МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кваліфікаційна наукова
праця на правах рукопису

ШАПОВАЛОВА АНАСТАСІЯ СЕРГІЇВНА

УДК 621.391

ДИСЕРТАЦІЯ

ПОТОКОВІ МОДЕЛІ БЕЗПЕЧНОЇ ТА ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ В ПРОГРАМНО-КОНФІГУРОВАНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Спеціальність: 05.12.02 – телекомунікаційні системи та мережі
Галузь знань: 05 «Технічні науки»
Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А.С. Шаповалова
Науковий керівник: Євдокименко Марина Олександрівна, доктор технічних наук, доцент

Ідентичність всіх примірників дисертації засвідчую:
Учений секретар спеціалізованої вченої ради /О.С. Єременко/

Харків – 2021

АНОТАЦІЯ

Шаповалова А.С. Потокові моделі безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих телекомунікаційних мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі». – Харківський національний університет радіоелектроніки, Харків, 2021.

У дисертації вирішено актуальну науково-прикладну задачу, що полягає в забезпеченні відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, які функціонують в умовах відмов та компрометації мережного обладнання, шляхом розроблення та вдосконалення відповідних математичних моделей маршрутизації. За результатами вирішення задачі сформульовано висновки.

Унаслідок проведеного аналізу встановлено, що важливим технологічним інструментом підвищення рівня безпеки та відмовостійкості ТКМ в умовах можливих збоїв в апаратному чи програмному забезпеченні мережного обладнання, перевантаження або порушення рівня інформаційної безпеки є протоколи маршрутизації. Зазначено, що підвищення ефективності рішень щодо безпечної та відмовостійкої маршрутизації, як правило, потребує відповідного вдосконалення наявних та розроблення нових математичних моделей і методів на основі адекватного врахування інформації про стан ТКМ: топології мережі, характеристик потоків пакетів, пропускної здатності каналів зв’язку та показників мережної безпеки елементів (вузлів та каналів).

Удосконалено потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Новизна розробленої моделі полягає в тому, що для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв’язку ТКМ та відповідно до рекомендацій NIST CVSS v.3

враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку реалізації наявних вразливостей; беруть до уваги показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом унаслідок реалізації зазначених вразливостей. Як показали результати проведеного дослідження, використання запропонованої моделі безпечної маршрутизації дозволяє розрахувати та застосувати маршрути з мінімальним ризиком інформаційної безпеки, забезпечивши цим максимальний рівень мережної безпеки пакетам, які передаються в ТКМ.

Удосконалено потокову модель безпечної маршрутизації з балансуванням навантаження на основі врахування параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах. До новизни запропонованої моделі належить модифікація умов балансування навантаження в ТКМ, які орієнтують на мінімізацію верхнього динамічно керованого порогу завантаженості каналів зв’язку, зваженого щодо ймовірності їхньої компрометації; використання множини моделей блокування каналів зв’язку, за допомогою яких можна регулювати вплив імовірності компрометації каналів на поріг їхньої завантаженості. Відповідно до результатів дослідження, отримані за допомогою запропонованої моделі маршрутні рішення враховують як пропускну здатність каналів зв’язку, так і їхні параметри безпеки, представлені ймовірностями компрометації під час визначення порядку балансування навантаження.

Уперше запропоновано модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіку в програмно-конфігурованих телекомунікаційних мережах. Новизна моделі полягає в тому, що, по-перше, модифіковано умови збереження потоку, які враховують пріоритетне обмеження трафіку на границі ТКМ у випадку її ймовірного перевантаження, викликаного, з одного боку, зростанням навантаження, а з іншого, – реалізацією схем захисту елементів мережі та її пропускної здатності під час швидкої перемаршрутизації;

по-друге, запропоновано систему критеріїв оптимальності маршрутних рішень, використання яких орієнтує на мінімізацію верхнього порогу завантаженості каналів зв'язку та відмов в обслуговуванні на границі мережі, зважених щодо пріоритету та інтенсивності потоків, з метою запобігання її перевантаження.

Удосконалено потокову модель безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку на границі ТКМ. Новизна моделі полягає в забезпеченні захисту елементів (вузлів, каналів, маршрутів) мережі та її пропускної здатності в процесі реалізації швидкої перемаршрутизації на основі врахування під час балансування навантаження в каналах зв'язку ймовірності їхньої компрометації, а в разі диференційованого обмеження трафіку на границі ТКМ – вимог потоків пакетів щодо рівня мережної безпеки.

Ключові слова: потокова модель, мережна безпека, відмовостійкість, безпечна маршрутизація, швидка перемаршрутизація, ризик інформаційної безпеки, базові метрики, критичність вразливостей, балансування навантаження, диференційоване обмеження трафіку.

ABSTRACT

Shapovalova A.S. Secure and fault-tolerant flow-based routing model with load balancing in software-defined telecommunication networks. – Qualification research work as a manuscript.

Dissertation for the Candidate of Technical Sciences degree in the speciality 05.12.02 – Telecommunication systems and networks. – Kharkiv National University of Radio Electronics, Kharkiv, 2021.

The dissertation is devoted to solving the relevant scientific and applied problem, which is to ensure fault tolerance and network security in software-defined telecommunication networks, which operate in conditions of failure and compromise of network equipment, by developing and improving appropriate mathematical models of routing.

As a result of the analysis it was found that improving the efficiency of solutions for secure and fault-tolerant routing requires appropriate improvement of existing and development of new mathematical models and methods based on adequate consideration of information about the state of the telecommunications network: network topology, packet flow characteristics, communication bandwidth and indicators network security elements (nodes and links).

The flow-based routing model has been improved, taking into account information security risks using base score metrics of criticality vulnerabilities. The novelty of the developed model is that the calculation of route metrics uses expressions that, in accordance with the recommendations of NIST CVSS v.3, characterize the risk of information security in the communication channels of the telecommunications network. The use of the proposed model of secure routing allows to calculate and use routes with minimal risk of information security, thus ensuring the maximum level of network security for packets transmitted in the telecommunications network.

The flow-based model of secure routing with load balancing under network security parameters in software-defined telecommunication networks has been improved. The novelty of the proposed model is the modification of load balancing conditions in telecommunication network, which focus on minimizing the upper bound of the network links utilization, weighted by the probability of their compromise. The use of the proposed model allows to take into account both the bandwidth of communication links and their security parameters, represented by the probabilities of compromise when determining the order of load balancing.

For the first time, a model of fast rerouting with load balancing based on the principles of Traffic Engineering (TE) and differentiated traffic policing in software-defined telecommunication networks has been proposed. The novelty of the model is that, firstly, the conditions of flow conservation have been modified, take into account the traffic priority policing at the network edge in case of its probable overload, caused by load increase; and secondly, a system of criteria for optimization of route solutions is proposed, the use of which focuses on minimizing the upper bound of

communication links utilization and denials of service at the network edge, weighted on the priority and intensity of flows to prevent congestion.

The flow-based secure fast rerouting model with load balancing and differentiated traffic policing in software-defined telecommunication networks has been improved. The novelty of the model is to ensure the protection of elements (nodes, links, routes) of the network and its bandwidth in the process of fast rerouting based on the probability of compromising communication links, and in the case of differentiated traffic policing at the network edge ensuring the requirements of packet flows regarding the level of network security.

Keywords: flow-based model, network security, fault tolerance, secure routing, fast rerouting, information security risk, basic metrics, criticality vulnerabilities, load balancing, differentiated traffic policing.

Список публікацій здобувачки:

1. Carlsson A., Duravkin E. V., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 1. Features of realization of low-intensity HTTP attacks. Проблеми телекомунікацій. 2013. № 3 (13). С. 61–70. URL: http://pt.nure.ua/wp-content/uploads/2020/01/133_carlsson_attack.pdf.

2. Duravkin E. V., Carlsson A., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. Method of detecting Slow HTTP attacks. Проблеми телекомунікацій. 2014. № 1 (14). С. 96–100. URL: http://pt.nure.ua/wp-content/uploads/2020/01/141_carlsson_attack.pdf.

3. Duravkin E. V., Carlsson A., Loktionova A.S. Method of slow-attack detection. Системи обробки інформації. 2014. № 8. С. 102–106.

4. Євдокименко М. О., Шаповалова А. С. Метод оцінювання впливу атак на інфокомунікаційну мережу з урахуванням наявних вразливостей. Вчені записки Таврійського національного університету імені В.І. Вернадського. 2018. Т. 29 (68), № 4. С. 67–72.

5. Yevdokymenko M. O., Shapovalova A. S., Nevzorova O. S. Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability Assessment. International Journal of Science and Engineering Investigations. 2019. Vol. 8 (91). P. 167–173. URL: http://www.ijsei.com/papers/ijsei-89119-22.pdf.

6. Лемешко О. В., Шаповалова А. С., Єременко О. С., Євдокименко М. О., Хайлан А. М. Математична модель швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіка в мережах SD-WAN. Системи управління, навігації та зв'язку. 2019. № 4 (56). С. 63–71. DOI:10.26906/SUNZ.2019.4.063.

7. Lemeshko O., Yevdokymenko M., Yeremenko O., Shapovalova A. Investigation of Load-Balancing Fast ReRouting Model with Providing Fair Priority-Based Traffic Policing. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing. Springer, Cham. 2020. Vol. 1247. P. 108–119 DOI: 10.1007/978-3-030-55506-1_10 **(SCOPUS)**

8. Lemeshko O., Shapovalova A., Al-Dulaimi A. M. K., Yeremenko O., Yevdokymenko M. Flow-Based Routing Model With Load Balancing Under Network Security Parameters. Information and Telecommunication Sciences. No. 2 (2020). P. 44–50. DOI: 10.20535/2411-2976.22020.44-50.

9. Євдокименко М. О., Шаповалова А. С., Шаповал М. М. Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Проблеми телекомунікацій. 2020. № 1 (26). С. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.

10. Локтіонова А. С. Оцінка економічної доцільності впровадження системи менеджменту інформаційної безпеки. Інформаційні технології в сучасному світі: дослідження молодих вчених: матеріали Міжнародної науково-практичної конференції молодих вчених, аспірантів та студентів (м. Харків, 2013). Харків: ХНЕУ, 2013. С. 68.

11. Duravkin I., Loktionova A., Carlsson A. Method of slow-attack detection. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the First International Scientific-Practical Conference, Kharkov, Ukraine, 2014. IEEE, 2014. P. 171–172. DOI: 10.1109/INFOCOMMST.2014.6992341.

12. Yevdokymenko M., Shapovalova A., Voloshchuk O., Carlsson A. Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fifth International Scientific-Practical Conference, Kharkov, Ukraine, 9–12 October 2018. IEEE, 2018. P. 609–612. DOI: 10.1109/INFOCOMMST.2018.8632079. **(SCOPUS)**

13. Lemeshko O. V., Yeremenko O. S., Yevdokymenko M. O., Shapovalova A. S. Advanced solution of the Fast ReRoute based on principles of Traffic Engineering and Traffic Policing. Science and Technology «AVIA-2019»: Proceedings of the Fourteenth International Conference, Ukraine, 23–25 April 2019. P. 8.21–8.23.

14. Єременко О. С., Євдокименко М. О., Шаповалова А. С. Підвищення відмовостійкості мереж засобами швидкої перемаршрутизації з балансуванням навантаження та профілюванням трафіка. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології»: зб. наук. праць. (м. Харків, 2019). Харків: ХНУРЕ, 2019. С. 131.

15. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Ilyashenko A., Sleiman B. Traffic Engineering Fast ReRoute Model with Support of Policing. Electrical and Computer Engineering (UKRCON): Proceedings of the 2nd International Conference, Lviv, Ukraine, 2–6 July, 2019. IEEE, 2019. P. 842–845. DOI: 10.1109/UKRCON.2019.8880006. **(SCOPUS)**

16. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Hailan A. M., Mersni A. Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS): Proceedings of the 10th IEEE International Conference, Metz, France, 2019. IEEE, 2019. P. 117–122. DOI: 10.1109/IDAACS.2019.8924294. **(SCOPUS)**

17. Yevdokymenko M., Shapovalova A. Investigation of the Impact of HTTP DoS Attacks on the Cloud Web Server. Natural science and technology (ICONAT): Proceedings of the International conference, Kharkiv, 2019. P. 25.

18. Lemeshko O., Yeremenko O., Hailan A. M., Yevdokymenko M., Shapovalova A. Policing Based Traffic Engineering Fast ReRoute in SD-WAN Architectures: Approach Development and Investigation. In: Al-Bakry A. et al. (eds) New Trends in Information and Communications Technology Applications. NTICT 2020. Communications in Computer and Information Science. Springer, Cham. Vol. 1183. P. 29–43. DOI: 10.1007/978-3-030-55340-1_3. **(SCOPUS)**

19. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Radivilova T., Ageyev D. Secure Based Traffic Engineering Model in Softwarized Networks. Advanced Trends in Information Theory (ATIT): Proceedings of the IEEE International Conference, Kyiv, 2020. P. 143–147. DOI: 10.1109/ATIT50783.2020.9349301. (**SCOPUS**)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІКТ	інформаційно-комунікаційні технології
КЗ	канал зв’язку
ПЗ	пропускна здатність
РІБ	ризик інформаційної безпеки
ТКМ	телекомунікаційна мережа
AI (Artificial Intelligence)	штучний інтелект
API (Application Programming Interface)	прикладний програмний інтерфейс
COBIT (Control Objectives for Information and Related Technology)	контрольні цілі для інформаційних та суміжних технологій
COSO (Committee of Sponsoring Organizations of the Treadway Commission)	комітет спонсорських організацій Комісії Тредвей
CVE (Common Vulnerabilities і Exposures)	загальновідомі вразливості та ризики
CVSS (Common Vulnerability Scoring System)	загальна система оцінки вразливостей
DSCP (Differentiated Services Code Point)	точка коду диференційованих послуг
DiffServ (Differentiated Services)	диференційоване обслуговування
EGP (Exterior Gateway Protocol)	протокол зовнішнього шлюзу
EIGRP (Enhanced Interior Gateway Routing Protocol)	вдосконалений протокол внутрішньої маршрутизації між шлюзами
FN (Future Networks)	мережі майбутнього
FRR (Fast ReRoute)	швидка перемаршрутизація
H-SDN (Hybrid SDN)	гібридні програмно-конфігуровані мережі

HSRP (Hot Standby Router Protocol)	протокол маршрутизатора гарячого резерву
ICMP (Internet Control Message Protocol)	міжмережний протокол керуючих повідомлень
IGP (Interior Gateway Protocol)	протокол внутрішнього шлюзу
IGRP (Interior Gateway Routing Protocol)	протокол внутрішньої маршрутизації між шлюзами
IntServ (Integrated Services)	інтегроване обслуговування
IoT (Internet of Things)	інтернет речей
IP (Internet Protocol)	протокол міжмережної взаємодії
IPS (Intrusion Prevention System)	система запобігання проникненню
IPsec (Internet Protocol Security)	протокол для забезпечення захисту даних
ITU (International Telecommunication Union)	міжнародний союз телекомунікацій
ISO (International Organization for Standardization)	міжнародна організація стандартизації
LB (Load Balancing)	балансування навантаження
MILP (Mixed Integer Linear Programming)	змішане цілочисельне лінійне програмування
MINLP (Mixed Integer NonLinear Programming).	змішане цілочисельне нелінійне програмування
ML (Machine Learning)	машинне навчання
MPLS (Multiprotocol Label Switching)	багатопротокольна комутація за мітками
NFV (Network Function Virtualization)	віртуалізація мережних функцій
NGN (Next Generation Network)	мережа наступного покоління
NIST(National Institute of Standards and Technology)	Національний інститут стандартів і технології

NLP (Nonlinear Programming)	нелінійне програмування
NP	мережна продуктивність
NS3 (Network Simulator v.3)	мережний симулятор версії 3
OSI (Open Systems Interconnection)	еталонна модель взаємодії відкритих систем
OSPF (Open Shortest Path First)	протокол маршрутизації по найкоротшому шляху
PQ (Priority Queuing)	черги за пріоритетами
QoS (Quality of Service)	якість обслуговування
RED (Random Early Detection)	механізм випадкового раннього виявлення перевантаження
RN (Resilient Networks)	відмовостійкі мережі
RIP (Routing Information Protocol)	протокол маршрутної інформації
RSVP (Resource Reservation Protocol)	протокол резервування ресурсів
SD-WAN (Software-Defined Networking in a Wide Area Network)	програмно-конфігуровані територіально-розподілені мережі
SDN (Software Defined Networking)	програмно-конфігуровані мережі
SecTE (Secure Traffic Engineering)	безпечний інжиніринг трафіка
SLA (Service Level Agreement)	угода про рівень надання послуги
SON (Self-Organized Networks)	самоорганізовані мережі
TE (Traffic Engineering)	інжиніринг трафіка
ToS (Type of Service)	тип обслуговування
TP (Traffic Policing)	полісінг трафіку
VoIP (Voice over IP)	передача голосу через IP
VRRP (Virtual Router Redundancy Protocol)	протокол резервування віртуального маршрутизатора
WFQ (Weighted Fair Queuing)	зважена справедлива черга

ВСТУП

Актуальність теми. У сучасних умовах інтенсивної інформатизації суспільства та цифрової трансформації економіки забезпечення мережної безпеки та відмовостійкості під час проектування та функціонування програмно-конфігурованих телекомунікаційних мереж (ТКМ) є одним із найважливіших завдань. Це пояснюється постійним розширенням потреб користувачів щодо множини та якості телекомунікаційних сервісів, збільшенням обсягів різнорідного типу трафіку, а також стрімким зростанням атак та втручань у роботу ТКМ. В умовах обмеженості мережного ресурсу зазначені чинники нерідко спричиняють перевантаження ТКМ, збій в апаратно-програмному забезпеченні мережного обладнання та зниження рівня якості обслуговування й мережної безпеки взагалі. З огляду на зазначені умови, важливо забезпечити ефективне (збалансоване) використання доступного мережного ресурсу, що сприяло б покращенню відмовостійкості, мережної безпеки та якості обслуговування.

Вагомий внесок у вирішення завдань щодо боротьби з перевантаженнями, управління мережним ресурсом і забезпечення мережної безпеки здійснили такі іноземні фахівці, як R. Gallager, W. Stallings, M. Berreiros, D. S. Rao, T. Gomes, G. Schudel, D. J. Smith, T. Kenyon, та вітчизняні вчені, зокрема В. В. Поповський, Л. Н. Беркман, В. А. Романюк, І. В. Стрелковська, В. О. Хорошко, О. Ю. Євсєєва, О. С. Єременко, О. В. Лемешко, С. В. Толюпа та багато інших.

Установлено [1–6], що для забезпечення високого рівня відмовостійкості та мережної безпеки необхідно використовувати всі наявні технологічні та протокольні засоби управління трафіком у ТКМ, серед яких важливе місце відводиться протоколам маршрутизації в поєднанні з функціоналом засобів резервування ресурсів, механізмів профілювання та обмеження трафіку тощо [7–12]. Проведений аналіз [13–20] дозволив сформулювати множину вимог, які

висуваються до протоколів безпечної та відмовостійкої маршрутизації в програмно-конфігурованих ТКМ:

– забезпечення адаптивної реакції мережі на можливі відмови (оптимізація здатності до вчасної та належної реакції на відмови та атаки в разі обмеження їхніх негативних наслідків на функціонування мережі);

– використання ресурсної та функціональної надмірності (резервування) для забезпечення захисту критично важливих елементів мережі та її ресурсів;

– урахування ризиків інформаційної безпеки, що ґрунтуються на наявних та нових виявлених вразливостях на елементах мережі;

– урахування характеристик мережного трафіку та вимог щодо рівня якості обслуговування та мережної безпеки;

– забезпечення збалансованого використання доступного мережного ресурсу на принципах Traffic Engineering.

Розроблення нових протоколів маршрутизації в ТКМ та їхнє докорінне вдосконалення повністю мають ґрунтуватися на відповідному перегляді математичних моделей і методів. Тому набуває актуальності **науково-прикладна** задача, що полягає в забезпеченні відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, які функціонують в умовах відмов та компрометації мережного обладнання, шляхом розроблення та вдосконалення відповідних математичних моделей маршрутизації.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційна робота пов’язана з виконанням положень «Концепції державної політики у сфері цифрової інфраструктури», «Концепції розвитку телекомунікацій в Україні», «Стратегії національної безпеки України», «Концепції розвитку цифрових компетентностей до 2025 року», рекомендацій щодо «Реформ у галузі інформаційно-комунікаційних технологій та розвитку інформаційного простору України», «Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки» та «Концепції конвергенції телефонних мереж і мереж із пакетною комутацією в Україні» [21–27].

Мета дисертаційної роботи полягає в підвищенні рівня відмовостійкості та мережної безпеки в програмно-конфігурованих телекомунікаційних мережах.

Для розв'язання поставленої науково-прикладної задачі в межах дисертаційного дослідження вирішувалися такі **завдання**:

– аналіз теоретичних і протокольних рішень щодо безпечної та відмовостійкої маршрутизації в програмно-конфігурованих телекомунікаційних мережах;

– розроблення потокової моделі безпечної маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей у програмно-конфігурованих телекомунікаційних мережах;

– удосконалення потокової моделі безпечної маршрутизації з балансуванням навантаження в програмно-конфігурованих ТКМ;

– розроблення потокової моделі швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіку в програмно-конфігурованих ТКМ;

– удосконалення потокової моделі безпечної швидкої перемаршрутизації з балансуванням навантаження та обмеженням трафіку на границі програмно-конфігурованої телекомунікаційної мережі;

– перевірка адекватності та дослідження ефективності запропонованих рішень щодо безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих ТКМ.

Об'єкт дослідження – процеси безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих телекомунікаційних мережах.

Предмет дослідження – математичні моделі безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих ТКМ.

Методи дослідження. У процесі розроблення та вдосконалення математичних моделей був використаний апарат дослідження операцій і теорія

множин. Для опису топології програмно-конфігурованих ТКМ застосовувалася теорія графів. З метою формування маршрутних метрик під час організації безпечної маршрутизації використовувались елементи теорії ризиків. Для розв'язання оптимізаційних задач безпечної та відмовостійкої маршрутизації застосовувалися методи лінійного та квадратичного програмування, реалізовані в середовищі MATLAB Optimization Toolbox.

Наукові положення, розроблені особисто дисертанткою, та їхня новизна.

1. Удосконалено потокову модель безпечної маршрутизації в телекомунікаційних мережах. Новизна моделі полягає в тому, що для розрахунку маршрутних метрик застосовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку ТКМ та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу в разі використання наявних вразливостей; беруть до уваги показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом.

2. Удосконалено потокову модель безпечної маршрутизації з балансуванням навантаження на основі врахування параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах. До новизни запропонованої моделі належать:

- по-перше, модифікація умов балансування навантаження в ТКМ, які орієнтують на мінімізацію верхнього динамічно керованого порогу завантаженості каналів зв'язку, зваженого щодо ймовірності їхньої компрометації;

- по-друге, використання множини моделей блокування каналів зв'язку, за допомогою яких можна регулювати вплив імовірності компрометації каналів на поріг їхньої завантаженості.

3. Уперше запропоновано модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering

та диференційованого обмеження трафіку в програмно-конфігурованих телекомунікаційних мережах. Новизна моделі полягає в тому, що

- по-перше, модифіковано умови збереження потоку, які враховують пріоритетне обмеження трафіку на границі ТКМ у випадку її ймовірного перевантаження, викликаного, з одного боку, зростанням навантаження, а з іншого, – реалізацією схем захисту елементів мережі та її пропускної здатності в процесі швидкої перемаршрутизації;

- по-друге, запропоновано систему критеріїв оптимальності маршрутних рішень, використання яких орієнтує на мінімізацію верхнього порогу завантаженості каналів зв’язку та відмов в обслуговуванні на границі мережі, зважених щодо пріоритету та інтенсивності потоків, з метою запобігання її перевантаження.

4. Удосконалено потокову модель безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку на границі ТКМ. Новизна моделі полягає в забезпеченні захисту елементів мережі та її пропускної здатності в умовах реалізації швидкої перемаршрутизації на основі врахування в процесі балансування навантаження в каналах зв’язку ймовірності їхньої компрометації, а в разі диференційованого обмеження трафіку на границі ТКМ – вимог потоків пакетів щодо рівня мережної безпеки.

Обґрунтованість і достовірність наукових результатів, висновків і рекомендацій, сформульованих у дисертації, підтверджувалася результатами проведеного імітаційного моделювання, коректним використанням математичного апарату, представленого елементами теорії графів, теорії множин, а також теорії ризиків. Адекватність отриманих рішень підтверджувалася коректністю вибору вихідних даних відповідно до рекомендацій NIST. Достовірність отриманих наукових результатів підкріплювалася відповідними актами впровадження та апробацією на міжнародних конференціях і форумах.

Практичне значення дисертаційної роботи. Практична цінність результатів дослідження полягає в тому, що запропоновані в дисертації моделі та методи мають стати основою математичного та алгоритмічного забезпечення перспективних протоколів безпечної та відмовостійкої маршрутизації (швидкої перемаршрутизації) як у традиційних телекомунікаційних, так і програмно-конфігурованих мережах. Отримані результати були використані на підприємстві «ХДРНТЦ ТЗІ», у ТОВ «Воркнест» та ПрАТ «Фарлеп-Інвест», а також у навчальному процесі кафедри інфокомунікаційної інженерії ім. В. В. Поповського Харківського національного університету радіоелектроніки в процесі проведення лекційних і практичних занять із дисциплін «Information Security in Information and Communication Systems» та «Control and Routing in Telecommunication Systems» для іноземних студентів першого (бакалаврського) рівня спеціальності 172 – Телекомунікації та радіотехніка.

Особистий внесок здобувачки. Усі основні наукові результати, висвітлені в дисертаційній роботі, авторка отримала самостійно. Крім того, у роботі [28] здобувачкою на низці розрахункових прикладів досліджено особливості реалізації низькоінтенсивних HTTP-атак для оцінювання ризиків інформаційної безпеки програмно-конфігурованих мереж; у статті [29] дисертанткою проведено аналіз та дослідження методу виявлення повільних атак HTTP у програмно-конфігурованих телекомунікаційних мережах; у публікації [30] здобувачкою проаналізовано та досліджено метод виявлення повільної атаки в програмно-конфігурованих мережах з оцінкою рівня безпеки телекомунікаційної мережі; у роботі [31] удосконалено метод оцінювання впливу атак на телекомунікаційну мережу з урахуванням наявних уразливостей для підвищення відмовостійкості мережі загалом; у публікації [32] дисертанткою вдосконалено та досліджено проактивний підхід щодо оцінювання рівня мережної безпеки, який базується на розрахунку ризиків на рівні користувача та мережі через наявність вразливостей; у роботі [33] здобувачкою запропоновано та досліджено математичну модель швидкої перемаршрутизації з балансуванням навантаження та диференційованим

обмеженням трафіку в територіально розподілених програмно-конфігурованих мережах; у статті [34] авторкою розроблено та досліджено потокову модель швидкої перемаршрутизації з балансуванням навантаження та диференційованим справедливим обмеженням трафіку в територіально розподілених програмно-конфігурованих мережах; у публікації [35] здобувачкою розроблено та досліджено потокову модель маршрутизації з балансуванням навантаження з урахуванням параметрів мережної безпеки; у статті [36] авторкою вдосконалено потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей.

Апробація. Основні результати дисертації доповідалися та були схвалені на 37 міжнародних наукових конференціях, форумах і семінарах, зокрема: на Міжнародній науково-практичній конференції молодих учених, аспірантів та студентів «Інформаційні технології в сучасному світі: дослідження молодих вчених» (м. Харків, 2013); на I та V IEEE конференціях «Problems of Infocommunications Science and Technology (PIC S&T)» (м. Харків, ХНУРЕ, 2014, 2018); на XIV Міжнародній науково-технічній конференції «ABIA-2019» (м. Київ, НАУ, 2019); на III Міжнародній науково-технічній конференції «Комп'ютерні та інформаційні системи і технології» (м. Харків, ХНУРЕ, 2019); на II IEEE конференції «Electrical and Computer Engineering (UKRCON)» (м. Львів, НУ ЛП, 2019); на X IEEE конференції «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)» (м. Мец, Франція, 2019); на Міжнародній конференції «Природничі науки та технології (ICONAT)» (м. Харків, ХНУРЕ, 2019); на Міжнародній конференції «New Trends in Information and Communications Technology Applications», NTICT 2020 (м. Багдад, Ірак, 2020), на IEEE конференції «Advanced Trends in Information Theory (ATIT)» (м. Київ, 2020).

Публікації. За матеріалами дисертації опубліковано 19 робіт, зокрема: 9 статей, серед яких 7 – у наукових фахових виданнях України [28–31, 33, 35, 36] та 2 статті в закордонних журналах [32, 34], з яких 1 індексується наукометричною базою Scopus [34]. Отримані результати та висновки

апробовано на 10 міжнародних наукових конференціях та форумах [37–46], з яких 5 індексуються наукометричною базою Scopus [39, 42, 43, 45, 46].

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів і двох додатків. Загальний обсяг дисертації становить 180 сторінок, обсяг основного тексту – 140 сторінок. Робота містить 47 рисунків, 39 таблиць, список використаних джерел містить 124 найменування, викладених на 17 сторінках.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНОГО СТАНУ ТЕОРЕТИЧНИХ І ТЕХНОЛОГІЧНИХ РІШЕНЬ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ ТА ВІДМОВОСТІЙКОСТІ ПРОГРАМНО-КОНФІГУРОВАНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1. Огляд рішень і сучасних засобів забезпечення кіберстійкості в телекомунікаційних мережах

Важливість забезпечення кіберстійкості інфокомунікаційних мереж обумовлена їхнім функціонуванням в умовах постійних, прихованих і складних атак на кіберресурси та є ключовим елементом під час побудови та розгортання мереж. Зі свого боку відмовостійкість інформаційних систем у [47–49] визначається як здатність такої системи продовжувати функціонувати в несприятливих умовах, навіть у стані деградації, зберігаючи водночас необхідні операційні можливості, а також як здатність оперативно відновлювати свою функціональність за відповідний час.

Отже, кіберстійкість – це здатність передбачати (anticipate), витримувати (withstand) несприятливі умови, атаки зловмисників або компрометації в системах, що містять кіберресурси, а також здатність відновлюватися (recover) після реалізації вразливостей та адаптуватися (adapt) до них [47]. Наведене визначення може бути застосовано до інфокомунікаційних мереж загалом, їхніх компонентів та елементів, інфраструктури тощо. Варто зазначити, що кіберстійкість, як і інформаційна безпека, є складним технологічним завданням і має забезпечуватися на всіх рівнях інфокомунікаційної системи. Тому цілі кіберстійкості, зазначені вище, мають бути пов’язаними з рішеннями щодо управління ризиками на рівнях бізнес-процесів і системи, а також стратегією управління ризиками (рис. 1.1) [50].

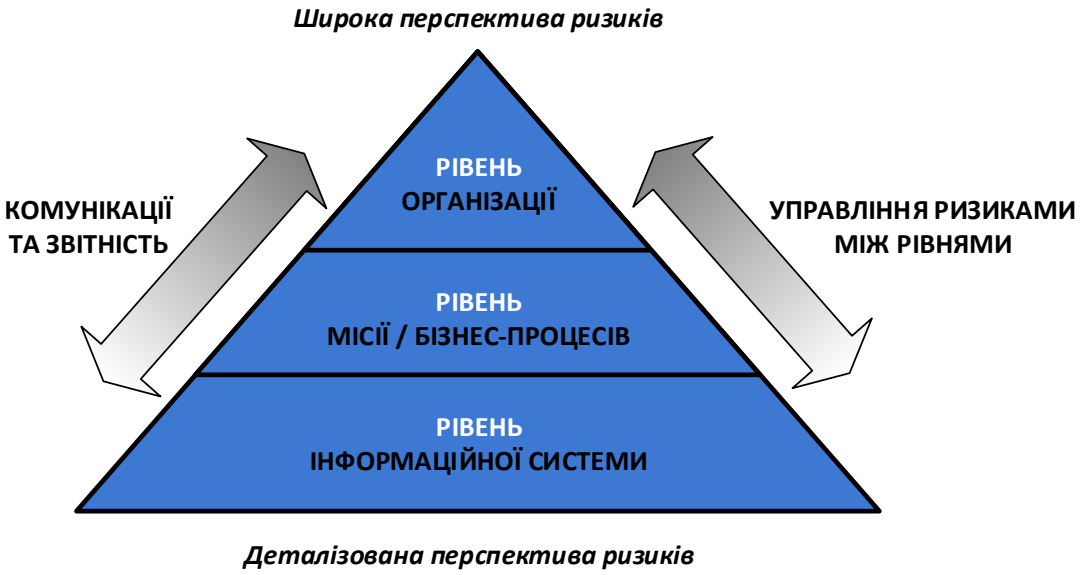


Рис. 1.1. Підхід до управління ризиками в процесі забезпечення кіберстійкості інформаційної системи організації [47]

Однією зі складових кіберстійкості є саме мережна стійкість (Network Resilience) як здатність забезпечувати та підтримувати прийнятний рівень обслуговування в умовах відмов різного походження та викликів щодо нормального функціонування мережі через випадкові та антагоністичні впливи (рис. 1.2), які призводять до значних змін як структурних, так і функціональних параметрів, а також властивостей мережі, спричинених відмовами обладнання, перевантаженням мережі та компрометацією з точки зору безпеки мережі (табл. 1.1).

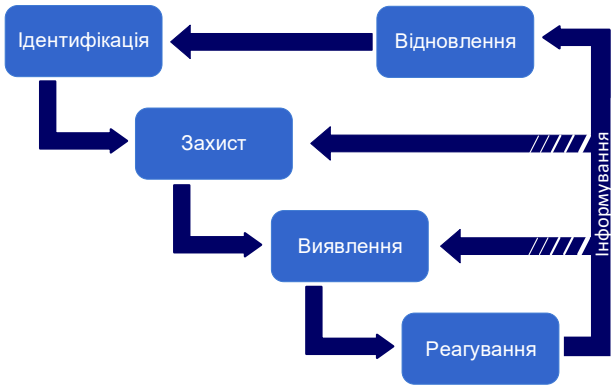


Рис. 1.2. Загальна структура фреймворка забезпечення кіберстійкості [51]

Таблиця 1.1

Фреймворк кіберстійкості

	Вимоги відповідності				Ядро	Базовий	Розширений					Вбудований		
	Ваші юридичні та нормативні зобов'язання				Початковий рівень кібербезпеки	Побудова структури для кібербезпеки	Посилення стійкості за допомогою постачальників безпеки, послуг та безперервності					Цілі та заходи щодо кіберстійкості в поєднанні з ширшими бізнес-цілями		
	GDPR	PCI DSS	NIS Regulations (OES)	DSP Toolkit	Основи кібербезпеки	NIST CSF	ISO 27001	ISO 22301	ISO 27035	ISO 27036	ISO 27017 & ISO 27018	COBIT	ISO 27014	Структура кібер-уряду
Управління та захист														
Управління активами	V	V	V	V		V	V		V		V			V
Політики інформаційної безпеки	V	V	V	V		V	V		V	V	V			V
Ідентифікація та контроль доступу	V	V	V	V	V	V	V			V				V
Захист від шкідливих програм	V	V	V	V	V	V	V			V	V			V
Конфігурація та управління виправленнями	V	V	V	V	V	V	V			V				V
Шифрування	V	V	V	V		V	V			V				V
Захист системи	V	V	V	V	V	V	V			V	V			V
Мережева та безпека коммунікацій	V	V	V	V	V	V	V			V				V
Компетентність та підготовка фахівців з безпеки	V	V	V	V		V	V			V				V
Підвищення кваліфікації персоналу	V	V	V	V		V	V		V	V				V
Комплексна програма управління ризиками	V	V	V			V	V	V	V	V	V	V	V	V
Управління ризиками поставок	V	V	V			V	V			V	V			V
Ідентицікація та виявлення														

Розглянемо більш детально наявні розробки та підходи до підвищення кіберстійкості інфокомунікаційних мереж [48, 49, 52–60]. Так, у роботах [48, 49, 52] проведено загальну характеристику кіберстійкості, показано взаємозв'язок між кібербезпекою та кіберзахистом із метою досягнення кіберстійкості.

Варто зауважити, що відповідно до моделі кіберстійкості, представленої в [49], забезпечення інформаційної безпеки пов'язано із захистом ТКМ від відомих загроз і вразливостей. Так само питання щодо кібербезпеки пов'язані із захистом від більш складних загроз, які не підпадають під загальновизначену класифікацію [49]. Тоді як забезпечення саме кіберстійкості відбувається в умовах невизначеності, коли ТКМ має функціонувати та бути захищеною від невідомих загроз, атак і вразливостей (рис. 1.3).

Рис. 1.3. Модель кіберстійкості [49]

Крім того, у [53] подано систему забезпечення кіберстійкості для промислових систем управління. Також у межах системи оцінювання кіберстійкості (Cyber Resilience Assessment Model, CRAM) показано місце використання резервування

компонентів промислових систем управління та запропоновано підхід щодо формулювання метрик відмовостійкості, який може використовуватися під час аналізу мережної відмовостійкості таких систем загалом (рис. 1.4).

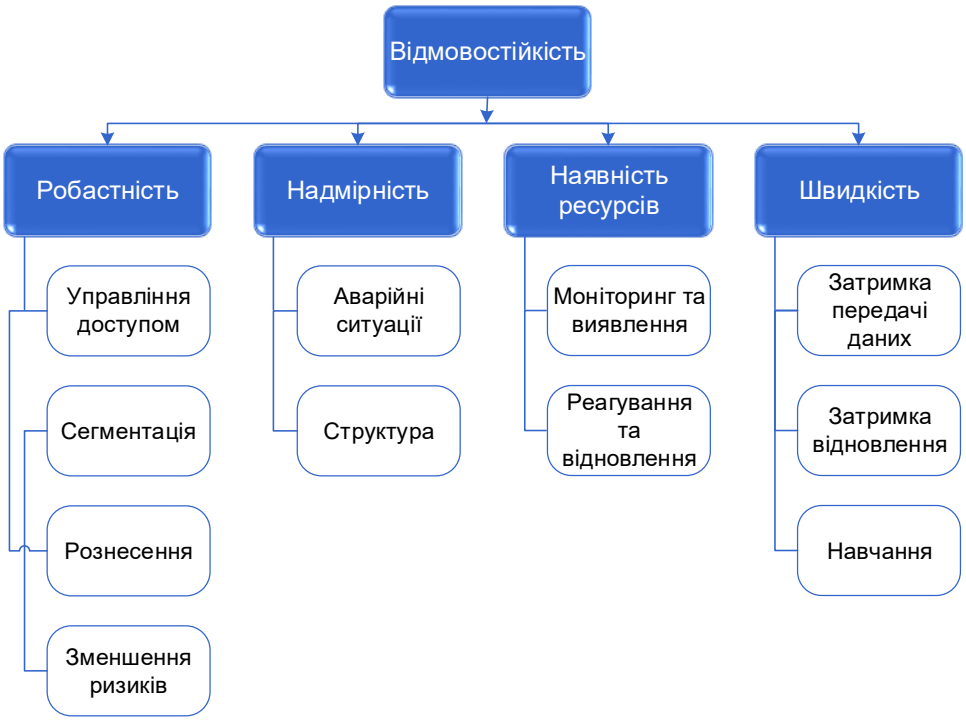


Рис. 1.4. Узагальнена система метрик кіберстійкості [53]

У роботі [54] запропоновано новий підхід до аналітичного моделювання кібератак на основі методу перетворення стохастичних мереж. Крім того, запропонований метод оцінки кіберстійкості мережі дозволяє визначити її характеристики (коефіцієнт справності мережі) й обґрунтувати таку її структуру, яка буде стійкою, а також сформулювати вимоги до частоти зміни параметрів обладнання, що використовується для захисту мережі.

Зі свого боку в [56] запропоновано метод підвищення кіберстійкості на основі кількісного визначення стійкості, оснований на реалізації гри кібербезпеки (Cyber Security Game, CSG). Тобто в зазначеному методі використовується теоретико-ігровий підхід, спрямований на оцінювання кіберризику системи. У роботах [57, 58]

проведено аналіз кіберстійкості та відповідних метрик у системах управління критичними інфраструктурами. Забезпечення належного функціонування таких систем набуває великого значення у зв’язку з появою складних атак, яким стає дедалі важче протидіяти.

Окремої уваги заслуговують рішення, пов’язані із забезпеченням кіберстійкості програмно-конфігурованих мереж (Software-Defined Networks, SDN) [59, 60]. Так, у [59] запропоновано архітектуру щодо виявлення аномалій за різними сценаріями з наступною реконфігурацією та розгортанням відмовостійких стратегій у реальному часі. Крім того, подальший розвиток цього рішення передбачає введення технологій балансування навантаження, толерантності до порушень та безпеки. Тоді як у [60] запропоновано схему захисту саме SDN контролера в межах концепції кіберстійкості.

Загалом аналіз наявних підходів [47–60] дозволяє сформулювати конкретні вимоги щодо забезпечення кіберстійкості телекомунікаційних мереж:

– адаптивна реакція мережі на можливі відмови (оптимізація здатності вчасної та належної реакції на відмови та атаки за умови обмеження їхніх негативних наслідків на функціонування мережі);

– використання ресурсної та функціональної надмірності (резервування) з метою забезпечення захисту критично важливих елементів мережі та її ресурсів;

– збалансоване використання вже задіяного мережного ресурсу на основі Traffic Engineering;

– застосування обмеження трафіку (Traffic Policing) на границі мережі як за основними, так і за резервними шляхами з урахуванням пріоритетів потоків;

– сегментація мережі відповідно до важливості захисту тих чи інших елементів мережі;

– забезпечення погодженості та ефективності різнотипних механізмів захисту елементів мережі.

1.2. Аналіз підходів до забезпечення відмовостійкості в програмно-конфігурованих мережах

Відмовостійкість є важливим аспектом загальної стійкості до внутрішніх і зовнішніх негативних впливів на функціонування телекомунікаційної мережі. Варто зауважити, що механізми відмовостійкості необхідні для забезпечення високої готовності та надійності систем. Водночас широке застосування програмно-конфігурованих мереж (SDN) висунуло не тільки нові вимоги, але й відкрило нові шляхи щодо розроблення сучасних стратегій, архітектур і стандартів забезпечення та підтримки відмовостійкості. У цьому підрозділі розглядаються нові підходи до забезпечення відмовостійкості та відновлення після відмов у SDN та технології OpenFlow [61–65]. Зі свого боку уточнимо, що механізм, який використовується для відновлення після відмов у відмовостійких мережах (carrier-grade networks), містить фази як виявлення, так і відновлення. Крім того, висвітлюються специфічні для SDN технологічні проблеми щодо відмовостійкості та зроблено огляд сучасних досліджень щодо відмовостійкості SDN. Аналіз структуровано відповідно до трьох площинам SDN, а саме площини даних, управління та застосунків/програмного забезпечення (рис. 1.5).

Отже, у [61] проведено глибокий аналіз і систематизація наявних рішень щодо відмовостійкості в SDN і визначено перспективи подальших досліджень з урахуванням технік і підтримки функцій відновлення після відмов на різних рівнях мережі (табл. 1.2). Так само подібний огляд зроблено в роботах [62–64] щодо управління відмовами в програмно-конфігурованих мережах і засобів вирішення завдань відмовостійкості на кожній площині SDN. Тоді як у [64] досліджено традиційні підходи до відмовостійкості та проаналізовано їхній зв’язок із SDN, проведено порівняння механізмів виявлення та відновлення після відмов (каналів і вузлів) у площині даних.

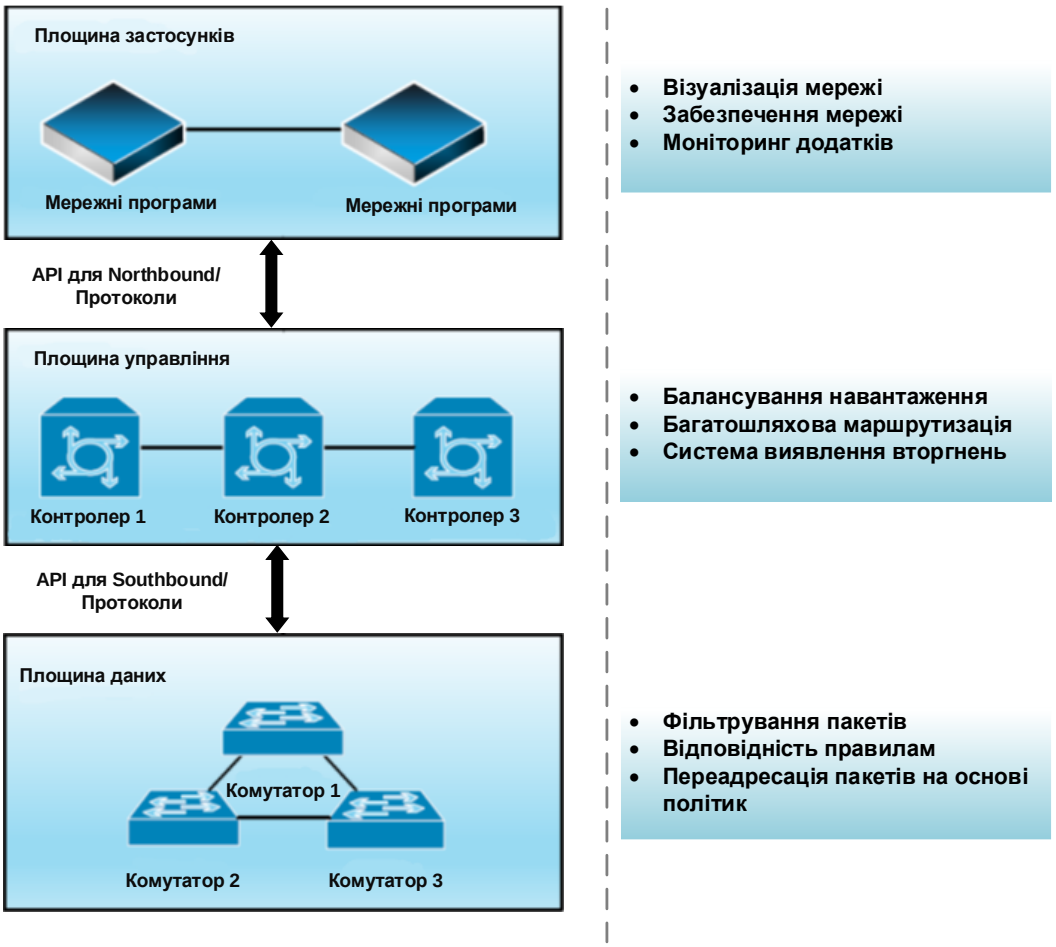


Рис. 1.5. Узагальнена структура програмно-конфігурованої мережі та інтерфейси взаємодії між її рівнями [61, 64]

1.2.1. Підтримка відмовостійкості в площині даних програмно-конфігурованої мережі

Відмовостійкість площини даних SDN пов’язана з тими самими технологічними проблемами, які існують у традиційних архітектурах, наприклад, у технології багатопротокольної комутації за мітками (Multiprotocol Label Switching, MPLS). Завдяки статичній природі традиційних мереж ці підходи дозволяють досягти високої ефективності у разі відмов таких мережних елементів та сегментів, як канали, вузли та маршрути.

Таблиця 1.2

Деталізація технік відмовостійкості телекомунікаційних мереж [61]

Виявлення відмов (помилок) / Error Detection	1. Одночасне виявлення: під час нормального функціонування мережі. 2. Попереджувальне виявлення: у разі порушення нормального режиму роботи мережі, під час перевірки прихованих, «сплячих» помилок і несправностей.
Відновлення після відмов (оброблення помилок) / Recovery (Error Handling)	1. Відкат (Rollback): відновлення стану системи до останніх попередньо збережених відомих конфігурацій перед виникненням відмови (помилки). 2. Відновлення вперед (Rollforward): ініціювання нового стану системи без виявлених помилок. 3. Компенсація: відновлення системи зі стану з відмовою шляхом її маскування за рахунок надмірності.
Відновлення після відмов (усунення несправностей) / Recovery (Fault Handling)	1. Діагностика: визначення локалізації відмов (помилок) та їхніх типів. 2. Ізоляція: запобігання залучення несправних компонентів у комунікаційний процес, які можуть призвести до відмови в обслуговуванні. 3. Реконфігурація: перепризначення завдань серед компонентів, що справно функціонують. 4. Повторна ініціалізація: перевірка та оновлення системи на основі нових конфігурацій.

Однак підходи до виявлення та відновлення після відмов у динамічних мережах, таких як SDN, мають бути удосконалені та адаптовані з урахуванням високої динаміки змін стану програмно-конфігурованих мереж. Традиційно для

забезпечення відмовостійкості застосовувалися реактивний і проактивний підходи [65]. У реактивному підході альтернативний (резервний) шлях обчислюється після виявлення відмови. Тоді як у проактивних технологічних рішеннях ресурси та резервні шляхи розраховуються заздалегідь, тобто до виникнення відмови. У цьому разі лише коли елемент мережі відмовляє, починає діяти проактивна логіка захисту, використовуються попередньо розраховані резервні маршрути, і таким чином система відновлюється після відмови. Розглянемо основні підходи щодо виявлення відмов та їхнього усунення.

1) Підходи до виявлення відмов.

Висока доступність площини даних відіграє важливу роль для підтримки необхідного зв’язку між відправниками та отримувачами потоків пакетів, що передаються в мережі. Водночас для досягнення високого рівня відмовостійкості в площині даних потрібно, по-перше, розроблення та аналіз топології за наявності відомих і невідомих відмов чи збоїв у мережі, а, по-друге, розрахування альтернативних (резервних) шляхів відповідно до типу характерних для мережі відмов. Зауважується, що у відмовостійких мережах існують два широко відомі механізми виявлення відмов у площині даних, а саме:

- механізм втрати сигналу – Loss of Signal (LOS);
- використання мережного протоколу для виявлення помилок з’єднання між двома маршрутизаторами – Bidirectional Forwarding Detection, BFD [66].

LOS виявляє збої в певному порту передавального пристрою, тоді як BFD може виявити відмову шляху між будь-якими двома мережними пристроями (маршрутизаторами). Обидва методи забезпечують достатньо швидке виявлення відмов незалежно від типу середовища передачі даних і протоколів маршрутизації (наприклад, OSPF чи EIGRP).

2) Підходи до відновлення після відмов.

Відомо, що у відмовостійких мережах механізм відновлення має гарантувати процес відновлення протягом 50 мс [67]. З цією метою відновлення та захист

(резервування) широко використовуються для відновлення після відмов обслуговування мережею – методи, основані на реактивному та проактивному підходах.

Отже, захист визначається як реактивна технологія, тоді як відновлення – проактивна. У процесі відновлення альтернативний маршрут установлюється лише після відмови, а ресурси не резервуються до її виникнення, тоді як шляхи визначаються заздалегідь або розподіляються динамічно. Однак у випадку захисту елемента мережі альтернативні маршрути вже зарезервовані та призначені до виникнення відмови.

Таке рішення не потребує додаткового оброблення (сигналізації) для відновлення після відмови. І навпаки, під час проактивного відновлення необхідна додаткова сигналізація після відмови. У великих мережах часто таке рішення не має високої масштабованості. Водночас реактивний підхід захисту (резервування) елементів мережі є достатньо швидким і в разі забезпечення часу процесу відновлення після відмови в межах 50 мс підходить для застосування у відмовостійких транспортних мережах.

1.2.2. Наявні рішення щодо забезпечення відмовостійкості на різних рівнях програмно-конфігурованих мереж

Стосовно рівня даних SDN виокремлюють два основних технологічних завдання, а саме: виявлення відмов і відновлення мережі після них. Зазвичай ці завдання виникають через відмови каналів або вузлів мережі. Як уже зазначалося вище, у традиційних мережах для виявлення відмов у мережі використовуються певні протоколи, такі як LOS і BFD [68]. Також для відновлення після відмови мережі широко застосовуються підходи відновлення та захисту/резервування. Однак вирішення цих проблем у середовищі SDN є складним завданням через централізований характер управління мережею контролером.

Так, наприклад, у програмно-конфігурованому середовищі контролеру може знадобитися значно більше часу, щоб виявити та відновити функціонування мережі внаслідок відмови каналу зв'язку або вузла через швидку зміну її топології (динамічна топологія). Тому існує нагальна потреба в розробленні відповідних механізмів для SDN мереж, які можуть забезпечити більш швидке відновлення [61].

У табл. 1.3 зазначено окремі рішення щодо відмовостійкості в площинах даних та управління SDN мереж.

1.3. Характеристика основних принципів централізованого управління програмно-конфігурованою телекомунікаційною мережею

Відомий підхід централізованого управління мережею з використанням контролера було розглянуто в роботі [78]. Він представлений чотирирівневою архітектурою та був названий 4D відповідно до назв рівнів, а саме: *decision* – рішення, *dissemination* – поширення, *discovery* – виявлення, *data* – дані.

У [79] зазначається, що такий підхід пропонує повний рефакторинг функціонування мережі, віддалено від автономних пристроїв, та ідею концентрації роботи площини управління як окремої незалежної системи.

Вважається, що стан традиційних транспортних мереж, які зазвичай складалися з множини розподілених автономних систем, є надзвичайно нестабільним та постійно балансує на межі збою. Навіть невеликий локальний збій, наприклад, неправильна конфігурація протоколу маршрутизації, може мати серйозний глобальний вплив на функціонування мережі загалом. Основною причиною цього є той факт, що функції управління мережею реалізовувалися на самих мережних елементах.

Таблиця 1.3

Рішення щодо відмовостійкості в площинах даних та управління програмно-конфігурованими мережами

Пос.	Площина SDN	Запропоноване рішення
[65]	Площина даних	Перевірка несправностей портів комутаційного пристрою та послідовний контроль виявлення несправностей між двома каналами зв'язку для підтримки стандартизованих методів виявлення відмов, таких як BFD та LOS.
[68]	Площина даних	Підвищення швидкості виявлення відмов у реалізаціях на основі Open vSwitch.
[69], [70]	Площина управління	Задоволення вимог щодо відновлення після відмов у високонадійних мережах операторського рівня.
[71]	Площина управління	Покращення адресної пам'яті (TCAM) та ефективності пропускної здатності у разі одиничних відмов каналів зв'язку в SDN за рахунок зменшення кількості правил передавання потоків резервними маршрутами.
[72]	Площина управління	Обчислення резервних маршрутів між окремими парами відправників та отримувачів потоків пакетів, що передаються в SDN мережі.
[73]	Площина управління	Відновлення після системних збоїв у реалізаціях контролерів на основі технології OpenFlow.
[74]	Площина управління	Розроблення системи відмовостійкості, здатної до відновлення після множинних відмов каналів у площині даних SDN мережі.
[75]	Площина управління	Представлення моделі для проєктування самостабілізуючих розподілених площин управління SDN.
[76]	Площини даних та управління	Механізм швидкого відновлення зі зниженим споживанням пам'яті за допомогою концепції тегування VLAN.
[77]	Площини даних та управління	Оцінювання відключень і відмов у приватній глобальній мережі SDN WAN.

Отже, підхід 4D складається з таких принципів проєктування:

1. **Цілі мережного рівня**: цілі та завдання системи управління мережею мають бути викладені у відповідних термінах та охоплювати мережу загалом, окремо від елементів мережі чи продуктивності мережних пристроїв.

2. **Інформація щодо мережі загалом**: наявність актуальної інформації про мережу, а саме її топологію, трафік та події з усієї системи, на якій базуються рішення та дії щодо управління мережею.

3. **Управління**: системи контролю та управління повинні мати змогу здійснювати безпосередній контроль над мережними елементами з можливістю програмування таблиць маршрутизації для кожного комутаційного пристрою, а не лише маніпулювати деякими віддаленими та окремими параметрами конфігурації, як це має місце в традиційних мережах.

На рис. 1.6 показано загальну архітектуру підходу 4D із централізованим управлінням мережею з використанням системи контролю та управління. Зі свого боку в межах підходу 4D виокремлюють проблеми, з якими стикається запропонована централізована архітектура та які потребують подальшого вивчення та вдосконалення відповідних технологічних рішень. Ці проблеми залишаються актуальними для програмно-конфігурованих мереж різного призначення і сьогодні.

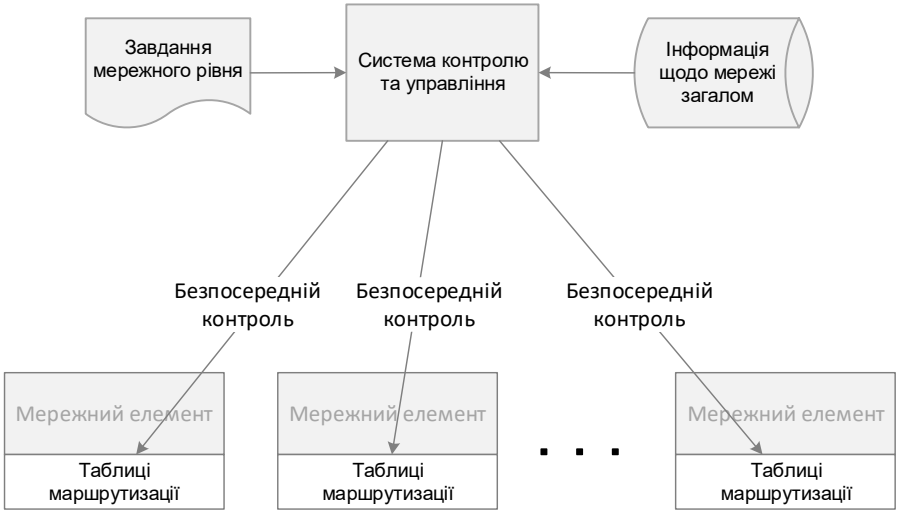


Рис. 1.6. Принципи 4D [79]

Розглянемо основні з них.

1. **Затримка**. Наявність централізованого контролера означає, що прийняття рішень займає достатньо значний час, оскільки елемент мережі вимагає від контролера керуючих вказівок відповідно до прийнятих політик. Крім того, потрібно враховувати, що центральний контролер має надавати рекомендації щодо політик великої кількості мережних пристроїв одночасно.

2. **Масштабованість**. Наявність централізованого контролера означає, що відповідальність за топологічну організацію мережі, визначення оптимальних шляхів та реагування на зміни повинен виконувати саме контролер.

3. **Висока доступність (High Availability, HA)**. Централізований контролер не повинен бути єдиною точкою відмови для мережі (Single Point of Failure, SPOF), тобто такою, що може вивести з ладу всю систему. Це передбачає необхідність використання відповідних схем резервування. По-перше, мають бути наявними резервні контролери, потужність яких була б доступна в разі виходу з ладу одного контролера. По-друге, актуальні дані, що використовуються множиною контролерів, мають відзеркалюватися таким чином, щоб вони могли послідовно програмно керувати мережними пристроями. По-третє, канали зв’язку між окремими контролерами також мають резервуватися, гарантуючи, що між комутатором і принаймні одним контролером завжди існує функціонуючий канал.

4. **Безпека**. Наявність централізованого контролера означає, що зловмисні атаки можуть бути спрямовані саме на цю єдину точку відмови – контролер, і, отже, існує ймовірність того, що такий тип рішення є більш вразливим до атак, ніж розподілена система. Тобто важливо розглянути, які додаткові кроки необхідно вжити для захисту як централізованого контролера, так і каналів зв’язку між ним та мережними пристроями.

Отже, головною перевагою розподіленого управління, коли використовується пул контролерів для управління мережею, є відсутність єдиної точки відмови. Тоді як відмови, наприклад, вузлів чи каналів у площині даних

відмовостійкої SDN мережі не вплинуть на її працездатність. У цьому випадку відмови в інфраструктурі не заважатимуть реконфігурації щодо виключення елемента мережі з резервного маршруту. Однак потрібно зазначити, що в Open SDN архітектурах часто використовується єдиний контролер, відповідальний за управління всією мережею [79].

На рис. 1.7 показано відновлення після відмови одного вузла в мережі SDN. У цьому випадку саме контролер SDN виконує реконфігурацію мережі, щоб виключити вузол, який відмовив, із розраховуваного резервного маршруту. Однією з передумов SDN є те, що центральний контролер зможе детерміновано переконфігурувати мережу оптимальним та ефективним способом на основі глобальних знань про мережу.

Отже, з рис. 1.7 видно, що, відповідно до загальної інформації про мережу, яку має у своєму розпорядженні контролер SDN, він перенаправляє потоки F_1 та F_2 різними шляхами. Одним із сценаріїв, який міг би спричинити подібну ситуацію, було б те, що вказані два потоки мають конкретні гарантії щодо якості обслуговування, які неможливо виконати, якщо обидва потоки передаються одним (спільним) резервним шляхом. Пошук оптимальних шляхів для різних потоків є відносно простим у межах, наприклад, моделі Open SDN, проте його зазвичай дуже складно реалізувати в традиційних мережах з автономними пристроями [79].

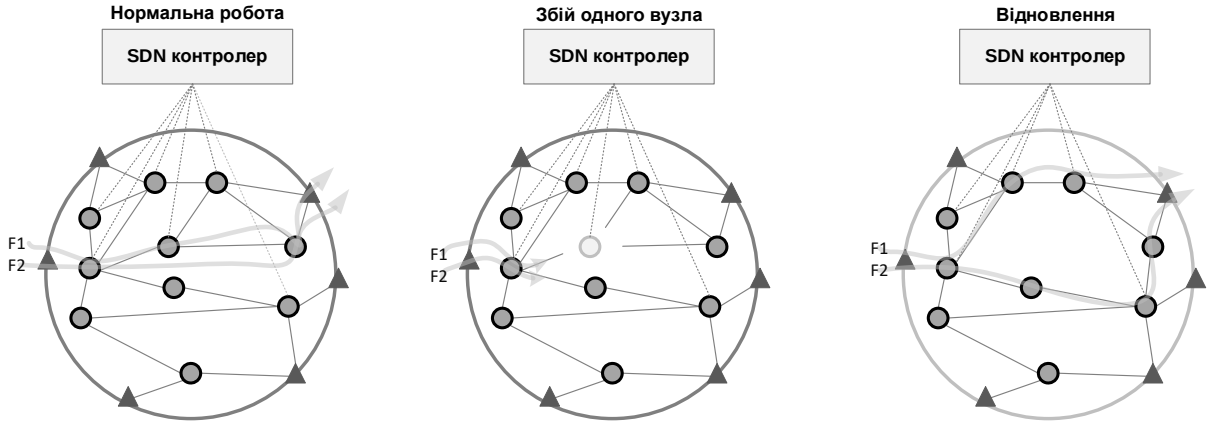


Рис. 1.7. Приклад відновлення після відмови SDN мережі [79]

Проте, якщо єдиною точкою відмови є сам контролер, мережа вразлива, як це показано на рис. 1.8. Поки в мережі не відбуваються зміни, що вимагають модифікації таблиць маршрутизації, мережа може продовжувати працювати без контролера.

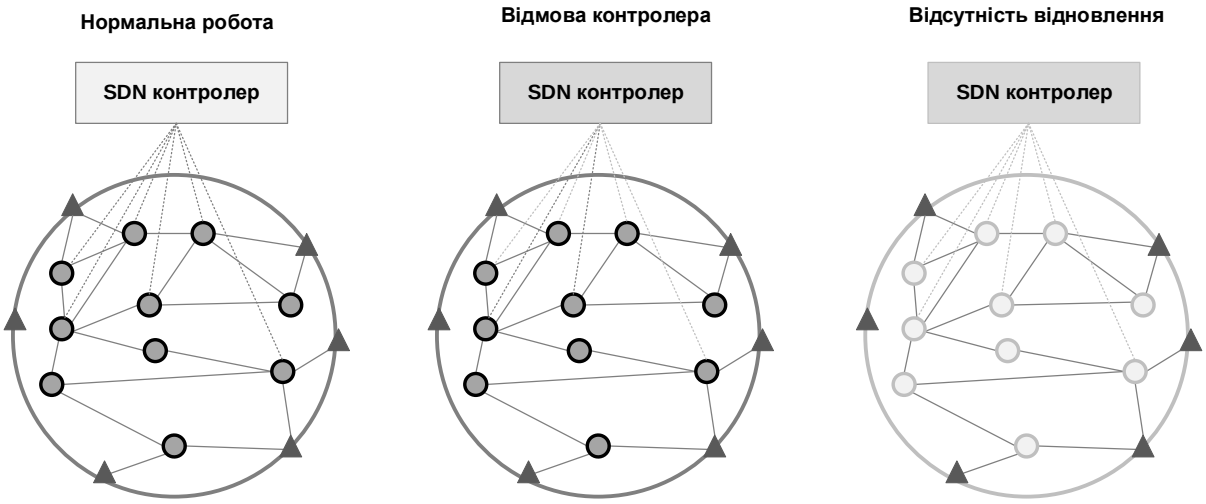


Рис. 1.8. SDN контролер як єдина точка відмови [79]

Однак, якщо відбуваються будь-які зміни в топології, мережа більше не може адаптуватися. Втрата контролера призводить до переходу мережі в стан зниженої функціональності, коли вона не в змозі адаптуватися до виходу з ладу інших компонентів. Отже, вихід з ладу централізованого контролера може потенційно створити ризик для всієї мережі. Контролер SDN вразливий як до апаратних і програмних збоїв, так і до зловмисних атак.

Контролери SDN повинні використовувати методи високої доступності (High Availability, HA) та/або надмірність. Варто зазначити, що контролери SDN – не єдині системи, які мають бути високодоступними. На рис. 1.9 наведено приклад добре розробленої конфігурації контролера із резервними контролерами та базами даних резервних контролерів. У межах запропонованого прикладу застосовується схема резервування N + 1, коли один резервний контролер (гаряче резервування) готовий взяти на себе навантаження будь-якого з N активних контролерів. Інколи використовується схема, коли для кожного контролера є відповідний резервний.

Зі свого боку варіант гарячого режиму резервування для кожного окремого контролера полягає у запровадженні принципів високої доступності на рівні його апаратного забезпечення шляхом використання надлишковості для всіх важливих компонентів сервера (наприклад, дзеркальні диски, резервні джерела живлення тощо).

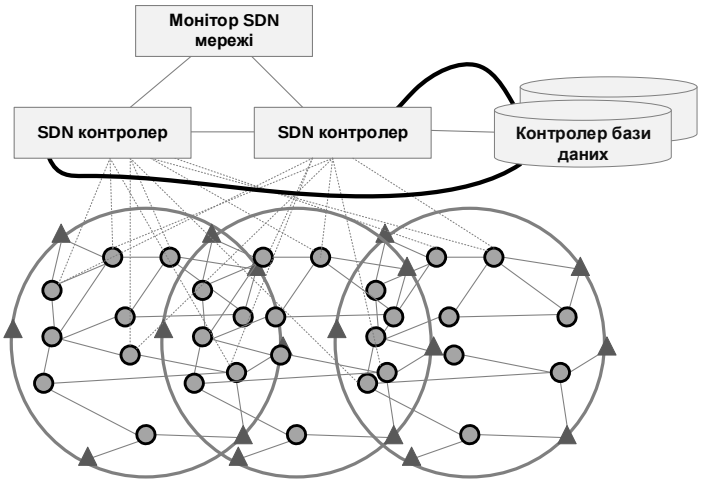


Рис. 1.9. Приклад високої доступності контролера та монітор SDN мережі [79]

Отже, відмовостійкість SDN мереж є активною сферою досліджень. Окрім технологічних завдань щодо забезпечення високої доступності контролерів, цей напрямок перетинається з рядом інших дисциплін, таких як живучість, надійність, толерантність трафіку мережі та безпека. Водночас виникають питання забезпечення кіберстійкості мережі загалом. Також постають питання, що стосуються конкретно узгодженості між основним і резервним контролерами SDN мережі, а саме дослідження стратегії їх розміщення.

1.4. Архітектура, функції та переваги використання територіально-розподілених програмно-конфігурованих мереж – SD-WAN

Варто зауважити, що в межах сучасного цифрового світу хмарні обчислення (Cloud Computing, CC) швидко витісняють традиційні рішення від застосунків до

мережних комунікацій. Особливий інтерес викликає те, як СС трансформує середовище глобальних мереж WAN із появою підходу, відомого як програмно-конфігурована WAN. Отже, SD-WAN безпосередньо характеризується застосуванням так званого «хмарно орієнтованого» (Cloud-centric) доступу до мережі, широко використовуючи принципи, визначені для програмно-конфігурованих мереж. Сьогодні SD-WAN є одним з найактуальніших напрямів, що значно впливає на послуги СС та WAN, а також їхніх користувачів, до яких так само належить державний сектор та освіта [80].

Сьогодні SD-WAN розглядається як технологія, що може революціонізувати використання послуг WAN. Вона підтримує нову концепцію, відому як мережа, що керується додатками (Application-driven networking), де очікується, що ця мережа буде відповідати потребам програмного забезпечення, послуг і користувачів [80]. Отже, така концепція SD-WAN дозволяє замінити традиційні послуги WAN, що надаються за допомогою високовартісної технології MPLS (MultiProtocol Label Switching) VPN (Virtual Private Networks), і зменшити витрати на адміністрування мережі шляхом використання централізованих та автоматизованих елементів адміністрування.

Вищезазначене також має значні переваги під час розгортання корпоративних мереж, а також мереж підприємств. З іншого боку, SD-WAN може експлуатуватися через більшу кількість окремих з’єднань WAN, зокрема доступних за ціною широкосмугових каналів зв’язку загального користування (рис. 1.10). SD-WAN пропонує цьому сегменту користувачів доступ до нових і більш якісних послуг, що випливають із функціоналу технології SD-WAN. Обслуговування SD-WAN із збалансованою пропозицією нових функцій та широкосмуговим доступом має потенціал для того сегменту клієнтів, для яких приватна послуга MPLS VPN була недоступною за вартістю або через технології доступу тощо [80]. Крім того, SD-WAN може запропонувати більшу зручність і стабільність пропонованих

інфокомунікаційних послуг завдяки інтеграції та використанню послуг СС, гарантуючи водночас високий рівень безпеки.

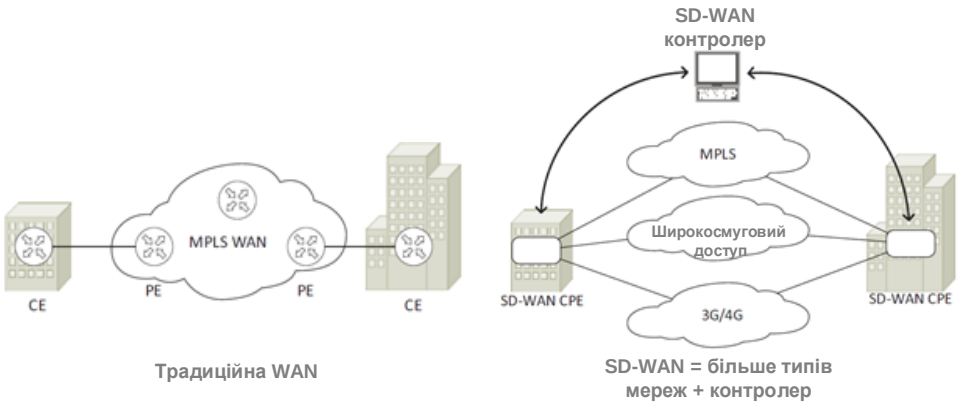


Рис. 1.10. Порівняння традиційної WAN і SD-WAN [80]

Технологія SD-WAN, як згадувалося раніше, на сьогодні є однією з найбільш перспективних, оскільки поєднує послуги SDN, NFV, СС і WAN (наприклад, широкосмуговий інтернет). Архітектура SD-WAN, подібно до архітектури SDN, складається з трьох архітектурних площин. Це площина інфраструктури або даних (infrastructure or data plane), площина управління (control plane) та площина оркестрації (orchestration plane) [79, 80].

Площина даних

Площина даних здатна встановлювати зв’язок як через приватну, так і через публічну інфраструктуру IP/WAN. Вона призначена для спрощення комунікацій між географічно відокремленими ділянками, а також із хмарними застосунками та сервісами. Для цього SD-WAN створює власну, керовану програмним забезпеченням, логічну інфраструктуру над наявною фізичною інфраструктурою. Цей тип мережі називається *Overlay*, тоді як наявна фізична інфраструктура − *Underlay*. Хоча накладення SD-WAN Overlay, як правило, є однорідним і послідовним, фізична інфраструктура опорних мереж WAN найчастіше неоднорідна та фрагментована. Деякі рішення можуть використовувати лише одну висхідну лінію зв’язку (тобто MPLS). Інші рішення здатні використовувати лише

локальне підключення до інтернету з одним висхідним каналом чи застосовувати комбінації каналів і технологій (DSL, 4G/5G тощо), навіть їхні комбінації з орендованими лініями, або інші приватні рішення WAN.

Оверлейні мережі можуть логічно створювати кілька типів каналів (наприклад, hub & spoke, full mesh, partial mesh, point-to-point, controller-behind-branch, branch-behind-branch тощо). Функції накладання мережі містять підтримку мереж VPN або VPN другого (L2 VPN) чи третього рівня (L3 VPN). З погляду маршрутизації мережа підтримує адресацію IPv4 та IPv6, а також багатоадресну передачу.

Звичайно, SD-WAN підтримує функції безпеки, які мають пропонувати всі виробники відповідного обладнання та програмного забезпечення. Це може бути, наприклад, можливість упровадження та поширення сертифікатів інфраструктури відкритих ключів PKI (Public Key Infrastructure) між контролером та обладнанням кінцевих користувачів (Customer Premises Equipment, CPE) SD-WAN. Щодо шифрування, то можна поділити захищений трафік на дві частини: шифрування рівня управління та шифрування рівня даних. На рівні управління можна шифрувати керуючу інформацію контролера до пристроїв CPE. Можливе використання IPSec, симетричного/асиметричного шифрування за допомогою сертифікатів PKI, TLS/DTLS тощо. Шифрування рівня даних означає шифрування самого трафіку клієнта, де переважно застосовується сімейство протоколів IPSec або SSL VPN. Інший варіант − розгортання та використання сторонніх пристроїв і функцій безпеки.

Площина управління

Принцип функціонування SD-WAN, як і SDN, оснований на відокремленні площини управління для централізації логіки управління від площини даних. Основним об’єктом площини управління є контролер (або кілька контролерів), який може бути розташований у центрі оброблення даних, у хмарі тощо. Цей рівень відповідає за контроль конфігурації підключених пристроїв, тоді як CPE

підключений до контролера за допомогою безпечного керуючого з'єднання (південний інтерфейс – southbound API). Кластер контролерів може бути реалізовано за допомогою східно-західного інтерфейсу (East-West API) (MP-BGP або спеціальні рішення). Цей рівень також відповідає за оптимізацію потоків інформації, що надходять через тунель VPN до кожного з різних типів послуг, таких як послуги центрів оброблення даних і хмарні сервіси. Програмування обслуговування SD-WAN через оркестратор (orchestrator entity) реалізується через північний API інтерфейс (Northbound API), де здебільшого використовується RestAPI.

Площина оркестрації

Площина оркестрації забезпечує структуру бізнес-політики та стосується політики безпеки послуг і стратегій корпоративного управління [80].

Рівень управління – це абстракція високого рівня для дотримання політики (централізоване та уніфіковане управління політикою), управління конфігурацією, усунення несправностей, моніторинг, аналітика, прогнозування, кореляція, звітування та сповіщення. Також є функції, пов'язані з послугами (service-related functions), такі як створення та управління послугами. Консолідація цих функцій створює інтерфейс управління, який може легко керувати територіально розподіленими мережами. Концепція таких масштабних розгортань відома як автоматичне налаштування параметрів Zero-Touch Provisioning (ZTP). У випадку з ZTP не потрібно, щоб кожний пристрій CPE був індивідуально налаштований, але натомість він завантажує свою конфігурацію із централізованого рівня управління після автентифікації [80].

Сам рівень управління може бути розміщений в IT-інфраструктурі в локальному середовищі (on premises) або в хмарі. Основним об'єктом на цьому рівні є об'єкт – оркестратор, тоді як деякі виробники також мають об'єкт, який називають менеджером. Оркестратор – це компонент, орієнтований на інтеграцію та оркестрацію всього рішення SD-WAN, тоді як аналіз показав, що це є суто

пропрієтарними рішеннями, коли кожен виробник має власне програмне рішення для цього об’єкта, який також називається по-різному. Реалізація може бути як самостійним рішенням, так і компонентом, інтегрованим у контролер, що містить декілька підгруп об’єктів (sub-entities).

1.5. Огляд рішень щодо швидкої перемаршрутизації з балансуванням навантаження в програмно-конфігурованих мережах

Серед досліджень щодо відмовостійкості в SDN мережах можна виділити роботи [81–84]. Так, наприклад, у [81] запропоновано алгоритм локальної швидкої перемаршрутизації (Local Fast Reroute, LFR) з агрегацією потоків у програмно-конфігурованих мережах. В алгоритмі LFR у разі виявлення відмови каналу зв’язку всі потоки трафіку, уражені відмовою, агрегуються в так званий «великий» потік. Далі контролером SDN розгортається локальний резервний шлях для динамічної перемаршрутизації агрегованого потоку. Отже, алгоритм LFR зменшує кількість поточних операцій між контролером SDN і комутаційним обладнанням. Проведені числові результати довели, що LFR забезпечує швидке відновлення працездатності SDN.

Зростання складності сучасних мережних застосунків і величезний попит на інтернет-ресурси потребують від SDN здатності адаптуватися до вимог високого ступеня робастності та надійності. Як було зазначено вище, у SDN надзвичайно актуальним є саме завдання підвищення відмовостійкості та вчасне оновлення інформації про стан мережі, яким присвячено дослідження [82]. У ньому визначені нові алгоритми, спрямовані на покращення пошуку резервних шляхів у мережах великої розмірності у випадку поодиноких відмов каналів зв’язку з мінімальними часовими витратами на оновлення інформації про стан мережі. Нове рішення спрямоване на підвищення ефективності та зменшення операцій з оброблення службової інформації під час відмов каналів зв’язку.

У роботі [84] запропоновано схему адаптивного динамічного обчислення множини шляхів з метою забезпечення ефективного управління мережними ресурсами для організації маршрутизації та розподілу ресурсів за умови централізованого управління програмно-конфігурованою мережею. Така система може забезпечити необхідну інфраструктуру для інтеграції збору даних та аналітики, оцінювання продуктивності мережі в процесі використання різних алгоритмів оптимізації.

З іншої боку, як показано в роботах [85, 86], необхідність реалізації схеми захисту пропускної здатності мережі, особливо в разі реалізації багатошляхової стратегії маршрутизації, як правило, призводить до нелінійної постановки оптимізаційної задачі швидкої перемаршрутизації, що негативно впливає на обчислювальну складність кінцевих протокольних рішень. Крім того, у зазначених роботах не запропоновано варіанти дій, коли задача не має рішень, що може бути викликано, наприклад, відсутністю необхідного канального ресурсу для реалізації схем захисту пропускної здатності мережі, що має місце у випадку її перевантаження. Отже, актуальним науковим та прикладним завданням є формалізація та забезпечення узгодженого вирішення таких складних мережних завдань, як швидка перемаршрутизація (FRR), балансування навантаження на принципах TE та обмеження трафіку (TP) у випадку ймовірного перевантаження мережі. Це завдання пропонується розв’язати на підставі розроблення відповідної математичної моделі, яка, ґрунтуючись на досвіді створення та дослідження моделей QoS маршрутизації з підтримкою TP [87, 88], моделей і методів FRR і TE FRR [86], має відповідати таким ключовим вимогам:

– урахування особливостей структурної та функціональної побудови SD-WAN;

– підтримка багатошляхової стратегії маршрутизації в мережі;

– реалізація відомих схем забезпечення захисту елементів мережі, а також їхньої пропускної здатності;

– прийнятна обчислювальна складність та масштабованість кінцевих рішень, які підлягатимуть подальшій протокольній реалізації.

1.6. Аналіз рішень щодо безпечної маршрутизації в програмно-конфігурованих мережах

Загалом головною ідеєю, покладеною в основу протоколів безпечної маршрутизації, є підвищення безпеки та кіберстійкості ТКМ. Усі протоколи безпечної маршрутизації можна поділити на проактивні та реактивні [89–97]. Проактивні протоколи безпечної маршрутизації базуються на попередній оцінці ризиків інформаційної безпеки та використанні в процесі передачі пакетів найбезпечніших мережних елементів. Так, протокол SEAD (Secure Efficient Ad hoc Distance-Vector) [90] ґрунтується на принципах роботи проактивного дистанційно-векторного протоколу DSDV (Destination Sequenced Distance Vector) [91]. Особливістю протоколу є нестандартний механізм аутентифікації записів оновлень у таблицях маршрутизації, оснований на хеш-ланцюжках та дереві Меркла [92], із присвоєнням вищих порядкових номерів, перехоплення яких не дозволяє порушнику згенерувати оновлення з більш високим порядковим номером. Розвитком SEAD є протокол SDSDV (Secure DSDV), який не передбачає побудови дерева Меркла, а оновлення таблиць маршрутизації проводиться на основі додаткових полів AL (Alteration Field) та AC (Accumulation Field), які використовуються для захисту від зниження значення метрики та підвищення порядкових номерів, що присвоюються з кожним оновленням [93].

Реактивні протоколи безпечної маршрутизації, на відміну від проактивних, базуються на розрахунку маршруту на вимогу [94–99]. Одним із прикладів таких протоколів є протокол реактивної маршрутизації на основі довіри TSDRP (Trust Based Secure on Demand Routing Protocol), використання якого гарантує, що дані не будуть передаватися через зловмисні вузли [95]. Іншим представником реактивного протоколу є протокол для надійної доставки даних SPREAD (Security Protocol for REliable dAta Delivery) [96], що забезпечує захист даних завдяки зниженню ймовірності втрати секретного повідомлення в умовах передачі по незахищеній

ТКМ. Також відомим протоколом безпечної маршрутизації є SAR (Security-Aware Ad-hoc Routing) [97], що забезпечує високий ступінь безпеки ТКМ за допомогою присвоєння кожному вузлу визначеного рівня безпеки, що є головною метрикою маршруту. Для підвищення відмово- та кіберстійкості на сьогодня все частіше використовують протоколи швидкої перемаршрутизації [98, 99], які мають здебільшого реактивний характер та орієнтовані на захист таких мережних елементів, як вузол, канал зв'язку, маршрут тощо. Проте, незважаючи на більш високу ефективність з боку підвищення безпеки ТКМ, порівняно з проактивними протоколами безпечної маршрутизації реактивні програють за показниками якості обслуговування в ТКМ, насамперед за показником середньої затримки в мережі. Це пов'язано з тим, що спочатку необхідно оцінити стан безпеки мережі та її елементів на основі аналізу параметрів безпеки, а потім уже розрахувати маршрут за потребою, використовуючи ці параметри.

Базуючись на проведеному аналізі протоколів безпечної маршрутизації, варто зазначити, що всі вони є вдосконаленням традиційних протоколів маршрутизації (RIP, EIGRP, OSPF) [100–102] з використанням метрик безпеки.

Окреме місце посідають рішення щодо безпечної маршрутизації в програмно-конфігурованих мережах [103–106]. Завдяки розділенню площини даних від площини управління в SDN мережах можлива ефективна реалізація інноваційних підходів щодо безпечної маршрутизації (табл. 1.4). Зі свого боку традиційні маршрутні протоколи не враховують специфіку SDN мереж. Варто зазначити, що необхідність забезпечення безпеки на мережному рівні постає в різних типах програмно-конфігурованих мереж: проводових, безпроводових, вбудованих системах.

Таблиця 1.4

Рішення щодо безпечної маршрутизації
в програмно-конфігурованих мережах

Пос.	Сутність рішення
[103]	Запропоновано надійний механізм безпечної маршрутизації RouteGuardian у SDN мережі, який враховує можливості SDN комутаторів спільно з фреймворком Network Security Virtualization. У цій схемі ефективно використовуються розподілені мережні пристрої захисту для забезпечення аналізу аномального трафіку та ізоляції зловмисних вузлів. Крім того, механізм RouteGuardian підтримує динамічну реконфігурацію маршрутизації відповідно до останнього зафіксованого стану мережі.
[104]	Запропоновано механізм безпечної маршрутизації для промислових безпроводових сенсорних мереж, основаних на SDN парадигмі, у межах якого внутрішні зловмисні вузли знаходилися шляхом обчислення значення показника довіри до вузла. Розроблено евристичний біологічний алгоритм, який застосовувався для розрахунку безпечного шляху передавання потоків даних у мережі. Крім того, алгоритм відповідає вимогам до затримок у промисловому середовищі.
[105]	Розроблено новий безпечний комунікаційний SDN протокол, оснований на підході домовленості щодо групового ключа, для внутрішнього зв’язку в масштабованій архітектурі багатопроцесорної системи MPSoC – Cloud-of-Chips (CoC).
[106]	Проведено порівняння з боку безпеки застосунків SDN маршрутизації, таких як Plug-n-Serve й ElasticTree, запропоновано техніки пом’якшення відомих загроз безпеці, а також перевірено, чи має застосунок вбудований контрзахід проти цих загроз.

Отже, подальше вдосконалення протоколів і моделей безпечної маршрутизації для усунення недоліків наявних рішень має відповідати таким вимогам:

- урахування особливостей структурної та функціональної побудови ТКМ;
- підтримка потокового характеру різноманітних типів трафіку;
- урахування параметрів безпеки як окремих елементів, так і мережі загалом;
- урахування ризиків інформаційної безпеки, що ґрунтуються на наявних і виявлених уразливостях на елементах мережі;
- підтримка рекомендованих показників якості обслуговування;
- прийнятна обчислювальна складність та масштабованість кінцевих рішень, які підлягатимуть подальшій протокольній реалізації.

1.7. Постановка науково-прикладної задачі та формулювання завдань дослідження

Ґрунтуючись на результатах аналізу відомих рішень, спрямованих на забезпечення відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, проведеного в попередніх підрозділах, варто зазначити, що розробниками, провідними інженерами та науковцями накопичено достатній досвід, який підтверджується різноманіттям використовуваних підходів у цьому напрямі. Але незважаючи на значну кількість запропонованих рішень із цього питання, до програмно-конфігурованих телекомунікаційних мереж постійно висуваються нові вимоги, викликані інтенсивним розвитком інфокомунікаційних технологій та постійним процесом глобальної цифровізації.

З огляду на викладене, у цій дисертаційній роботі запропоновано підхід, оснований на розробленні та вдосконаленні математичних моделей маршрутизації, у межах яких би вдалося забезпечити відмовостійкість та мережну безпеку програмно-конфігурованих ТКМ та які використовувалися б під час розроблення

нових протоколів безпечної та відмовостійкої маршрутизації. Розроблені математичні моделі маршрутизації мають відповідати таким сучасним вимогам:

– ураховувати структурно-функціональні особливості програмно-конфігурованих ТКМ (топологію мережі, пропускну здатність каналів зв'язку, використання мережного ресурсу, відмови елементів мережі тощо);

– забезпечувати ефективне (збалансоване) використання мережного ресурсу з урахуванням характеристик (типу) трафіку та заданого рівня якості обслуговування;

– підтримувати механізми диференційованого (за пріоритетами) обмеження трафіку на границі мережі;

– ураховувати різноманітні критерії вибору (метрики) для визначення найбільш раціонального маршруту не тільки за структурно-функціональними особливостями мережі (пропускною здатністю, кількістю переприйомів тощо), але й за показниками мережної безпеки;

– забезпечувати адаптивну реакцію мережі на можливі відмови та атаки з мінімізацією наслідків та швидким відновленням функціонування мережі;

– забезпечувати захист критично важливих елементів мережі (вузлів, каналів, маршрутів, сегментів тощо) та її ресурсів;

– ураховувати ризики інформаційної безпеки, що ґрунтуються на наявних та нових виявлених вразливостях на елементах мережі, з мінімізацією можливих збитків;

– узгоджено розв'язувати задачі забезпечення якості обслуговування, відмовостійкості та мережної безпеки;

– забезпечувати прийнятну обчислювальну складність розрахункових рішень.

Ґрунтуючись на зазначених вимогах, що висуваються до математичних моделей маршрутизації, які можуть бути покладені в основу перспективних протоколів безпечної та відмовостійкої маршрутизації, виникає актуальна **науково-прикладна** задача, що полягає в забезпеченні відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, які функціонують в умовах відмов та

компрометації мережного обладнання, шляхом розроблення нових та вдосконалення вже наявних потокових моделей маршрутизації.

Для вирішення сформульованої наукової задачі та досягнення поставленої мети в дисертаційній роботі необхідно виконати такі завдання дослідження:

- розробити та дослідити потокову модель безпечної маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей у програмно-конфігурованих ТКМ;
- розробити та дослідити потокову модель безпечної маршрутизації з балансуванням навантаження в програмно-конфігурованих ТКМ;
- розробити та дослідити потокову модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційного обмеження трафіку в програмно-конфігурованих ТКМ;
- розробити та дослідити потокову модель безпечної швидкої перемаршрутизації з балансуванням навантаження та обмеженням трафіку на границі програмно-конфігурованої телекомунікаційної мережі;
- дослідити адекватність та ефективність запропонованих рішень щодо безпечної та відмовостійкої маршрутизації із балансуванням навантаження в програмно-конфігурованих ТКМ.

1.8. Висновки до першого розділу

1. Проведений у першому розділі аналіз показав, що в сучасних умовах інтенсивної інформатизації суспільства та цифрової трансформації економіки забезпечення мережної безпеки та відмовостійкості під час проєктування та функціонування програмно-конфігурованих ТКМ є одним із найважливіших завдань. Це пояснюється постійним розширенням потреб користувачів щодо множини та якості телекомунікаційних сервісів, збільшенням обсягів різнорідного типу трафіку, а також стрімким зростанням атак і втручань у роботу ТКМ. В умовах обмеженості мережного ресурсу зазначені чинники нерідко спричиняють

перевантаження ТКМ, збій в апаратно-програмному забезпеченні мережного обладнання та зниження рівня якості обслуговування та мережної безпеки взагалі. З огляду на зазначені умови, важливо забезпечити ефективне (збалансоване) використання доступного мережного ресурсу, що сприяло б покращенню відмовостійкості, мережної безпеки та якості обслуговування.

2. Аналіз відомих рішень щодо забезпечення відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ показав, що важливим технологічним інструментом підвищення рівня безпеки та відмовостійкості ТКМ в умовах можливих збоїв у апаратному чи програмному забезпеченні мережного обладнання, перевантаження або порушення рівня інформаційної безпеки є протоколи маршрутизації. Унаслідок проведеного аналізу наявних протокольних рішень зазначено, що підвищення ефективності рішень щодо безпечної та відмовостійкої маршрутизації, як правило, потребує відповідного вдосконалення наявних та розроблення нових математичних моделей і методів на основі адекватного врахування інформації про стан ТКМ: топології мережі, характеристик потоків пакетів, пропускної здатності каналів зв’язку та показників мережної безпеки елементів (вузлів та каналів).

3. Для усунення недоліків та відповідного подальшого вдосконалення протоколів і моделей безпечної та відмовостійкої маршрутизації зазначено вимоги, що висуваються до математичних моделей маршрутизації, покладених в їхню основу. Ґрунтуючись на отриманих вимогах, сформульовано науково-прикладну задачу, пов’язану із забезпеченням відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, які функціонують в умовах відмов та компрометації мережного обладнання, шляхом розроблення та вдосконалення відповідних математичних моделей маршрутизації. Для досягнення визначеної в дисертаційній роботі мети проведено декомпозицію поставленої науково-прикладної задачі на окремі завдання дослідження.

РОЗДІЛ 2
ПОТОКОВА МОДЕЛЬ МАРШРУТИЗАЦІЇ З УРАХУВАННЯМ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ БАЗОВИХ МЕТРИК КРИТИЧНОСТІ ВРАЗЛИВОСТЕЙ

У цьому розділі запропоновано вдосконалення потокової моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Удосконалення моделі полягатиме у введенні в традиційну потокову модель маршрутних метрик вагових коефіцієнтів, що характеризуватимуть ризики, які створюються наявними на вузлах ТКМ уразливостями та кількісно відображатимуть умовну вартість використання каналів зв’язку.

Розрахунок вагових коефіцієнтів базувався на методиці використання зазначених у рекомендації NIST CVSS v3 [107] базових метрик критичності вразливостей, що застосуються як допоміжний додаток із метою оцінювання ризиків і необхідної надмірності в ресурсах і процедурах для усунення потенційних порушень безпеки.

Зазначені метрики критичності вразливості дозволяють врахувати збитки від порушення конфіденційності, цілісності та доступності у випадку використання вразливостей на вузлах телекомунікаційної мережі, імовірність використання вразливостей зловмисником, а також показники системи оцінювання вразливості відповідно до бази даних загальновідомих уразливостей інформаційної безпеки (Common Vulnerabilities і Exposures, CVE). Використання даних вагових коефіцієнтів у межах потокової моделі маршрутизації дозволить здійснювати передачу потоків пакетів за найбільш безпечними маршрутами в телекомунікаційній мережі.

Матеріали другого розділу опубліковані в роботах [31, 32, 36, 39].

2.1. Базова потокова модель маршрутизації в телекомунікаційній мережі

Нехай структура мережі описується графом $G=(R, E)$, у якому $R=\left\{R_i;\ i=\overline{1,m}\right\}$ – це множина вершин, що моделюють маршрутизатори, а $E=\left\{E_{i,j};\ \ i,j=\overline{1,m},\ i\neq j\right\}$ – множина дуг, що представляють канали зв'язку (КЗ) у ТКМ. Тоді кожній дузі $E_{i,j}\in E$ ставиться у відповідність її пропускна здатність $\varphi_{i,j}$ (1/с). Нехай у ТКМ циркулює множина потоків пакетів K, які генеруються відповідними мережними додатками. Для кожного k-го потоку відомі такі вихідні дані:

λ^k – середня інтенсивність потоку трафіку, яка вимірюється в пакетах за секунду (1/с);

s_k і d_k – вузол-відправник і вузол-отримувач пакетів k-го потоку відповідно.

Тоді порядок маршрутизації в мережі визначають маршрутні змінні $x_{i,j}^k$, кожна з яких характеризує долю (частину) k-го потоку, що протікає в каналі зв'язку (КЗ) між i-м та j-м вузлами (маршрутизаторами) телекомунікаційної мережі. Виходячи з фізичного змісту введених маршрутних змінних, залежно від реалізованої стратегії маршрутизації на них накладаються умови вигляду

$$x_{i,j}^k\in\{0,1\} \tag{2.1}$$

або

$$0\le x_{i,j}^k\le 1. \tag{2.2}$$

Уведення умови (2.1) відповідає за реалізацію в ТКМ одношляхової стратегії маршрутизації. У випадку виконання умови (2.2) буде підтримуватися багатошляхова маршрутизація (не забороняючи одночасне використання й одношляхових рішень), за якої змінні $x_{i,j}^{k}$ можуть приймати крайні зі своїх можливих значень – нуль або одиницю (2.1). Множина застосованих шляхів надалі буде називатися мультишляхом.

Крім того, під час розрахунку маршрутних змінних мають виконуватися умови збереження потоку на маршрутизаторах мережі [19, 108]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 1, \ k \in K, \ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 0, \ k \in K, \ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = -1, \ k \in K, \ R_i = d_k. \end{cases} \quad (2.3)$$

У разі виконання умов (2.3) гарантується відсутність втрат пакетів на кожному маршрутизаторі та в мережі загалом, а також забезпечується зв’язність розрахованих маршрутів між відправником та отримувачем пакетів k-го потоку.

Для запобігання перевантаження каналів зв’язку ТКМ необхідно забезпечити виконання таких умов [19]:

$$\sum_{k\in K} \lambda^{k} x_{i,j}^{k} \leq \varphi_{i,j}, \ E_{i,j} \in E, \quad (2.4)$$

кількість яких відповідає кількості каналів зв’язку в мережі.

Для розрахунку оптимальних шляхів у ТКМ використаємо, наприклад, наступний лінійний критерій оптимальності [19]:

$$\sum_{k \in K} \sum_{E_{i,j} \in E} w_{i,j} x_{i,j}^{k} \Rightarrow \mathbf{min}, \tag{2.5}$$

де вагові коефіцієнти $w_{i,j}$ – це фактично маршрутні метрики, які мають ураховувати основні характеристики безпеки КЗ.

2.2. Методика розрахунку метрик маршрутизації на основі оцінки ризику інформаційної безпеки каналів зв'язку

Оцінювання вразливостей ТКМ є досить складним завданням з огляду на гетерогенність мережного обладнання та його програмного забезпечення. Найчастіше для цього використовується спеціалізоване апаратне або програмне забезпечення (наприклад, GFI LanGuard, Nessus, XSpider тощо), яке сканує мережу на предмет виявлення «слабких» місць у системі безпеки та попереджає про зони ризику в ТКМ [109–111]. Такі програми дозволяють оцінити мережну безпеку за допомогою активного та пасивного аналізу.

Під активним аналізом (наприклад, тестування на проникнення) розуміється імітація атак зловмисника, яка перевіряє наявність уразливостей у мережі [112].

Пасивний аналіз полягає в пошуках уразливостей за непрямими ознаками без підтвердження їхньої наявності, наприклад, наявність відритих портів, зміст заголовків пакетів тощо [113–115].

Водночас у деяких дослідженнях уже пропонуються для більш точного оцінювання безпеки мережі використовувати вищезазначені аналізи поетапно [116, 117]. Так, на першому етапі рекомендують застосовувати пасивний аналіз як більш швидкий, але менш точний; а на другому етапі, після усунення

виявлених уразливостей унаслідок пасивного аналізу, пропонують використовувати активний аналіз, що потребує більше часу, але є точнішим.

Додатково для оцінювання безпеки та ризиків у ТКМ можуть застосовуватися різноманітні організаційні стандарти та рекомендації щодо функціонування брандмауерів та їхніх політик безпеки, а також методи штучного інтелекту тощо [118]. Це підтверджується наявністю багатьох досліджень вітчизняних та іноземних науковців, що відображено в міжнародних стандартах і рекомендаціях [119–121], зокрема ISO 17799 (BS7799), ISO 15408, COBIT, COSO.

Ще одним із напрямів оцінювання рівня захищеності мережі загалом є підходи, основані на побудові уявлення можливих дій порушників у вигляді дерев або графів атак і подальшої перевірки властивостей цього дерева (графа) на підставі використання різних методів, наприклад, методів верифікації на моделі (model checking), а також обчислення різноманітних метрик захищеності щодо виявлення аномалій за різними сценаріями [118].

Одним з ефективних засобів забезпечення захисту ТКМ є попереднє оцінювання ризику інформаційної безпеки (РІБ). Процес оцінювання РІБ спрямований на запобігання використання відомих уразливостей, потенційно наявних у мережі, що захищається. Основний очікуваний результат у цьому разі – це значне ускладнення або повне позбавлення для зловмисників можливостей використання цих уразливостей. РІБ може розраховуватися за допомогою використання зазначених у рекомендації NIST CVSS v3 [107] метрик критичності вразливостей: базових, часових і метрик навколишнього середовища користувачів.

У межах запропонованого рішення для розрахунку вагових коефіцієнтів $w_{i,j}$ обрано базові метрики, які, на відміну від часових метрик та метрик навколишнього середовища користувача, характеризують незмінні за часом наявні вразливості на елементах мережі та дозволяють оцінити ризик інформаційної безпеки телекомунікаційної мережі загалом, а не для окремих випадків компрометації мережних елементів.

Введемо такі позначення:

$U = \left\{ U_i^q ; q = \overline{1,Q}, i = \overline{1,m} \right\}$ – множина вразливостей, які виявлені на вузлах (маршрутизаторах) ТКМ, де U_i^q – це q-та вразливість на i-му вузлі ТКМ;

$U_i^* \subset U$ – множина вразливостей на i-му вузлі ТКМ;

BS_i^q – показник критичності q-ї вразливості на i-му вузлі ТКМ, що розраховується за допомогою базових метрик системи оцінювання вразливостей, які представлені в рекомендації NIST CVSS v3 [107], та характеризує умовні збитки від використання вразливості U_i^q зловмисником;

P_i^q – імовірність використання q-ї вразливості зловмисником на i-му вузлі мережі, що за фізичним змістом є ймовірністю компрометації.

Відповідно до [107] для розрахунку ризику інформаційної безпеки від використання наявних уразливостей на i-му вузлі ТКМ використано такий вираз:

$$R^i = \sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q . \qquad (2.6)$$

Згідно з рекомендацією NIST збитки щодо базових метрик уразливостей на вузлах мережі [107] розраховуються як

$$BS_i^q = (0,6 \cdot Imp_i^q + 0,4 \cdot Ex_i^q - 1,5) \cdot f(Imp_i^q), \qquad (2.7)$$

де Imp_i^q – потенційний збиток від використання q-ї вразливості зловмисником на i-му вузлі мережі;

Ex_i^q – складність використання q-ї вразливості зловмисником на i-му вузлі ТКМ;

$f(Imp_i^q)$ – функція від потенційного збитку в разі використання q-ї вразливості зловмисником на i-му вузлі мережі.

Так, потенційний збиток від використання вразливості розраховується як [107]

$$Imp_i^q = 10,41\left[1-(1-Conf_i^q)\cdot(1-Int_i^q)\cdot(1-Av_i^q)\right], \quad (2.8)$$

де $Conf_i^q$ – збитки від порушення конфіденційності інформації, яка передається мережею та не може бути отримана неавторизованим, наприклад, зовнішнім, користувачем (зловмисником);

Int_i^q – збитки від порушення цілісності мережі, що характеризуються модифікацією, зміною та руйнуванням інформації неавторизованим користувачем (зловмисником) ТКМ;

Av_i^q – збитки від порушення доступності мережного ресурсу у випадку використання q-ї вразливості на i-му вузлі ТКМ.

Три метрики базової групи $Conf_i^q$, Int_i^q та Av_i^q визначають можливі наслідки використання зловмисником q-ї вразливості на i-му вузлі мережі.

У кожній із цих метрик збитки від використання вразливості можуть бути:

- *відсутніми* із значенням 0;
- *частковими* із значенням 0,275;
- *повними* із значенням 0,66 [107].

Значення метрик $Conf_i^q$, Int_i^q та Av_i^q представлені в табл. 2.1.

Таблиця 2.1

Значення показників для розрахунку базових метрик уразливостей елементів ТКМ [122]

Збиток конфіденційності $Conf_i^q$		
Відсутній (В)	Можливість порушення конфіденційності інформації відсутня	0,0
Частковий (Ч)	Існує значне, однак обмежене розголошення конфіденційної інформації	0,275
Повний (П)	Існує повне розкриття конфіденційної інформації	0,66
Збиток цілісності Int_i^q		
Відсутній (В)	Можливість порушення цілісності інформації відсутня	0,0
Частковий (Ч)	Існує можливість часткової модифікації даних або системних файлів	0,275
Повний (П)	Існує можливість модифікації будь-яких даних вузла	0,66
Збиток доступності Av_i^q		
Відсутній (В)	Можливість порушення доступності ресурсу відсутня	0,0
Частковий (Ч)	Існує можливість зниження продуктивності або виведення з ладу деяких функцій вузла	0,275
Повний (П)	Існує можливість повного виведення вузла з ладу	0,66

Складність використання вразливості розраховується за допомогою такого виразу:

$$Ex_i^q = 20 \cdot Ac_i^q \cdot Au_i^q \cdot AcV_i^q, \qquad (2.9)$$

де Ac_i^q – показник системи оцінки вразливості, що характеризує складність отримання доступу (вектор доступу);

Au_i^q – показник системи оцінки вразливості, що відповідає за вимоги до автентифікації;

AcV_i^q – показник системи оцінки вразливості, який відображає спосіб використання q-ї вразливості на i-му вузлі ТКМ, що за фізичним змістом характеризується «віддаленістю» зловмисника, тобто кількістю пристроїв та/або обмежень доступу, через які зловмисник може досягнути i-го вузла ТКМ для здійснення атаки.

Зазначені показники є базовими метриками [107, 122], які характеризують загальну складність реалізації атаки у використанні тієї чи іншої вразливості на i-му вузлі мережі (табл. 2.2).

Таблиця 2.2

Значення показників системи оцінки вразливості, які характеризують складність використання вразливостей [122]

Значення	Опис	Числова характеристика
Вектор доступу Ac_i^q		
Потрібен локальний доступ (Л)	Зловмисникові потрібен безпосередній фізичний доступ до об’єкта, на якому розташована вразливість	0,395
Можливий доступ із суміжної мережі (СмМ)	Зловмисникові потрібен доступ у межах однієї локальної мережі (одного широкомовного домену) до вразливого об’єкта	0,646
Можливий доступ із будь-якої мережі (М)	Зловмисник може використовувати вразливість віддалено з будь-якої ділянки мережі, зокрема через інтернет	1,0

Продовження таблиці 2.2

Вимоги до автентифікації Au_i^q		
Множинна (М)	Зловмисник повинен зробити більше ніж одну процедуру автентифікації для експлуатації вразливості вузла	0,45
Одинична (О)	Зловмиснику досить один раз автентифікуватися для експлуатації вразливості вузла	0,56
Відсутня (В)	Зловмисникові не потрібно проходити процедуру автентифікації для експлуатації вразливості вузла	0,704
Складність доступу до вузла AcV_i^q		
Складна (Ск)	Існує низка жорстких обмежень доступу до вузла. Наприклад, експлуатація вразливості вузла можлива тільки в дуже короткий проміжок часу або вимагає застосування соціальної інженерії, коли зловмисника може бути опізнано	0,35
Середня (Ср)	Існують деякі обмеження доступу до вузла. Наприклад, підключення до вразливого пристрою можливе тільки з певних вузлів або вразливий пристрій має функціонувати з нестандартними налаштуваннями	0,61
Легка (Л)	Немає особливих умов доступу до вразливості вузла. Наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на множині вузлів мережі	0,71

Функція від потенційного збитку $f(Imp_i^q)$ відповідно до [107] приймає значення 0, якщо збитку немає, тобто $f(Imp_i^q)=0$. У цьому разі розглядатиметься випадок, коли потенційний збиток наявний ($Imp_i^q \neq 0$). Тобто у подальших розрахунках використаємо $f(Imp_i^q)=1{,}176$ [107].

Тоді для кількісного оцінювання найгіршого сценарію ризик інформаційної безпеки за умови компрометації каналу зв'язку $E_{i,j} \in E$, що виходить з i-го вузла, використаємо такий вираз експоненціального характеру [123]:

$$R_{i,j} = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}, \tag{2.10}$$

де $w_{i,j}$ – вагові коефіцієнти (вага компрометації), які використовуються для оцінювання ризику, створюваного використанням уразливостей на i-му вузлі ТКМ. Фактично коефіцієнти $w_{i,j}$ кількісно характеризують потенційний збиток у разі застосування наявних на i-му вузлі ТКМ уразливостей.

Зазначимо, що у випадку, коли компрометація каналу зв'язку $E_{i,j} \in E$ відбувається тільки через використання вразливостей на i-му вузлі, тоді ризики інформаційної безпеки вузла та каналу зв'язку тотожно рівні, тобто

$$\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}. \tag{2.11}$$

Розрахунок вагових коефіцієнтів $w_{i,j}$ ґрунтується на припущенні, що компрометація каналу зв'язку $E_{i,j} \in E$ відбуватиметься внаслідок компрометації i-го вузла ТКМ, тобто шляхом використання наявних уразливостей на цьому вузлі.

У зазначеному випадку ймовірність компрометації i-го вузла залежить від наявності та використання вразливостей на ньому та розраховується як ризик інформаційної безпеки.

З огляду на (2.6)–(2.11), значення кожного з вагових коефіцієнтів (метрик маршрутизації) $w_{i,j}$ у виразі (2.5) можна розрахувати за допомогою такого виразу:

$$w_{i,j} = \frac{\sum\limits_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q}{\ln \sum\limits_{U_i^q \in U_i^*} e^{BS_i^q}}. \qquad (2.12)$$

2.3. Дослідження запропонованої потокової моделі безпечної маршрутизації з урахуванням ризиків інформаційної безпеки

Проведено дослідження запропонованої потокової моделі безпечної маршрутизації для підтвердження її працездатності, адекватності та ефективності отриманих результатів розрахунку.

У межах розрахункового прикладу обрано структуру телекомунікаційної мережі, зображеної на рис. 2.1. Мережа складається з п’яти вузлів (маршрутизаторів). У процесі дослідження генерувався один потік потоків, тобто $k = 1$, коли вузлом-джерелом пакетів був маршрутизатор R_1, а вузлом-отримувачем – маршрутизатор R_5.

Інтенсивність потоку пакетів змінювалася від 0 до 400 1/с. У розривах каналів зв’язку (рис. 2.1) показана їхня пропускна здатність (1/с).

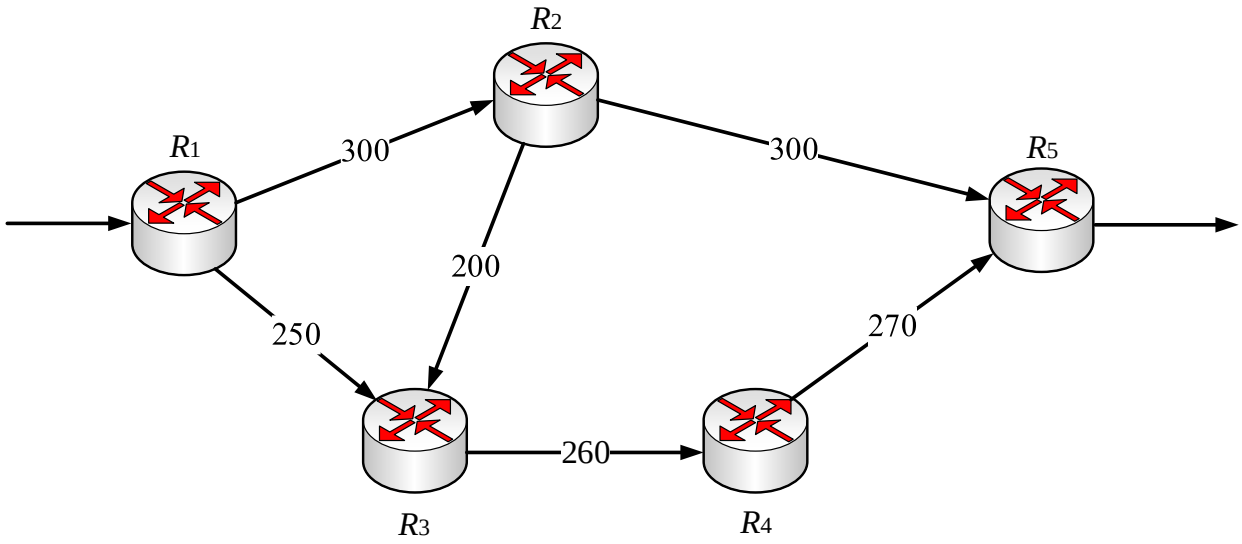


Рис. 2.1. Досліджуваний фрагмент структури ТКМ

Для розрахунку вагових коефіцієнтів $w_{i,j}$ ($E_{i,j} \in E$) використовувався вираз (2.12) спільно з виразами (2.6)–(2.11). У цьому випадку показник критичності q-ї вразливості на i-му вузлі ТКМ BS_i^q, що залежав від базових метрик системи оцінки вразливостей (табл. 2.1), визначався для різних маршрутизаторів із відповідною ймовірністю використання цієї q-ї вразливості на i-му вузлі мережі P_i^q, як показано в табл. 2.3.

Так, у табл. 2.3 кожному вузлу (маршрутизатору) мережі відповідав спеціальний опис наявної вразливості згідно з базою даних загальновідомих уразливостей інформаційної безпеки CVE. Зазначена база даних CVE призначена для збирання, зберігання та поширення інформації про виявлені вразливості. Кожній вразливості надається ідентифікаційний номер, опис і низка загальнодоступних посилань з описом.

Наприклад, для першого вузла R_1, яким є маршрутизатор Cisco RV042, характерна вразливість CVE-2020-3294. У цьому випадку CVE-2020-3294 – це унікальний номер, який описує вразливість у вебінтерфейсі управління маршрутизаторами Cisco RV042. Використання зазначеної вразливості дозволяє автентифікованому віддаленому зловмиснику з адміністративними привілеями

виконувати довільний код на враженому пристрої та надсилати створені великі за розміром запити на пошкоджений пристрій, викликаючи переповнення стека.

Таблиця 2.3

Характеристики вразливостей мережного обладнання для дослідження

Вузол ТКМ	Маршрутизатор	Базова оцінка BS_i^q	Імовірність використання вразливості P_i^q	Опис вразливості відповідно до спеціалізованої бази даних	Рівень критичності вразливості
R_1	Cisco RV042	7,2	0,1	CVE-2020-3294	Високий
R_2	Cisco Small Business RV160W	9,8	0,6	CVE-2021-1289	Критичний
R_3	NETGEAR R7450 1.2.0.62_1.0.1	6,5	0,2	CVE-2020-35839	Середній
R_4	Xiaomi RM1800	7,5	0,3	CVE-2020-14098	Високий
R_5	Cisco RV260	9,8	0,6	CVE-2021-1292	Критичний

Результати розв’язання задачі маршрутизації з використанням розробленої *моделі* 1 і *моделі* 2 наведені в табл. 2.4 та на рис. 2.2 та 2.3 відповідно. На цих рисунках у розривах каналів зв’язку вказані (згори донизу) їхні пропускні здатності (1/с), інтенсивність потоку, що протікає в каналі зв’язку (1/с), і для *моделі* 1 додатково зазначені вагові коефіцієнти $w_{i,j}$ для кожного каналу зв’язку $E_{i,j} \in E$.

Таблиця 2.4

Результати порівняльного аналізу *моделі* 1 та *моделі* 2 за умови інтенсивності потоку пакетів $\lambda^1 = 400$ 1/с

Канали зв'язку	Пропускна здатність КЗ, $\varphi_{i,j}$, 1/с	*Модель* 1		*Модель* 2
		Інтенсивність потоку, 1/с	Вагові коефіцієнти $w_{i,j}$	Інтенсивність потоку, 1/с
$E_{1,2}$	300	150	0,1	300
$E_{1,3}$	250	250	0,1	100
$E_{2,3}$	200	0	0,59	0
$E_{2,5}$	300	150	0,59	300
$E_{3,4}$	260	250	0,19	100
$E_{4,5}$	270	250	0,29	100

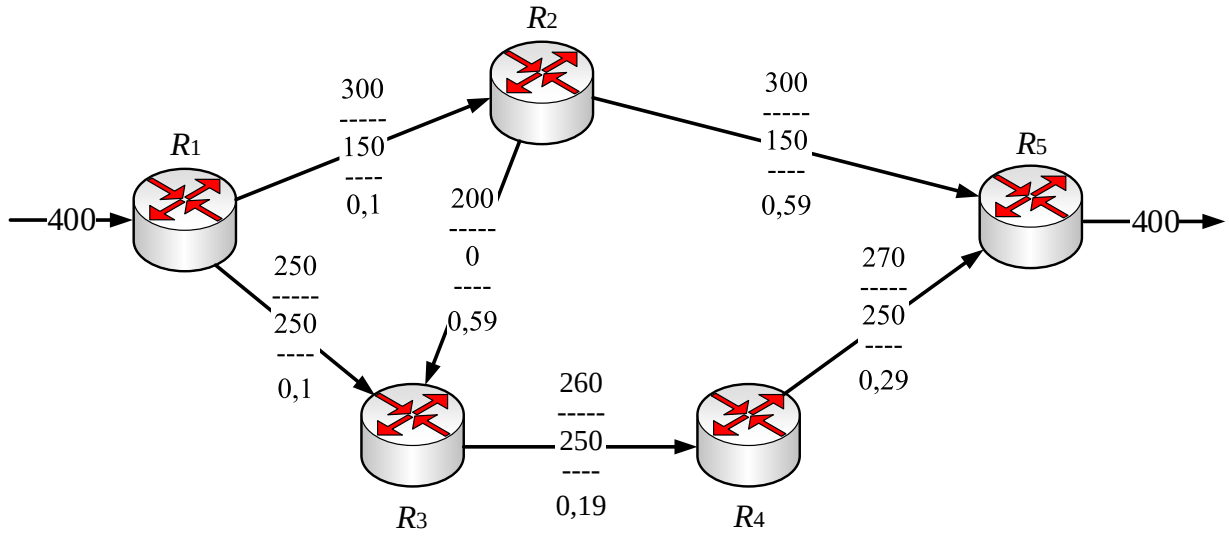


Рис. 2.2. Результат розв'язання задачі маршрутизації з використанням *моделі* 1

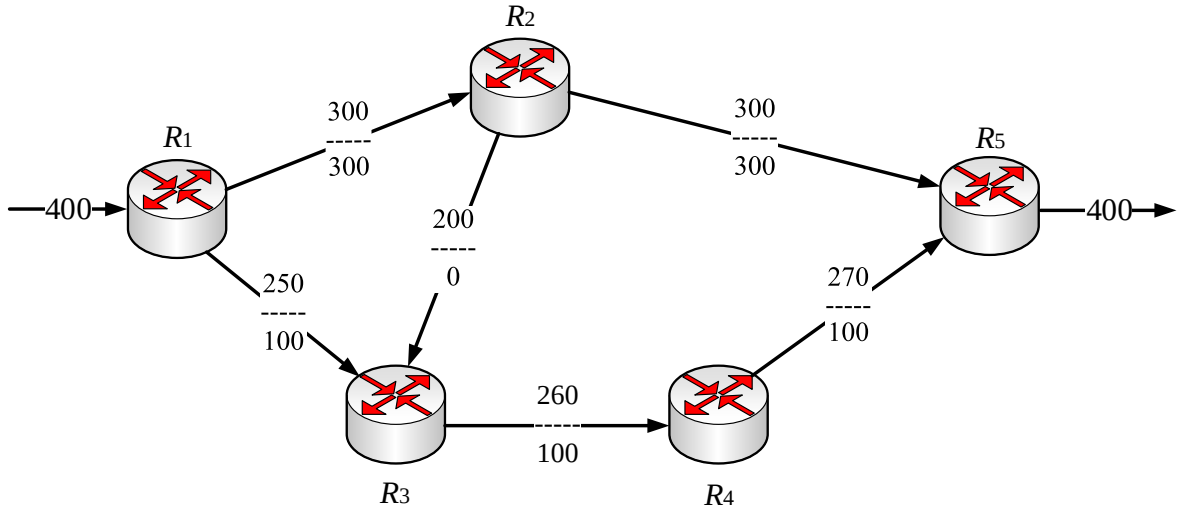


Рис. 2.3. Результат розв’язання задачі маршрутизації з використанням *моделі* 2

Як показано на рис. 2.1, унаслідок розв’язання маршрутної задачі за допомогою запропонованої моделі (*модель* 1) потік пакетів з інтенсивністю 250 1/с передавався маршрутом $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$, який містив найменш вразливі канали зв’язку. У разі перевантаження цього маршруту решта потоку (150 1/с) передавалася вже по наступному за вразливістю шляху $R_1 \rightarrow R_2 \rightarrow R_5$.

На відміну від *моделі* 1, під час використання *моделі* 2 спочатку (до 300 1/с) завантажувався найкращий з погляду пропускної здатності та кількості переприйомів (хопів), але найбільш вразливий шлях $R_1 \rightarrow R_2 \rightarrow R_5$. Решта потоку (100 1/с) передавалася маршрутом $R_1 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5$.

Порядок використання шляхів у ТКМ для різних інтенсивностей потоку пакетів під час використання *моделей* 1 і 2 представлений у табл. 2.5.

Таблиця 2.5

Порядок використання шляхів у ТКМ
для різних інтенсивностей потоку пакетів

Інтенсивність потоку пакетів, λ^1 1/с	*Модель* 1	*Модель* 2
	Використані шляхи	
$\lambda^1 \in (0;250]$	$R_1 \to R_3 \to R_4 \to R_5$	$R_1 \to R_2 \to R_5$
$\lambda^1 \in (250;300]$	$R_1 \to R_3 \to R_4 \to R_5$	$R_1 \to R_2 \to R_5$
	$R_1 \to R_2 \to R_5$	
$\lambda^1 \in (300;400]$	$R_1 \to R_3 \to R_4 \to R_5$	$R_1 \to R_2 \to R_5$
	$R_1 \to R_2 \to R_5$	$R_1 \to R_3 \to R_4 \to R_5$

У межах другого розрахункового прикладу обрано структуру телекомунікаційної мережі, яка зображена на рис. 2.4.

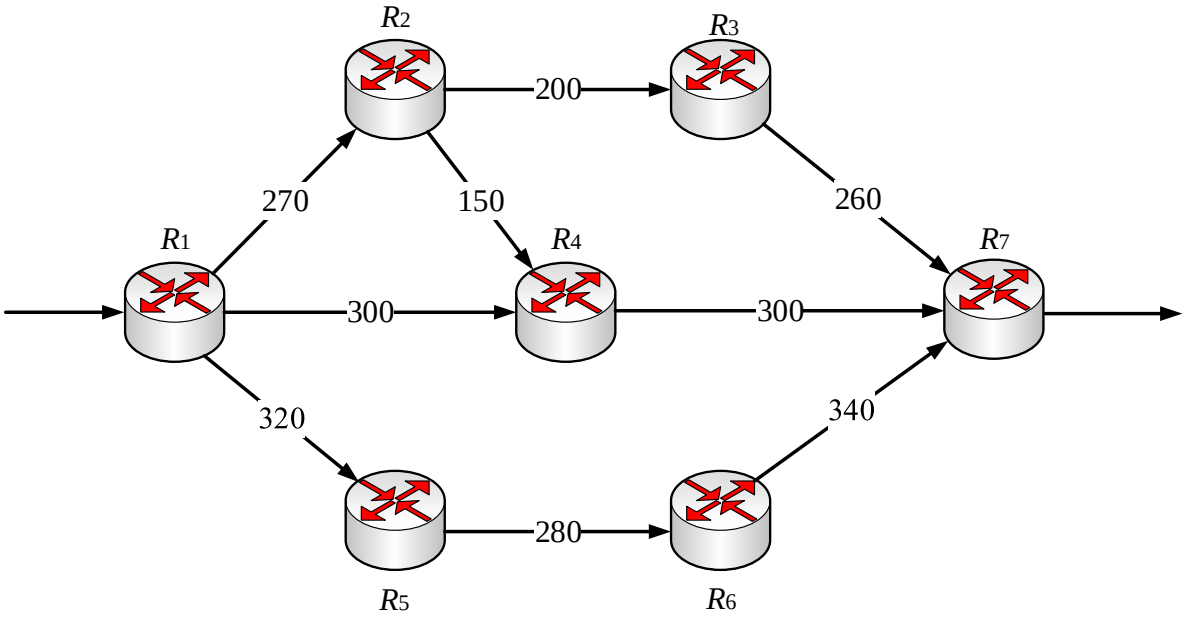


Рис. 2.4. Досліджуваний фрагмент другої структури ТКМ

Мережа складається із семи вузлів (маршрутизаторів). У дослідженні також генерувався один потік потоків, тобто $k=1$, коли вузлом-джерелом пакетів був маршрутизатор R_1, а вузлом-отримувачем – маршрутизатор R_7. Інтенсивність потоку пакетів змінювалася від 0 до 750 1/с. У розривах каналів зв'язку (рис. 2.4) показана їхня пропускна здатність (1/с). Для розрахунку вагових коефіцієнтів $w_{i,j}$ $(E_{i,j} \in E)$ використовувалися характеристики вразливостей мережного обладнання, представлені в табл. 2.6.

Таблиця 2.6

Характеристики вразливостей мережного обладнання для дослідження

Вузол ТКМ	Маршрутизатор	Базова оцінка BS_i^q	Імовірність використання вразливості P_i^q	Опис вразливості відповідно до спеціалізованої бази даних	Рівень критичності вразливості
R_1	Cisco RV325 Dual Gigabit WAN VPN Routers	7,5	0,3	CVE-2019-1653	Високий
R_2	Cisco RV042	5	0,2	CVE-2020-3291	Середній
R_3	Cisco Small Business RV160W	9,8	0,5	CVE-2021-1289	Критичний
R_4	D-Link DIR-817LW A1-1.04	7,6	0,4	CVE-2020-14098	Високий
R_5	Cisco RV260W	9,8	0,6	CVE-2021-1292	Критичний
R_6	Juniper EX2300	5,8	0,4	CVE-2019-0002	Середній
R_7	Xiaomi RM1800	5,5	0,2	CVE-2018-7100	Середній

Аналогічно з дослідженням, проведеним на першій структурі ТКМ (рис. 2.1), виконаємо порівняльний аналіз запропонованої моделі (2.1)–(2.5)

(*модель* 1), (2.12), із потоковою моделлю, із метрикою протоколу EIGRP (*модель* 2). Результати розв'язання задачі маршрутизації з використанням розробленої *моделі* 1 і *моделі* 2 наведені в табл. 2.7 та на рис. 2.5 і 2.6 відповідно, на яких червоним кольором указано канали зв'язку з найбільшими за критичністю ваговими коефіцієнтами.

Таблиця 2.7

Результати порівняльного аналізу *моделі* 1 та *моделі* 2 за умови інтенсивності потоку пакетів $\lambda^1 = 450$ 1/с

Канали зв'язку	Пропускна здатність КЗ, $\varphi_{i,j}$, 1/с	*Модель* 1		*Модель* 2
		Інтенсивність потоку, 1/с	Вагові коефіцієнти $w_{i,j}$	Інтенсивність потоку, 1/с
$E_{1,2}$	270	250	0,1	300
$E_{1,4}$	200	200	0,1	100
$E_{1,5}$	320	0		
$E_{2,3}$	200	150	0,59	0
$E_{2,4}$	150	100	0,59	300
$E_{3,7}$	260	150	0,19	100
$E_{4,7}$	300	300	0,29	100
$E_{5,6}$	280	0	0,29	100
$E_{6,7}$	340	0	0,19	100

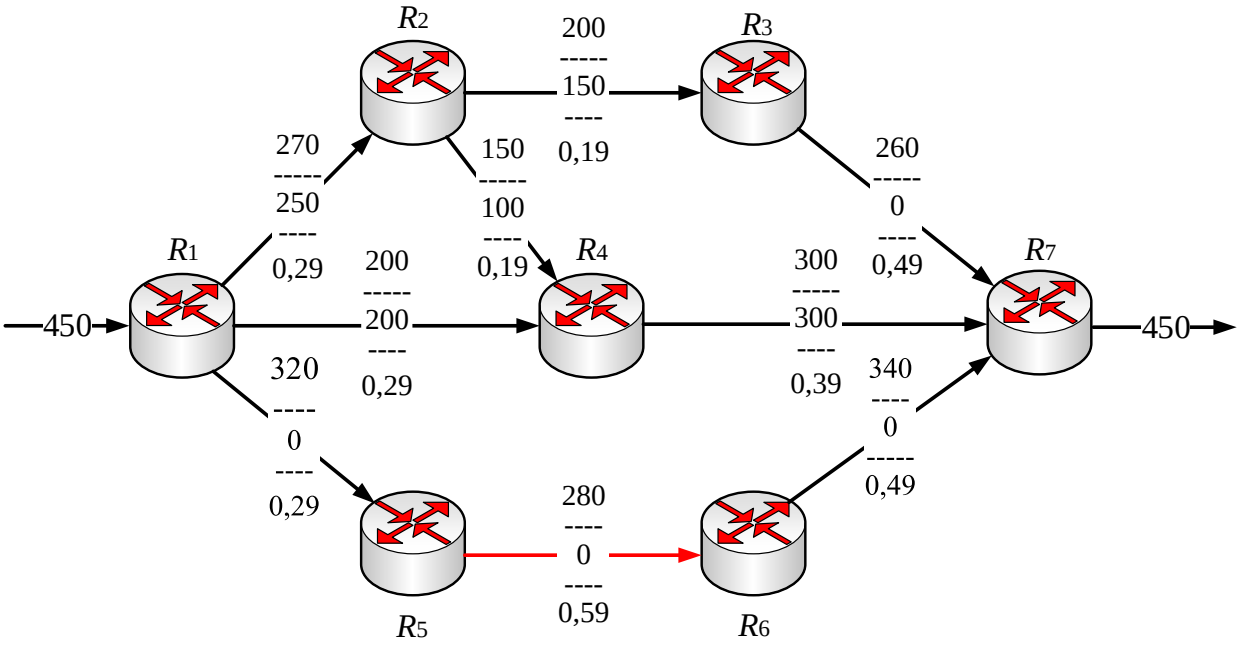


Рис. 2.5. Результат розв’язання задачі маршрутизації з використанням *моделі* 1

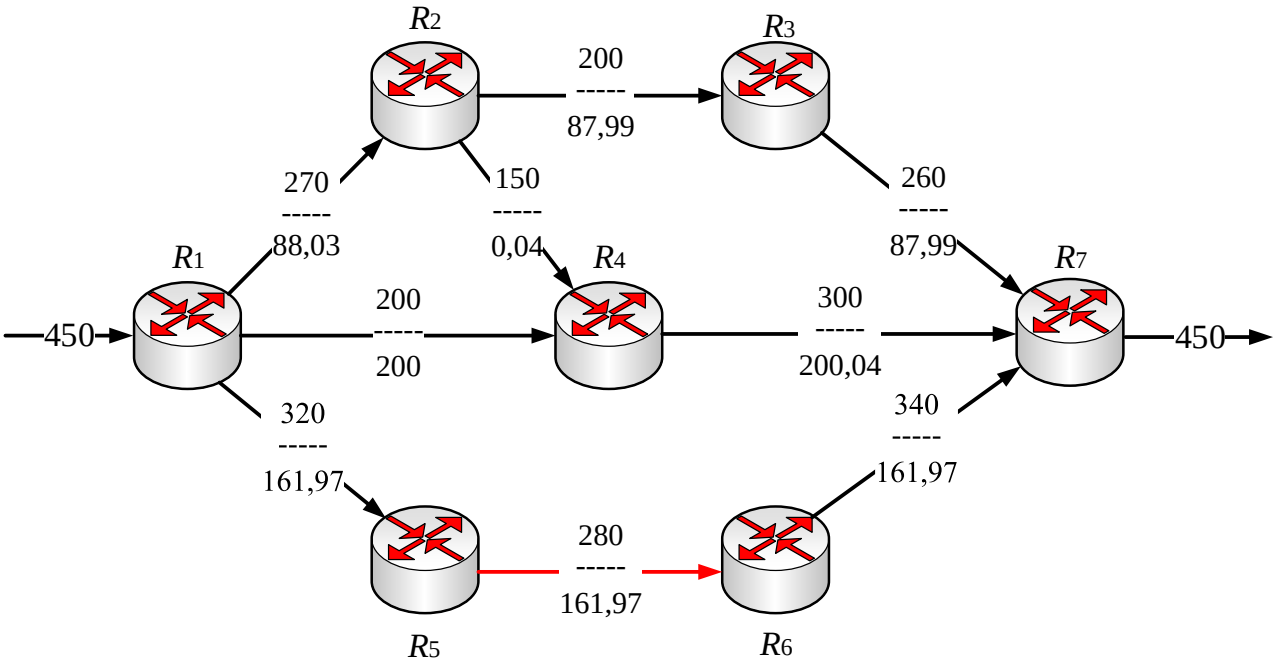


Рис. 2.6. Результат розв’язання задачі маршрутизації з використанням *моделі* 2

Загалом, результати використання шляхів у ТКМ для різних інтенсивностей потоку пакетів під час використання *моделей* 1 та 2 наведені в табл. 2.8.

Таблиця 2.8

Порядок використання шляхів у ТКМ
для різних інтенсивностей потоку пакетів

Інтенсивність потоку пакетів, λ^1 1/с	*Модель* 1	*Модель* 2
	Використані шляхи	
$\lambda^1 \in (0;200]$	$R_1 \to R_4 \to R_7$	$R_1 \to R_4 \to R_7$
$\lambda^1 \in (200;300]$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$ $R_1 \to R_2 \to R_3 \to R_7$ $R_1 \to R_5 \to R_6 \to R_7$
$\lambda^1 \in (300;470]$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$ $R_1 \to R_2 \to R_3 \to R_7$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$ $R_1 \to R_2 \to R_3 \to R_7$ $R_1 \to R_5 \to R_6 \to R_7$
$\lambda^1 \in (470;750]$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$ $R_1 \to R_2 \to R_3 \to R_7$ $R_1 \to R_5 \to R_6 \to R_7$	$R_1 \to R_4 \to R_7$ $R_1 \to R_2 \to R_4 \to R_7$ $R_1 \to R_2 \to R_3 \to R_7$ $R_1 \to R_5 \to R_6 \to R_7$

Як показано на рис. 2.5, унаслідок розв’язання маршрутної задачі за допомогою запропонованої моделі (*модель* 1) потік пакетів з інтенсивністю 200 1/с передавався маршрутом $R_1 \to R_4 \to R_7$, який містив найменш вразливі канали зв’язку. Під час перевантаження цього маршруту решта потоку (250 1/с) передавалася вже наступними вразливими шляхами: 100 1/с $R_1 \to R_2 \to R_4 \to R_7$ (100 1/с) та $R_1 \to R_2 \to R_3 \to R_7$ (150 1/с).

Водночас варто зауважити, що шлях $R_1 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7$, який містив найбільш уразливі за ваговими коефіцієнтами канали зв'язку за умови інтенсивності $\lambda^1 = 450$ 1/с, не використовувався взагалі.

На відміну від *моделі* 1, під час використання *моделі* 2 спочатку (до 200 1/с включно) завантажувався найкращий із погляду пропускної здатності, кількості переприйомів (хопів) та в цьому випадку найменш вразливий шлях $R_1 \rightarrow R_4 \rightarrow R_7$. Решта потоку (250 1/с) розподілялася між шляхами $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_7$ (0,04 1/с), $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_7$ (87,99 1/с) та $R_1 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7$ (161,97 1/с) відповідно до їхньої пропускної здатності за умови однакової кількості переприйомів (хопів). Унаслідок цього, по найбільш вразливому шляху $R_1 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7$, канали якого мали кращу пропускну здатність, передавався потік пакетів із більшою інтенсивністю та становив 161,97 1/с, порівняно з іншими шляхами.

2.4. Висновки до другого розділу

1. Запропоновано вдосконалену потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей (2.1)–(2.12). Основу моделі становлять умови реалізації одно- та багатошляхової маршрутизації (2.1), (2.2), збереження потоку (2.3) та запобігання перевантаженню каналів зв'язку ТКМ (2.4). У межах запропонованої моделі задача безпечної маршрутизації сформульована в оптимізаційній формі з критерієм оптимальності (2.5). Новизна розробленої моделі полягає в тому, що для розрахунку маршрутних метрик використовуються вирази (2.12), які характеризують ризик інформаційної безпеки в каналах зв'язку ТКМ та відповідно до рекомендацій NIST CVSS v.3 ураховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних уразливостей; беруть до уваги показники складності

застосування вразливостей на вузлах мережі та отримання доступу до мережних елементів зокрема та мережі загалом унаслідок використання зазначених уразливостей.

2. Проведено порівняльний аналіз розв'язань задачі маршрутизації на низці структур ТКМ, отриманих за допомогою двох моделей: запропонованої моделі безпечної маршрутизації (2.1)–(2.12) та моделі маршрутизації (2.1)–(2.5), що використовує метрику протоколу EIGRP. Результати дослідження показали, що в межах удосконаленої потокової моделі безпечної маршрутизації із зростанням інтенсивності потоку пакетів насамперед завантажувалися ті шляхи в ТКМ, які містили канали зв'язку з найменшими ваговими коефіцієнтами, тобто мали найменшу вагу компрометації. Передача потоку пакетів після перевантаження найбезпечнішого шляху здійснювалася наступними шляхами відповідно до значень вагових коефіцієнтів каналів зв'язку. Шляхи в ТКМ, які містили канали зв'язку з найбільшими ваговими коефіцієнтами, завантажувались останніми.

На відміну від запропонованої моделі, шляхи в межах моделі багатошляхової маршрутизації із метрикою EIGRP завантажувалися згідно з їхньою пропускної здатністю та кількістю переприйомів (хопів), не враховуючи ризики інформаційної безпеки взагалі. Потрібно зазначити, що для найгіршого сценарію в процесі використання q-ї вразливості на i-му вузлі ТКМ, тобто за умови 100 % компрометації каналу зв'язку з найбільшим ваговим коефіцієнтом, виграш удосконаленої моделі (2.1)–(2.12) порівняно з традиційними моделями в ділянці низьких навантажень ТКМ становив 37 %, у ділянці середніх навантажень – 25 % та поступово знижувався. Це пов'язано з тим, що в умовах перевантажень застосовуються всі доступні шляхи в ТКМ незалежно від ваги компрометації каналів зв'язку.

3. Як показали результати проведеного дослідження (табл. 2.3 та 2.6), застосування запропонованої моделі безпечної маршрутизації дозволяє розраховувати та використовувати маршрути з мінімальним ризиком інформаційної безпеки, тим самим забезпечивши максимальний рівень

мережної безпеки пакетам, які передаються в ТКМ. Запропонований підхід до формування маршрутних метрик може бути застосований комплексно в процесі розв’язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування. Перспективами розвитку отриманих рішень варто визнати синтез моделей і методів безпечної маршрутизації, за допомогою яких вдалося б гарантувати заданий рівень мережної безпеки на підставі розрахунку та використання відповідних маршрутів у ТКМ.

РОЗДІЛ 3
ПОТОКОВА МОДЕЛЬ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Для узгодженого розв’язання задач щодо забезпечення заданого рівня мережної безпеки та якості обслуговування технологічними засобами маршрутизації необхідно вдосконалити наявні або розробити нові математичні моделі та методи маршрутизації, які б стали основою перспективних протоколів. До того ж на рівні математичного опису треба забезпечити адекватне та взаємодоповнювальне врахування значень мережних параметрів, які мають відношення як до QoS, так і до мережної безпеки. Ідеться про топологію мережі, пропускні здатності та завантаженість каналів зв’язку та маршрутизаторів, а також про показники їхньої безпеки, наприклад, імовірності компрометації елементів ТКМ.

У попередньому розділі пропонується підхід до розв’язання задачі безпечної маршрутизації на підставі модифікації маршрутних метрик, які характеризують ризик інформаційної безпеки в каналах зв’язку ТКМ відповідно до рекомендацій NIST. У цьому, третьому, розділі пропонується потокова модель безпечної маршрутизації з балансуванням навантаження в ТКМ та подаються результати її дослідження. Запропонована модель маршрутизації відповідає вимогам концепції Traffic Engineering (TE) щодо забезпечення збалансованого використання доступного мережного ресурсу, що орієнтує на підвищення рівня QoS у ТКМ. Врахування ймовірності компрометації каналів зв’язку на рівні умов балансування навантаження дозволяє перерозподілити потоки таким чином, щоб більш безпечні канали завантажувалися інтенсивніше, ніж небезпечні. Результати дослідження запропонованої моделі маршрутизації представлені для різних мережних топологій та моделей блокування каналів зв’язку.

Матеріали розділу опубліковані в роботах [35, 46].

3.1. Математичний опис моделі безпечної маршрутизації з балансуванням навантаження в ТКМ на принципах Traffic Engineering

Для математичного опису моделі безпечної маршрутизації із балансуванням навантаження в ТКМ за основу будуть прийняті вирази (2.1)–(2.4). Тоді середню інтенсивність *k*-го потоку пакетів у каналі $E_{i,j} \in E$ (1/с) можна розрахувати таким чином:

$$\lambda_{i,j}^{k} = \lambda^{k} x_{i,j}^{k}. \tag{3.1}$$

Аналіз робіт, присвячених балансуванню навантаження в ТКМ [8, 10, 11, 19], показав, що дуже ефективним рішенням у цьому напрямі є реалізація положень концепції Traffic Engineering. В основу цього рішення покладена ідея мінімізації в процесі маршрутизації потоків пакетів верхнього рівня завантаженості всіх каналів зв'язку в ТКМ. Це має знизити ймовірність створення перевантажених ділянок у мережі за наявності недовантажених каналів зв'язку та покращити рівень якості обслуговування в ТКМ загалом. Тоді відповідно до моделі (2.1)–(2.4) коефіцієнти використання (завантаженості) каналів зв'язку будуть визначатися за формулою

$$\alpha_{i,j} = \frac{\sum\limits_{k \in K} \lambda^{k} x_{i,j}^{k}}{\varphi_{i,j}}. \tag{3.2}$$

У роботах [8, 11] для реалізації принципів, закладених у концепції Traffic Engineering, пропонується умови запобігання перевантаженню каналів зв'язку ТКМ записати в такому вигляді:

$$\sum_{k \in K} \lambda^{k} x_{i,j}^{k} \le \alpha \varphi_{i,j}, \tag{3.3}$$

де α – це додатково введена керуюча змінна, що кількісно визначає верхній поріг завантаженості каналів зв'язку, тобто є максимальним значенням серед (3.3). Це досягається тим, що, по-перше, ця змінна має відповідати таким умовам:

$$0 \le \alpha \le 1. \tag{3.4}$$

По-друге, критерієм оптимальності маршрутних рішень, які відповідають вимогам концепції Traffic Engineering [19], має бути така умова:

$$\min_{x,\alpha} \alpha. \tag{3.5}$$

Отже, класична задача маршрутизації з балансуванням навантаження на принципах Traffic Engineering сформульована в оптимізаційні формі з критерієм (3.5) та обмеженнями (2.1) або (2.2), (2.3), (3.3) та (3.4). Її рішення спрямоване на забезпечення оптимального балансування навантаження з мінімізацією верхнього порогу коефіцієнтів використання (3.2) кожного з каналів зв'язку мережі.

Для розширення функціональності наведеного рішення задачі маршрутизації в бік урахування параметрів мережної безпеки до умови балансування навантаження (3.3) пропонується внести певну модифікацію, щоб більш безпечні канали завантажувалися більш інтенсивно, ніж небезпечні КЗ. У процесі розв'язанні цієї задачі варто врахувати, що в загальному випадку з кожним маршрутизатором і каналом зв'язку пов'язана множина параметрів, які характеризують їхній рівень безпеки [10]. Одним із найбільш важливих із них є ймовірність компрометації. Загалом кожен маршрутизатор у межах графової моделі може бути умовно представлений еквівалентним каналом зв'язку. Тому в цьому дослідженні буде розглядатися випадок, коли для прикладу враховується лише компрометація каналів зв'язку. Тоді ймовірність

компрометації каналу $E_{i,j} \in E$ позначимо через $p_{i,j}$. У цьому випадку значення цих параметрів безпеки вважаються відомими величинами та визначаються статистикою щодо ефективності роботи встановлених на маршрутизаторах засобів протидії вторгненням та атакам (Intrusion Prevention System, IPS).

Основна ідея рішення, яке пропонується в цій роботі, полягає в тому, щоб забезпечити більш інтенсивне використання каналів із мінімальними ймовірностями компрометації, і навпаки – канали з високою $p_{i,j}$ повинні завантажуватися мінімально або навіть повністю блокуватися. Тому вдосконалена версія умов балансування навантаження (3.3) буде мати вигляд [35]:

$$\sum_{k \in K} \lambda^k x_{i,j}^k \le \alpha v_{i,j} \varphi_{i,j}, \tag{3.6}$$

де в правій частині нерівності вагові коефіцієнти $v_{i,j}$ мають відповідати таким граничним умовам:

$$v_{i,j} = \begin{cases} 0, & \text{якщо } p_{i,j} = 1; \\ 1, & \text{якщо } p_{i,j} = 0. \end{cases} \tag{3.7}$$

Тобто у випадку зростання ймовірності компрометації $p_{i,j}$ від 0 до 1, ваговий коефіцієнт $v_{i,j}$ має зменшуватися від 1 до 0. Безпосередньо залежність вагового коефіцієнта $v_{i,j}$ від $p_{i,j}$ буде задаватись спадною функцією на всьому проміжку

$$p_{i,j} \in [0;1]. \tag{3.8}$$

Сама ж функція $v_{i,j}(p_{i,j})$ буде називатися моделлю блокування каналів зв’язку за умови безпечного балансування навантаження в ТКМ. Саме значення

цієї функції вказує на те, яка частина пропускної здатності КЗ не буде використовуватися (тобто буде блокуватися) в процесі маршрутизації з причини зростання ймовірності його компрометації. Отже, задача безпечної маршрутизації на принципах Traffic Engineering була сформульована в оптимізаційній формі. Критерієм оптимальності залишається умова (3.5), а обмеженнями – вирази (2.1) або (2.2), (2.3), (3.4) та (3.6). Ця оптимізаційна задача в процесі реалізації одношляхової маршрутизації (2.1) належить до класу задач змішаного лінійного програмування (Mixed Integer Linear Programming, MILP), а за умови використання багатошляхової маршрутизації (2.2) – до класу задач лінійного програмування (LP).

3.2. Моделі блокування каналів зв'язку в умовах безпечного балансування навантаження в ТКМ

У межах проведеного дослідження множина допустимих значень $p_{i,j}$ (3.8) умовно буде розділена на декілька підмножин, кожній з яких відповідає свій сценарій компрометації ТКМ та її каналів зв'язку (табл. 3.1):

– *перший сценарій* охоплював діапазон імовірностей компрометації каналів від 0 до 0,5 (рівень небезпеки «умовно низький»);

– *другий сценарій* відповідав діапазону ймовірностей компрометації каналів від 0,35 до 0,85 (рівень небезпеки «умовно середній»);

– *третій сценарій* охоплював діапазон імовірностей компрометації каналів від 0,5 до 1 (рівень небезпеки «умовно високий»);

– *четвертий сценарій* відповідав діапазону ймовірностей компрометації каналів від 0 до 1 (рівень небезпеки «непрогнозований»).

Усі інші сценарії компрометації ТКМ та її каналів зв'язку можуть бути деякою комбінацією наведених у табл. 3.1 базових сценаріїв.

Таблиця 3.1

Відповідність сценаріїв компрометації значенням $p_{i,j}$

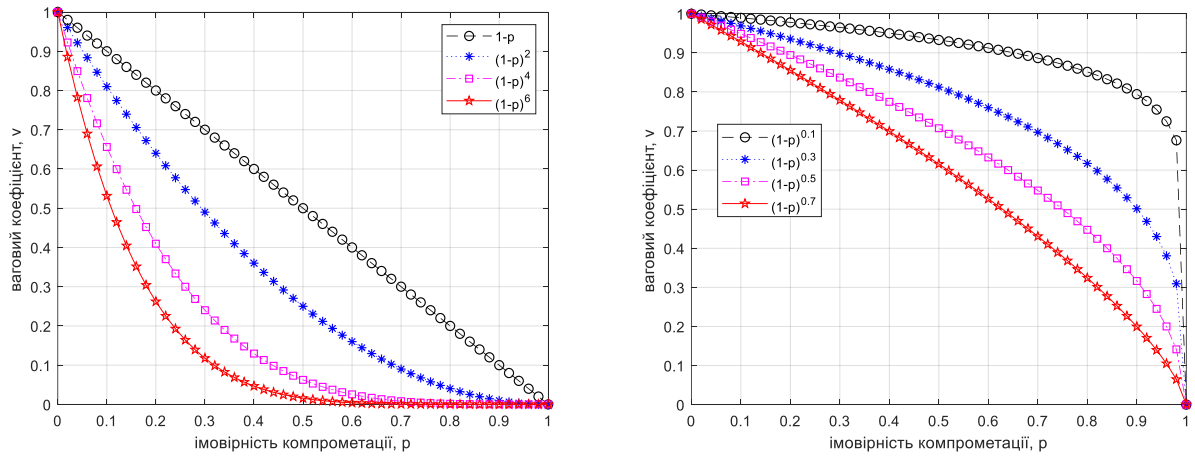
Перший сценарій	Другий сценарій	Третій сценарій	Четвертий сценарій
$p_{i,j} \in [0;0,5]$	$p_{i,j} \in [0,3;0,8]$	$p_{i,j} \in [0,5;1]$	$p_{i,j} \in [0;1]$

Загалом обмеженням (3.7) та (3.8) може відповідати множина різноманітних функцій, на прикладах дослідження яких варто зупинитись окремо. У першому випадку для розрахунку коефіцієнтів $v_{i,j}$ може використовуватися функціональна залежність:

$$v_{i,j} = (1 - p_{i,j})^n, \tag{3.9}$$

де n – це керуючий параметр, за допомогою якого здійснюється регулювання чутливості вагового коефіцієнта $v_{i,j}$ до значень імовірності компрометації каналу $p_{i,j}$.

З огляду на обраний діапазон значень n характер залежності (3.9) може суттєво змінюватися (рис. 3.1).



а) якщо $n \geq 1$ б) якщо $n < 1$

Рис. 3.1. Візуалізація моделі блокування каналів зв’язку (3.9)

Тоді за результатами аналізу, зображеними на рис. 3.1, можна зробити важливий висновок: модель блокування КЗ, представлена виразом (3.9), досить універсальна та може використовуватися для будь-якого з наведених сценаріїв компрометації (табл. 3.1):

- якщо $n>1$, ця модель блокування досить чутлива до ймовірностей компрометації КЗ, оскільки навіть за мінімальних значень $p_{i,j}$ пропускна здатність КЗ може блокуватися на 10–50 % і вище (рис. 3.1, *а*). Тому її краще використовувати, наприклад, у першому та другому сценаріях компрометації;

- за умови зростання параметра n (якщо $n>4$) цю модель блокування рекомендовано застосувати лише за першим сценарієм компрометації, оскільки вже в разі $n\geq 0{,}5$ канали зв'язку будуть повністю блоковані (рис. 3.1, *а*);

- якщо $0<n<1$, модель (3.9) слабко чутлива до компрометації каналів за першим сценарієм та помірно чутлива до рівня компрометації КЗ за другим та третім сценаріями (рис. 3.1, *б*).

Другим типом моделі блокування каналів зв'язку може бути функція

$$v_{i,j}=1-p_{i,j}^{n}, \tag{3.10}$$

у якій також керуючий параметр n суттєво впливає на характер чутливості $v_{i,j}$ до значень імовірності компрометації каналу $p_{i,j}$ (рис. 3.2).

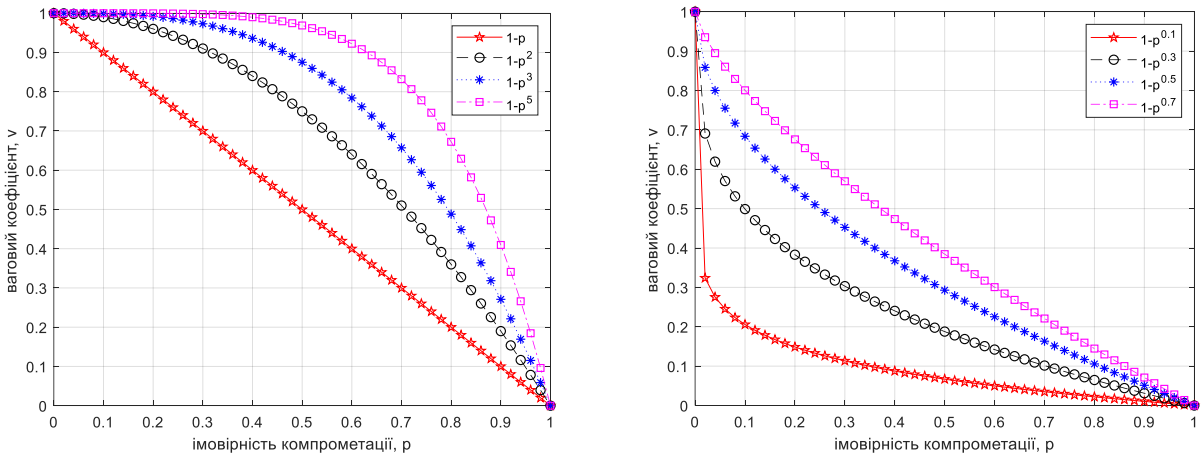
За результатами аналізу, зображеними на рис. 3.2, можна зробити важливий висновок: модель блокування КЗ, представлена виразом (3.10), також досить універсальна та може використовуватися для будь-якого з наведених сценаріїв компрометації (табл. 3.1), але ситуація щодо впливу параметра n практично дзеркальна порівняно з (3.9):

- якщо $0<n<1$ (рис. 3.2, *б*), модель блокування (3.10), порівнюючи з рис. 3.1, *а*, є більш чутливою до мінімальних імовірностей компрометації КЗ та

менш чутливою до середніх та високих значень $p_{i,j}$ (другий та третій сценарії компрометації);

- якщо $n>1$ (рис. 3.2, *а*), модель (3.10) порівняно з рис. 3.1, *б* забезпечує меншу чутливість до $p_{i,j}$ за першим та другим сценаріями (табл. 3.1) та вищу чутливість до високих значень $p_{i,j}$ (третій сценарій);

- у разі зростання параметру n (якщо $n>5$) цю модель рекомендовано застосувати лише за третім сценарієм компрометації, оскільки за умови $0<p_{i,j}<0{,}5$ канали зв'язку блокуватися не будуть (рис. 3.2, *а*).



а) якщо $n\geq 1$ б) якщо $n<1$

Рис. 3.2. Візуалізація моделі блокування каналів зв'язку (3.10)

Третім варіантом моделі блокування каналів зв'язку може бути експоненціальна функція вигляду

$$v_{i,j}=\exp(-n\cdot p_{i,j}), \qquad (3.11)$$

у якій для забезпечення виконання умов (3.7) необхідно, щоб $n\geq 7$ (рис. 3.12).

За результатами аналізу, зображеними на рис. 3.3, можна зробити висновок: модель блокування КЗ, яка представлена виразом (3.11), рекомендовано використовувати лише за першим сценарієм компрометації КЗ

ТКМ (табл. 3.1), оскільки в разі $p_{i,j} \geq 0,6$ відповідний канал зв'язку фактично блокується.

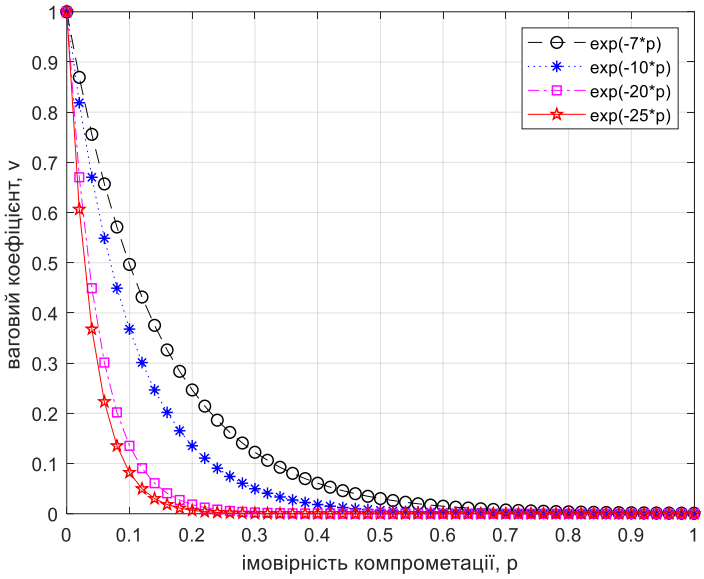


Рис. 3.3. Візуалізація моделі блокування каналів зв'язку (3.11)

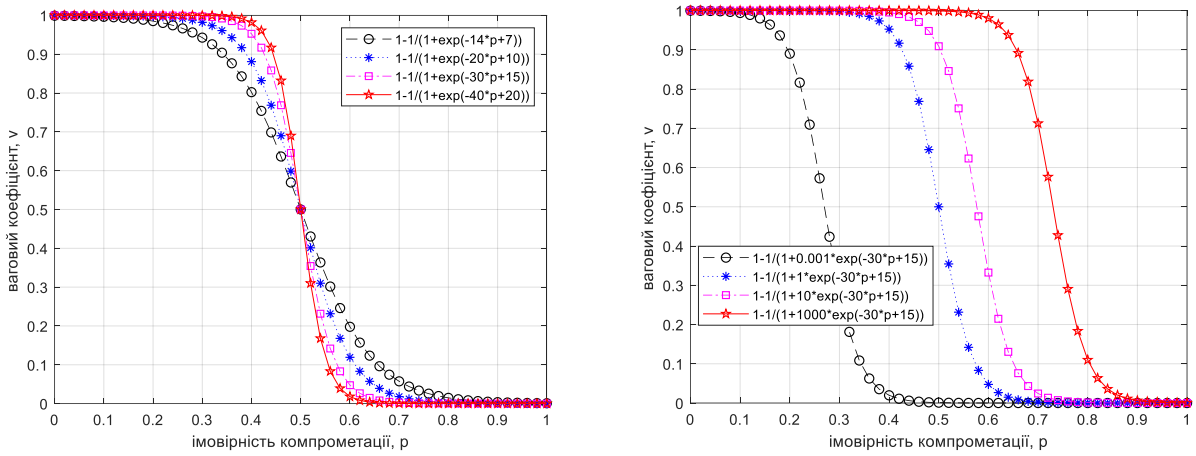
Модель (3.11) порівняно з моделями (3.9) (рис. 3.1, *а*) та (3.10) (рис. 3.2, *б*) забезпечує більшу чутливість до невеликих та середніх значень імовірності компрометації $p_{i,j}$.

Моделі (3.9)–(3.11) належать до простих моделей блокування каналів зв'язку ТКМ, що можуть пояснити роботу більш складних моделей. Так, наприклад, модель блокування КЗ може бути описана більш складною порівняно з (3.9)–(3.11) функціональною залежністю

$$v_{i,j} = 1 - \frac{1}{1 + n \cdot \exp(-r \cdot p_{i,j} + b)}, \qquad (3.12)$$

у якій для виконання умов (3.7) та (3.8) $r = 2b$, $b \geq 7$, $n > 0$ (рис. 3.4).

Як показано на рис. 3.4, *а*, якщо $p_{i,j} \in [0;0,5]$, модель (3.12) якісно нагадує поведінку моделі (3.10), де $n \geq 1$ (рис. 3.2, *а*). Коли $p_{i,j} \in [0,5;1]$, модель (3.12) дещо схожа на моделі (3.10) та (3.9), де $n \geq 1$ (рис. 3.1, *а*).



а) $n = 1$ б) $r = 30$, $b = 15$

Рис. 3.4. Візуалізація моделі блокування каналів зв'язку (3.12)

Використання моделі блокування КЗ (3.12) явно орієнтоване на певний діапазон значень $p_{i,j}$ (сценарій компрометації). Середнє значення цього діапазону можна задати за допомогою параметра r (рис. 3.4, *б*). Ширина обраного діапазону значень $p_{i,j}$ регулюється шляхом зміни значень параметрів n та b (рис. 3.4, *а*).

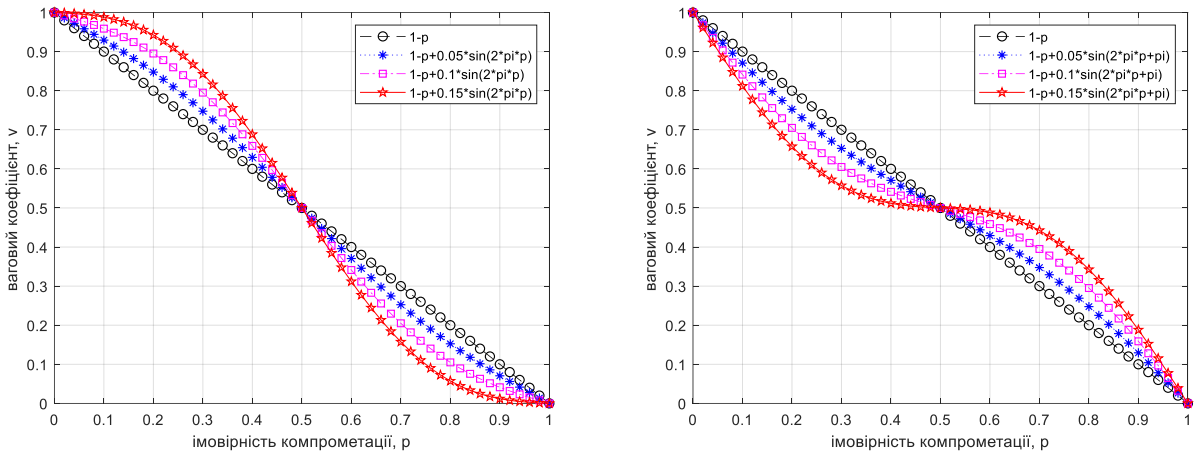
Ще одним прикладом складної моделі блокування може бути вираз

$$v_{i,j} = 1 - p_{i,j} + n\sin(2\pi p_{i,j} + \theta), \qquad (3.13)$$

де для виконання умов (3.7) та (3.8) $n \leq 0,15$ та $\theta \in \{0;\pi\}$ (рис. 3.5).

Модель блокування (3.13) загалом також досить універсальна, оскільки може використовуватися в будь-якому з наведених у табл. 3.1 сценаріїв компрометації.

У разі $\theta = 0$ модель (3.13) слабше реагує на мінімальні значення $p_{i,j}$, ніж якщо $\theta = \frac{\pi}{2}$, але більш чутлива до великих значень $p_{i,j}$ порівняно з $\theta = \frac{\pi}{2}$. Крім того, за умови максимальних значень n ($n = 0{,}15$) та якщо $\theta = \frac{\pi}{2}$ модель блокування (3.13) несуттєво реагує на зміну $p_{i,j}$ у межах другого сценарію компрометації (табл. 3.1).



а) $\theta = 0$ б) $\theta = \pi$

Рис. 3.5. Візуалізація моделі блокування каналів зв’язку (3.13)

Отже, залежно від стану ТКМ і прогнозованого сценарію компрометації мережних елементів можна обрати ту чи іншу запропоновану модель блокування КЗ (3.9)–(3.13) у разі безпечного балансування навантаження (3.9) із виконанням умов (3.7) та (3.8).

Таблиця 3.2

Чутливість моделі блокування каналів зв'язку до значень імовірності їхньої компрометації

Тип моделі блокування КЗ	Перший сценарій $p_{i,j} \in [0;0,5]$	Другий сценарій $p_{i,j} \in [0,35;0,85]$	Третій сценарій $p_{i,j} \in [0,5;1]$	Четвертий сценарій $p_{i,j} \in [0;1]$
(3.9), якщо $n \geq 1$	Висока	Висока	Критична	Висока
(3.9), якщо $n < 1$	Дуже низька	Низька	Середня	Невисока
(3.10), якщо $n \geq 1$	Дуже низька	Низька	Середня	Невисока
(3.10), якщо $n < 1$	Дуже висока	Висока	Критична	Висока
(3.11), якщо $n \geq 7$	Дуже висока	Критична	Критична	Дуже висока
(3.12), якщо $n = 1$	Дуже низька	Середня	Дуже висока	–
(3.13), якщо $\theta = 0$	Низька	Середня	Висока	Середня
(3.13), якщо $\theta = \pi$	Невисока	Середня	Невисока	Середня

3.3. Дослідження процесів балансування навантаження в ТКМ відповідно до вимог мережної безпеки

Під час проведеного дослідження аналізувався вплив структури ТКМ, сценаріїв компрометації (табл. 3.1) та моделей блокування КЗ (3.9)–(3.13) на показники завантаженості мережі (3.2) та рівня мережної безпеки. Рівень мережної безпеки оцінювався за таким показником, як імовірність компрометації пакетів *k*-го потоку вздовж множини використаних шляхів

$$p_{E2E}^{k} = \sum_{s \in S^{k}} \frac{\lambda_{s}^{k}}{\lambda^{k}} p_{s}, \tag{3.14}$$

де S^{k} – множина шляхів (маршрутів), які використовуються для передачі пакетів k-го потоку між заданою парою маршрутизаторів у ТКМ;

λ_{s}^{k} – інтенсивність k-го потоку пакетів, які передаються s-м шляхом у ТКМ;

p_{s} – імовірність компрометації s-го шляху, яка визначається відповідно до формули

$$p_{s} = 1 - \prod_{E_{i,j} \in Path_{s}} (1 - p_{i,j}), \tag{3.15}$$

у якій $Path_{s} = \{E_{i,j}\}$ – це множина каналів зв'язку мережі, які утворюють у ній s-й шлях.

Позначимо також через α^{*} максимальне значення з множини коефіцієнтів завантаженості (3.2), оскільки у використанні умов балансування (3.6) значення α характеризує верхній поріг завантаженості пропускної здатності КЗ, яка залишилася після блокування відповідно до значень імовірності компрометації цього каналу.

У проведеному дослідженні розглядалися різні варіанти мережних топологій. Основні результати досліджень та закономірності будуть запропоновані для двох основних мережних структур.

3.3.1. Дослідження процесів безпечного балансування навантаження в ТКМ на першій мережній структурі

Нехай структура досліджуваної мережі зображена на рис. 3.6. Інтенсивність вхідного потоку, який передавався від першого до четвертого маршрутизатора, становила 350 1/с.

У табл. 3.3 наведені пропускні здатності каналів зв’язку та варіанти ймовірностей їхньої компрометації відповідно до обраних стратегій компрометації ТКМ (табл. 3.1). Згідно з інформацією про структуру ТКМ (рис. 3.6) та характеристикою її КЗ, у табл. 3.4 наведені дані про доступні маршрути між R_1 та R_4, а також імовірності їхньої компрометації.

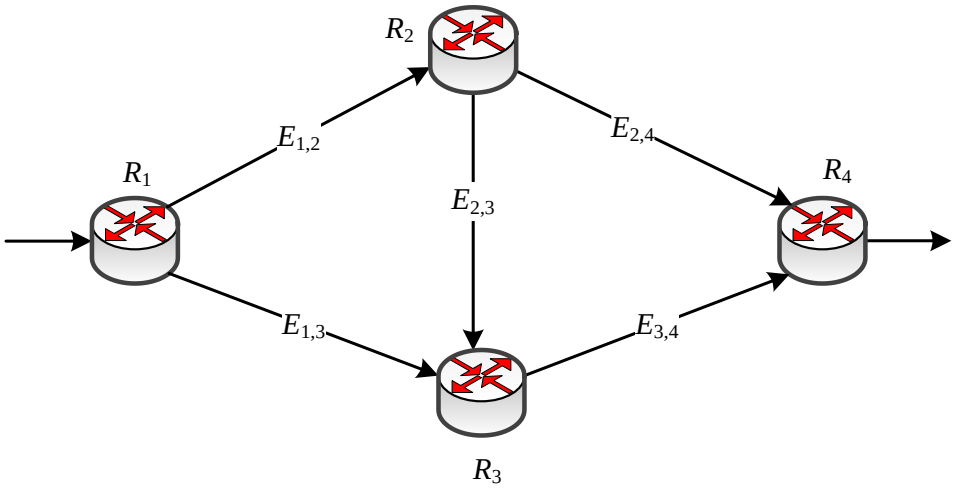


Рис. 3.6. Варіант першої досліджуваної структури ТКМ

Таблиця 3.3

Характеристики каналів зв’язку ТКМ

Канал зв’язку	Пропускна здатність	Імовірності компрометації каналів зв’язку			
		Перший сценарій	Другий сценарій	Третій сценарій	Четвертий сценарій
$E_{1,2}$	700	0,1	0,3	0,5	0,1
$E_{2,4}$	600	0,5	0,7	0,9	0,9
$E_{1,3}$	400	0,4	0,7	0,9	0,7
$E_{3,4}$	600	0,2	0,4	0,6	0,3
$E_{2,3}$	800	0,2	0,3	0,5	0,4

Таблиця 3.4

Імовірності компрометації маршрутів у ТКМ

Маршрут		Перший сценарій	Другий сценарій	Третій сценарій	Четвертий сценарій
1	$R_1 \to R_2 \to R_4$	0,55	0,79	0,95	0,91
2	$R_1 \to R_3 \to R_4$	0,52	0,82	0,96	0,79
3	$R_1 \to R_2 \to R_3 \to R_4$	0,424	0,706	0,9	0,622

Для дослідження першого сценарію компрометації каналів зв'язку (табл. 3.3 та 3.4) у першому випадку за модель блокування КЗ була обрана залежність (3.9), де $n \geq 1$. Тоді в табл. 3.5 показано результати розрахунків, отримані з використанням класичної ТЕ-моделі (2.2), (2.3), (3.3)–(3.5) та запропонованої моделі Secure Traffic Engineering (SecTE): (2.2), (2.3), (3.4)–(3.6).

Таблиця 3.5

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.9)

Канал зв'язку	$p_{i,j}$	Traffic Engineering рішення		Рішення з безпечної маршрутизації (n=3,2)	
		$\lambda^1_{i,j}$	$\alpha_{i,j}$	$\lambda^1_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	0,1	222,7273	0,3182	350	0,5
$E_{2,4}$	0,5	190,9091	0,3182	63,6398	0,1061
$E_{1,3}$	0,4	127,2727	0,3182	0	0
$E_{3,4}$	0,2	159,0909	0,2652	286,3602	0,4773
$E_{2,3}$	0,2	31,8182	0,0398	286,3602	0,3580

Відповідно до рішення (табл. 3.5), отриманого для моделі ТЕ (2.2), (2.3), (3.3)–(3.5), верхній поріг завантаженості каналів зв'язку становив 0,3182.

За першим маршрутом пакети передавалися з інтенсивністю 190,9091 1/с, за другим – 127,2727 1/с, за третім – 31,8182 1/с. Тому згідно з табл. 3.4 ймовірність компрометації пакетів у ТКМ (3.14) становила 0,5276.

У табл. 3.6 наведені результати порівняльного аналізу досліджуваних рішень: ТЕ-моделі та SecTE (3.9) за умови різних значень керуючого параметра *n*. За цими результатами можна зробити висновок, що використання вдосконаленої моделі SecTE (2.2), (2.3), (3.4)–(3.6) дозволяє забезпечити балансування навантаження в КЗ відповідно до їхніх імовірностей компрометації. Так, наприклад, завантаженість найбільш небезпечного каналу $E_{2,4}$ ($p_{2,4} = 0,5$) знизилася з 0,3182 до 0,1061, що спричинило більше навантаження на безпечніші КЗ (табл. 3.5). У кінцевому результаті реалізація моделі SecTE (3.9) дозволила знизити ймовірність компрометації пакетів у ТКМ (3.14) від 12,93 % до 15,3 % порівняно з рішенням на основі ТЕ-моделі (табл. 3.6). Як і зазначалося в попередньому підрозділі, зі збільшенням *n* маршрутні рішення ставали чутливішими до параметрів мережної безпеки.

Таблиця 3.6

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.9)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
2	0,5	0,6554	0,4594	12,93 %
2,5	0,5	0,7786	0,4537	14,01 %
3	0,5	0,9158	0,4487	14,96 %
3,2	0,5	0,9747	0,4469	15,3 %

На рис. 3.7, відповідно до змісту табл. 3.6, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.9). Завдяки зміні параметра *n* можна зменшити

ймовірність компрометації пакетів (від 12,93 % до 15,3 %) з підвищенням на 57 % верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.7).

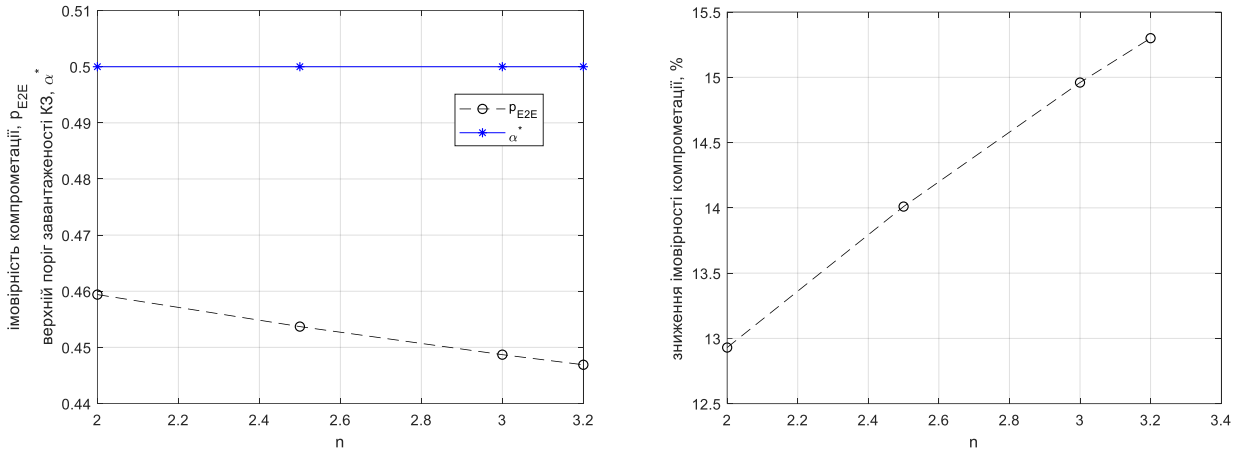


Рис. 3.7. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.9)

У другому випадку за модель блокування КЗ обрана залежність (3.12), де $r = 30$ та $b = 15$. Тоді в табл. 3.7 наведені результати розв'язання маршрутної задачі з балансуванням навантаження, коли керуючий параметр *n* приймав, для прикладу, значення 0,1 та 0,01.

Таблиця 3.7

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.12)

Канал зв'язку	$p_{i,j}$	Рішення з безпечної маршрутизації (*n*=0,1)		Рішення з безпечної маршрутизації (*n*=0,01)	
		$\lambda^1_{i,j}$	$\alpha_{i,j}$	$\lambda^1_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	0,1	350	0,5	350	0,5
$E_{2,4}$	0,5	29,1997	0,0487	3,4733	0,0058
$E_{1,3}$	0,4	0	0	0	0
$E_{3,4}$	0,2	320,8003	0,5347	346,5267	0,5775
$E_{2,3}$	0,2	320,8003	0,4010	346,5267	0,4332

Модель блокування (3.12) зі зменшенням n забезпечує більш високу чутливість імовірностей компрометації КЗ. Як показано в табл. 3.7, це позначалося на зниженні завантаженості найбільш небезпечних каналів, наприклад, каналу $E_{2,4}$. У табл. 3.8 наведені результати порівняльного аналізу досліджуваних рішень: ТЕ-моделі та SecTE (3.12) за умови різних значень керуючого параметра n, які підтвердили попередні висновки щодо області застосування зазначеної моделі блокування КЗ та впливу на цей процес значень керуючих змінних. Загалом у процесі зменшення значень n від 0,1 до 0,01 зниження ймовірності компрометації пакетів у ТКМ відбувалося в діапазоні від 17,65 % до 19,4 %.

Таблиця 3.8

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.12)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
0,01	0,5775	0,5847	0,4253	19,4 %
0,02	0,572	0,5756	0,4264	19,18 %
0,03	0,5668	0,5691	0,4276	18,98 %
0,04	0,5617	0,5634	0,4287	18,75 %
0,05	0,5568	0,5581	0,4297	18,55 %
0,06	0,552	0,5532	0,4308	18,36 %
0,07	0,5475	0,5484	0,4317	18,17 %
0,08	0,543	0,5439	0,4327	17,99 %
0,09	0,5388	0,5395	0,4336	17,82 %
0,1	0,5347	0,5353	0,4345	17,65 %

На рис. 3.8, відповідно до змісту табл. 3.8, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.12). Завдяки зміні параметра n можна зменшити

ймовірність компрометації пакетів (від 17,65 % до 19,4 %) з підвищенням (від 68 % до 81,5 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.8).

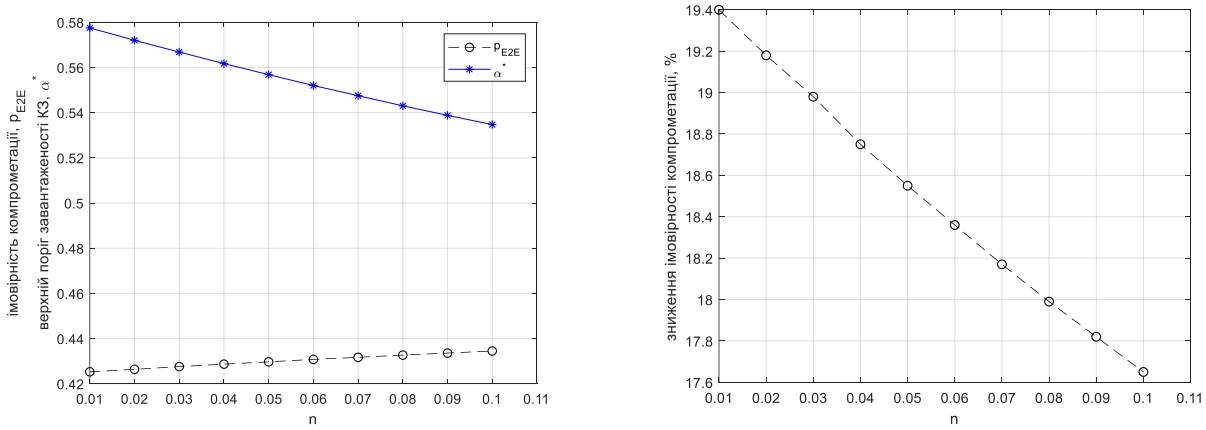


Рис. 3.8. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.12)

У третьому випадку за модель блокування КЗ обрана експоненціальна залежність (3.11). У табл. 3.9 наведені результати порівняльного аналізу досліджуваних рішень: ТЕ-моделі та SecTE (3.11). Загалом у процесі збільшення значень параметра *n* від 1 до 3,5 значення ймовірності компрометації пакетів у ТКМ покращувалися від 4,76 % до 13,45 %.

Таблиця 3.9

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.11)

n	α^*	α	p_{E2E}	Покращення p_{E2E}
1	0,3703	0,4093	0,5025	4,76 %
1,5	0,4139	0,4808	0,4896	7,21 %
2	0,46	0,56	0,4763	9,73 %
2,5	0,5	0,6532	0,4644	11,98 %
3	0,5	0,7557	0,4604	12,74 %
3,5	0,5	0,8702	0,4567	13,45 %
4	0,5	0,9977	0,4317	18,17 %

На рис. 3.9, відповідно до змісту табл. 3.9, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.11). Завдяки зміні параметра n можна зменшити (від 4,76 % до 13,45 %) імовірність компрометації пакетів, але з підвищенням (від 16,5 % до 57 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.9).

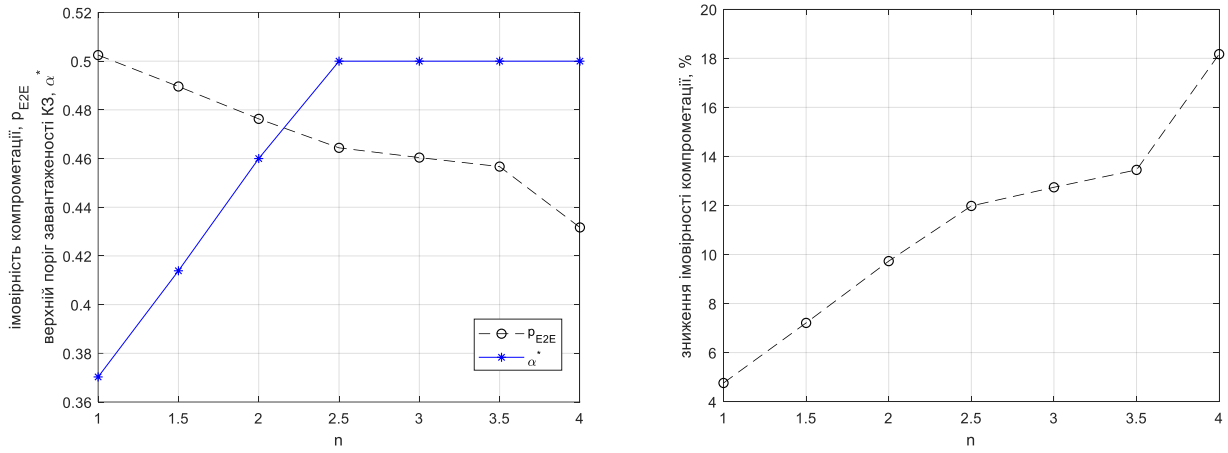


Рис. 3.9. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.11)

Для дослідження другого сценарію компрометації каналів зв'язку (табл. 3.3 та 3.4) за модель блокування КЗ, наприклад, була обрана залежність (3.12), де $n=1$. Зі зміною сценарію компрометації використання ТЕ-моделі (2.2), (2.3), (3.3)–(3.5) забезпечило значення p_{E2E} на рівні 0,7933. У табл. 3.10 наведені результати порівняльного аналізу досліджуваних рішень: ТЕ-моделі та SecTE (3.12). Зростання значень керуючих параметрів r та b у виразі (3.12) забезпечувало більш інтенсивне врахування ймовірностей компрометації КЗ у процесі балансування навантаження в ТКМ.

Таблиця 3.10

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.12)

r	b	α^*	α	p_{E2E}	Зниження p_{E2E}
14	7	0,5444	0,6787	0,7116	10,2954 %
20	10	0,5717	0,649	0,7077	10,7897 %
30	15	0,5818	0,6108	0,7062	10,9742 %
40	20	0,5831	0,5938	0,706	10,998 %

Для цього ж другого сценарію компрометації в табл. 3.11 наведені результати порівняльного аналізу досліджуваних рішень: TE-моделі та SecTE (3.13), де $\theta = 0$. Із зростанням n від 0 до 0,15 забезпечувалося більш інтенсивне врахування ймовірностей компрометації КЗ, а покращення ймовірності компрометації пакетів у ТКМ коливалося від 6,1413 % до 9,0311 % (табл. 3.11).

Таблиця 3.11

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.13)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
0	0,4537	0,6481	0,7446	6,1413 %
0,05	0,4945	0,6615	0,7313	7,8123 %
0,1	0,5	0,6754	0,7259	8,4895 %
0,15	0,5	0,6899	0,7216	9,0311 %

На рис. 3.10, відповідно до змісту табл. 3.11, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.13). Завдяки зміні параметра n можна зменшити (від 6,1413 % до 9,0311 %) імовірність компрометації пакетів, але з

підвищенням (від 42,6 % до 57 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.10).

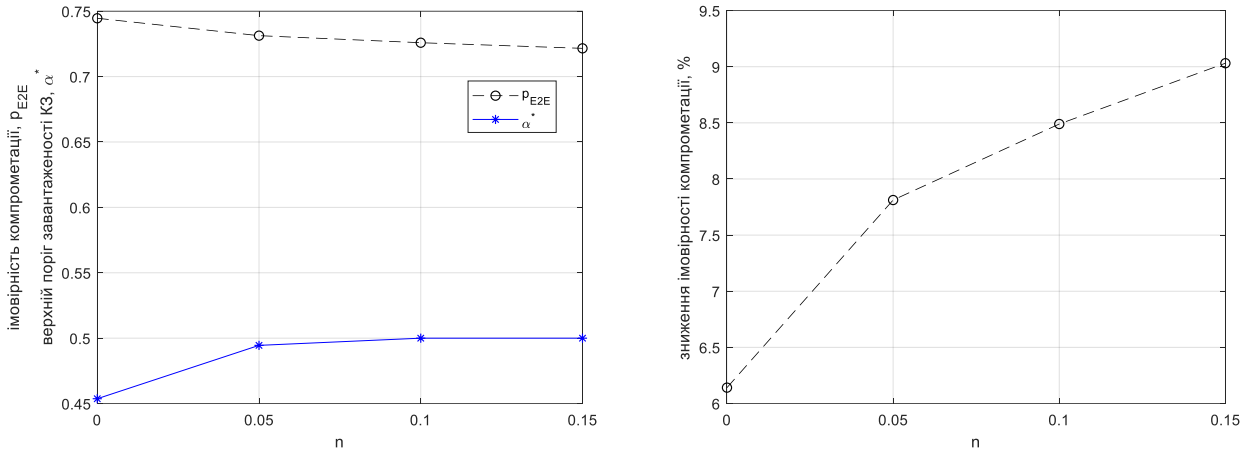


Рис. 3.10. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.13)

Для дослідження третього сценарію компрометації каналів зв'язку (табл. 3.3 та 3.4) за модель блокування КЗ, наприклад, була обрана залежність (3.10), де $n \geq 1$. Зі зміною сценарію компрометації використання ТЕ-моделі (2.2), (2.3), (3.3)–(3.5) забезпечило значення p_{E2E} на рівні 0,9491. У табл. 3.12 наведені результати порівняльного аналізу досліджуваних рішень: ТЕ-моделі та SecTE (3.10).

Таблиця 3.12

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.10)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
1	0,5	0,8560	0,9107	4,0422 %
2	0,5	0,7028	0,9114	3,9664 %
3	0,4838	0,5529	0,9148	3,6144 %
5	0,4243	0,438	0,9245	2,5957 %

Водночас зі зменшенням значень n від 5 до 1,5 виграш за ймовірністю компрометації пакетів у ТКМ змінювався від 2,5957 % до 4,0422 % (табл. 3.12). Такий досить незначний виграш щодо значень p_{E2E} пояснювався відсутністю необхідного канального резерву для балансування навантаження з відносно невисоким рівнем компрометації.

На рис. 3.11, відповідно до змісту табл. 3.12, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n у моделі (3.10). Завдяки зміні параметра n можна зменшити (від 2,5957 % до 4,0422 %) імовірність компрометації пакетів, але з підвищенням (від 33,3 % до 57 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.11).

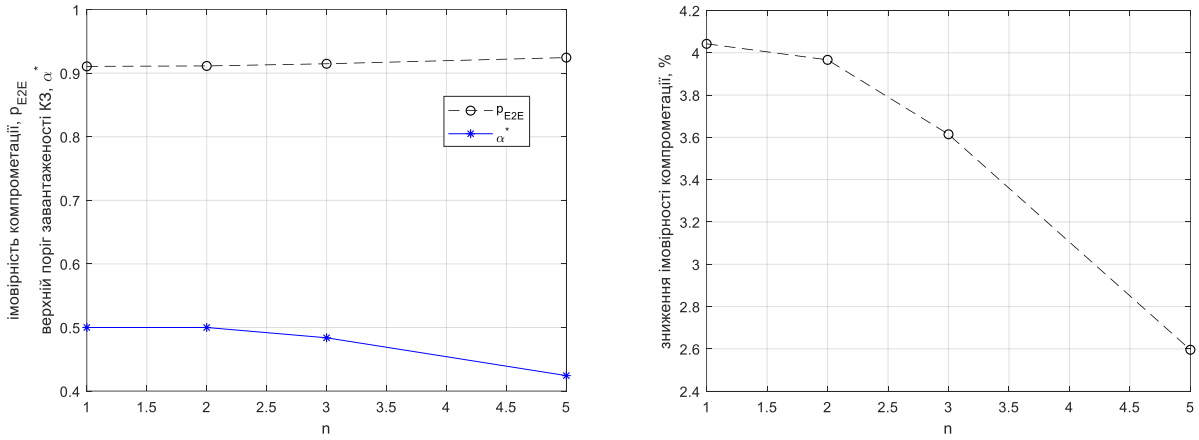


Рис. 3.11. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.10)

Подібна ситуація зі зниженням імовірності компрометації пакетів у ТКМ (від 2,8374 % до 3,7596 %) було характерна в процесі використанні моделі блокування КЗ (3.13), коли $\theta = \pi$, а значення керуючого параметра n варіювалось від 1,5 до 0,08.

У реалізації в ТКМ четвертого сценарію компрометації КЗ (табл. 3.3 та 3.4) відбулися зміни щодо значень p_{E2E} до рівня 0,8402, яке забезпечувалося використанням ТЕ-моделі (2.2), (2.3), (3.3)–(3.5). Якщо обрати за модель блокування КЗ, наприклад, залежність (3.13), де $\theta = 0$, то в табл. 3.13 можна

побачити результати порівняльного аналізу рішень, отриманих за допомогою ТЕ-моделі та SecTE. Отже, у процесі зростання n виграш щодо ймовірності компрометації пакетів у ТКМ змінювався від 21,6836 % до 25,4938 %.

Таблиця 3.13

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.13), коли $\theta = 0$

n	α^*	α	p_{E2E}	Зниження p_{E2E}
0	0,5104	0,7292	0,658	21,6836 %
0,05	0,533	0,713	0,6469	23,0101 %
0,1	0,5546	0,6975	0,6362	24,2789 %
0,15	0,5753	0,6827	0,626	25,4938 %

На рис. 3.12, відповідно до змісту табл. 3.13, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.13).

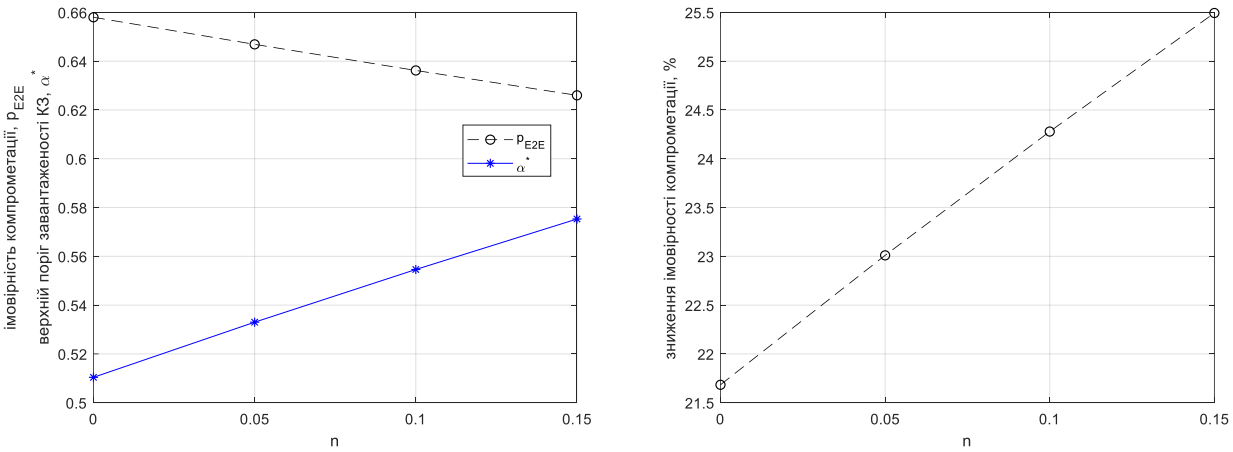


Рис. 3.12. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.13)

Завдяки зміні параметра *n* можна зменшити (від 21,6836 % до 25,4938 %) імовірність компрометації пакетів, але з підвищенням (від 60,4 % до 80,8 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.12).

У випадку використання моделі блокування КЗ (3.13), коли $\theta = \pi$, покращення ймовірності компрометації пакетів у ТКМ становило від 17,3165 % до 21,6836 % (табл. 3.14).

Таблиця 3.14

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.13), коли $\theta = \pi$

n	α^*	α	p_{E2E}	Зниження p_{E2E}
0	0,5104	0,7292	0,658	21,6836 %
0,05	0,5	0,7461	0,6697	20,2956 %
0,1	0,5	0,7639	0,6819	18,8415 %
0,15	0,5	0,7825	0,6947	17,3165 %

На рис. 3.13, відповідно до змісту табл. 3.14, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.13). Завдяки зміні параметра *n* можна зменшити (від 17,3165 % до 21,6836 %) імовірність компрометації пакетів, але з підвищенням (від 57 % до 60,4 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.13).

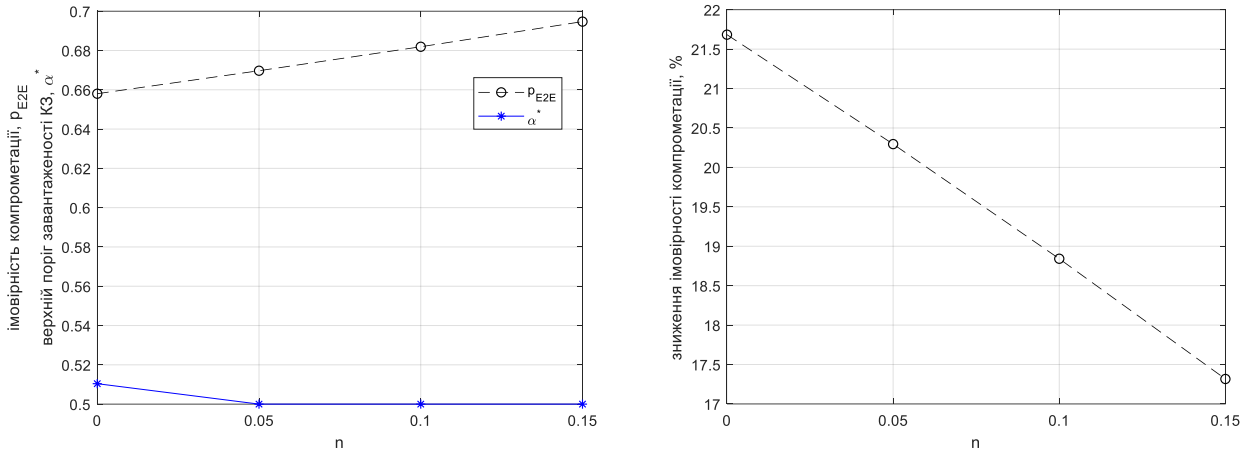


Рис. 3.13. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.13)

3.3.2. Дослідження процесів безпечного балансування навантаження в ТКМ на другій мережній структурі

Другий варіант структури досліджуваної мережі зображено на рис. 3.14. Інтенсивність вхідного потоку, який передавався від першого до дванадцятого маршрутизатора, становила 400 1/с.

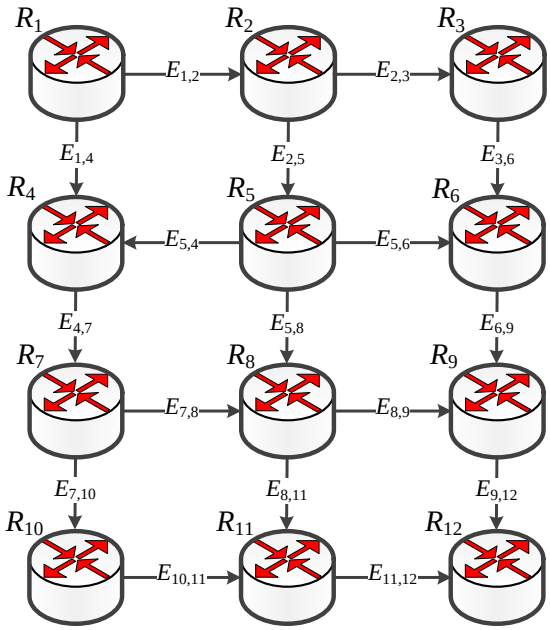


Рис. 3.14. Варіант другої досліджуваної структури ТКМ

У табл. 3.15 наведені пропускні здатності каналів зв’язку та варіанти ймовірностей їхньої компрометації відповідно до обраних стратегій (табл. 3.1).

Таблиця 3.15

Характеристики каналів зв’язку ТКМ

Канал зв’язку	Пропускна здатність	Імовірності компрометації каналів зв’язку	
		Перший сценарій	Четвертий сценарій
$E_{1,2}$	800	0,1	0,1
$E_{2,3}$	500	0,3	0,4
$E_{1,3}$	850	0,1	0,2
$E_{2,4}$	900	0,1	0,1
$E_{3,6}$	700	0,2	0,2
$E_{5,4}$	800	0,5	0,4
$E_{5,6}$	500	0,4	0,8
$E_{4,7}$	700	0,2	0,2
$E_{5,8}$	500	0,1	0,5
$E_{6,9}$	800	0,3	0,7
$E_{7,8}$	400	0,1	0,1
$E_{8,9}$	500	0,3	0,3
$E_{7,10}$	500	0,4	0,9
$E_{8,11}$	900	0,2	0,6
$E_{9,12}$	800	0,1	0,2
$E_{10,11}$	700	0,4	0,4
$E_{11,12}$	900	0,1	0,1

Відповідно до інформації про структуру ТКМ (рис. 3.14) та характеристики її КЗ (табл. 3.15), у табл. 3.16 наведені дані про доступні маршрути між R_1 та R_{12}, а також імовірності їхньої компрометації.

Таблиця 3.16

Імовірності компрометації маршрутів у ТКМ

Маршрут		Перший сценарій	Четвертий сценарій
1	$R_1 \to R_2 \to R_3 \to R_6 \to R_9 \to R_{12}$	0,68248	0,89632
2	$R_1 \to R_2 \to R_5 \to R_6 \to R_9 \to R_{12}$	0,69382	0,96112
3	$R_1 \to R_2 \to R_5 \to R_8 \to R_9 \to R_{12}$	0,54073	0,7732
4	$R_1 \to R_2 \to R_5 \to R_8 \to R_{11} \to R_{12}$	0,47512	0,8542
5	$R_1 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{12}$	0,76672	0,96544
6	$R_1 \to R_2 \to R_5 \to R_4 \to R_7 \to R_{10} \to R_{11} \to R_{12}$	0,895024	0,979
7	$R_1 \to R_2 \to R_5 \to R_4 \to R_7 \to R_8 \to R_9 \to R_{12}$	0,816292	0,804
8	$R_1 \to R_2 \to R_5 \to R_4 \to R_7 \to R_8 \to R_{11} \to R_{12}$	0,790048	0,874
9	$R_1 \to R_4 \to R_7 \to R_8 \to R_9 \to R_{12}$	0,59176	0,67744
10	$R_1 \to R_4 \to R_7 \to R_8 \to R_{11} \to R_{12}$	0,53344	0,79264

Для дослідження першого сценарію компрометації каналів зв’язку (табл. 3.15 та 3.16) за модель блокування КЗ була обрана залежність (3.9), де $n \geq 1$. Тоді в табл. 3.17 показано результати розрахунків, які отримані з використанням класичної ТЕ-моделі (2.2), (2.3), (3.3)–(3.5) та запропонованої моделі SecTE (2.2), (2.3), (3.4)–(3.6) для $n = 4$.

Реалізація ТЕ-моделі забезпечила балансування навантаження таким чином (табл. 3.17): по третині потоку передавалися першим та п’ятим шляхами, 0,2 від потоку передавалася другим маршрутом, а решта, 0,1333 потоку, – за допомогою десятого шляху.

Тому, відповідно до виразу (3.14) та табл. 3.16, значення p_{E2E} відповідало рівню 0,693, а верхній поріг завантаженості каналів зв’язку становив 0,2667 (табл. 3.17).

Таблиця 3.17

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.9)

Канал зв'язку	$p_{i,j}$	Traffic Engineering рішення		Рішення з безпечної маршрутизації ($n=4$)	
		$\lambda_{i,j}^{1}$	$\alpha_{i,j}$	$\lambda_{i,j}^{1}$	$\alpha_{i,j}$
$E_{1,2}$	0,1	213,33	0,2667	277,87	0,3473
$E_{2,3}$	0,3	133,33	0,2667	65,04	0,13
$E_{1,3}$	0,1	186,67	0,2196	122,13	0,1437
$E_{2,4}$	0,1	80	0,0889	212,83	0,2365
$E_{3,6}$	0,2	133,33	0,1905	65,04	0,0929
$E_{5,4}$	0,5	0	0	0	0
$E_{5,6}$	0,4	80	0,16	35,11	0,0702
$E_{4,7}$	0,2	186,67	0,2667	122,13	0,1745
$E_{5,8}$	0,1	0	0	177,72	0,3554
$E_{6,9}$	0,3	213,33	0,2667	100,14	0,1252
$E_{7,8}$	0,1	53,33	0,1333	87,03	0,2176
$E_{8,9}$	0,3	0	0	65,04	0,1301
$E_{7,10}$	0,4	133,33	0,2667	35,11	0,0702
$E_{8,11}$	0,2	53,33	0,0593	199,71	0,2219
$E_{9,12}$	0,1	213,33	0,2667	165,18	0,2065
$E_{10,11}$	0,4	133,33	0,1905	35,11	0,0502
$E_{11,12}$	0,1	186,67	0,2074	234,82	0,2609

Використання SecTE-моделі реалізувало балансування навантаження шістьма шляхами (табл. 3.17). Першим шляхом передавалося 0,1626 потоку пакетів, другим – 0,0878, третім – 0,1626, четвертим – 0,2817, п'ятим – 0,0878, десятим – 0,2176. Отже, значення p_{E2E} дорівнювало 0,577. Зниження ймовірності компрометації пакетів у ТКМ забезпечувалося розвантаженням

найбільш небезпечних КЗ, наприклад, з $p_{i,j} \geq 0,4$. Загалом застосування моделі SecTE (3.9) дозволило знизити ймовірність компрометації пакетів у ТКМ (3.14) від 9,5493 % до 20,7484 % порівняно з рішенням на онові ТЕ-моделі (табл. 3.18). Водночас зі збільшенням n маршрутні рішення ставали більш чутливими до параметрів мережної безпеки.

Таблиця 3.18

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.9)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
1,5	0,2885	0,3379	0,6268	9,5493 %
2	0,2956	0,365	0,6157	11,1537 %
2,5	0,3027	0,3939	0,6012	13,2518 %
3	0,3097	0,4248	0,5875	15,2257 %
3,5	0,3193	0,4617	0,585	15,578 %
4	0,3554	0,5418	0,577	16,742 %
4,5	0,3946	0,6339	0,5702	17,7261 %
5	0,4368	0,7397	0,5633	18,7215 %
5,5	0,4823	0,8609	0,5563	19,7287 %
6	0,5311	0,9994	0,5492	20,7484 %

На рис. 3.15, відповідно до змісту табл. 3.18, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.9). Завдяки зміні параметра n можна зменшити (від 9,5493 % до 20,7484 %) імовірність компрометації пакетів, але з підвищенням (від 8,2 % до 99 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.15).

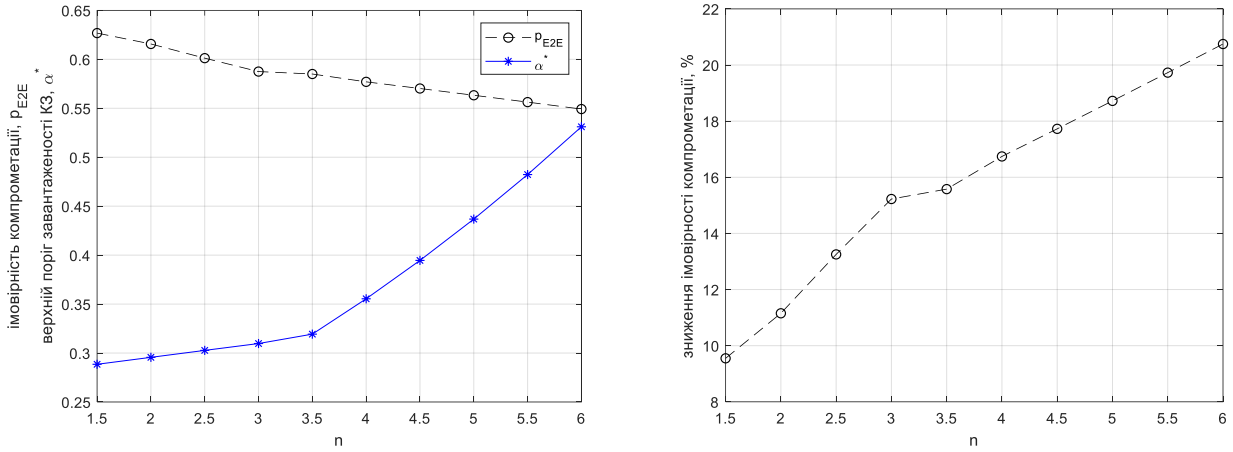


Рис. 3.15. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра *n* в моделі (3.9)

Для дослідження четвертого сценарію компрометації каналів зв'язку (табл. 3.15 та 3.16) за модель блокування КЗ була обрана залежність (3.13), коли $\theta = 0$. Тоді у використанні ТЕ-моделі балансування значення p_{E2E} становило 0,9185.

У табл. 3.19 наведені результати порівняльного аналізу рішень, отриманих за допомогою SecTE для значень *n* у (3.16) на рівні 0,05 та 0,15.

Загалом застосування моделі SecTE з (3.13) дозволило знизити ймовірність компрометації пакетів у ТКМ (3.14) від 11,629 % до 15,1773 % (табл. 3.20). До того ж зі збільшенням *n* маршрутні рішення ставали більш чутливими до параметрів мережної безпеки.

Як і в попередньому випадку, зниження ймовірності компрометації пакетів у ТКМ забезпечувалося розвантаженням найбільш небезпечних КЗ, наприклад, з $p_{i,j} \geq 0,4$ (табл. 3.19).

Таблиця 3.19

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.13)

Канал зв'язку	$p_{i,j}$	Рішення з безпечної маршрутизації (n=0,05)		Рішення з безпечної маршрутизації (n=0,15)	
		$\lambda^1_{i,j}$	$\alpha_{i,j}$	$\lambda^1_{i,j}$	$\alpha_{i,j}$
$E_{1,2}$	0,1	210,45	0,2631	193,49	0,2419
$E_{2,3}$	0,4	94,04	0,1881	64,79	0,1296
$E_{1,3}$	0,2	189,55	0,223	206,51	0,243
$E_{2,4}$	0,1	116,41	0,1293	128,69	0,143
$E_{3,6}$	0,2	94,04	0,1343	64,79	0,0926
$E_{5,4}$	0,4	0	0	0	0
$E_{5,6}$	0,8	0	0	0	0
$E_{4,7}$	0,2	189,55	0,2708	206,51	0,295
$E_{5,8}$	0,5	116,41	0,2328	128,69	0,2574
$E_{6,9}$	0,7	94,04	0,1175	64,79	0,081
$E_{7,8}$	0,1	173,11	0,4328	203,47	0,5087
$E_{8,9}$	0,3	174,05	0,3481	216,88	0,4338
$E_{7,10}$	0,9	16,44	0,0329	3,05	0,0061
$E_{8,11}$	0,6	115,47	0,1283	115,27	0,1281
$E_{9,12}$	0,2	268,09	0,3351	281,68	0,3521
$E_{10,11}$	0,4	16,44	0,0235	3,05	0,0044
$E_{11,12}$	0,1	131,91	0,1466	118,32	0,1315

На рис. 3.16, відповідно до змісту табл. 3.20, показана динаміка зміни показників завантаженості КЗ та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.13).

Таблиця 3.20

Результати порівняльного аналізу отриманих рішень щодо безпечного балансування навантаження з використанням моделі блокування КЗ (3.13)

n	α^*	α	p_{E2E}	Зниження p_{E2E}
0	0,4	0,4444	0,8117	11,629 %
0,05	0,4328	0,4656	0,8019	12,6989 %
0,08	0,454	0,4794	0,7955	13,3913 %
0,1	0,4688	0,489	0,791	13,876 %
0,12	0,4843	0,499	0,7864	14,3806 %
0,15	0,5087	0,5148	0,7791	15,1773 %

Завдяки зміні параметра n можна зменшити (від 11,629 % до 15,1773 %) імовірність компрометації пакетів, але з підвищенням (від 50 % до 90,7 %) верхнього порогу завантаженості каналів зв'язку ТКМ (рис. 3.16).

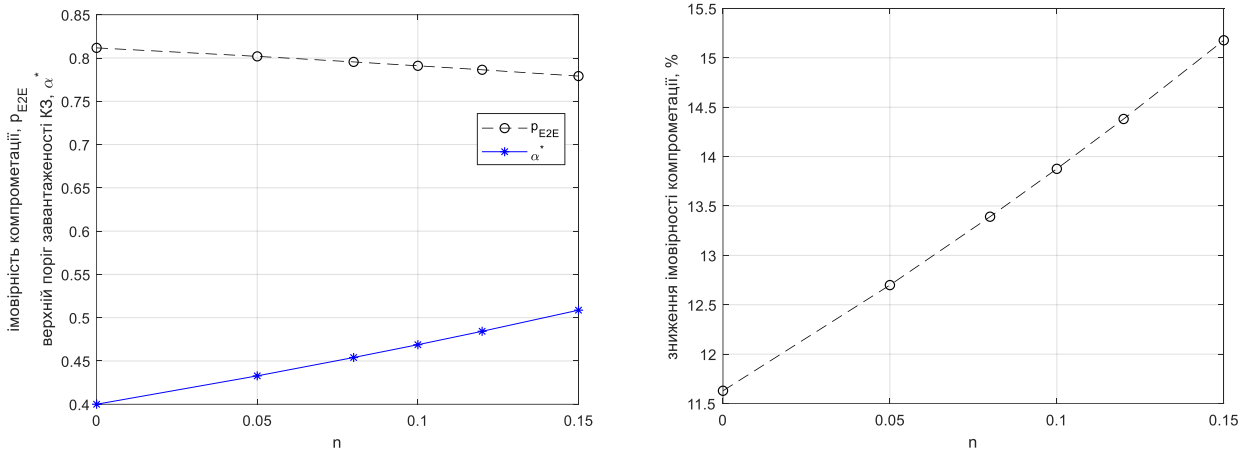


Рис. 3.16. Динаміка зміни показників завантаженості та мережної безпеки в ТКМ залежно від значень параметра n в моделі (3.13)

3.4. Висновки до третього розділу

1. Перспективними напрямами розвитку та вдосконалення рішень щодо забезпечення мережної безпеки є вдосконалення засобів управління трафіком та маршрутизації. Новітні рішення щодо управління трафіком та маршрутизації мають враховувати не тільки параметри мережної продуктивності (пропускну здатність, затримання та рівень втрат пакетів), але й параметри мережної безпеки, що характеризують ефективність роботи задіяних у мережі систем виявлення вторгнень та аналізу вразливостей і ризиків.

2. У цьому розділі вдосконалено потокову модель безпечної маршрутизації з балансуванням навантаження відповідно до концепції Traffic Engineering на основі врахування параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах, яка представлена виразами (2.1) або (2.2), (2.3), (3.4)–(3.6). У межах цієї моделі вирішення технологічної задачі безпечної маршрутизації з балансуванням навантаження в ТКМ було зведено до розв’язання оптимізаційної задачі з критерієм оптимальності (3.5) та обмеженнями – (2.1) або (2.2), (2.3), (3.4) та (3.6). У реалізації одношляхової маршрутизації (2.1) сформульована оптимізаційна задача належить до класу задач змішаного лінійного програмування (MILP), а у використанні багатошляхової маршрутизації (2.2) – до класу задач лінійного програмування (LP).

3. Новизною запропонованої моделі можна вважати:

- по-перше, модифікацію умов балансування навантаження в ТКМ (3.6), які орієнтують на мінімізацію верхнього динамічно керованого порогу завантаженості каналів зв’язку (3.5), зваженого щодо ймовірності їхньої компрометації;

- по-друге, використання множини моделей блокування каналів зв’язку (3.9)–(3.13), за допомогою яких можна регулювати вплив імовірності компрометації каналів $p_{i,j}$ на поріг їхньої завантаженості $\alpha_{i,j}$ та ТКМ загалом.

4. Результати дослідження процесів безпечної маршрутизації з балансуванням навантаження в ТКМ підтвердили її ефективність щодо врахування стану ТКМ: її топології, характеристик потоків, пропускної здатності та завантаженості каналів зв’язку, а також імовірностей їхньої компрометації. Це дозволило зорієнтувати отримані маршрутні рішення на зменшення завантаженості каналів зв’язку, що мають високу ймовірність компрометації, шляхом перерозподілу трафіку на більш безпечні канали. Зазвичай інтенсивніше завантажувалися ті канали, які мали високу пропускну здатність і низьку ймовірність компрометації.

5. У процесі дослідження запропонованих моделей блокування каналів зв’язку (3.9)–(3.13) установлено характер впливу їхніх керуючих параметрів на чутливість процесів балансування навантаження параметрів мережної безпеки, якими були ймовірності компрометації каналів зв’язку. Зниження ймовірності компрометації пакетів, що передавалися мережею, забезпечувалося, як правило, шляхом підвищення порогу завантаженості каналів зв’язку ТКМ, що негативно позначалося на рівні QoS. Тому в кожному конкретному випадку необхідно враховувати стан мережі, прогнозовані сценарії компрометації її елементів та вимоги потоків пакетів до рівня якості обслуговування та мережної безпеки, щоб обрати найбільш доцільну модель блокування каналів із налаштуванням її керуючих параметрів.

РОЗДІЛ 4
ПОТОКОВІ МОДЕЛІ ШВИДКОЇ ПЕРЕМАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ ТА ОБМЕЖЕННЯМ ТРАФІКУ НА ГРАНИЦІ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Розглянуті в попередніх розділах моделі маршрутизації належать до проактивних рішень щодо забезпечення якості обслуговування та мережної безпеки. Проте сучасні ТКМ мають також підтримувати технологічні рішення, орієнтовані на використання реактивного підходу, коли мережа повинна оперативно реагувати на ймовірні відмови комутаційного та серверного обладнання або його програмного забезпечення. У зв’язку із цим четвертий розділ присвячений розробленню та подальшому вдосконаленню математичних моделей швидкої перемаршрутизації та безпечної швидкої перемаршрутизації потоків пакетів у програмно-конфігурованих телекомунікаційних мережах у напрямі забезпечення узгодженого вирішення завдань щодо відмовостійкої маршрутизації, балансування навантаження, обмеження трафіку та забезпечення мережної безпеки.

Запропоновані рішення орієнтують на забезпечення захисту як структурних елементів ТКМ – її вузлів та каналів, так і пропускної здатності мережі. До того ж виникаюча надмірність у застосуванні мережних ресурсів під час підтримки базових схем захисту елементів мережі компенсується забезпеченням збалансованого використання доступного мережного ресурсу на принципах Traffic Engineering та застосуванням функції обмеження навантаження на мережу, а саме, інструментарію Traffic Policing (TP). Крім того, у розділі запропоновано математичне рішення задачі безпечної швидкої перемаршрутизації, коли в умовах балансування навантаження та обмеження трафіку на границі ТКМ враховуються не тільки вимоги щодо рівня якості обслуговування та пріоритетів потоків пакетів, але й показників мережної безпеки каналів зв’язку мережі.

Матеріали розділу опубліковані в роботах [33, 34, 40–43, 45].

4.1. Розроблення та дослідження математичної моделі швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в програмно-конфігурованих ТКМ

4.1.1. Потокова модель швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в програмно-конфігурованих телекомунікаційних мережах

Ґрунтуючись на рішеннях, запропонованих у роботах [19, 33, 34], результатом розв'язання задачі швидкої перемаршрутизації є обчислення двох типів маршрутних змінних $x_{i,j}^k$ та $\bar{x}_{i,j}^k$, що характеризують частку інтенсивності k-го потоку пакетів, які передаються в каналі зв'язку $E_{i,j} \in E$, що міститься в складі основного або резервного шляхів відповідно. У випадку, коли в ТКМ використовується багатошляхова стратегія маршрутизації, на маршрутні змінні цих двох типів накладаються обмеження вигляду [19, 33, 34]:

$$0 \le x_{i,j}^k \le 1 \quad \text{та} \quad 0 \le \bar{x}_{i,j}^k \le 1. \tag{4.1}$$

Також на маршрутні змінні накладаються обмеження, представлені умовами збереження потоку [33, 34], що порівняно з виразами (2.3) модифікуються в напрямі додаткового врахування під час опису процесів маршрутизації такою функцією обмеження трафіку (ТР). Для основного шляху вони мають вигляд:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 0;\ k \in K,\ R_i \ne s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 1-\beta^k;\ k \in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = \beta^k - 1;\ k \in K,\ R_i = d_k; \end{cases} \tag{4.2}$$

де β^k є часткою інтенсивності k-го потоку, який у реалізації політики ТР отримує відмову в обслуговуванні (обмежується) на границі мережі під час використання пакетами основного шляху.

На маршрутні змінні резервного шляху також накладаються умови, подібні до (4.2):

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^k = 0;\ k \in K,\ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^k = 1 - \bar{\beta}^k;\ k \in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^k = \bar{\beta}^k - 1;\ k \in K,\ R_i = d_k; \end{cases} \quad (4.3)$$

де $\bar{\beta}^k$ є часткою інтенсивності k-го потоку, який обмежується на границі мережі під час використання пакетами вже резервного шляху.

У процесі багатошляхової швидкої перемаршрутизації в разі реалізації схеми захисту каналу $E_{i,j} \in E$ має місце таке обмеження [33, 34, 98, 99]:

$$0 \le \bar{x}_{i,j}^k \le \delta_{i,j}^k, \quad (4.4)$$

де

$$\delta_{i,j}^k = \begin{cases} 0, \text{ у разі захисту каналу зв'язку } E_{i,j}; \\ 1, \text{ в іншому випадку.} \end{cases} \quad (4.5)$$

Виконання лінійних умов (4.4) і (4.5) гарантує, що канал $E_{i,j} \in E$, який захищається, у разі багатошляхової маршрутизації не буде використовуватися резервним маршрутом.

Так само у разі реалізації схеми захисту вузла $R_i \in R$ умови (4.4) і (4.5) узагальнюються на випадок захисту вже множини каналів зв’язку, інцидентних

вузлу, який захищається [34, 35, 98, 99]. Тоді під час використання багатошляхової стратегії мають виконуватися такі обмеження:

$$0 \le \bar{x}_{i,j}^{k} \le \delta_{i,j}^{k},\ R_j \in R_i^*,\ j = \overline{1,m}, \tag{4.6}$$

де значення $\delta_{i,j}^{k}$ визначаються відповідно до (4.5);

R_i^* – множина маршрутизаторів, які є суміжними (сусідніми) до вузла R_i .

Варто зауважити, що виконання зазначених вище умов (4.5) і (4.6) гарантує захист вузла $R_i \in R$, забороняючи використання резервним маршрутом усіх каналів, які містить цей вузол. Більш того, відповідно до умов (4.4), оскільки захисту підлягають лише транзитні маршрутизатори, заборона на використання вихідних каналів зв'язку запобігає включенню до резервного шляху і вхідних каналів. Так реалізується захист конкретного вузла R_i мережі.

Умови захисту пропускної здатності ТКМ фактично відповідають за своїм фізичним змістом умовам запобігання перевантаженню каналів зв'язку в разі реалізації швидкої перемаршрутизації:

$$\sum_{k \in K} \lambda^k \cdot \max\left[x_{i,j}^{k}, \bar{x}_{i,j}^{k}\right] \le \varphi_{i,j},\ E_{i,j} \in E. \tag{4.7}$$

Нелінійні умови (4.7) охоплюють найбільш загальний (асиметричний) випадок, коли перемикатися на резервні маршрути можуть не всі потоки одночасно, а лише деякі з них, оскільки для різних потоків можуть резервуватися різні елементи (вузли або канали) мережі. Коли ж у разі відмов елементів мережі всі потоки одночасно переходять на використання резервних маршрутів (симетричний випадок), то мають місце такі умови захисту пропускної здатності ТКМ:

$$\sum_{k\in K} \lambda^k \cdot x_{i,j}^k \le \varphi_{i,j} \text{ та } \sum_{k\in K} \lambda^k \cdot \bar{x}_{i,j}^k \le \varphi_{i,j}. \quad (4.8)$$

Як показано в роботах [32–34], в умовах реалізації багатошляхової маршрутизації для запобігання перевантаження та забезпечення балансування навантаження в мережі на принципах ТЕ нелінійні умови (4.7) заміняються лінійними аналогами:

$$\sum_{k\in K} \lambda^k \cdot u_{i,j}^k \le \alpha \cdot \varphi_{i,j},\ E_{i,j} \in E \quad (4.9)$$

у разі

$$x_{i,j}^k \le u_{i,j}^k \text{ та } \bar{x}_{i,j}^k \le u_{i,j}^k, \quad (4.10)$$

де $u_{i,j}^k$ – множина додаткових керуючих змінних, що кількісно характеризують верхній поріг значень відповідних маршрутних змінних $x_{i,j}^k$ та $\bar{x}_{i,j}^k$, на які накладаються обмеження вигляду

$$0 \le u_{i,j}^k \le 1. \quad (4.11)$$

Крім того, у модель вводиться ще одна керуюча змінна α, яка кількісно визначає верхній поріг завантаженості каналів зв’язку мережі, відповідаючи таким умовам:

$$0 \le \alpha \le \alpha_{TH}, \quad (4.12)$$

де α_{TH} – граничне значення верхнього порогу завантаженості каналів зв’язку мережі, величина якої попередньо задається на основі аналізу вимог щодо рівня якості обслуговування в мережі. Це обумовлено тим, що всі основні показники

якості обслуговування – продуктивність мережі, середня міжкінцева затримка та ймовірність втрат пакетів – є функцією від цього параметра. Чим вищий рівень QoS-вимог у мережі, тим нижчим обирається значення порогу α_{TH}.

Введення умов (4.12) є новизною запропонованого підходу порівняно з моделями, запропонованими в роботах [10, 11, 32]. До того ж збереження лінійності моделі (4.1)-(4.12) та орієнтація на забезпечення заданого рівня QoS є основними перевагами запропонованого рішення.

Важливу роль у структурі моделі швидкої перемаршрутизації відіграють критерії оптимальності кінцевих рішень. У цьому розділі залежно від постановки маршрутного завдання пропонується система критеріїв оптимальності, які ґрунтуються на мінімізації таких цільових функцій:

$$J = \sum_{k \in K} w_k \cdot \beta^k + \sum_{k \in K} \bar{w}_k \cdot \bar{\beta}^k + c \cdot \alpha \to \min, \tag{4.13}$$

$$J = \sum_{k \in K} w_k \cdot (\beta^k)^2 + \sum_{k \in K} \bar{w}_k \cdot (\bar{\beta}^k)^2 + c \cdot \alpha \to \min. \tag{4.14}$$

У виразах (4.13) та (4.14) вагові коефіцієнти мають відповідати таким умовам:

$$w_k > \bar{w}_k > w_p > \bar{w}_p > \ldots > c, \tag{4.15}$$

де пріоритет пакетів k-го потоку (PR^k) перевищує пріоритет пакетів p-го потоку (PR^p).

Отже, чим вищий пріоритет пакетів потоку, тим вагові коефіцієнти мають бути більшими. Наприклад, в IP-мережі у разі використання трьох біт у заголовку пакета для кодування пріоритету його значення перебуває в діапазоні від 0 до 7, а за умови застосування політик DSCP (Differentiated Services Code

Point) пріоритети змінюються від 0 до 63. Тоді згідно з (4.14) пропонується використовувати в критеріях (4.13) та (4.14) такі значення вагових коефіцієнтів:

$$w_k = PR^k + 1,\ \bar{w}_k = PR^k + 0{,}5,\ c = 0{,}25. \qquad (4.16)$$

Критерій оптимальності (4.13) фокусується на мінімізації умовних витрат, пов'язаних із узгодженим вирішенням завдань швидкої перемаршрутизації (FRR), балансування навантаження (TE) та диференційованого обмеження трафіку (TP). У цьому випадку перший член визначає умовну вартість відмов в обслуговуванні пакетів потоків, що передаються за допомогою основних шляхів; другий – умовну вартість відмов в обслуговуванні (обмеженні) потоків, що передаються резервними шляхами; третій член у (4.13) описує зважений верхній поріг завантаженості каналів зв'язку мережі.

Введена ієрархія значень вагових коефіцієнтів (4.15), (4.16) обґрунтована тим, що в умовах перевантаження на першому місці за важливістю є рішення задачі обмеження трафіка. Варто зазначити, що для одного й того самого потоку умовна вартість обмеження трафіку у використанні основного шляху має бути вищою за подібну вартість у разі застосування цим же потоком резервного маршруту.

Критерій оптимальності (4.14) також фокусується на мінімізації умовних витрат, пов'язаних з узгодженим розв'язанням задач FRR, TE та TP. На відміну від критерію (4.13), уведення у виразі (4.14) квадратичної форми змінних β^k та $\bar{\beta}^k$ дає змогу запровадити більш справедливий режим обмеження трафіку на основі так званих відносних пріоритетів [124]. Це полягає в тому, що в разі перевантаження мережі обмеження трафіку буде більш збалансованим, тобто потоки з високим пріоритетом будуть обмежені меншою мірою, ніж потоки пакетів із низьким пріоритетом. Це унеможливлює ситуацію, коли допускається повне блокування потоків із низьким пріоритетом, що має місце у використанні лінійного аналога цільової функції (4.13).

4.1.2. Дослідження запропонованої моделі швидкої перемаршрутизації в ТКМ за умови використання лінійного критерію оптимальності

Проведено аналіз запропонованої моделі швидкої перемаршрутизації з балансуванням навантаження на різних мережних конфігураціях для різної кількості потоків та їхніх характеристик. Особливості моделі продемонструємо на розрахунковому прикладі. Структура досліджуваної мережі показана на рис. 4.1, а в розривах каналів зв'язку мережі наведені їхні пропускні здатності. Припустимо, що існує необхідність у розв'язанні задач швидкої перемаршрутизації із забезпеченням захисту пропускної здатності мережі та каналу $E_{11,12}$ для двох потоків пакетів:

– перший потік передається від вузла R_1 до вузла R_{16} зі змінюваною інтенсивністю $\lambda^1 = 10 \div 1100$ 1/с та пріоритетом $PR^1 = 4$;

– другий потік передається від вузла R_5 до вузла R_{12} зі змінюваною інтенсивністю $\lambda^2 = 10 \div 1100$ 1/с та пріоритетом $PR^2 = 1$.

Отже, другий потік має нижчий пріоритет, ніж перший. Передбачається, що в першому випадку граничне значення верхнього порогу завантаженості каналів зв'язку мережі становило $\alpha_{TH} = 0,75$.

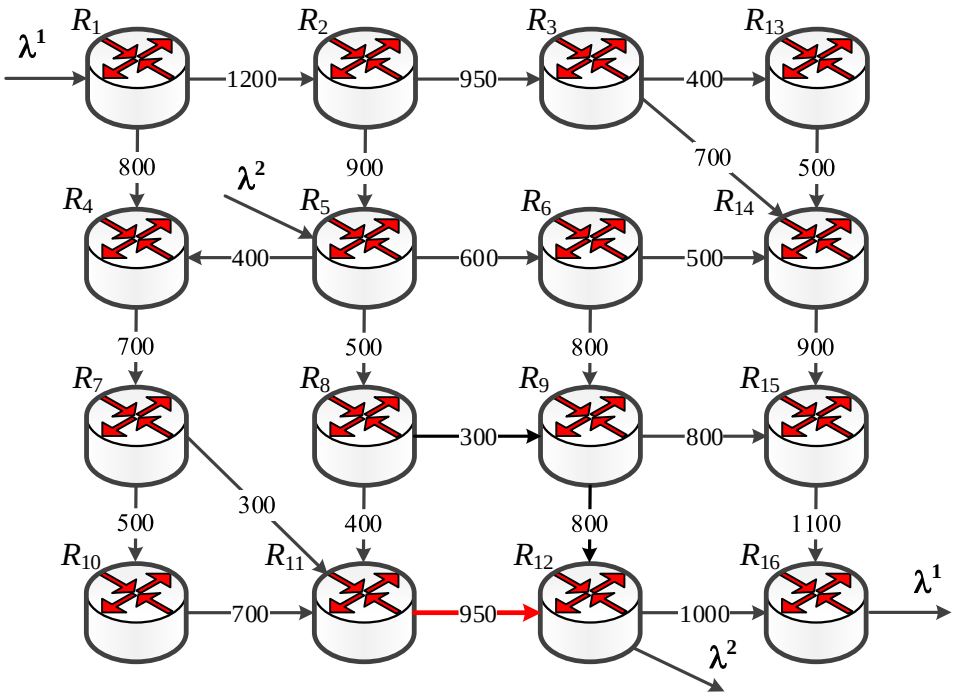
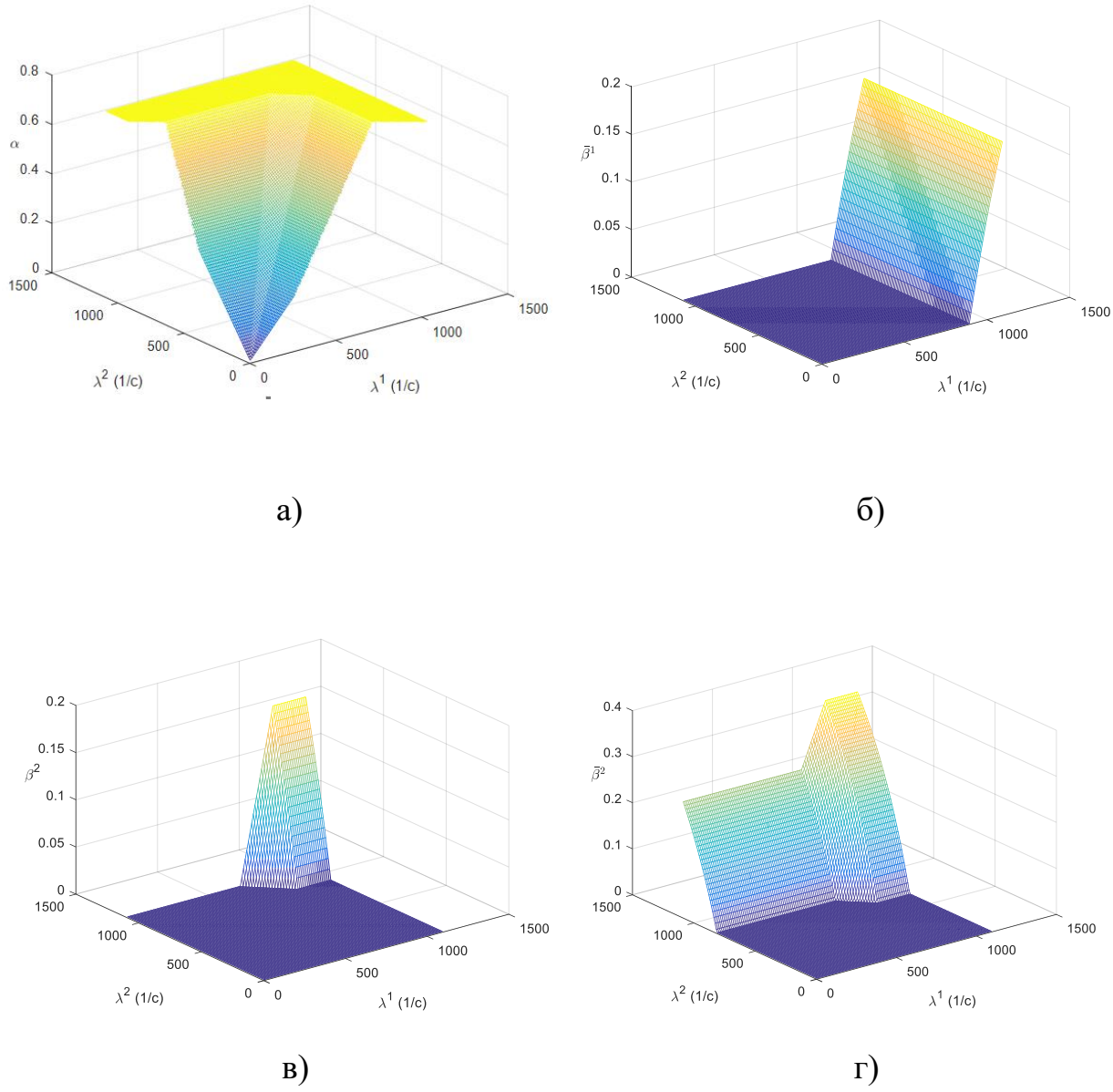


Рис. 4.1. Структура мережі для дослідження моделі швидкої перемаршрутизації в ТКМ із використанням лінійного критерію оптимальності (4.13)

Як показали результати досліджень, зображені на рис. 4.2, зі збільшенням навантаження на мережу верхній поріг завантаженості каналів зв'язку мережі також поступово зростав. Відсутність різких коливань у значеннях α (рис. 4.2, *а*) позитивно впливає на якість обслуговування в мережі загалом. Водночас у разі невисокої завантаженості мережі, коли $\lambda^1 \le 900$ 1/с та $\lambda^2 \le 830$ 1/с, виконання умови $0 \le \alpha \le \alpha_{TH}$ (4.12) не викликало обмеження інтенсивності потоків на границі мережі, тобто $\beta^1 = \bar{\beta}^1 = \beta^2 = \bar{\beta}^2 = 0$ (рис. 4.2).

Проте в разі надмірного навантаження на мережу виконання умови (4.12) забезпечувалося в спосіб, коли $\alpha = \alpha_{TH}$ (рис. 4.2, *а*) за рахунок обмеження інтенсивностей потоків, що протікали як основними, так і резервними шляхами.



а) б)

в) г)

Рис. 4.2. Результати дослідження для $\alpha_{TH} = 0,75$

Як видно з рис. 4.2, обмеження трафіку відбувалося за двома основними принципами:

– обмеження насамперед стосувалися того потоку, який є джерелом перевантаження за умовою (4.12);

– якщо перевантаження створювали декілька потоків, то обмеження стосувалися потоку з меншим пріоритетом відповідно до умов (4.15) та (4.16).

Підтвердженням цих висновків є те, що в разі зазначених вихідних даних перший (високопріоритетний) потік пакетів у процесі використання основного

маршруту за своєю інтенсивністю не обмежувався, тобто $\beta^1 = 0$. Раніше за всіх та з більшою інтенсивністю обмежувався другий (низькопріоритетний) потік під час використання ним резервного шляху (рис. 4.2, *г*). Дещо пізніше і з меншою інтенсивністю обмежувався другий потік у процесі використання ним основного шляху (рис. 4.2, *в*). Перший потік, який мав високий пріоритет, обмежувався лише у випадку створення ним перевантаження каналів, що містив резервний шлях (рис. 4.2, *б*).

Для наочності розглянемо більш детально отримані результати (рис. 4.2), коли $\lambda^1 = 950$ 1/с та $\lambda^2 = 1000$ 1/с. У табл. 4.1 наведено результати розв'язання задач FRR, TE, TP для двох описаних потоків. Розрахунок коефіцієнта використання $\alpha_{i,j}$ для кожного каналу мережі можна провести, як зазначено в [33, 34], за формулою:

$$\alpha_{i,j} = \frac{\sum_{k \in K} \lambda^k \max(x_{i,j}^k, \bar{x}_{i,j}^k)}{\varphi_{i,j}}. \qquad (4.17)$$

Як показали результати дослідження, запропонована модель дозволяє, з одного боку, забезпечити диференційоване обмеження трафіку на основі пріоритетів, а з іншого, – можливість обмеження саме того потоку, який є джерелом перевантажень.

Це полягає в тому, що в разі перевантаження спільно використовуваних розглянутих двох потоків каналів ($E_{5,4}$, $E_{5,6}$, $E_{5,8}$, $E_{7,11}$ та $E_{8,9}$) за своєю інтенсивністю обмежувався саме другий (менш пріоритетний) потік (табл. 4.1). З огляду на ймовірне порушення умови (4.12), викликане перевантаженням невикористовуваних другим потоком каналів $E_{1,2}$ та $E_{14,15}$ (табл. 4.1), обмежувався і перший (високопріоритетний) потік, як це показано на рис. 4.2, *б*.

Таблиця 4.1

Порядок багатошляхової маршрутизації двох потоків, отриманий із застосуванням запропонованої моделі (захист каналу $E_{11,12}$)

Канал зв'язку	Інтенсивність першого потоку в каналах зв'язку		Інтенсивність другого потоку в каналах зв'язку		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	788,17	900	0	0	0,75
$E_{2,3}$	592,87	675	0	0	0,71
$E_{1,4}$	161,83	0	0	0	0,2
$E_{2,5}$	195,30	225	0	0	0,25
$E_{3,14}$	406,66	449,18	0	0	0,64
$E_{5,4}$	0	0	300	225	0,75
$E_{5,6}$	113,98	129,87	320,13	320,13	0,75
$E_{4,7}$	161,83	0	300	225	0,66
$E_{5,8}$	81,32	95,13	279,87	129,87	0,75
$E_{6,9}$	86,95	129,87	320,13	320,13	0,56
$E_{7,11}$	0	0	189,75	225	0,75
$E_{8,9}$	52,59	95,13	96,84	129,87	0,75
$E_{7,10}$	161,83	0	110,25	0	0,54
$E_{8,11}$	28,73	0	183,03	0	0,53
$E_{9,12}$	66,14	126,71	416,97	450	0,72
$E_{10,11}$	161,83	0	110,25	0	0,39
$E_{11,12}$	190,56	0	293,28	0	0,51
$E_{3,13}$	186,21	225,82	0	0	0,56
$E_{13,14}$	186,21	225,82	0	0	0,45
$E_{6,14}$	27,03	0	0	0	0,05
$E_{14,15}$	619,90	675	0	0	0,75
$E_{9,15}$	73,40	98,29	0	0	0,12
$E_{15,16}$	693,30	773,29	0	0	0,7
$E_{12,16}$	256,70	126,71	0	0	0,26

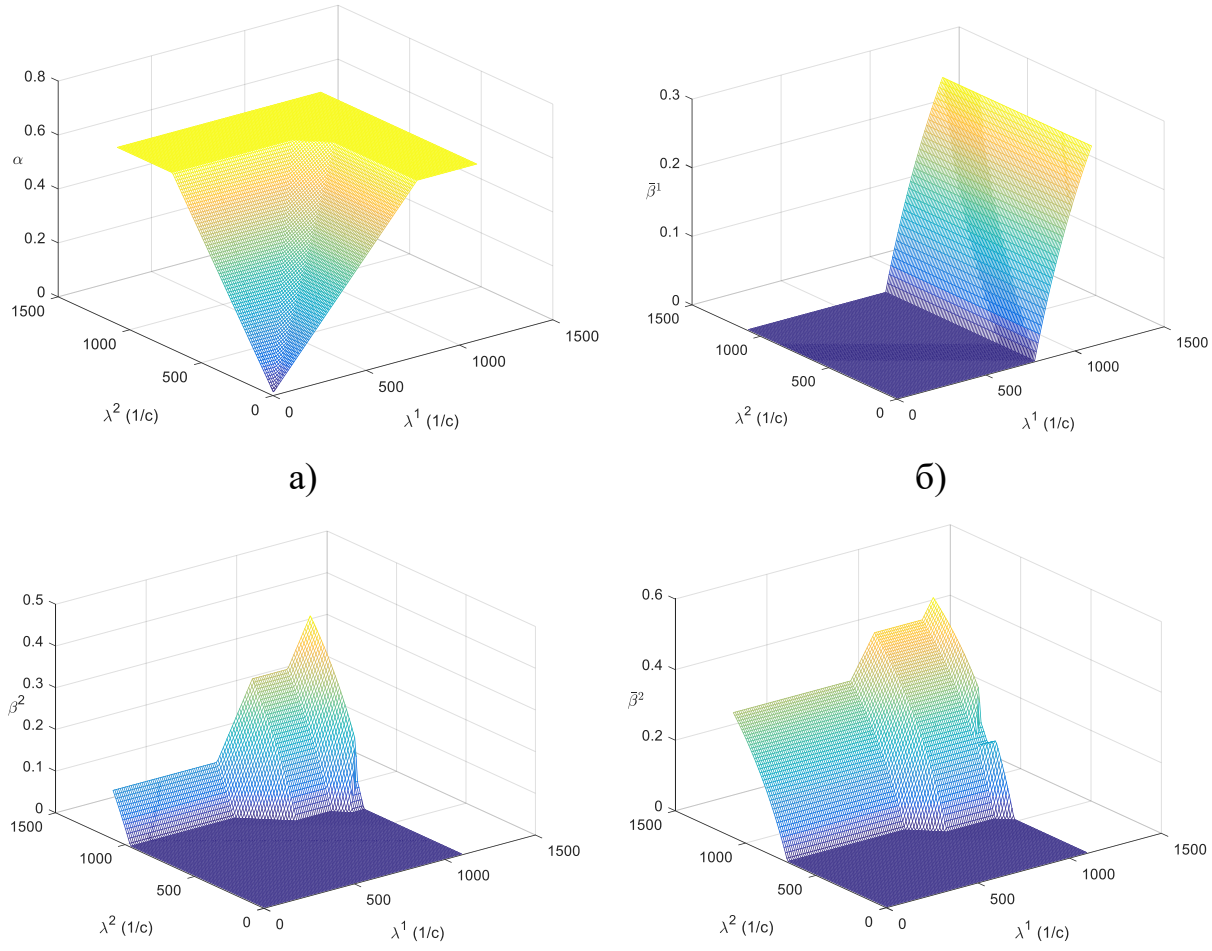
Далі розглянемо другий випадок, коли граничне значення верхнього порогу завантаженості каналів зв'язку мережі буде мати нижче порівняно з

першим прикладом значення – $\alpha_{TH} = 0,65$. Зауважимо, що зниження порогового значення α_{TH} може бути викликане, наприклад, підвищенням вимог до рівня якості обслуговування в ТКМ.

Результати розрахунків для другого випадку представлені на рис. 4.3 за умови вихідних даних, що відповідали попередньому прикладу. Отримані результати дослідження (рис. 4.3) підтвердили попередній висновок, що зростання навантаження на мережу призводить до поступового збільшення верхнього порогу завантаженості каналів зв'язку (рис. 4.3, *а*). Як і раніше, під час невисокої завантаженості мережі ($0 \le \alpha \le \alpha_{TH}$) обмеження інтенсивності потоків на границі мережі було відсутнє, тобто $\beta^1 = \overline{\beta}^1 = \beta^2 = \overline{\beta}^2 = 0$. Але завдяки тому, що граничне значення $\alpha_{TH} = 0,65$ стало більш жорстким, обмеження трафіку починалося за умови дещо менших значень інтенсивностей вхідних потоків: $\lambda^1 > 780$ 1/с, $\lambda^2 > 720$ 1/с (рис. 4.3, *а*).

У подальшому збільшенні навантаження на мережу умови (4.12) виконувалися лише, якщо $\alpha = \alpha_{TH}$ (рис. 4.3, *а*) за рахунок обмеження інтенсивностей потоків, які протікали основними та резервними шляхами. За такої умови, як і в попередньому прикладі, обмеження трафіку відбувалося диференційовано відповідно до пріоритетів потоків (4.15) та залежно від того, який саме потік пакетів провокував перевантаження каналів мережі з невиконанням умови (4.12).

Як і в попередньому випадку (рис. 4.2), за умови зазначених вихідних даних перший потік пакетів, який мав високий пріоритет, у разі використання основного маршруту за своєю інтенсивністю не обмежувався ($\beta^1 = 0$). З більшою інтенсивністю обмежувався другий потік, який мав низький пріоритет та передавався резервним шляхом (рис. 4.3, *г*). Тоді як під час використання основного шляху другий потік обмежувався менш інтенсивно (рис. 4.3, *в*). Перший потік, що мав високий пріоритет, обмежувався лише в разі перевантаження каналів, які містив резервний шлях (рис. 4.3, *б*).



а) б)

в) г)

Рис. 4.3. Результати дослідження для $\alpha_{TH} = 0,65$

4.1.3. Дослідження запропонованої моделі швидкої перемаршрутизації в ТКМ за умови використання лінійно-квадратичного критерію оптимальності

Дослідження запропонованої моделі швидкої перемаршрутизації із балансуванням навантаження та диференційованим обмеженням трафіку в ТКМ із використанням лінійно-квадратичного критерію оптимальності (4.14) було проведено також для декількох структур мережі. Так, наприклад, особливості розв’язання поставленої задачі будуть продемонстровані на структурі ТКМ, що складається з шістнадцяти вузлів і двадцяти чотирьох

каналів зв'язку та представлена на рис. 4.4. У розривах КЗ вказана їхня пропускна здатність.

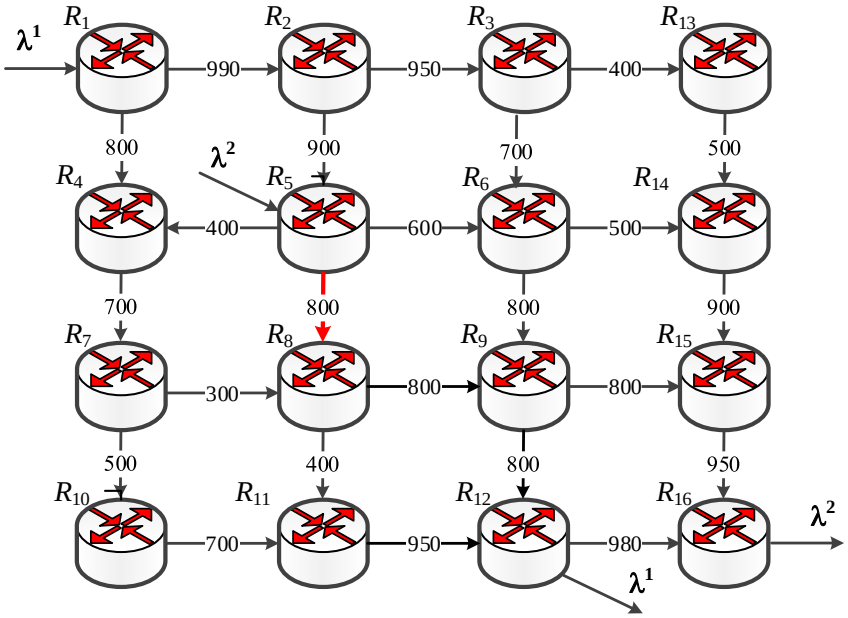


Рис. 4.4. Структура мережі для дослідження моделі швидкої перемаршрутизації в ТКМ із захистом каналу зв'язку $E_{5,8}$ на основі використання лінійно-квадратичного критерію оптимальності (4.14)

Для розв'язання задачі швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіку на основі відносних пріоритетів елементом мережі, що підлягав захисту, було обрано канал зв'язку $E_{5,8}$. Моделювався випадок, коли в мережі циркулювали два потоки пакетів, які мали такі характеристики:

– перший потік передавався від вузла R_1 до вузла R_{12} зі змінюваною інтенсивністю $\lambda^1 = 10 \div 1200$ 1/с та пріоритетом $PR^1 = 4$;

– другий потік передавався від вузла R_5 до вузла R_{16} зі змінюваною інтенсивністю $\lambda^2 = 10 \div 1200$ 1/с та пріоритетом $PR^2 = 1$.

Передбачалося, що граничне значення верхнього порогу завантаженості каналів зв'язку мережі обрано $\alpha_{TH} = 0{,}8$, а розрахунок коефіцієнта використання $\alpha_{i,j}$ для кожного каналу зв'язку відбувався за формулою (4.17).

Тоді на рис. 4.5 показана динаміка змін верхнього порогу перевантаження каналів зв'язку (α)залежно від інтенсивності двох потоків пакетів, що надходять до мережі. На основі результатів досліджень, зображених на рис. 4.5, можна зробити висновок, що із збільшенням навантаження (інтенсивності першого та другого потоків пакетів) також зросла верхня границя використання каналів зв’язку. Водночас варто зазначити, що в умовах низького навантаження на границі мережі обмежень потоків не відбувалось. Обмеження потоків пакетів розпочиналося тільки в умовах перевантаження мережі, коли $\alpha \to \alpha_{TH}$.

Як показано на рис. 4.6 та 4.7, функції обмеження трафіку були реалізовані на основі врахування пріоритетів потоку. Порівняно із результатами дослідження моделі, що базується на використанні лінійного критерію оптимальності (4.13), результати дослідження моделі із використанням лінійно-квадратичного критерію оптимальності (4.14) свідчать про відсутність повного блокування потоку пакетів із найменшим пріоритетом.

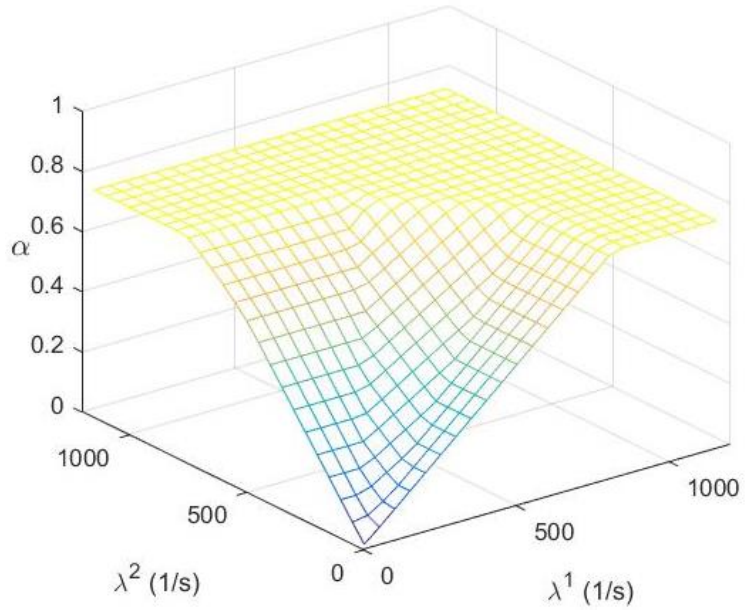
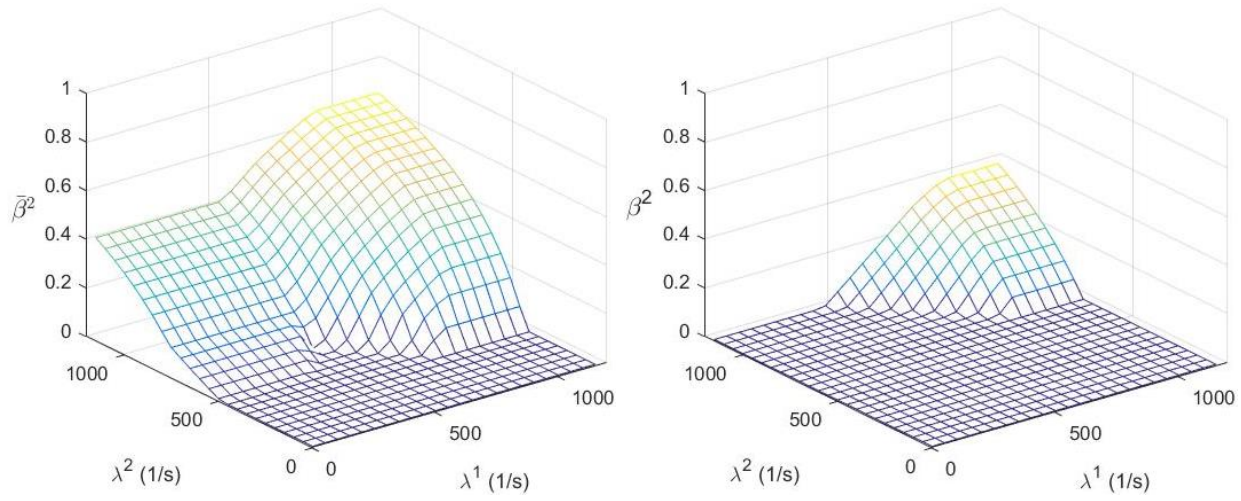
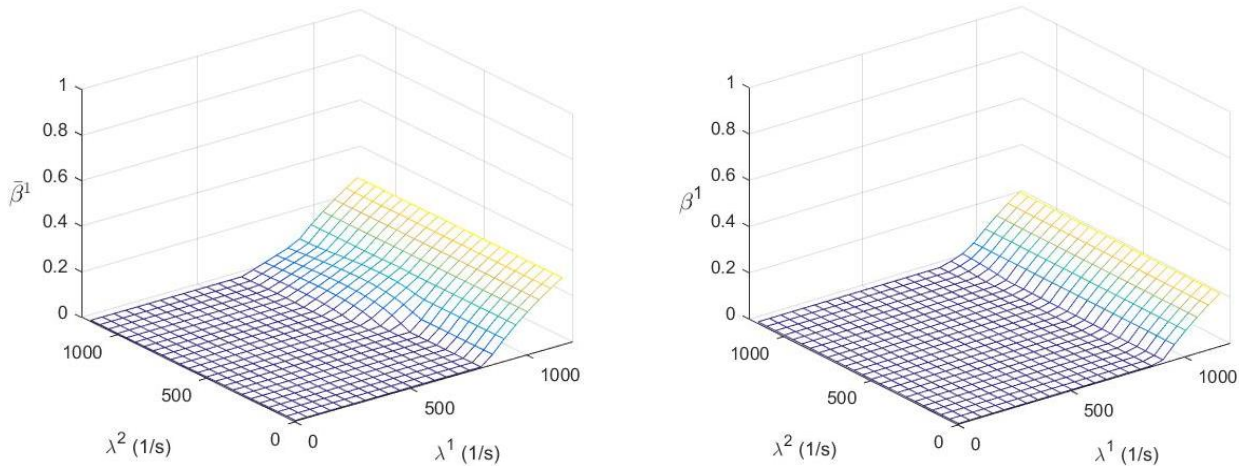


Рис. 4.5. Залежність верхнього порогу завантаженості каналів зв’язку від інтенсивності першого (λ^1) та другого (λ^2) потоків пакетів, що передаються в мережі ($\alpha_{TH} = 0{,}8$)



а) б)

Рис. 4.6. Аналіз результатів обмеження інтенсивності другого потоку пакетів залежно від навантаження на ТКМ ($\alpha_{TH} = 0{,}8$)



а) б)

Рис. 4.7. Аналіз результатів обмеження інтенсивності першого потоку пакетів залежно від навантаження на ТКМ ($\alpha_{TH} = 0{,}8$)

Відповідно до результатів аналізу, показаних на рис. 4.6 та 4.7, варто зазначити, що механізм справедливого обмеження трафіку для двох потоків із

різними пріоритетами в мережі здійснюється відповідно до умови (4.15), та запускається в разі досягнення максимально допустимого порогу використання каналу, тобто коли $\alpha = \alpha_{TH}$. Згідно з (4.15) в умовах перевантаження найбільш інтенсивне обмеження зазнає той потік, пакети якого мають найнижчий IP-пріоритет і передаються резервним шляхом.

Так, на рис. 4.6, *а* показано, що обмеження другого потоку із пріоритетом $PR^2 = 1$, який передається резервним шляхом, починаються приблизно за умови інтенсивності $\lambda^2 = 388$ 1/с. Більше того, у разі низької інтенсивності першого (більш пріоритетного) потоку ($\lambda^1 \le 500$ 1/с) обмеження другого потоку, що передається резервним шляхом, було менш інтенсивним, ніж за умови високої інтенсивності першого потоку ($\lambda^1 > 500$ 1/с).

Як показано на рис. 4.6, *б*, відповідно до справедливого обмеження трафіку другий потік, що передавався основним шляхом, почав обмежуватися набагато пізніше в разі інтенсивності $\lambda^2 = 737$ 1/с. Водночас цей самий потік не був повністю заблокований, коли використовувався резервний шлях (рис. 4.6, *а*). Отримані результати показали, що другий потік був менш обмеженим під час використання основного маршруту, ніж коли використовувався резервний маршрут, що підтверджує адекватність запропонованого рішення на основі умови (4.15).

У межах запропонованого рішення із справедливим обмеженням трафіку подібна ситуація також була характерною і для першого потоку, який мав більш високий IP-пріоритет – $PR^1 = 4$ (рис. 4.7). Перший потік в умовах використання резервного маршруту (рис. 4.7, *а*) обмежувався, починаючи з $\lambda^1 = 853$ 1/с. У використанні основного маршруту цей потік обмежувався, починаючи лише з $\lambda^1 = 931$ 1/с (рис. 4.7, *б*). Для наочності отримані результати дослідження, якщо $\lambda^1 = 900$ 1/с та $\lambda^2 = 900$ 1/с, наведені в табл. 4.2.

Таблиця 4.2

Порядок маршрутизації потоків за умови використання запропонованої моделі з критерієм оптимальності (4.14) (захист каналу $E_{5,8}$)

Канал зв'язку	Інтенсивність першого потоку в каналах зв'язку		Інтенсивність другого потоку в каналах зв'язку		$\alpha_{i,j}$
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях	
$E_{1,2}$	660,01	587,32	0	0	0,67
$E_{2,3}$	560,00	560,00	0	0	0,70
$E_{1,4}$	239,99	239,99	0	0	0,25
$E_{2,5}$	100,01	27,32	0	0	0,11
$E_{3,6}$	560,00	560,00	0	0	0,80
$E_{5,4}$	0	0	0	0	0
$E_{5,6}$	27,32	27,32	452,68	452,68	0,80
$E_{4,7}$	239,99	239,99	0	0	0,34
$E_{5,8}$	72,69	0	367,31	0	0,55
$E_{6,9}$	587,32	587,32	52,68	52,68	0,80
$E_{7,8}$	239,99	239,99	0	0	0,80
$E_{8,9}$	11,79	5,34	348,21	0	0,45
$E_{7,10}$	0	0	0	0	0
$E_{8,11}$	300,89	234,66	19,11	0	0,80
$E_{9,12}$	599,11	592,66	40,89	40,89	0,80
$E_{10,11}$	0	0	0	0	0
$E_{11,12}$	300,89	234,66	19,11	0	0,34
$E_{3,13}$	0	0	0	0	0
$E_{13,14}$	0	0	0	0	0
$E_{6,14}$	0	0	400,00	400,00	0,80
$E_{14,15}$	0	0	400,00	400,00	0,44
$E_{9,15}$	0	0	360,00	11,79	0,45
$E_{15,16}$	0	0	760,00	411,79	0,80
$E_{12,16}$	0	0	60,00	40,90	0,06

У процесі забезпечення дотримання умови (4.12) було встановлено, що

– під час використання резервного шляху перший потік, який мав високий пріоритет, отримував відмову в обслуговуванні на границі мережі з інтенсивністю, яка становила 72,68 1/с;

– під час використання основного шляху другий потік, який мав низький пріоритет, отримував відмову в обслуговуванні на границі мережі з інтенсивністю 80 1/с;

– під час використання резервного шляху другий потік отримував відмову в обслуговуванні на границі мережі з інтенсивністю 447,31 1/с.

4.2. Удосконалення та дослідження моделі безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в ТКМ

4.2.1. Потокова модель безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в ТКМ

У цьому підрозділі запропоновано підхід до забезпечення якості обслуговування та мережної безпеки в ТКМ, які функціонують в умовах відмов мережного обладнання. Підхід ґрунтується на застосуванні швидкої перемаршрутизації з підтримкою балансування навантаження та диференційованого обмеження трафіку з урахуванням показників мережної безпеки. З цією метою, відповідно до результатів, отриманих у третьому розділі, у моделі (4.1)–(4.16) модифікуються умови запобігання перевантаження каналів зв’язку (4.9) для забезпечення балансування навантаження, ураховуючи імовірності їхньої компрометації каналів:

$$\sum_{k \in K} \lambda^k \cdot u_{i,j}^k \le \alpha v_{i,j} \varphi_{i,j}, \; E_{i,j} \in E, \tag{4.18}$$

де граничні значення коефіцієнтів $v_{i,j}$ визначаються відповідно до (3.7).

У третьому розділі запропоновано множину варіантів представлення функціональної залежності $v=f(p)$ (3.9)–(3.13), що відповідають умовам (3.7) та (3.8). Ці вирази можуть бути використані і в моделі (4.18) залежно від сценарію компрометації, а також вимог щодо рівня якості обслуговування та мережної безпеки.

Далі, як приклад, розглянемо модель блокування пакетів (3.10):

$$v_{i,j} = 1 - p_{i,j}^{n}, \tag{4.19}$$

де $n \geq 1$. Як видно з рис. 3.2, збільшення параметра n залежно від (4.19) зменшує чутливість балансування навантаження до загроз щодо мережної безпеки.

Зазначимо, що як критерій оптимальності пропонується до використання вираз (4.13) за умови виконання (4.15). Для організації обмеження трафіку на границі ТКМ із урахуванням вимог щодо рівня мережної безпеки пропонується вирази (4.16) модифікувати до такого вигляду:

$$w_k = CF^k + 1,\ \bar{w}_k = CF^k + 0{,}5,\ c = 0{,}25, \tag{4.20}$$

де $CF^k(PR^k, CL^k)$ – клас обслуговування k-го потоку, значення якого в запропонованій моделі має залежати як від IP-пріоритету пакетів цього потоку (PR^k), так і від рівня його конфіденційності (CL^k).

Так, відповідно до [14] може вводитися чотирирівнева ієрархія конфіденційності: конфіденційно (найвищий рівень конфіденційності); обмежений (середній рівень конфіденційності); внутрішнє використання (найнижчий рівень конфіденційності); загальнодоступний (будь-хто може мати доступ до цієї інформації). Загалом кожен із цих рівнів конфіденційності може бути уточнений та деталізований. Наприклад, НАТО вводить класифікацію з чотирма конфіденційними рівнями та двома рівнями публічного доступу [14].

Отже, у межах запропонованої моделі (4.1)–(4.8), (4.10)–(4.16), (4.18), (4.20) технологічна задача безпечної швидкої перемаршрутизації (FRR) з балансуванням навантаження (TE) та диференційованим обмеженням трафіку (TP) на границі ТКМ була зведена до оптимізаційної задачі лінійного, з критерієм (4.13), або квадратичного, з критерієм (4.14), програмування. Обмеженнями, які накладалися на маршрутні керуючі змінні $x_{i,j}^k$, $\overline{x}_{i,j}^k$, $u_{i,j}^k$ та α, були вирази (4.1)–(4.4), (4.6), (4.10)–(4.12), (4.18).

4.2.2. Дослідження моделі безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в ТКМ

Дослідження запропонованої моделі проводилося на декількох мережних конфігураціях під час передавання множини потоків, які мали різні класи обслуговування. Продемонструємо основні особливості функціонування моделі на структурі мережі, що показана на рис. 4.1. Вихідні дані для дослідження, а саме пропускні здатності каналів зв'язку мережі та ймовірності їхньої компрометації, наведено в табл. 4.3.

Нехай у процесі безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку передавалися пакети двох потоків за умови реалізації схеми захисту каналу зв'язку $E_{11,12}$ (рис. 4.1).

Припустимо, що потоки, які передавались, мали такі характеристики:

– R_1 – вузол-відправник, R_{16} – вузол-отримувач, інтенсивність потоку змінюється в межах діапазону $\lambda^1 = 10 \div 1100$ 1/с, клас потоку $CF^1 = 4$;

– R_5 – вузол-відправник, R_{12} – вузол-отримувач, інтенсивність потоку змінюється в межах діапазону $\lambda^2 = 10 \div 1100$ 1/с, клас потоку $CF^2 = 1$.

Таблиця 4.3

Вихідні дані для дослідження моделі безпечної швидкої перемаршрутизації з підтримкою балансування навантаження та диференційованого обмеження трафіку в ТКМ

Канал зв'язку	Пропускна здатність, 1/с	Імовірність компрометації, $p_{i,j}$	Канал зв'язку	Пропускна здатність, 1/с	Імовірність компрометації, $p_{i,j}$
$E_{1,2}$	1200	0,2	$E_{7,10}$	500	0,4
$E_{2,3}$	950	0,5	$E_{8,11}$	400	0,2
$E_{1,4}$	800	0,3	$E_{9,12}$	800	0,5
$E_{2,5}$	900	0,4	$E_{10,11}$	700	0,3
$E_{3,14}$	700	0,1	$E_{11,12}$	950	0,2
$E_{5,4}$	400	0,5	$E_{3,13}$	400	0,1
$E_{5,6}$	600	0,2	$E_{13,14}$	500	0,3
$E_{4,7}$	700	0,2	$E_{6,14}$	500	0,4
$E_{5,8}$	500	0,1	$E_{14,15}$	900	0,2
$E_{6,9}$	800	0,4	$E_{9,15}$	800	0,5
$E_{7,11}$	300	0,1	$E_{15,16}$	1100	0,3
$E_{8,9}$	300	0,3	$E_{12,16}$	1000	0,2

Крім того, припустимо, що в наведеному прикладі граничне значення верхнього порогу завантаженості каналів зв'язку мережі $\alpha_{TH} = 0,65$, а показникова функція (4.19) мала такий вигляд: $v_{i,j} = 1 - p_{i,j}^2$, тобто $n = 2$.

Відповідно до результатів досліджень, зображених на рис. 4.8, зі зростанням мережного навантаження верхній поріг завантаженості каналів зв'язку мережі також поступово зростав. Відсутність різких коливань у значеннях α (рис. 4.8) позитивно впливає на якість обслуговування в мережі загалом. За цих умов у разі невисокої завантаженості мережі, коли $\lambda^1 \le 590$ 1/с

та $\lambda^2 \le 750$ 1/с, виконання умови $0 \le \alpha \le \alpha_{TH}$ (4.12) не викликало обмеження інтенсивності потоків на границі мережі, тобто $\beta^1 = \bar{\beta}^1 = \beta^2 = \bar{\beta}^2 = 0$ (рис. 4.8).

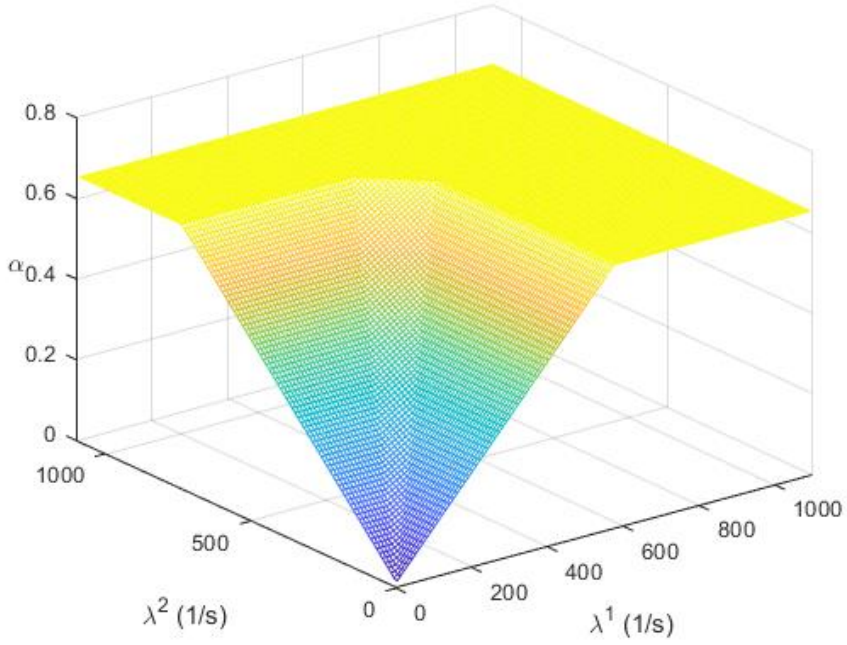


Рис. 4.8. Залежність верхнього порогу завантаженості каналів зв'язку мережі від інтенсивностей потоків, що передаються в ТКМ

Проте у випадку надмірного навантаження на мережу виконання умови (4.12) забезпечувалося в спосіб, коли $\alpha = \alpha_{TH}$ (рис. 4.8) за рахунок обмеження інтенсивностей потоків, які протікали як основними, так і резервними шляхами. Відповідно до рис. 4.8–4.12, обмеження трафіку для потоків, що передавалися, відбувалося за такими принципами:

– обмеження застосовувалися до того потоку, який був джерелом перевантаження за умовою (4.12);

– якщо перевантаження створювали декілька потоків, то обмеження насамперед стосувалися потоку з меншим класом відповідно до умови (4.15) та (4.20);

– балансування навантаження відбувалося відповідно до умови (4.18) таким чином, щоб канали зв'язку з меншою ймовірністю компрометації завантажувалися більше, ніж небезпечніші канали.

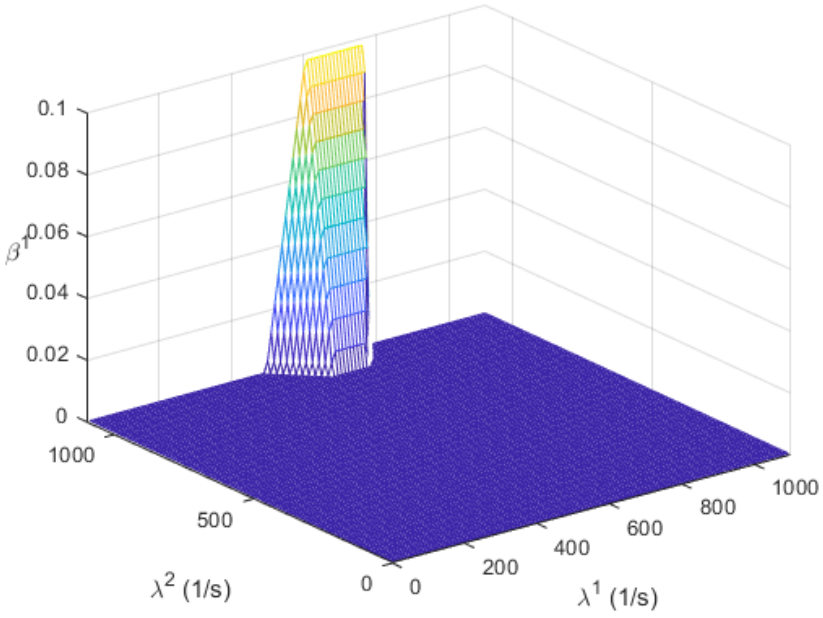


Рис. 4.9. Рішення задачі безпечної швидкої перемаршрутизації для першого потоку пакетів (основний шлях)

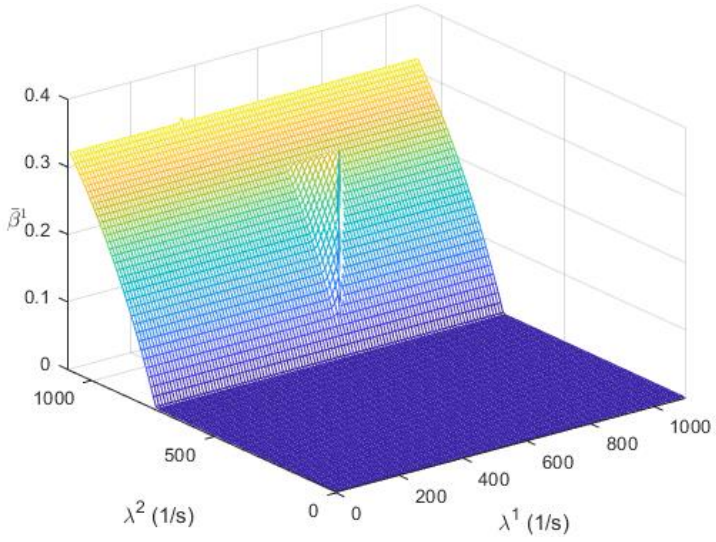


Рис. 4.10. Рішення задачі безпечної швидкої перемаршрутизації для першого потоку пакетів (резервний шлях)

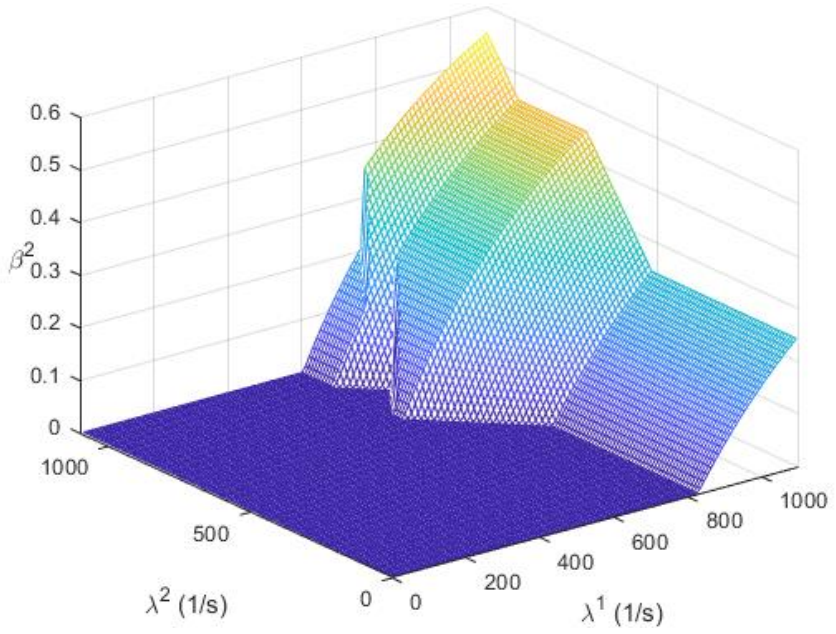


Рис. 4.11. Рішення задачі безпечної швидкої перемаршрутизації для другого потоку пакетів (основний шлях)

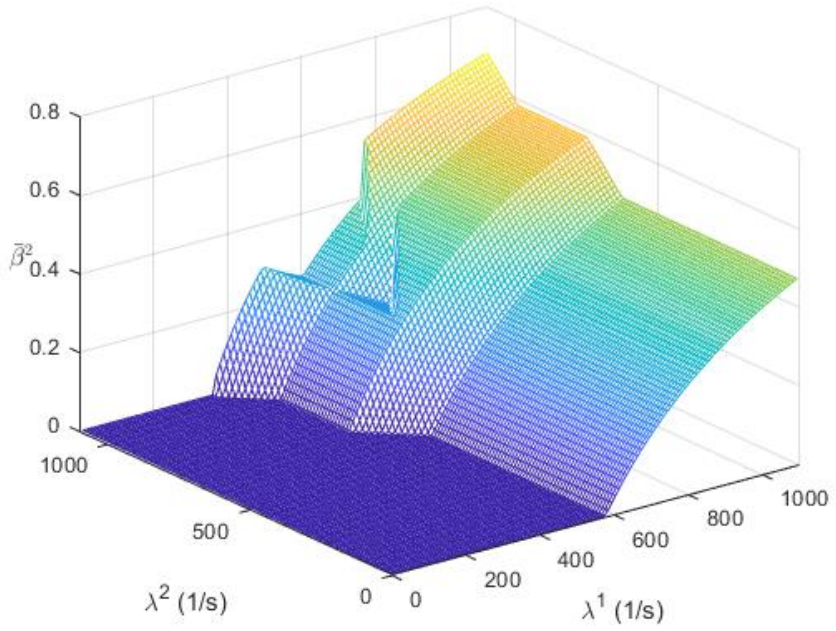


Рис. 4.12. Рішення задачі безпечної швидкої перемаршрутизації для другого потоку пакетів (резервний шлях)

Крім того, проведене дослідження показало насамперед, що за умови зазначених вихідних даних перший потік пакетів у процесі використання основного маршруту за своєю інтенсивністю обмежувався найменше. На підтвердження до зазначених вище принципів, перший потік обмежувався у випадку створення ним перевантаження каналів, що містив основний, так і резервний шляхи (рис. 4.9 та 4.10). Проте раніше за всіх та з більшою інтенсивністю обмежувався другий потік, який мав нижчий клас обслуговування, у разі використання ним резервного шляху (рис. 4.12). Дещо пізніше і з меншою інтенсивністю обмежувався другий потік під час використання основного шляху (рис. 4.11). Отже, результати дослідження загалом підтверджують працездатність запропонованої моделі безпечної швидкої перемаршрутизації в ТКМ та адекватність отриманих за допомогою неї рішень.

4.2.3. Дослідження впливу показників мережної безпеки на порядок безпечної швидкої перемаршрутизації в ТКМ

Розглянемо випадок, коли в мережі так само передаються в ТКМ (рис. 4.1) два потоки, характеристики яких наведені в табл. 4.4, під час реалізації захисту каналу $E_{11,12}$.

Таблиця 4.4

Характеристики досліджуваних потоків

№ потоку	Відправник та отримувач пакетів	Інтенсивність потоку, 1/с	Клас обслуговування
1	$s_k=R_1$, $d_k= R_{16}$	$\lambda^1=950$	$CF^1=4$
2	$s_k=R_5$, $d_k= R_{12}$	$\lambda^2=1000$	$CF^2=1$

Нехай граничне значення верхнього порогу завантаженості каналів зв’язку мережі $\alpha_{TH} = 0,75$. Тоді в табл. 4.5 та 4.6 показано розрахований порядок безпечної швидкої перемаршрутизації двох потоків із застосуванням запропонованої моделі з урахуванням двох випадків значень керуючого параметра у функції (4.19), а саме n=2 та n=3.

Таблиця 4.5

Порядок безпечної швидкої перемаршрутизації двох потоків (захист каналу $E_{11,12}$, n=2)

Канал зв'язку	Інтенсивність першого потоку, 1/с		Інтенсивність другого потоку, 1/с	
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях
$E_{1,2}$	750,75	864	0	0
$E_{2,3}$	534,375	534,375	0	0
$E_{1,4}$	199,25	0	0	0
$E_{2,5}$	216,375	329,625	0	0
$E_{3,14}$	519,75	519,75	0	0
$E_{5,4}$	0	0	225	222,75
$E_{5,6}$	216,375	329,625	102,375	102,375
$E_{4,7}$	199,25	0	225	222,75
$E_{5,8}$	0	0	371,25	204,75
$E_{6,9}$	216	216	102,375	102,375
$E_{7,11}$	0	0	222,75	222,75
$E_{8,9}$	0	0	204,75	204,75
$E_{7,10}$	199,25	0	2,25	0
$E_{8,11}$	0	0	166,5	0
$E_{9,12}$	0	113,25	307,125	307,125
$E_{10,11}$	199,25	0	2,25	0
$E_{11,12}$	199,25	0	168,75	0
$E_{3,13}$	14,625	14,625	0	0
$E_{13,14}$	14,625	14,625	0	0
$E_{6,14}$	0,375	113,625	0	0
$E_{14,15}$	534,75	648	0	0
$E_{9,15}$	216	102,75	0	0
$E_{15,16}$	750,75	750,75	0	0
$E_{12,16}$	199,25	113,25	0	0

Таблиця 4.6

Порядок безпечної швидкої перемаршрутизації двох потоків

(захист каналу $E_{11,12}$, n=3)

Канал зв'язку	Інтенсивність першого потоку, 1/с		Інтенсивність другого потоку, 1/с	
	Основний шлях	Резервний шлях	Основний шлях	Резервний шлях
$E_{1,2}$	802,725	892,8	0	0
$E_{2,3}$	623,4375	623,4375	0	0
$E_{1,4}$	147,275	0	0	0
$E_{2,5}$	179,2875	269,3625	0	0
$E_{3,14}$	524,475	524,475	0	0
$E_{5,4}$	0	0	262,5	224,775
$E_{5,6}$	179,2875	269,3625	177,0375	177,0375
$E_{4,7}$	147,275	0	262,5	224,775
$E_{5,8}$	0	0	374,625	218,925
$E_{6,9}$	179,2875	223,2	177,0375	177,0375
$E_{7,11}$	0	0	224,775	224,775
$E_{8,9}$	0	0	218,925	218,925
$E_{7,10}$	147,275	0	37,725	0
$E_{8,11}$	0	0	155,7	0
$E_{9,12}$	0	90,075	395,9625	395,9625
$E_{10,11}$	147,275	0	37,725	0
$E_{11,12}$	147,275	0	193,425	0
$E_{3,13}$	98,9625	98,9625	0	0
$E_{13,14}$	98,9625	98,9625	0	0
$E_{6,14}$	0	46,1625	0	0
$E_{14,15}$	623,4375	669,6	0	0
$E_{9,15}$	179,2875	133,125	0	0
$E_{15,16}$	802,725	802,725	0	0
$E_{12,16}$	147,275	90,075	0	0

За результатами розрахунків і порівняльного аналізу (табл. 4.5 та 4.6) можна зробити такі висновки. По-перше, рішення щодо безпечної швидкої перемаршрутизації, отримані за допомогою запропонованої моделі, базувалися на адекватному врахуванні трьох основних характеристик каналів зв'язку: пропускної здатності (показника QoS), імовірності компрометації (показника мережної безпеки) та місця каналу в топології мережі. Зазвичай більш інстенсивно завантажувалися ті канали, що мали високу пропускну здатність і низьку ймовірність компрометації (табл. 4.5 та 4.6).

Проте зі зменшенням значення показника *n* функції (4.19) модель стає більш чутливою до параметрів безпеки (імовірності компрометації каналів зв'язку). У цьому разі більш небезпечні канали завантажуються менше. Це чітко видно з табл. 4.5 та 4.6 під час порівняння розподілу навантаження, наприклад, каналами $E_{2,3}$, $E_{5,4}$, $E_{9,12}$, $E_{9,15}$, що мали найвищу ймовірність компрометації, а саме 0,5. Так, чим сильніше запропонована модель безпечної швидкої перемаршрутизації реагує на показники безпеки, тим більше будуть розвантажуватися небезпечні канали зв'язку ТКМ.

Отже, продуктивність мережі знижується через необхідність урахування ймовірності компрометації каналів у процесі забезпечення заданого рівня верхнього порогу завантаженості каналів зв'язку мережі α_{TH}, провокуючи більшу інтенсивність відмов в обслуговуванні (обмеження) трафіку на границі мережі (табл. 4.7).

Таблиця 4.7

Інтенсивності відмов на границі мережі залежно від показника функції (4.19)

Параметр	$\bar{\beta}^1$	Інтенсивність відмов, 1/с	β^2	Інтенсивність відмов, 1/с	$\bar{\beta}^2$	Інтенсивність відмов, 1/с
n=2	0,0905	86	0,3014	301,375	0,4701	470,125
n=3	0,0602	57,2	0,1858	185,8375	0,3793	379,2625

Отримані числові результати показали (табл. 4.7), що перший потік із високим класом обслуговування під час використання основного шляху не був обмежений на границі мережі, тобто $\beta^1 = 0$. Порівняння інтенсивностей відмов в обслуговуванні (обмеження) потоків на границі мережі, а саме для першого потоку за умови використання основного шляху, а також другого потоку під час використання як основного, так і резервного шляхів, показано в табл. 4.7. Аналіз розрахунків дозволяє зробити висновок, що, коли n=2, підвищується чутливість маршрутних рішень та рішень щодо обмеження навантаження до параметрів безпеки (4.19), це спричиняє вищу інтенсивність відмов на границі мережі.

4.3. Рекомендації щодо практичного застосування запропонованих у роботі маршрутних рішень у програмно-конфігурованих телекомунікаційних мережах

Запропоновані в дисертаційній роботі потокові моделі безпечної та відмовостійкої маршрутизації орієнтовані насамперед на використання в сучасних програмно-конфігурованих телекомунікаційних мережах [1–6] як математичної та алгоритмічної основи перспективних маршрутних протоколів. Це пов’язано з тим, що лише використання багаторівневої ієрархії SDN, варіант якої зображено на рис. 4.13, оптимізоване під вирішення основних мережних задач щодо управління трафіком, маршрутизації, забезпечення заданого рівня якості обслуговування та мережної безпеки.

У межах запропонованої архітектури визначається кілька функціональних рівнів: *площина даних*, що представлена мережним обладнанням (комутатори, маршрутизатори, сервери); *площина управління*, що містить множину контролерів, які відповідають за високу функціональність площини даних; *площина застосування*, що дозволяє візуалізувати та керувати мережею за допомогою програмних застосунків. Усі математичні моделі безпечної та відмовостійкої маршрутизації, запропоновані в другому, третьому та

четвертому розділах роботи, орієнтують на централізацію маршрутних рішень, що мають синтезуватися на SDN-контролерах (рис. 4.13) та забезпечувати ефективне розв'язання задач маршрутизації/перемаршрутизації, балансування навантаження та диференційованого обмеження трафіку на границі мережі, представленою площиною даних.

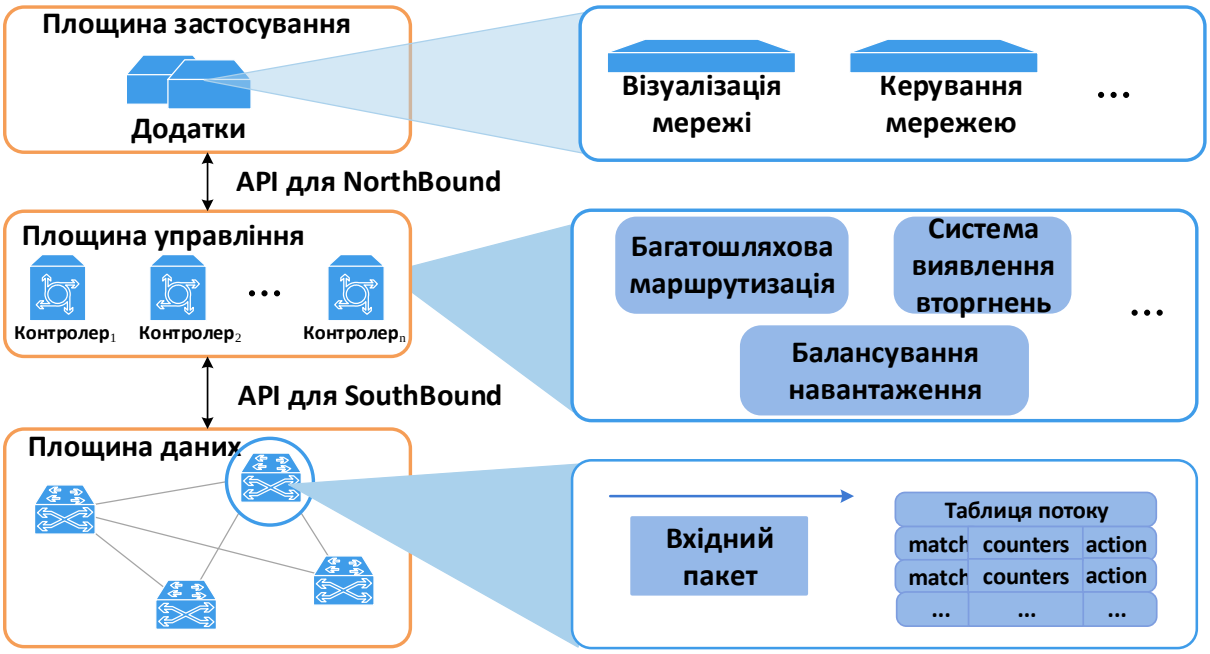


Рис. 4.13. Варіант багаторівневої архітектури SDN

Упровадження запропонованих у роботі маршрутних рішень передбачає певний перегляд функціоналу *площини управління* (контролерів) програмно-конфігурованих телекомунікаційних мереж (рис. 4.14) у бік модифікації та оновлення їхнього алгоритмічно-програмного забезпечення. Саме SDN-контролери, які належать до площини управління, мають забезпечити моніторинг, збір та аналіз такої інформації про стан мережі:

- топологічні дані, що містять інформацію про кількість маршрутизаторів та каналів зв'язку між ними, яка використовується у формалізації умов збереження потоку;

- параметри маршрутизаторів та каналів зв'язку, до яких належить інформація про їхню пропускну здатність, завантаженість, імовірні вразливості, а також про активність зловмисників, інтенсивність мережних атак та їхню

результативність для обчислення ймовірності компрометації елементів ТКМ, ризиків інформаційної безпеки та збитків від реалізації тієї чи іншої вразливості;

- статистичні дані про надійність і відмови мережного (комутаційного, серверного) обладнання з метою визначення типу схеми захисту (каналу, вузла, маршруту), яку необхідно реалізувати в поточний момент часу;

- характеристики інформаційних потоків, що надходять у мережу. Ці характеристики містять дані про вимоги щодо рівня якості обслуговування, середні інтенсивності (швидкості передачі), IP-пріоритети та рівня інформаційної безпеки, які впливають на розрахунок маршрутних метрик, визначення значень керуючих параметрів у моделях блокування каналів зв’язку та вагових коефіцієнтів, що визначають порядок диференційованого обмеження трафіку в процесі перевантаження ТКМ.

На підставі аналізу інформації про стан ТКМ на SDN-контролері оцінюються параметри, пов’язані з надійністю та мережною безпекою, значення яких визначають вибір

- схем захисту елементів ТКМ та її пропускної здатності (4.4)–(4.9);

- сценарію компрометації елементів мережі та ТКМ загалом (табл. 3.1);

- моделі блокування каналів зв’язку (3.9)–(3.13) у процесі реалізації безпечної маршрутизації з балансуванням навантаження;

- базових метрик критичності вразливостей під час реалізації моделі безпечної маршрутизації (2.1)–(2.12).

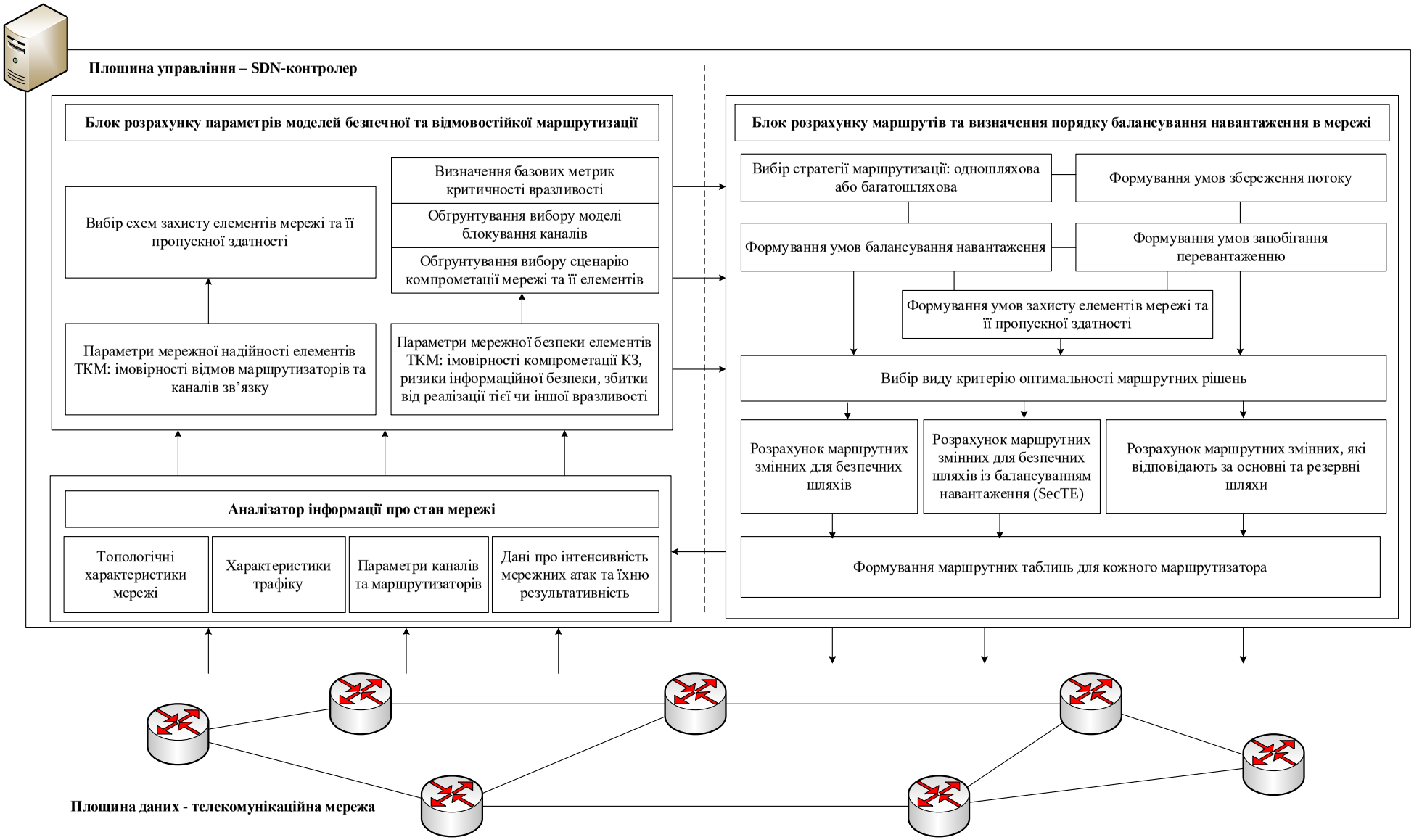


Рис. 4.14. Функціональна архітектура SDN-контролера, розширена під впровадження запропонованих у роботі моделей безпечної та відмовостійкої маршрутизації

На основі обраних параметрів моделі формалізуються умови реалізації одно- або багатошляхової маршрутизації, збереження потоку та балансування навантаження, а також захисту елементів ТКМ та її пропускної здатності.

Відповідно до вимог щодо рівня QoS, відмовостійкості та мережної безпеки обирається вид критерію оптимальності, згідно з яким відбувається розрахунок маршрутних змінних. Саме ці змінні визначають множину розрахованих шляхів (основних та резервних) та порядок балансування навантаження вздовж них. Маршрутні змінні об’єднуються у відповідні маршрутні таблиці та надсилаються на кожен із маршрутизаторів ТКМ для організації пересилання пакетів від маршрутизатора-джерела до маршрутизатора-отримувача пакетів із заданими показниками мережної безпеки та відмовостійкості.

Загалом варто зазначити, що практична реалізація розроблених потокових моделей безпечної та відмовостійкої маршрутизації з балансуванням навантаження не пов’язана з докорінним переглядом принципів побудови й функціонування наявних програмно-конфігурованих ТКМ, а може бути представлена програмно-алгоритмічною надбудовою, завдяки використанню якої дані мережі зможуть більшою мірою відповідати вимогам сучасної концепції щодо побудови та функціонування кіберстійких програмно-конфігурованих телекомунікаційних мереж.

4.4. Висновки до четвертого розділу

1. Розроблено математичну модель швидкої перемаршрутизації з балансуванням навантаження на принципах ТЕ та диференційованим обмеженням трафіку в ТКМ (4.1)–(4.16). Основу моделі становлять умови реалізації багатошляхової маршрутизації (4.1), модифіковані умови збереження потоку (4.2), (4.3), які враховують пріоритетне обмеження трафіку на границі мережі у випадку її ймовірного перевантаження, викликаного, з одного боку, зростанням навантаження, а з іншого, – реалізацією схем захисту елементів

мережі та її пропускної здатності в процесі швидкої перемаршрутизації. У роботі під нові вимоги адаптовані умови забезпечення захисту (резервування) вузла, каналу (4.4)–(4.6) та пропускної здатності мережі (4.7)–(4.9).

2. Перевагою запропонованого рішення також є формулювання технологічної задачі швидкої перемаршрутизації як оптимізаційної задачі з критеріями оптимальності, що були представлені в лінійній (4.13) та лінійно-квадратичній формі (4.14). Використання лінійного критерію оптимальності (4.13) орієнтує на мінімізацію, по-перше, верхнього динамічно керованого порогу завантаженості каналів зв'язку α, що відповідає вимогам концепції ТЕ, а по-друге, відмов в обслуговуванні на границі мережі, зважених щодо IP-пріоритету та інтенсивності потоків. Використання лінійно-квадратичного критерію оптимальності (4.13) дає змогу запровадити справедливий режим обмеження трафіку на основі відносних пріоритетів. Це проявляється в тому, що в умовах перевантаження мережі обмеження трафіку буде збалансованим, тобто потоки з високим пріоритетом будуть обмежені меншою мірою, ніж потоки пакетів з низьким пріоритетом, що загалом унеможливлює ситуацію повного блокування потоків із низьким пріоритетом. Під час пріоритезації потоків, які передаються основним або резервним шляхом (мультишляхом), застосування зазначених критеріїв оптимальності (4.13) та (4.14) відбувалося з виконанням умови (4.15).

3. Обмеженнями в процесі оптимізації були умови реалізації багатошляхової маршрутизації (4.1), збереження потоку (4.2), (4.3), а також захисту каналу (4.4), вузла (4.6) та пропускної здатності мережі (4.9). Лінійність сформульованої оптимізаційної задачі забезпечувалася деяким розширенням числа керуючих змінних (4.10), (4.11), які визначали верхній поріг для маршрутних змінних основного та резервного шляхів. Використання запропонованого підходу дозволяє знизити обчислювальну складність розрахунку маршрутних змінних, що відповідають за формування основного та резервного шляхів. Крім того, забезпечується збалансована завантаженість каналів зв'язку мережі, що відповідає вимогам концепції Traffic Engineering.

4. Дослідження процесів швидкої перемаршрутизації з використанням запропонованої моделі (4.1)–(4.16) на декількох числових прикладах (рис. 4.1–4.3) підтвердило адекватність та ефективність отриманих на її основі маршрутних рішень як щодо забезпечення їхньої відмовостійкості та балансування навантаження, так і щодо обмеження трафіку. У процесі обмеження трафіку реалізувалися два важливі принципи: по-перше, обмеження насамперед стосувалися того потоку, який є джерелом перевантаження за умовою (4.12); по-друге, якщо перевантаження створювали декілька потоків, то обмеження стосувалися потоку з меншим пріоритетом відповідно до умов (4.15).

5. Сформульовано та вирішено завдання, пов’язане з розробленням і дослідженням потокової моделі безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеження трафіку. У межах цієї моделі завдання безпечної швидкої перемаршрутизації було представлено у вигляді задачі лінійного програмування, коли критерієм була умова (4.13), а обмеженнями були вирази (4.1)–(4.4), (4.6), (4.9)–(4.12).

6. Удосконаленням моделі є модифікація умов балансування навантаження та захисту пропускної здатності під час швидкої перемаршрутизації (4.18), у яких, окрім QoS-показника пропускної здатності каналу, також враховується ймовірність його компрометації як показника мережної безпеки. Отримані в межах запропонованої моделі маршрутні рішення орієнтовані на зменшення завантаженості каналів зв’язку з високою ймовірністю компрометації шляхом перерозподілу трафіка для передавання пакетів більш безпечними каналами мережі.

7. Запропоноване рішення є компромісним у розв’язанні задач щодо забезпечення якості обслуговування, з одного боку, та підвищення відмовостійкості та мережної безпеки, з іншого. Реалізація схем захисту структурних елементів мережі та її пропускної здатності вимагає введення надлишковості у використання (резервування) мережного ресурсу. Урахування показників мережної безпеки в моделі (4.1)–(4.8), (4.10)–(4.16), (4.18), (4.20) також приводить до недозавантаженості найбільш небезпечних каналів зв’язку

відповідно до їхньої ймовірності компрометації. Оскільки обсяги мережного ресурсу завжди обмежені, то ці заходи можуть спричинити перевантаження мережі, що супроводжується обмеженням навантаження на її границі. Перевагою запропонованого рішення є те, що в умовах перевантаження реалізується балансування навантаження на принципах ТЕ та за необхідності диференційоване обмеження навантаження, яке надходить в мережу, відповідно до значень класу обслуговування потоку: його IP-пріоритету, інтенсивності потоків та рівня безпеки. Додатковою перевагою запропонованої оптимізаційної моделі безпечної швидкої перемаршрутизації є її лінійність, що орієнтує на невисоку обчислювальну складність її протокольної реалізації на практиці.

8. У розділі запропоновані рекомендації щодо практичного використання запропонованих у роботі моделей безпечної та відмовостійкої маршрутизації в програмно-конфігурованих телекомунікаційних мережах. Рекомендації стосуються модифікації алгоритмічно-програмного забезпечення SDN-контролерів, на які покладаються функції щодо збору та аналізу інформації про стан ТКМ, а також розв’язання сформульованих у розділах оптимізаційних задач щодо розрахунку маршрутних змінних, які становлять основу маршрутних таблиць для маршрутизаторів ТКМ (площини даних).

ВИСНОВКИ З РОБОТИ

У дисертації вирішено актуальну науково-прикладну задачу, що полягає в забезпеченні відмовостійкості та мережної безпеки в програмно-конфігурованих ТКМ, які функціонують в умовах відмов та компрометації мережного обладнання, шляхом розроблення та вдосконалення відповідних математичних моделей маршрутизації. За результатами вирішення задачі можна зробити висновки.

1. Унаслідок проведеного аналізу встановлено, що важливим технологічним інструментом підвищення рівня безпеки та відмовостійкості ТКМ в умовах можливих збоїв в апаратному чи програмному забезпеченні мережного обладнання, перевантаження або порушення рівня інформаційної безпеки є протоколи маршрутизації. Зазначено, що підвищення ефективності рішень щодо безпечної та відмовостійкої маршрутизації, як правило, потребує відповідного вдосконалення наявних та розроблення нових математичних моделей і методів на основі адекватного врахування інформації про стан ТКМ: топології мережі, характеристик потоків пакетів, пропускної здатності каналів зв’язку та показників мережної безпеки елементів (вузлів та каналів).

2. Удосконалено потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Новизна розробленої моделі полягає в тому, що для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв’язку ТКМ та відповідно до рекомендацій NIST CVSS v.3 враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку реалізації наявних вразливостей; беруть до уваги показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів і мережі загалом унаслідок реалізації зазначених вразливостей. Як показали результати проведеного дослідження, використання запропонованої моделі безпечної маршрутизації дозволяє розраховувати та використовувати

маршрути з мінімальним ризиком інформаційної безпеки, тим самим забезпечуючи максимальний рівень мережної безпеки пакетам, які передаються в ТКМ. Запропонований підхід до формування маршрутних метрик може бути застосований також під час забезпечення комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування. До перспектив розвитку отриманих рішень належать синтез моделей і методів безпечної маршрутизації, за допомогою яких вдалося б гарантувати заданий рівень мережної безпеки на підставі розрахунку й використання відповідних маршрутів у ТКМ.

3. Удосконалено потокову модель безпечної маршрутизації з балансуванням навантаження на основі врахування параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах. До новизни запропонованої моделі належать модифікація умов балансування навантаження в ТКМ, які орієнтують на мінімізацію верхнього динамічно керованого порогу завантаженості каналів зв'язку, зваженого щодо ймовірності їхньої компрометації; використання множини моделей блокування каналів зв'язку, за допомогою яких можна регулювати вплив імовірності компрометації каналів на поріг їхньої завантаженості. Відповідно до результатів дослідження, отримані за допомогою запропонованої моделі маршрутні рішення враховують як пропускну здатність каналів зв'язку, так і їхні параметри безпеки, представлені ймовірностями компрометації під час визначення порядку балансування навантаження. Результати дослідження процесів безпечної маршрутизації з балансуванням навантаження в ТКМ підтвердили її ефективність щодо врахування стану ТКМ: її топології, характеристик потоків, пропускної здатності та завантаженості каналів зв'язку, а також імовірностей їхньої компрометації. Це дозволило спрямувати отримані маршрутні рішення на зменшення завантаженості каналів зв'язку, які мають високу ймовірність компрометації, шляхом перерозподілу трафіку на більш безпечні канали. Зазвичай інтенсивніше

завантажувалися ті канали, які мали високу пропускну здатність і низьку ймовірність компрометації.

4. Уперше запропоновано модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіку в програмно-конфігурованих телекомунікаційних мережах. Новизна моделі полягає в тому, що, по-перше, модифіковано умови збереження потоку, які враховують пріоритетне обмеження трафіку на границі ТКМ у випадку її ймовірного перевантаження, викликаного, з одного боку, зростанням навантаження, а з іншого, – реалізацією схем захисту елементів мережі та її пропускної здатності під час швидкої перемаршрутизації; а по-друге, запропоновано систему критеріїв оптимальності маршрутних рішень, використання яких орієнтує на мінімізацію верхнього порогу завантаженості каналів зв’язку та відмов в обслуговуванні на границі мережі, зважених щодо пріоритету та інтенсивності потоків, з метою запобігання її перевантаження. Перевагою запропонованого рішення є те, що в процесі обмеження трафіку реалізувалися два важливі принципи: по-перше, обмеження насамперед стосувалися того потоку, який є джерелом перевантаження; по-друге, якщо перевантаження створювали декілька потоків, то обмеження стосувалися потоку з меншим пріоритетом.

5. Удосконалено потокову модель безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку на границі ТКМ. Новизна моделі полягає в забезпеченні захисту елементів (вузлів, каналів, маршрутів) мережі та її пропускної здатності в процесі реалізації швидкої перемаршрутизації на основі врахування під час балансування навантаження в каналах зв’язку ймовірності їхньої компрометації, а в разі диференційованого обмеження трафіку на границі ТКМ – вимог потоків пакетів щодо рівня мережної безпеки. Отримані внаслідок удосконалення запропонованої моделі маршрутні рішення орієнтовані на зменшення завантаженості каналів зв’язку з високою

ймовірністю компрометації шляхом перерозподілу трафіку для передавання пакетів більш безпечними каналами мережі. Перевагою запропонованого рішення є те, що в умовах перевантаження реалізується балансування навантаження на принципах ТЕ та за необхідності диференційоване обмеження навантаження, яке надходить в мережу, відповідно до значень класу обслуговування потоку: його IP-пріоритету, інтенсивності потоків та рівня безпеки. Додатковою перевагою запропонованої оптимізаційної моделі безпечної швидкої перемаршрутизації є її лінійність, що орієнтує на невисоку обчислювальну складність її протокольної реалізації на практиці.

6. Розроблено рекомендації щодо практичного використання запропонованих у роботі моделей безпечної та відмовостійкої маршрутизації в програмно-конфігурованих телекомунікаційних мережах, які спрямовані на модифікацію алгоритмічно-програмного забезпечення SDN-контролерів. Отримані в роботі наукові результати орієнтують на централізацію маршрутних рішень, що мають синтезуватися на SDN-контролерах та забезпечувати ефективне розв’язання задач маршрутизації/перемаршрутизації, балансування навантаження та диференційованого обмеження трафіку на границі мережі, представленою площиною даних. Практична реалізація розроблених рішень може бути подана у вигляді програмно-алгоритмічної надбудови, завдяки використанню якої вдасться забезпечити відмовостійкість та мережну безпеку програмно-конфігурованих телекомунікаційних мереж.

7. Отримані в дисертаційній роботі результати були використані в навчальному процесі ХНУРЕ, а також на підприємстві «ХДРНТЦ ТЗІ», у ТОВ «Воркнест» та ПрАТ «Фарлеп-Інвест», про що складені відповідні акти впровадження (додаток А).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 181 p.

2. Vidal I., Soto I., Banchs A., Garcia-Reinoso J., Lozano I., Camarillo G. Multimedia Networking Technologies, Protocols, & Architectures (Artech House Communications and Network Engineering), 1st edition, Artech House, 2019. 300 p.

3. Blokdyk G. Software-Defined Networking SDN production, 1st edition. 5STARCooks, 2019. 238 p.

4. Medhi D., Ramasamy K. Network Routing (Algorithms, Protocols, and Architectures), 2nd edition, Elsevier Inc, 2018. 1018 p.

5. Chapman C. Network Performance and Security (Testing and Analyzing Using Open Source and Low-Cost Tools), 1st edition, Syngress, 2016. 380 p.

6. Edgar T., Manz D. Research Methods for Cyber Security, 1st edition. Syngress, 2017. 428 p.

7. Стрелковська І. В., Соловська І. М. Маршрутизація в мережі MPLS-TE з додатковими напрямками передавання трафіку. *Зв'язок*. 2015. № 1. С. 25–30.

8. Лемешко О. В., Єременко О. С. Розробка та дослідження лінійної оптимізаційної моделі швидкої перемаршрутизації з балансуванням навантаження в телекомунікаційних мережах. *Радиоэлектроника и информатика*. 2017. № 4 (79). С. 18–25.

9. Lemeshko O. V., Arous K. M., Yeremenko O. S. Fault-Tolerant Unicast, Multicast and Broadcast Routing Flow-based Models. *Scholars Journal of Engineering and Technology (SJET)*. Vol. 3. Iss. 4A. 2015. P. 343–350.

10. Lemeshko O., Yeremenko O., Yevdokymenko M. MPLS Traffic Engineering Solution of Multipath Fast ReRoute with Local and Bandwidth Protection. Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in

INTELLIGENT Systems and Computing, Springer, Cham. Vol. 938. 2019. P. 113–125. DOI: 10.1007/978-3-030-16621-2_11.

11. Лемешко О. В., Євдокименко М. О. Вдосконалення потокової моделі маршрутизації в мультисервісній телекомунікаційній мережі із забезпеченням якості обслуговування. *Системи озброєння і військова техніка*. 2020. № 1(61). С. 31–43. DOI: 10.30748/soivt.2020.61.04.

12. Еременко А. С. Двухуровневый метод иерархическо-координационной QoS-маршрутизации на основе резервирования ресурсов. *Радиотехника*. 2018. Вып. 192. С. 71–83.

13. Чевардін В. Є., Романюк В. А., Шевченко В. С. Модель загроз безпеки інформації в сучасних телекомунікаційних мережах з динамічною топологією. *Збірник наукових праць ВІТІ НТУУ «КПІ»*. 2012. №2. С. 90–95.

14. ISO/IEC 27001:2013. Информационные технологии – Методы защиты – Системы менеджмента информационной безопасности – Требования. Международный Стандарт. Вторая редакция . 2013. 19 с.

15. Yeremenko O., Lemeshko O., Persikov A. Secure Routing in Reliable Networks: Proactive and Reactive Approach. Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, Springer, Cham. Vol. 689. 2018. P. 631–655. DOI: 10.1007/978-3-319-70581-1_44.

16. Yevdokymenko M., Manasse M., Zalushniy D., Sleiman B. Analysis of Methods for Assessing the Reliability and Security of Infocommunication Network, *Problems of Infocommunications Science and Technology (PIC S&T)*: Proceedings of the Fourth International Scientific-Practical Conference, Kharkov, Ukraine, 10–13 October, 2017. P. 199–202. DOI: 10.1109/INFOCOMMST.2017.8246379.

17. Kuzminykh I., Yevdokymenko M. Analysis of Security of Rootkit Detection Methods, *Advanced Trends in Information Theory (ATIT):* Proceedings of the International Conference, Kyiv, Ukraine. IEEE, 2019. P. 196–199. DOI: 10.1109/ATIT49449.2019.9030428.

18. Managing Cyber Risk (Transform your security with cyber resilience): IT covernance/Green paper, United Kingdom, 2019. 12 p.

19. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків, ХНУРЕ. 2020. 308 с.

20. Dobush Yu., Demydov I. Approach to Secure Distributed Data Storing by QuasiRandom FAT Network Mapping. *International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science*: Proceedings of the International Conference. Lviv, Ukraine, 2012. P. 335-335.

21. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: http://zakon3.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення: 14.03.2018).

22. Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України»: Постанова Верховної Ради України від 31.03.2016. № 1073-VIII. *Відомості Верховної Ради* . 2016. № 17, 191 с.

23. Про схвалення Концепції розвитку телекомунікацій в Україні та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 07.06.2006 р. № 316-р. URL: https://zakon.rada.gov.ua/laws/show/316-2006-%D1%80.

24. Про схвалення Стратегії національної безпеки України: Рішення ради національної безпеки і оборони України від 14.09.2020 р. № 932/2020. URL: https://zakon.rada.gov.ua/laws/show/n0005525-20.

25. Про схвалення Концепції державної політики у сфері цифрової інфраструктури: Бачення Міністерства цифрової трансформації України, грудень 2019 р.

26. Методичні рекомендації для представників закладів вищої освіти та інших партнерів проєктів Програми ЄС Еразмус+: Розвиток потенціалу вищої освіти (СВНЕ), щодо особливостей впровадження проєктів в Україні, лютий 2021 р.

27. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації від 03.03.2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80.

28. Carlsson A., Duravkin E. V., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 1. Features of realization of low-intensity HTTP attacks. *Проблеми телекомунікацій.* 2013. № 3 (13). С. 61–70. URL: http://pt.nure.ua/wp-content/uploads/2020/01/133_carlsson_attack.pdf.

29. Duravkin E. V., Carlsson A., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. Method of detecting Slow HTTP attacks. *Проблеми телекомунікацій*. 2014. № 1 (14). С. 96–100. URL: http://pt.nure.ua/wp-content/uploads/2020/01/141_carlsson_attack.pdf.

30. Duravkin E. V., Carlsson A., Loktionova A. S. Method of slow-attack detection. *Системи обробки інформації.* 2014. № 8. С. 102–106.

31. Євдокименко М. О., Шаповалова А. С. Метод оцінювання впливу атак на інфокомунікаційну мережу з урахуванням наявних вразливостей. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. 2018. Т. 29 (68). № 4. С. 67–72.

32. Yevdokymenko M. O., Shapovalova A. S., Nevzorova O. S. Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability Assessment. *International Journal of Science and Engineering Investigations*. Vol. 8(91). 2019. P. 167–173. URL: http://www.ijsei.com/papers/ijsei-89119-22.pdf.

33. Лемешко О. В., Шаповалова А. С., Єременко О. С., Євдокименко М. О., Хайлан А. М. Математична модель швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіка в мережах SD-WAN.

Системи управління, навігації та зв'язку. 2019. № 4 (56). С. 63–71. DOI: 10.26906/SUNZ.2019.4.063.

34. Lemeshko O., Yevdokymenko M., Yeremenko O., Shapovalova A., Hu Z., Petoukhov S., Dychka I., He M. Investigation of Load-Balancing Fast ReRouting Model with Providing Fair Priority-Based Traffic Policing. Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing. Springer, Cham. Vol. 1247. 2020. P. 108–119. DOI: 10.1007/978-3-030-55506-1_10 (SCOPUS).

35. Lemeshko O., Shapovalova A., Al-Dulaimi A. M. K., Yeremenko O., Yevdokymenko M. Flow-Based Routing Model With Load Balancing Under Network Security Parameters. *Information and Telecommunication Sciences*. 2020. No 2. P. 44–50. DOI: 10.20535/2411-2976.22020.44-50.

36. Євдокименко М. О., Шаповалова А. С., Шаповал М. М. Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. *Проблеми телекомунікацій*. 2020. № 1(26). С. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.

37. Локтіонова А. С. Оцінка економічної доцільності впровадження системи менеджменту інформаційної безпеки. *Інформаційні технології в сучасному світі: дослідження молодих вчених*. *Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів*. Харків. 2013. С. 68.

38. Duravkin I., Loktionova A., Carlsson A. Method of slow-attack detection. *Problems of Infocommunications Science and Technology (PIC S&T):* Proceedings of the First International Scientific-Practical Conference, Kharkov, Ukraine, 2014. IEEE, 2014. P. 171–172. DOI: 10.1109/INFOCOMMST.2014.6992341.

39. Yevdokymenko M., Shapovalova A., Voloshchuk O., Carlsson A. Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment. *Problems of Infocommunications Science and Technology (PIC S&T):*

Proceedings of the Fifth International Scientific-Practical Conference, Kharkov, Ukraine, 9–12 October 2018. IEEE, 2018. P. 609–612. DOI: 10.1109/INFOCOMMST.2018.8632079. (SCOPUS).

40. Lemeshko O. V., Yeremenko O. S., Yevdokymenko M. O., Shapovalova A. S. Advanced solution of the Fast ReRoute based on principles of Traffic Engineering and Traffic Policing. *Science and Technology (AVIA-2019):* Proceedings of the Fourteenth International Conference, Ukraine, 23–25 April 2019. P. 8.21–8.23.

41. Єременко О. С., Євдокименко М. О., Шаповалова А. С. Підвищення відмовостійкості мереж засобами швидкої перемаршрутизації з балансуванням навантаження та профілюванням трафіка. *Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології»:* збірник наукових праць. Харків: ХНУРЕ. 2019. С. 131.

42. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Ilyashenko A., Sleiman B. Traffic Engineering Fast ReRoute Model with Support of Policing. *Electrical and Computer Engineering (UKRCON):* Proceedings of the 2nd International Conference, Lviv, Ukraine, 2–6 July 2019. IEEE. 2019. P. 842–845. DOI: 10.1109/UKRCON.2019.8880006. (SCOPUS).

43. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Hailan A. M., Mersni A. Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS):* Proceedings of the 10th IEEE International Conference, Metz, France, 2019. IEEE, 2019. P. 117–122. DOI: 10.1109/IDAACS.2019.8924294. (SCOPUS).

44. Yevdokymenko M., Shapovalova A. Investigation of the Impact of HTTP DoS Attacks on the Cloud Web Server. *Natural science and technology (ICONAT)*: Proceedings of the International conference, Kharkiv, 2019. P. 25.

45. Lemeshko O., Yeremenko O., Hailan A. M., Yevdokymenko M., Shapovalova A. Al-Bakry A. Policing Based Traffic Engineering Fast ReRoute in SD-WAN

Architectures: Approach Development and Investigation. *New Trends in Information and Communications Technology Applications. (NTICT):* Proceedings of the 4th International Conference. Springer, Cham. Vol. 1183. 2020. P. 29–43. DOI: 10.1007/978-3-030-55340-1_3. (SCOPUS).

46. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Radivilova T., Ageyev D. Secure Based Traffic Engineering Model in Softwarized Networks. *Advanced Trends in Information Theory (ATIT):* Proceedings of the IEEE International Conference, Kyiv. 2020. P. 143–147. DOI: 10.1109/ATIT50783.2020.9349301. (SCOPUS).

47. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing cyber resilient systems: a systems security engineering approach. NIST Special Publication (SP) 800–160 Vol. 2 (Draft). National Institute of Standards and Technology, November 2019. DOI: 10.6028/NIST.SP.800-160v2.

48. Linkov I., Kott A. Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, Springer, Cham, 2019. P. 1–25.

49. Galinec D., Steingartner W. Combining cybersecurity and cyber defense to achieve cyber resilience. *International Scientific Conference on Informatics (ISCI)*: Proceedings of the IEEE 14th International Conference, November 2017. P. 87–93.

50. Radack S. M. Joint Task Force Transformation Initiative. Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication (SP) 800–39, National Institute of Standards and Technology, Gaithersburg, MD, 2011. DOI: 10.6028/NIST.SP.800-39.

51. Dickson F., Goodwin P. Five key technologies for enabling a Cyber-resilience framework. US45455119, IBM, White Paper, October 2020. 16 p.

52. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience–fundamentals for a definition. New contributions in information systems and technologies, Springer, Cham, 2015. P. 311–316.

53. Haque M. A., De Teyou G.K., Shetty S., Krishnappa B. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights. *International Conference on Intelligence and Security Informatics (ISI*): Proceedings of the International Conference, 9-11 Nov. 2018. P. 25–30.

54. Kotenko I., Saenko I., Lauta O. Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion. *Resilient Networks Design and Modeling (RNDM):* Proceedings of the 10th International Workshop, 27-29 Aug. 2018. P. 1–8.

55. Fink G. A., Griswold R. L., Beech Z. W. Quantifying cyber-resilience against resource-exhaustion attacks. *International Symposium on Resilient Control Systems (ISRCS):* Proceedings of the 2014 7th International Symposium, 19-21 Aug. 2014. P. 1–8.

56. Musman S. Assessing prescriptive improvements to a system`s cyber security and resilience. *Systems Conference (SysCon)*: Proceedings of the 2016 Annual IEEE Conference, 18-21 April 2016. P. 1–6.

57. Jacobs N., Hossain-McKenzie S., Vugrin E. Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example. *Resilience Week (RWS)*: Proceedings of the Conference, 20-23 Aug. 2018. P. 38–46.

58. Hossain-McKenzie S., Lai C., Chavez A., Vugrin E. Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense. *Industrial Electronics Socie*ty (*IECON)*: Proceedings of the 2018 44th Annual Conference, 21-23 Oct. 2018. P. 766–773.

59. Machado C. C., Granville L. Z., Schaeffer-Filho A. ANSwer: Combining NFV and SDN features for network resilience strategies. *IEEE Symposium on Computers and Communication (ISCC)*: Proceedings of the Symposium, 27-30 June 2016. P. 391–396.

60. Azab M., Fortes J. A. Towards proactive SDN-controller attack and failure resilience. *International Conference on Computing, Networking and Communications*

(ICNC): Proceedings of the 2017 International Conference, 26-29 Jan. 2017. P. 442–448.

61. Rehman A. U., Aguiar R. L., Barraca J. P. Fault-Tolerance in the Scope of Software-Defined Networking (SDN). *IEEE Access*, Vol. 7. 2019. P. 124474–124490, DOI: 10.1109/ACCESS.2019.2939115.

62. Fonseca P. C., Mota E. S. A Survey on Fault Management in Software-Defined Networks. *IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS):* Proceedings of the International Conference. Vol. 19. 2017. No. 4. P. 2284–2321. DOI: 10.1109/COMST.2017.2719862.

63. Yu Y., Li X., LenX. G., Song L., Bu K., Chen Y., Yang J., Zhang, L. K., Cheng Xiao X. Fault management in software-defined networking. *IEEE Communications Surveys & Tutorials*, Vol. 21. 2019. No. 1. P. 349–392. DOI: 10.1109/COMST.2018.2868922.

64. Da Silva A. S., Smith P., Mauthe A., Schaeffer-Filho A. Resilience support in software-defined networking. *Computer Networks,* Vol. 92. 2015. P. 189–207. DOI: 10.1016/j.comnet.2015.09.012I.

65. Chen J., Xu F., Yin M., Zhang W., Survey A., Wang G., Zomaya A., Martinez G., Li K. When Software Defined Networks Meet Fault Tolerance. Algorithms and Architectures for Parallel Processing. ICA3PP, 2015. Lecture Notes in Computer Science. Springer, Cham. Vol. 9530. 2015. P. 351–368. DOI:10.1007/978-3-319-27137-8_27.

66. Katz D., Ward D. Bidirectional forwarding detection (BFD). Internet Requests for Comments, RFC Editor, RFC 5880. June 2010. URL: https://www.rfc-editor.org/rfc/pdfrfc/rfc5880.txt.pdf.

67. Staessens D., Sharma S., Colle D., Pickavet M., Demeester P. Software defined networking: Meeting carrier grade requirements. *Local & Metropolitan Area Networks (LANMAN)*: Proceedings on the 18th IEEE Workshop, Chapel Hill, NC, USA, 2011. P. 1–6. DOI: 10.1109/LANMAN.2011.6076935.

68. Adrichem N. L. M., Van Asten B. J., Kuipers F. A. Fast Recovery in Software-Defined Networks. Third European Workshop on *Software Defined Networks*, Budapest, Hungary, 2014. P. 61–66. DOI: 10.1109/EWSDN.2014.13.

69. Sharma S., Staessens D., Colle D., Pickavet M., Demeester P. Fast failure recovery for in-band OpenFlow networks. *Design of Reliable Communication Network (DRCN):* Proceedings of the 9th International Conference, Budapest, Hungary, 2013. P. 52–59.

70. Sharma S., Staessens D., Colle D., Pickavet M., Demeester P. In-band control, queuing, and failure recovery functionalities for openflow. *IEEE Network*, Vol. 30. 2016. No. 1. P. 106–112. DOI: 10.1109/MNET.2016.7389839.

71. Mohan P., Truong-Huu M., Gurusamy M. Fault tolerance in TCAM-limited software defined networks. *Computer Networks*, Vol. 116. 2017. P.47–62.

72. Li H., Li Q., Jiang Y., Zhang T., Wang L. A declarative failure recovery system in software defined networks. *IEEE International Conference on Communications Kuala Lumpu (ICC):* Proceedings of the IEEE International Conference, Malaysia, 2016. P. 1–6. DOI: 10.1109/ICC.2016.7510887.

73. Kuźniar M., Perešíni P., Vasić N., Canini M., Kostić D. Automatic failure recovery for software-defined networks. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 2013. P. 159–160.

74. Hyojoon K., Schlansker M., Santos J. R., Tourrilhes J., Turner Y., Feamster N. CORONET: Fault tolerance for Software Defined Networks. *International Conference on Network Protocols (ICNP):* Proceedings of the 20th IEEE International Conference, Austin, TX, USA, 2012. P. 1–2. DOI: 10.1109/ICNP.2012.6459938.

75. Schiff L., Schmid S. Canini M. Ground Control to Major Faults: Towards a Fault Tolerant and Adaptive SDN Control Network. *Dependable Systems and Networks Workshop (DSN-W):* Proceedings of the 46th Annual IEEE/IFIP

International Workshop, Toulouse, France, 2016. P. 90–96. DOI: 10.1109/DSN-W.2016.48.

76. Chen J., Ling, Zhang W. Failure recovery using vlan-tag in SDN: High speed with low memory requirement. *International Performance Computing and Communications Conference (IPCCC):* Proceedings of the IEEE 35th International Conference, Las Vegas, NV, USA, 2016. P. 1–9. DOI: 10.1109/PCCC.2016.7820627.

77. Jain S., Kumar A., Mandal S., Ong, J., Poutievski L., Singh A., Venkata S., Wanderer J., Zhou J., Zhu M., Zolla J. B4: Experience with a globally-deployed software defined WAN. *ACM SIGCOMM Computer Communication Review*, Vol. 43(4). 2013. P. 3–14.

78. Greenberg A., Hjalmtysson G., Maltz D. A., Myers A., Rexford J., Xie G., Yan H., Zhan J., Zhang H. A clean slate 4D approach to network control and management. *ACM SIGCOMM Computer Communication Review*, Vol. 35(5). 2005. P. 41–54.

79. Goransson P., Black C., Culver T. Software defined networks: a comprehensive approach. *Morgan Kaufmann*. 2016. 438 p.

80. Segeč P., Moravčik M., Uramova J., Papan J. Yeremenko O. SD-WAN – architecture, functions and benefits. *International Conference on Emerging eLearning Technologies and Applications (ICETA):* Proceedings of the 18th International Conference, Košice, Slovakia, 2020. P. 593–599.

81. Zhang X., Cheng Z., Lin R., He L., Yu S., Luo H. Local fast reroute with flow aggregation in software defined networks. *IEEE Communications Letters*. Vol. 21. 2017. Iss. 4. P.785–788. DOI: 10.1109/LCOMM.2016.2638430.

82. Malik A., Aziz B., Adda M., Ke C. H. Optimisation methods for fast restoration of software-defined networks. *IEEE Access*. Vol. 5. 2017. P. 16111–16123. DOI: 10.1109/ACCESS.2017.2736949.

83. Rzym G., Wajda K., Chołda P. SDN-based WAN optimization: PCE implementation in multi-domain MPLS networks supported by BGP-LS. *Image Processing & Communications*. Vol. 22. Iss. 1. 2017. P. 35–48. DOI: 10.1515/ipc-2017-0004.

84. Luo M., Zeng Y., Li J., Chou W. An adaptive multi-path computation framework for centrally controlled networks. *Computer Networks*, Vol. 83. 2015. P. 30–44. DOI: 10.1016/j.comnet.2015.02.004.

85. Lemeshko O., Arous K., Tariki N. Effective solution for scalability and productivity improvement in fault-tolerant routing. *Problems of Infocommunications Science and Technology (PIC S&T)*. Proceedings of the Second International Conference , 2015. P. 76–78. DOI: 10.1109/INFOCOMMST.2015.7357274.

86. Lemeshko O., Yeremenko O., Yevdokymenko M. MPLS Traffic Engineering Solution of Multipath Fast ReRoute with Local and Bandwidth Protection In: Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, Springer, Vol. 938. 2019. P. 113–125.

87. Lemeshko O. V., Garkusha S. V., Yeremenko O. S., Hailan A. M. Policy-based QoS Management Model for Multiservice Networks. *International Siberian Conference on Control and Communications*. *(SIBCON):* Proceedings of the International Conference. IEEE, 2015. P. 1–4. DOI: 10.1109/SIBCON.2015.7147124.

88. Lemeshko A. V., Evseeva O. Y., Garkusha S. V. Research on tensor model of multipath routing in telecommunication network with support of service quality by greate number of indices. *Telecommun. Radio Engineering*. Vol. 73. 2014. Iss. 15. P. 1339–1360. DOI: 10.1615/TelecomRadEng.v73.i15.30.

89. Medhi D., Ramasamy K. Network Routing, Second Edition: Algorithms, Protocols, and Architectures. The Morgan Kaufmann Series in Networking, 2nd Edition, Cambridge, MA, USA, Elsevier Inc. 2018. 1018 p.

90. Govindasamy J., Punniakody S. A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. *Electrical Systems and Information Technology*, 2018. No. l 5(3). P. 735–744. DOI: 10.1016/j.jesit.2017.02.002.

91. Wadhwani G. K., Khatri S. K., Muttoo S. K. Critical Evaluation of Secure Routing Protocols for MANET, *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*: Proceedings of the International Conference, Greater Noida, India, 2018. P. 202–206. DOI: 10.1109/ICACCCN.2018.8748725.

92. Merkle R. C., Pomerance C. A digital signature based on a conventional encryption function. *Advances in Cryptology CRYPTO*. Lecture Notes in Computer Science, No. 293, Springer, Berlin, Heidelberg, 1987. P. 369–378. DOI: 10.1007/3-540-48184-2_32.

93. Shashikala R., Kavitha C. Secured data integrity routing for Wireless Sensor Networks, *International Conference on Advances in Electronics Computers and Communications (ICAECC):* Proceedings of the International Conference, Bangalore, India, 2014. P. 1–6. DOI: 10.1109/ICAECC.2014.7002419.

94. Khan S., Khan S., Loo J. Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks, *Wireless Personal Communications*, 2012. No. 62. P. 201–214. DOI: 10.1007/s11277-010-0048-y.

95. Aggarwal A., Gandhi S., Chaubey N. Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs, *International Conference on Advanced Computing & Communication Technologies (ACCT):* Proceedings of the Fourth International Conference, Rohtak, India, 2014. P. 432–438. DOI: 10.1109/ACCT.2014.95.

96. Lou W., Liu W., Fang Y. SPREAD: enhancing data confidentiality in mobile ad hoc networks, *IEEE Computer and Communications Societies* (*INFOCOM):* Proceedings of the International Conference, Hong Kong, China, 2004. No. 4. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.

97. Gu Q., Tilborg H.C.A., Jajodia S. Secure Routing Protocols, Encyclopedia of Cryptography and Security, Springer, Boston, MA, 2011. 690 p. DOI: 10.1007/978-1-4419-5906-5_641.

98. Lemeshko O., Yeremenko O., Sleiman B., Yevdokymenko M. Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in SDN, Advances in Electrical and Electronic Engineering, 2020. No. 18(1). P. 23–30. DOI: 10.15598/aeee.v18i1.3548.

99. Lemeshko O., Yevdokymenko M., Yeremenko O. Radivilova T., Ageyev D., Kryvinska N. Fast ReRoute Tensor Model with Quality of Service Protection Under Multiple Parameters, Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, Springer, Cham, 2020. No. 48. P. 489–512. DOI:10.1007/978-3-030-43070-2_22.

100. Diwan D., Narang V. K., Singh A. K. Security Mechanism in RIPv2, EIGRP and OSPF for Campus Network, *Computer Science Trends and Technology,* 2017. No. 5(2). P. 399–404.

101. Snihurov A., Chakrian V. Improvement of EIGRP Protocol Routing Algorithm Based on Information Security Metrics. *International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T-2015):* Proceedings of the Second International Conference, Kharkiv, 2015. P. 263–265. DOI: 10.1109/INFOCOMMST.2015.7357331.

102. Bhatia M., Hartman S., Zhang D. Security Extension for OSPFv2 When Using Manual Key Management, RFC 7474, 2015. URL: https:// tools.ietf.org/html/rfc7474.

103. Wang M., Liu J., Mao J., Cheng H., Chen J., Qi C. Route Guardian: Constructing secure routing paths in software-defined networking, Tsinghua Science and Technology, Vol. 22. 2017. No. 4. P. 400–412. DOI: 10.23919/TST.2017.7986943.

104. Li J., Yang Z., Yi X., Hong T., Wang X. A Secure Routing Mechanism for Industrial Wireless Networks Based on SDN, *International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*: Proceedings of the 14th International Conference, China, 2018. P. 158–164. DOI: 10.1109/MSN.2018.000-2.

105. Ellinidou S., Sharma G., Rigas T., Vanspouwen T., Markowitch O., Dricot J.M. SSPSoC: A secure SDN-based protocol over MPSoC. *Security and Communication Networks*, 2019. P. 1–12. DOI: 10.1155/2019/4869167.

106. Sagare A. A., Khondoker R. Security Analysis of SDN Routing Applications, SDN and NFV Security, Lecture Notes in Networks and Systems, Springer, Cham, Vol. 30. 2018. P.1–17. DOI: 10.1007/978-3-319-71761-6_1.

107. Scarfone K., Scarfone K., Mell P. NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)., National Institute of Standards and Technology, 2012. URL: http://csrc.nist.gov/publications/drafts/800-94- rev1/draft_sp800-94-rev1.pdf.

108. Лемешко А. В., Вавенко Т. В. Анализ решений задач однопутевой и многопутевой маршрутизации многопотокового трафика в телекоммуникационных сетях. *Системи обробки інформації*, 2011. № 8. С. 224–228.

109. Scarfone K., Scarfone K., Mell P., NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)., National Institute of Standards and Technology, 2012. URL: http://csrc.nist.gov/publications/drafts/800-94- rev1/draft_sp800-94-rev1.pdf.

110. Pattanavichai S. Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer *(MBSA), International Conference on ICT and Knowledge Engineering (ICT&KE): Proceedings of the* 15th, International Conference, Bangkok, 2017. P. 1–7. DOI: 10.1109/ICTKE.2017.8259628.

111. Chimmanee S., Veeraprasit T., Srisa-An C. A Performance Evaluation of Vulnerability Detection: NetClarity Audito Nessus and Retina, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 14. 2014. No. 3. P. 34–40.

112. Denis M., Zena C., Hayajneh T. Penetration testing: Concepts, attack methods, and defense strategies, *Long Island Systems, Applications and Technology Conference (LISAT)*: Proceedings of the Technology Conference, Farmingdale, NY, USA, 2016. P. 1–6. DOI: 10.1109/LISAT.2016.7494156.

113. Mallouli W., Bessayah F., Cavalli A., Benameur A. Security Rules Specification and Analysis Based on Passive Testing, *GLOBECOM IEEE Global Telecommunications Conference (GLOCOM):* Proceedings of the *Telecommunications Conference*, New Orleans, LA, USA, 2008. P. 1–6. DOI: 10.1109/GLOCOM.2008.ECP.400.

114. Liu D. Research on Data Security Analysis and Label Recognition Technology Based on Big Data Business Scenario, *International Conference on Electronics Information and Emergency Communication (ICEIEC)*: Proceedings of 10th International Conference, Beijing, China, 2020. P. 344–347. DOI: 10.1109/ICEIEC49280.2020.9152308.

115. Streilein W., Kratkiewicz K., Sikorski M., Piwowarski K., Webster S. PANEMOTO: Network Visualization of Security Situational Awareness Through Passive Analysis, *SMC Information Assurance and Security Workshop (IAW):* Proceedings of Security Workshop, West Point, NY, USA, 2007. P. 284–290. DOI: 10.1109/IAW.2007.381945.

116. Masys A. Networks and network analysis for defence and security, *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013):* Proceedings of the International Conference, Niagara Falls, ON, Canada, 2013. P. 1479–1480. DOI: 10.1145/2492517.2492602.

117. Sinchana K., Sinchana C., Gururaj H. L., Sunil Kumar, B. R. Performance Evaluation and Analysis of various Network Security tools, *International Conference*

on Communication and Electronics Systems (ICCES): Proceedings of the International Conference, Coimbatore, India, 2019. P. 644–650. DOI: 10.1109/ICCES45898.2019.9002531.

118. Peltier T. R. Information security risk analysis, *CRC press*, 2005. 344 p.

119. ISO/IEC 15408-1:2009. Information technology, Security techniques Evaluation criteria for IT security, Part 1: Introduction and general model. URL: https://www.iso.org/standard/50341.html.

120. COBIT 2019 Framework: Introduction & Methodology, ISACA, 2018. URL: https://www.isaca.org/resources/cobit.

121. COSO Enterprise Risk Management Integrating with Strategy and Performance, 2017. URL: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

122. Common Vulnerability Scoring System v3.0: Examples, Forum of Incident Response and Security Teams, URL: https://www.first.org/cvss/examples.

123. Abedin M., Nessa S., Al-Shaer E., Khan L. Vulnerability analysis For evaluating quality of protection of security policies. *Quality of Protection (QoP)*: Proceedings of the 2nd ACM Workshop, 2006. P. 49–52. DOI: 10.1145/1179494.1179505.

124. Добрышкин Ю. Н. Модель управления трафиком с его превентивным ограничением на основе абсолютных и относительных приоритетов, *Радиотехника*: Всеукр. межвед. науч.- техн. сб. Вып. 156. 2009. С. 13–19.

ДОДАТОК А

АКТИ ВПРОВАДЖЕННЯ

ЗАТВЕРЖУЮ

Перший проректор
Харківського національного
університету радіоелектроніки

д.т.н., професор І.В. Рубан
«25» 05 2021 р.

АКТ

про використання у освітньому процесі результатів дисертаційної роботи Шаповалової Анастасії Сергіївни, представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Комісія у складі:

голови – д.т.н., проф., зав. каф. ІКІ ім. В.В. Поповського, Лемешка О.В.;

членів – д.т.н., проф. каф. ІКІ ім. В.В. Поповського Єременко О.С.;

– к.т.н., доц., проф. каф. ІКІ ім. В.В. Поповського Радівілової Т.А.;

розглянула дисертаційну роботу Шаповалової А.С. та дійшла наступному висновку:

матеріали дисертації використовуються в освітньому процесі Харківського національного університету радіоелектроніки, а саме

- потокова модель безпечної маршрутизації в програмно-конфігурованих телекомунікаційних мережах із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей;
- потокова модель безпечної маршрутизації з балансуванням навантаження та врахуванням параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах;

що є частиною лекційного курсу та курсу практичних занять з дисциплін «Information Security in Information and Communication Systems» та «Control and Routing in Telecommunication Systems» для іноземних студентів першого (бакалаврського) рівня спеціальності 172 – Телекомунікації та радіотехніка.

Голова комісії О.В. Лемешко

Члени комісії О.С. Єременко

Т.А. Радівілова

ЗАТВЕРДЖУЮ
Директор ТОВ «ВОРКНЕСТ»
Колесніков О.К.
«14» січня 2021 р.

АКТ

про використання результатів дисертаційної роботи Шаповалової Анастасії Сергіївни за темою «ПОТОКОВІ МОДЕЛІ БЕЗПЕЧНОЇ ТА ВІДМОВОСТІЙКОЇ МАРШРУТИЗАЦІЇ З БАЛАНСУВАННЯМ НАВАНТАЖЕННЯ В ПРОГРАМНО-КОНФІГУРОВАНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ»,
представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Комісія у складі:

голови: - начальника відділу R&D Колесніков О.К.;

членів: - начальника відділу QA Гонтарь І.А.;

- провідного спеціаліста Вергеліс А.В.;

склала даний акт у тому, що результати дисертаційної роботи Шаповалової А.С., а саме:

- потокова модель безпечної маршрутизації в програмно-конфігурованих телекомунікаційних мережах із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей;
- потокова модель швидкої безпечної перемаршрутизації із балансуванням навантаження та обмеженням трафіку на границі телекомунікаційної мережі;

були використані під час розробки програмного забезпечення для додаткового налаштування мережного обладнання програмно-конфігурованих телекомунікаційних мереж з метою підвищення безпеки та відмовостійкості мережі в цілому.

Голова комісії	(підпис)	Колесніков О.К. (ініціали та прізвище)
Член комісії	(підпис)	Гонтарь І.А. (ініціали та прізвище)
Член комісії	(підпис)	Вергеліс А.В. (ініціали та прізвище)

ЗАТВЕРДЖУЮ

Харківський державний
регіональний науково-технічний центр
з питань технічного захисту інформації
Пономарьова Г.М.
«18» 01 2021 р.

АКТ

про використання результатів дисертаційної роботи Шаповалової Анастасії Сергіївни за темою «Потокові моделі безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих телекомунікаційних мережах», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Комісія у складі:
голови: Г.М.Пономарьова, Директор «ХДРНТЦ ТЗІ»;
членів: Сацюк В.В., «ХДРНТЦ ТЗІ»;
Тимашек Н.В., «ХДРНТЦ ТЗІ»;

склала даний акт у тому, що результати дисертаційної роботи Шаповалової А.С., а саме:

- потокова модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіка в програмно-конфігурованих телекомунікаційних мережах;
- потокова модель швидкої безпечної перемаршрутизації із балансуванням навантаження та обмеженням трафіку на границі телекомунікаційної мережі,

використані для оцінки відмовостійкості та навантаження у розгорнутій на підприємстві телекомунікаційній мережі із подальшим розробленням практичних рекомендацій для ефективного балансування мережного ресурсу, а також для забезпечення відмовостійкості телекомунікаційної мережі в цілому.

Голова комісії	(підпис)	Г.М.Пономарьова (ініціали та прізвище)
Член комісії	(підпис)	В.В.Сацюк (ініціали та прізвище)
Член комісії	(підпис)	Н.В.Тимашек (ініціали та прізвище)

ЗАТВЕРДЖУЮ

ПрАТ «Фарлеп-Інвест»

Сіренко А.В.

«14» 04 2021 р.

АКТ

про використання результатів дисертаційної роботи Шаповалової Анастасії Сергіївни за темою «Потокові моделі безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих телекомунікаційних мережах», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі

Комісія у складі:

голови: Сіренко Дмитрій Васильович, керівник;

членів: Мусатов Олександр Павлович, керівник;

Рощин Євгеній Олександрович, інженер

склала даний акт у тому, що результати дисертаційної роботи Шаповаловсї А.С., а саме:

- потокова модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіка в програмно-конфігурованих телекомунікаційних мережах;
- потокова модель швидкої безпечної перемаршрутизації із балансуванням навантаження та обмеженням трафіку на границі телекомунікаційної мережі,

впроваджено в діяльність підприємства ПрАТ «Фарлеп-Інвест» при розробці практичних рекомендації щодо підвищення рівня мережного захисту та відмовостійкості в телекомунікаційних мережах.

Голова комісії _____ (підпис) Сіренко А.В (ініціали та прізвище)

Член комісії _____ (підпис) Мусатов А.П (ініціали та прізвище)

Член комісії _____ (підпис) Рощин Є.А (ініціали та прізвище)

ДОДАТОК Б

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Carlsson A., Duravkin E. V., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 1. Features of realization of low-intensity HTTP attacks. Проблеми телекомунікацій. 2013. № 3 (13). С. 61–70. URL: http://pt.nure.ua/wp-content/uploads/2020/01/133_carlsson_attack.pdf

2. Duravkin E. V., Carlsson A., Loktionova A. S. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. Method of detecting Slow HTTP attacks. Проблеми телекомунікацій. 2014. № 1 (14). С. 96–100. URL: http://pt.nure.ua/wp-content/uploads/2020/01/141_carlsson_attack.pdf.

3. Duravkin E. V., Carlsson A., Loktionova A.S. Method of slow-attack detection. Системи обробки інформації. 2014. № 8. С. 102–106.

4. Євдокименко М. О., Шаповалова А. С. Метод оцінювання впливу атак на інфокомунікаційну мережу з урахуванням наявних вразливостей. Вчені записки Таврійського національного університету імені В.І. Вернадського. 2018. Т. 29 (68), № 4. С. 67–72.

5. Yevdokymenko M. O., Shapovalova A. S., Nevzorova O. S. Proactive Approach for Security of the PAAS Model of Cloud System Based on Vulnerability Assessment. International Journal of Science and Engineering Investigations. 2019. Vol. 8(91). P. 167–173. URL: http://www.ijsei.com/papers/ijsei-89119-22.pdf.

6. Лемешко О. В., Шаповалова А. С., Єременко О. С., Євдокименко М. О., Хайлан А. М. Математична модель швидкої перемаршрутизації з балансуванням навантаження та диференційованого обмеження трафіка в мережах SD-WAN. Системи управління, навігації та зв'язку. 2019. № 4 (56). С. 63–71. DOI:10.26906/SUNZ.2019.4.063.

7. Lemeshko O., Yevdokymenko M., Yeremenko O., Shapovalova A. Investigation of Load-Balancing Fast ReRouting Model with Providing Fair Priority-Based Traffic Policing. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in

Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing. Springer, Cham. 2020. Vol. 1247. P. 108–119 DOI: 10.1007/978-3-030-55506-1_10 **(SCOPUS)**

8. Lemeshko O., Shapovalova A., Al-Dulaimi A. M. K., Yeremenko O., Yevdokymenko M. Flow-Based Routing Model With Load Balancing Under Network Security Parameters. Information and Telecommunication Sciences. No 2 (2020). P. 44–50. DOI: 10.20535/2411-2976.22020.44-50.

9. Євдокименко М. О., Шаповалова А. С., Шаповал М. М. Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Проблеми телекомунікацій. 2020. № 1 (26). С. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.

10. Локтіонова А. С. Оцінка економічної доцільності впровадження системи менеджменту інформаційної безпеки. Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів «Інформаційні технології в сучасному світі: дослідження молодих вчених»: матеріали конференції. (м. Харків, 2013). Харків: ХНЕУ, 2013. С. 68.

11. Duravkin I., Loktionova A., Carlsson A. Method of slow-attack detection. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the First International Scientific-Practical Conference, Kharkov, Ukraine, 2014. IEEE, 2014. P. 171–172. DOI: 10.1109/INFOCOMMST.2014.6992341.

12. Yevdokymenko M., Shapovalova A., Voloshchuk O., Carlsson A. Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fifth International Scientific-Practical Conference, Kharkov, Ukraine, 9–12 October 2018. IEEE, 2018. P. 609–612. DOI: 10.1109/INFOCOMMST.2018.8632079. **(SCOPUS)**

13. Lemeshko O. V., Yeremenko O. S., Yevdokymenko M. O., Shapovalova A. S. Advanced solution of the Fast ReRoute based on principles of Traffic Engineering and Traffic Policing. Science and Technology «AVIA-2019»: Proceedings of the Fourteenth International Conference, Ukraine, 23–25 April 2019. P. 8.21–8.23.

14. Єременко О. С., Євдокименко М. О., Шаповалова А. С. Підвищення відмовостійкості мереж засобами швидкої перемаршрутизації з балансуванням навантаження та профілюванням трафіка. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології»: збірник наукових праць. (м. Харків, 2019). Харків: ХНУРЕ, 2019. С. 131.

15. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Ilyashenko A., Sleiman B. Traffic Engineering Fast ReRoute Model with Support of Policing. Electrical and Computer Engineering (UKRCON): Proceedings of the 2nd International Conference, Lviv, Ukraine, 2–6 July, 2019. IEEE, 2019. P. 842–845. DOI: 10.1109/UKRCON.2019.8880006. **(SCOPUS)**

16. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Hailan A. M., Mersni A. Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS): Proceedings of the 10th IEEE International Conference, Metz, France, 2019. IEEE, 2019. P. 117–122. DOI: 10.1109/IDAACS.2019.8924294. **(SCOPUS)**

17. Yevdokymenko M., Shapovalova A. Investigation of the Impact of HTTP DoS Attacks on the Cloud Web Server. Natural science and technology (ICONAT): Proceedings of the International conference, Kharkiv, 2019. P. 25.

18. Lemeshko O., Yeremenko O., Hailan A. M., Yevdokymenko M., Shapovalova A. Policing Based Traffic Engineering Fast ReRoute in SD-WAN Architectures: Approach Development and Investigation. In: Al-Bakry A. et al. (eds) New Trends in Information and Communications Technology Applications. NTICT 2020. Communications in Computer and Information Science. Springer, Cham. Vol. 1183. P. 29–43. DOI: 10.1007/978-3-030-55340-1_3. **(SCOPUS)**

19. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Radivilova T., Ageyev D. Secure Based Traffic Engineering Model in Softwarized Networks. Advanced Trends in Information Theory (ATIT): Proceedings of the IEEE International Conference, Kyiv. 2020. P. 143–147. DOI: 10.1109/ATIT50783.2020.9349301. (**SCOPUS**)