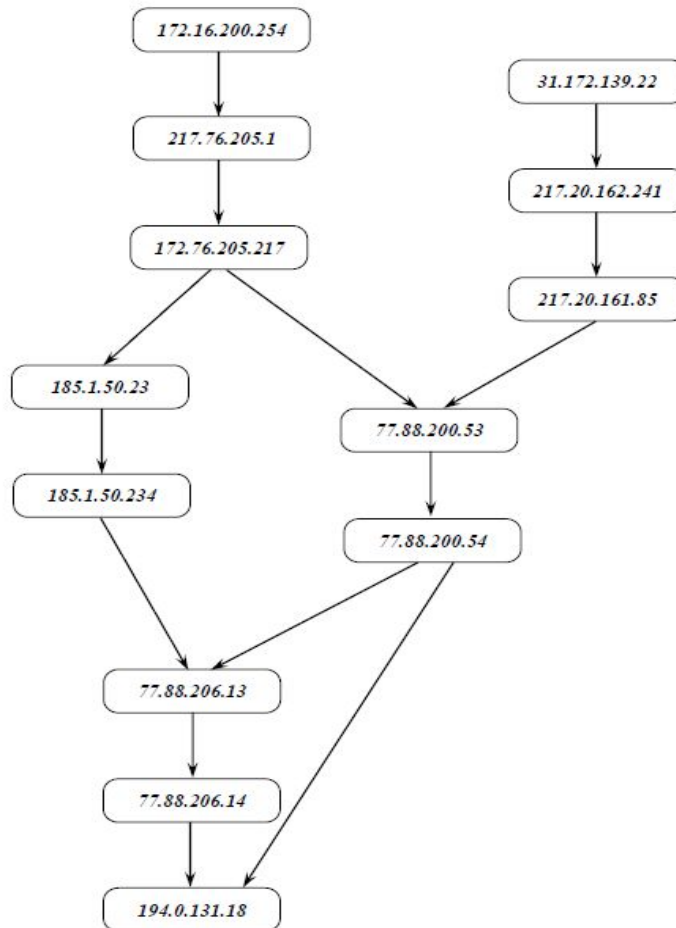


Рис. 7. Візуалізація роботи алгоритму пошуку альтернативних маршрутів за допомогою вузлів-агентів. Знайдено 3 маршрути від 172.16.200.254 до 194.0.131.18 за допомогою агента 31.172.139.22

При наявності експерта в області комп'ютерної безпеки можливо здійснити розкриття програмного та апаратного забезпечення, яке використовується на вузлі, та дати експертну оцінку надійності вузла. Під комплексним показником надійності до ННП  $e_t - \Gamma_0$  вузла розуміється нормоване чисельне значення згортки параметрів надійності, яке характеризує стійкість вузла зв'язку до впливів навмисних та ненавмисних завад. Порядок обчислення  $P_{K_i}$  відомий та описаний. Значення  $P_{K_i}$  обчислюють шляхом підсумовування, або перемножування, або як середнє арифметичне значення його параметрів надійності. При розрахунку надійності конкретного вузла може бути використана географічна інформація. Існують спеціальні бази даних (наприклад, geoip), які з високою точністю повертають інформацію про регіон вузла за його IP-адресою.

Ця ж сама інформація доступна через сервіс whois. Як правило, IP-адреси виділяються провайдером підмережами, тому може бути відсутня необхідність перевірки кожного вузла, якщо вони належать одному власникові. Запит інформації з першого транзитного вузла 217.16.205.1 з першого знайденого маршруту 172.16.200.254 --> 31.172.139.22 показав, що перші 2 транзитних вузла належать одному провайдеру (наведено неповний висновок):

```

inetmim: 217.76.192.0 - 217.76.205.255
netname: UA-CITYNET-20001129
descr: T.E.S.T. Ltd Ukraine
country: UA
organisation: ORG-CJ1-RIPE
org-name: "T.E.S.T." Ltd
fax-no: +380445911125
phone: +7 812 3323433
address: 6, Tulchinskaya str., 04080, Kiev,
Ukraine
    
```

У таблиці 2 представлена інформація з кожного вузла, що входить у маршрут. Як видно з таблиці, дані, отримані з сервісу whois, дозволяють довідатися про місце розташування (топологию) вузла по його IP-адресі.

Звичайно, такі дані можуть вимагати уточнення, тому що можуть повідомляти про місце розташування не самого вузла, а установи, на яку зареєстрована IP-адреса. З вищенаведеної відповіді "whois" ми бачимо, що трафік з мережі провайдера "Ukrainian Internet Exchange" попадає прямо у Київ на майданчик UA-IX через вузол 185.1.50.234. Малоймовірно, що середній провайдер має міжміські канали. З опису вузла виходить, що він належить точці обміну трафіком UA-IX (<https://www.ripe.net/manage-ips-and-asns/db/support>) до якої підключений провайдер.

Додаткову інформацію можна одержувати з назви вузла, так 185.1.50.234 має ім'я DE "Ukrainian Internet Exchange" (UA-IX), що підтверджує

припущення про розміщення цього вузла у Києві. Ця інформація також не має абсолютну достовірність.

Таблиця 2

№ вузла маршруту	IP-адреса вузла	Інформація про вузол, отримана із сервісу whois
1-3	217.76.192.0 217.76.205.255	Київ, Україна, компанія Т.Е.S.T
4	185.1.50.23	Київ, Україна, точка обміну трафіком "Ukrainian Internet Exchange" (UA-IX)
5	185.1.50.234	Київ, Україна, точка обміну трафіком "Ukrainian Internet Exchange" (UA-IX)
6	77.88.206.13	Київ, Україна, Компанія UA-TOPNET
7	77.88.206.14	Київ, Україна, Компанія UA-TOPNET
8	194.0.131.18	Київ, Україна, Компанія МЕТА-UA

Для розв'язання задачі знаходження альтернативних маршрутів також може бути використане багатоагентне ПЗ, агенти якого можуть перебувати як на вузлах у власності власника ГМ, так і на вузлах, що не належать йому. Як приклад такого ПЗ можна привести пропрієтарний продукт Visual Route (<http://www.visualroute.com/>). Це комплекс програм, який містить у собі агента MCS MyRoute та додаток для аналізу даних та моніторингу стану системи VisualRoute. На рис. 8 наведено приклад

маршрутів між двома вузлами мережі Інтернет. Як видно з рис. 8, VisualRoute дозволив знайти 128 однінних маршрутів до вузла мережі, котрий розшукувався (див. на рис. 8 IP 194.0.131.18) з мінімальною кількістю транзитних вузлів - 13. VisualRoute має можливість визначити прив'язку маршруту до карти. Використання в VisualRoute багатоагентної архітектури дозволяє одержати множини маршрутів до заданого вузла з декількох точок мережі. Так на рис. 9 наведено приклад, який зображує множини маршрутів до 80.81.193.180 з декількох територіально розподілених вузлів агентів.

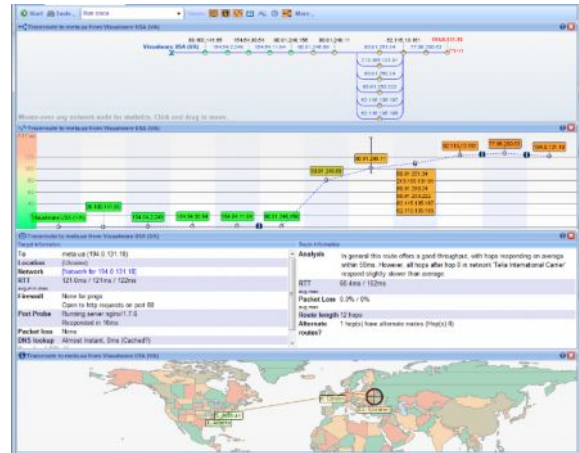


Рис. 8. Візуалізація процесу моніторингу структури ТМЗК

На рис.9 наведено приклад одержання маршрутів до деяких вузлів підмережі, у які входили транзитні вузли на маршруті від вихідного вузла (My Computer) до заданого (80.81.193.180)

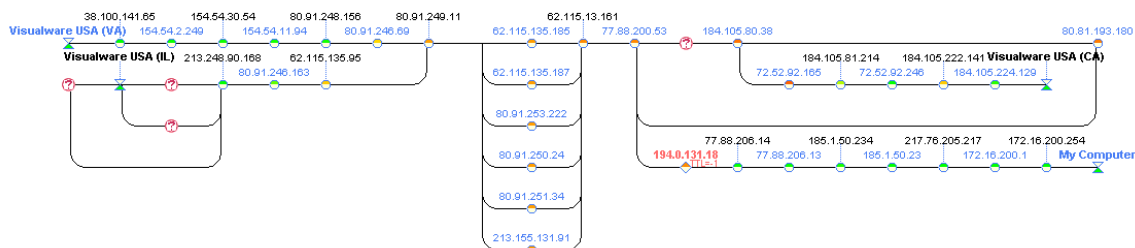


Рис. 9. Приклад побудови маршрутів до серверу 80.81.193.180 з 3 різних точок за допомогою VisualRoute

Здійснення процедури, яка описується, із множини ВУС ГМ і подальше сполучення всіх маршрутів у єдину схему, а також подальший їх моніторинг дозволять одержати докладну інформацію про структуру ГМ, а також здійснити прив'язку її транзитних ВУС до місцевості, тобто розкрити не тільки структуру, але і топологію ГМ. ПЗ VisualRoute дозволяє із заданою періодичністю здійснювати перевірку доступності вже знайдених маршрутів і знаходити нові, якщо такі з'явилися в ТМЗК, а також одержувати часові параметри затримок відповідей від усіх знайдених ВУС.

**Висновки й перспективи подальших досліджень**

Таким чином, запропоновані методичні рекомендації щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж для

альтернативних варіантів підключення дозволяють достатньо ефективно визначати та будувати гетерогенні мережі, які, у значній мірі, менш наражаються впливу зовнішніх та внутрішніх завад, що носять навмисний та ненавмисний характер. Крім того, їх використання надає можливість забезпечувати передачу інформації по визначеним маршрутам без її руйнування та втрат, що забезпечить стійкість функціонування як органів управління різного рівня так і елементів їх автоматизованих систем управління.

Топологія гетеродинних мереж для альтернативного підключення, що визначена на основі запропонованих методичних рекомендацій, потребує оцінки її функціонування, що може стати предметом подальших досліджень з цього питання.

### Література

1. Лізунов П.П., Васильєва Г. Л., Мінаєва Ю. І., Філімонова О.Ю. Комп'ютерні мережі і телекомунікації. К.: Київський національний університет будівництва і архітектури, 2017р.  
2. Пермяков О.Ю., Кільменінов О.А., Мельник Я.В. Застосування перколяційних алгоритмів для оцінки

надійності гетерогенних мереж військового призначення. К.: НУОУ, 2019 р. 3. Visual Route and virtual network computing exercises for computer network courses, Number AC 2007-944. American Society for Engineering Education, 2007 p.

## МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СУЩЕСТВУЮЩИХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОГРАММНЫХ УТИЛИТ ДЛЯ ОПРЕДЕЛЕНИЯ ТОПОЛОГИИ ГЕТЕРОГЕННЫХ СЕТЕЙ ДЛЯ НАХОЖДЕНИЯ АЛЬТЕРНАТИВНЫХ ВАРИАНТОВ ПОДКЛЮЧЕНИЯ

Ярослав Вячеславович Мельник

Виктор Евгеньевич Бобылев (кандидат военных наук, с.н.с.)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

*Современное информационное пространство постоянно подвергается влиянию внешних или внутренних помех. В современный период постоянного развития и совершенствования средств радиоэлектронной борьбы и методов воздействия на телекоммуникационные системы их защита становится очень важной и актуальной проблемой.*

*Существуют программное обеспечение и программные утилиты, которые обеспечивают совокупность подходов, которые предоставляют возможность строить телекоммуникационные сети устойчивыми к воздействию тех или иных помех. Но большинство из них касается технических аспектов построения сети. Что касается топологии таких сетей, то при их обосновании можно опираться только на их небольшое количество. Дело в том, что гетерогенные сети имеют в своей структуре большое количество узлов, непосредственно подверженных влиянию умышленных и неумышленных помех. Поэтому, возникает необходимость осуществлять замену узлов, через которые проходит информация, на другие, в связи с воздействием на них помех. Замена узлов, или переключение прохождения информации через другие узлы, на которые не влияют помехи, порождает изменение топологии гетерогенной сети, обеспечивающей альтернативные варианты их подключения.*

*В настоящее время не существует единых методических подходов к реализации действий по изменению топологии сетей. Их наличие предоставит возможность обоснованно изменять топологию гетерогенных сетей (ГС) для обеспечения альтернативных вариантов их подключения. Поэтому, ниже приведена статья, посвященная выработке методических рекомендаций по использованию существующих программного обеспечения и программных утилит для определения топологии гетерогенных сетей при поиске альтернативных вариантов их подключения.*

**Ключевые слова:** гетерогенная сеть; программное обеспечение; программные утилиты; топология сетей; маршрутизация; структура гетерогенных сетей.

## METHODOLOGICAL RECOMMENDATIONS FOR THE USE OF EXISTING SOFTWARE AND SOFTWARE UTILITIES FOR DETERMINING THE TOPOLOGY OF HETEROGENEOUS NETWORKS FOR FINDING ALTERNATIVE CONNECTION OPTIONS

Yaroslav Melnyk

Victor Bobylov (Candidate of military sciences, Senior Research Fellow)

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

*The modern information environment is constantly affected by external or internal interference. In the modern period of constant development and improvement of electronic warfare tools and methods of influencing telecommunication systems, their protection becomes a very important and urgent problem.*

*There are software and software utilities that are a set of approaches that make it possible to build telecommunications networks resistant to interference. But most of them relate to the technical aspects of building a network. With regard to the topology of such networks, their justification can only be based on a small number of them. The fact is that heterogeneous networks have in their structure a large number of nodes that are directly exposed to intentional and unintentional interference. Therefore, at times, it may be necessary to replace the nodes through which the information passes through to others due to their interference.*

*Replacing nodes, or switching information through other nodes that are not affected by interference, generates a change in the topology of the heterogeneous network, providing alternative options for connecting them.*

*Currently, there is no single methodological approach to implementing actions to change the topology of networks. Their availability will make it possible to reasonably change the topology of heterogeneous networks (HN) to provide alternative options for their connection. Therefore, the following article is devoted to providing guidance on using existing software and software utilities to determine the topology of heterogeneous networks when looking for alternative connectivity options.*

**Key words:** heterogeneous network; software; software utilities; network topology; routing; structure of heterogeneous networks.

### References

1. Lizunov P.P., Vasilyeva G.L., Minaeva Yu. I., Filimonova A.Yu. Computer networks and telecommunications. K.: Kyiv National University of Civil Engineering and Architecture, 2017. 2. Permyakov O.Y., Kilmeninov O.A., Melnik Y.V. Application of percolation

algorithms for the estimation of the reliability of heterogeneous wax networks. K.: NDUU, 2019. 3. Visual Route and virtual network computing exercises for computer network courses, Number AC 2007-944. American Society for Engineering Education, 2007 p.