МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

ШАПОВАЛОВА Анастасія Сергіївна

УДК 621.391

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

05.12.02 – Телекомунікаційні системи та мережі

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Харків – 2021

Дисертацією є рукопис

Робота виконана в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України

Науковий консультант: доктор технічних наук, доцент
ЄВДОКИМЕНКО Марина Олександрівна,
Харківський національний університет радіоелектроніки,
доцент кафедри інфокомунікаційної інженерії
імені В.В. Поповського

Офіційні опоненти: доктор технічних наук, професор
ТОЛЮПА Сергій Васильович,
Київський національний університет
імені Тараса Шевченка,
професор кафедри кібербезпеки та захисту інформації

кандидат технічних наук, доцент
СОЛОВСЬКА Ірина Миколаївна,
Державний університет інтелектуальних технологій і зв'язку, докторант

Захист відбудеться «27» квітня 2021 року о 13 годині на засіданні спеціалізованої вченої ради Д 64.052.09 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14

Автореферат розісланий «26» березня 2021 року.

Вчений секретар
спеціалізованої вченої ради О.С. Єременко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 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.

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, 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. Проведений аналіз 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».

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 із балансуванням навантаження та обмеженням трафіку на границі програмно-конфігурованої телекомунікаційної мережі;

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

Об’єкт дослідження – процеси безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих ТКМ.

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

Методи дослідження. У процесі розроблення та вдосконалення математичних моделей був використаний апарат дослідження операцій і теорія множин. Для опису топології програмно-конфігурованих ТКМ використовувалася теорія графів. Для 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 ін-

шого, – 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, підтверджувалась 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 та 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 [1] здобувачкою на низці розрахункових прикладів досліджено особливості реалізації

низькоінтенсивних HTTP-атак для оцінювання ризиків інформаційної безпеки програмно-конфігурованих мереж; у статті [2] дисертанткою проведено аналіз та дослідження методу виявлення повільних атак HTTP у програмно-конфігурованих телекомунікаційних мережах; у публікації [3] здобувачкою проаналізовано та досліджено метод виявлення повільної атаки в програмно-конфігурованих мережах із оцінкою рівня безпеки телекомунікаційної мережі; у роботі [4] вдосконалено метод оцінювання впливу атак на телекомунікаційну мережу з урахуванням наявних уразливостей для підвищення відмовостійкості мережі загалом; у публікації [5] 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 [6] здобувачкою запропоновано та досліджено математичну модель швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку в територіально розподілених програмно-конфігурованих мережах; у статті [7] авторкою розроблено та досліджено потокову модель швидкої перемаршрутизації з балансуванням навантаження та диференційованим справедливим обмеженням трафіку в територіально розподілених програмно-конфігурованих мережах; у публікації [8] здобувачкою розроблено та досліджено потокову модель маршрутизації з балансування навантаження з урахуванням параметрів мережної безпеки; у статті [9] 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 статей у наукових фахових виданнях України [1–4, 6, 8, 9] та 2 статті в закордонних журналах [5, 7], з яких 1 індексується наукометричною базою Scopus [7]. Отримані результати та висновки апробовано на 10 міжнародних наукових конференціях та форумах [10–19], з яких 5 індексуються наукометричною базою Scopus [12, 15, 16, 18, 19].

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.

ЗМІСТ РОБОТИ

У **вступі** проаналізовано загальний стан результатів вирішення завдань щодо забезпечення відмовостійкості та мережної безпеки в ТКМ, обґрунтовано актуальність теми дисертаційного дослідження, показано зв'язок роботи з науковими програмами й темами, визначено мету та завдання, об'єкт і предмет дослідження, сформульовано наукову новизну та практичне значення результатів роботи.

У **першому розділі** на основі проведеного аналізу з'ясовано, що в умовах перевантаження, можливих збоїв в апаратному чи програмному забезпеченні мережного обладнання та порушення інформаційної безпеки важливим технологічним інструментом підвищення рівня відмовостійкості й мережної безпеки в програмно-конфігурованих ТКМ є протоколи маршрутизації. У розділі проаналізовано наявні теоретичні та прикладні рішення завдань безпечної та відмовостійкої маршрутизації, установлено їхні переваги та недоліки, а також сформульовано вимоги, які висуваються до перспективних протоколів. Установлено, що узгоджене та взаємодоповнене вирішення завдань щодо безпечної та відмовостійкої маршрутизації на принципах балансування навантаження завжди потребує вдосконалення наявних і розроблення нових математичних моделей та методів маршрутизації, які є основою відповідних протокольних рішень, що обумовлює актуальність поставленого в роботі наукового завдання.

У **другому розділі** вдосконалено потокову модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Базовою обрано модель, у межах якої структура мережі описується графом $G = (R, E)$, де $R = \left\{ R_i ; i = \overline{1,m} \right\}$ – це множина вершин, що моделюють маршрутизатори, а $E = \left\{ E_{i,j} ; \quad i, j = \overline{1,m}, \ i \neq j \right\}$ – множина дуг, які представляють канали зв'язку (КЗ) у ТКМ. Кожен із каналів має свою пропускну

здатність $\varphi_{i,j}$, що вимірюється в пакетах за секунду **(**1/с). Нехай у ТКМ циркулює множина потоків пакетів K. Тоді для кожного k-го потоку відомі такі вихідні дані, як λ^k – середня інтенсивність потоку пакетів (1/с); s_k та d_k – вузол-відправник та вузол-отримувач відповідно.

Порядок маршрутизації в мережі визначають маршрутні змінні $x_{i,j}^k$, кожна з яких характеризує долю (частину) k-го потоку, що протікає в КЗ між i-м на j-м вузлами ТКМ, та на які накладаються умови вигляду

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

у разі реалізації одношляхової маршрутизації та

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

у випадку підтримки багатошляхових рішень.

Крім того, мають виконуватися умови збереження потоку на маршрутизаторах мережі:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 1, \ k \in K, \ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 0, \ k \in K, \ R_i \ne s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = -1, \ k \in K, \ R_i = d_k. \end{cases} \tag{2}$$

З метою запобігання перевантаження каналів зв’язку в ТКМ на маршрутні змінні $x_{i,j}^k$ також накладаються обмеження:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \varphi_{i,j}, \ E_{i,j} \in E. \tag{3}$$

Для розрахунку оптимальних шляхів у ТКМ, як приклад, може використовуватися наступний лінійний критерій оптимальності:

$$\sum_{k\in K} \sum_{E_{i,j}\in E} w_{i,j} x_{i,j}^k \Rightarrow \mathbf{min}, \tag{4}$$

де $w_{i,j}$ – вагові коефіцієнти, а фактично маршрутні метрики КЗ ТКМ.

Науковою новизною запропонованої моделі маршрутизації є підхід до формування вагових коефіцієнтів $w_{i,j}$. Відповідно до рекомендацій NIST для цього обрано базові метрики CVSS v.3, що, на відміну від часових метрик і метрик навколишнього середовища користувачів, характеризують незмінні за часом наявні вразливості на елементах мережі. Тоді для розрахунку $w_{i,j}$ у пото-

кову модель введено такі позначення: $U = \left\{ U_i^q ; q = \overline{1,Q}, i = \overline{1,m} \right\}$ – множина вразливостей, виявлених 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, та характеризує умовні збитки від використання зловмисником вразливості U_i^q; P_i^q – імовірність використання q-ї вразливості зловмисником на i-му вузлі мережі, що за фізичним змістом є ймовірністю компрометації.

Для розрахунку ризику інформаційної безпеки R_i від використання наявних вразливостей на i-му вузлі ТКМ використано такий вираз:

$$R^i = \sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q . \qquad (5)$$

де, за рекомендацією NIST, збитки щодо базових метрик критичності вразливостей на вузлах мережі розраховуються як

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

де Imp_i^q, Ex_i^q та $f(Imp_i^q)$ – потенційний збиток, складність використання та функція від потенційного збитку в разі використання q-ї вразливості на i-му вузлі мережі відповідно.

Потенційний збиток від використання вразливості розраховується як

$$Imp_i^q = 10,41\left[1 - (1 - Conf_i^q) \cdot (1 - Int_i^q) \cdot (1 - Av_i^q) \right], \qquad (7)$$

де $Conf_i^q$, Int_i^q та Av_i^q – збитки від порушення конфіденційності, цілісності та доступності у випадку використання q-ї вразливості на i-му вузлі ТКМ відповідно. Три метрики $Conf_i^q$, Int_i^q та Av_i^q визначають наслідки використання зловмисником q-ї вразливості на i-му вузлі мережі. У кожній із цих метрик збитки від використання вразливості можуть бути *відсутніми* (тоді їхнє числове значення дорівнюватиме 0), *частковими* із значенням 0,275 або *повними* із значенням 0,66. Складність використання q-ї вразливості розраховується за допомогою такого виразу:

$$Ex_i^q = 20 \cdot Ac_i^q \cdot Au_i^q \cdot AcV_i^q , \qquad (8)$$

де Ac_i^q , Au_i^q та AcV_i^q – показники системи оцінки вразливості, серед яких Ac_i^q характеризує складність отримання доступу (вектор доступу), Au_i^q відповідає за вимоги до автентифікації та AcV_i^q визначає спосіб використання q-ї вразливості на i-му вузлі ТКМ.

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

$$R_{i,j} = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q} , \tag{9}$$

де $w_{i,j}$ – вагові коефіцієнти (вага компрометації), які застосовуються для оцінювання ризику, створюваного використанням q-ї вразливості на i-му вузлі ТКМ. Фактично ці коефіцієнти кількісно характеризують потенційний збиток у разі використання наявних на i-му вузлі ТКМ вразливостей.

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

$$\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q = w_{i,j} \cdot \ln \sum_{U_i^q \in U_i^*} e^{BS_i^q} . \tag{10}$$

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 через використання наявних вразливостей на цьому вузлі. У такому випадку ймовірність компрометації i-го вузла залежить від наявності та використання вразливостей на цьому вузлі та розраховується як ризик інформаційної безпеки.

Виходячи з (5)–(10), значення кожного з вагових коефіцієнтів $w_{i,j}$ у виразі (4) можна розрахувати за допомогою формули

$$w_{i,j} = \frac{\sum_{U_i^q \in U_i^*} BS_i^q \cdot P_i^q}{\ln \sum_{U_i^q \in U_i^*} e^{BS_i^q}} . \tag{11}$$

У роботі для оцінювання працездатності вдосконаленої моделі (1)–(11) на низці прикладів структур ТКМ було проведено її дослідження. Для розрахунку вагових коефіцієнтів $w_{i,j}$ вихідними даними були характеристики наявних вра-

зливостей мережного обладнання (вузлів ТКМ) різних виробників згідно зі спеціалізованою базою даних CVSS v.3 (табл. 1). Результати проведеного дослідження підтвердили адекватність запропонованої моделі безпечної маршрутизації щодо розрахунку маршрутів у ТКМ із мінімальним ризиком інформаційної безпеки, забезпечивши цим максимальний рівень мережної безпеки пакетам, які передаються в ТКМ.

Таблиця 1

Приклад характеристик вразливостей мережного обладнання

Тип маршрутизатора	Базова оцінка BS_i^q	Імовірність використання вразливості P_i^q	Опис вразливості згідно зі спеціалізованою базою даних	Рівень критичності вразливості
Cisco RV042	7,2	0,1	CVE-2020-3294	високий
Cisco Small Business RV160W	9,8	0,6	CVE-2021-1289	критичний
NETGEAR R7450 1.2.0.62_1.0.1	6,5	0,2	CVE-2020-35839	середній
Xiaomi RM1800	7,5	0,3	CVE-2020-14098	високий
Cisco RV260	9,8	0,6	CVE-2021-1292	критичний

У **третьому розділі** вдосконалено потокову модель безпечної маршрутизації з балансуванням навантаження в телекомунікаційній мережі (1)–(3). *Новизною* моделі є модифікація умов балансування навантаження (3), у яких, окрім пропускної здатності каналу (показника якості обслуговування), також враховується ймовірність його компрометації (показник мережної безпеки). Основна ідея рішення, яке пропонується в цій роботі, полягає в тому, щоб забезпечити більш інтенсивне використання каналів із мінімальними ймовірностями компрометації $p_{i,j}$, і навпаки – канали з високою $p_{i,j}$ повинні завантажуватися мінімально або навіть повністю блокуватися. Удосконалена версія умови балансування навантаження (3) має вигляд

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \alpha v_{i,j}\varphi_{i,j}, \text{ якщо } 0 \le \alpha \le 1, \qquad (12)$$

де α – це додатково введена керуюча змінна, що кількісно визначає верхній поріг завантаженості каналів зв'язку, а $v_{i,j}$ – вагові коефіцієнти, які мають відповідати таким граничним умовам:

$$v_{i,j} = \begin{cases} 0, & \text{якщо } p_{i,j} = 1; \\ 1, & \text{якщо } p_{i,j} = 0. \end{cases} \qquad (13$$

Критерієм оптимальності маршрутних рішень, що відповідають вимогам концепції Traffic Engineering, є умова

$$\min_{x,\alpha} \alpha \,. \qquad (14)$$

з обмеженнями (1), (2) та (12).

У межах проведеного дослідження множина допустимих значень $p_{i,j}$ умовно розділена на декілька підмножин, кожній з яких відповідає свій сценарій компрометації ТКМ та її каналів зв'язку (табл. 2).

Таблиця 2

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

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

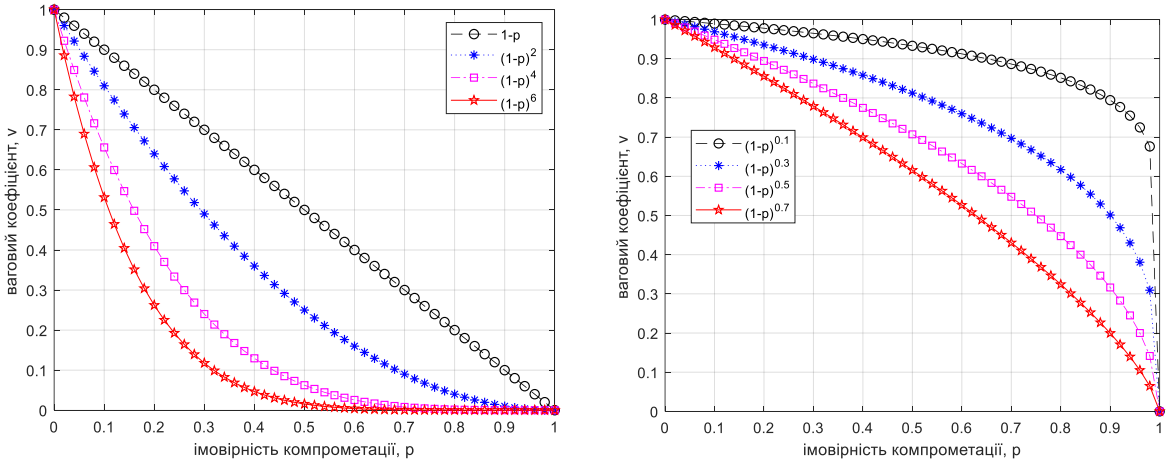
Для проведення дослідження використовувалися декілька моделей блокування каналів зв'язку в процесі безпечного балансування навантаження в ТКМ, які характеризують залежності вагових коефіцієнтів $v_{i,j}$ спадною функцією від імовірності компрометації $p_{i,j}$ в умовах (12):

$$v_{i,j} = (1 - p_{i,j})^n, \qquad (15) \qquad v_{i,j} = 1 - p_{i,j}^n, \qquad (16)$$

$$v_{i,j} = \exp(-n \cdot p_{i,j}), \qquad (17) \qquad v_{i,j} = 1 - \frac{1}{1 + n \cdot \exp(-r \cdot p_{i,j} + b)}, \qquad (18)$$

$$v_{i,j} = 1 - p_{i,j} + n \sin(2\pi p_{i,j} + \theta), \qquad (19)$$

де n – це керуючий параметр, за допомогою якого здійснюється регулювання чутливості вагового коефіцієнта $v_{i,j}$ до значень $p_{i,j}$. Інші параметри в (15)–(19) обиралися так, щоб виконувалась умова (12). Так, наприклад, у разі використання моделі блокування КЗ, представленої виразом (15), залежність імовірності компрометації КЗ $p_{i,j}$ від коефіцієнта n зображена на рис. 1.



а) якщо $n \geq 1$ б) якщо $n < 1$

Рис. 1. Графічне зображення моделі блокування каналів зв'язку (15)

Тоді за результатами аналізу (рис. 2), можна зробити важливий висновок: модель блокування КЗ (15) досить універсальна та може використовуватися для будь-якого з наведених сценаріїв компрометації (табл. 2), тобто

- за умови $n>1$ ця модель блокування досить чутлива до ймовірностей компрометації КЗ, оскільки навіть у разі мінімальних значень $p_{i,j}$ пропускна здатність КЗ може блокуватися на 10–50 % і вище (рис. 2, а). Тому її краще використовувати, наприклад, у першому та другому сценаріях компрометації;

- у випадку зростання параметру n (якщо $n>4$) зазначену модель рекомендовано застосувати лише за першим сценарієм компрометації, оскільки вже за умови $p_{i,j}\geq 0{,}5$ канали зв'язку будуть повністю блоковані (рис. 2, а);

- якщо $0<n<1$, модель (15) слабо чутлива до компрометації каналів за першим сценарієм та помірно чутлива до рівня компрометації КЗ за другим та третім сценаріями (рис. 2, б).

Крім того, у процесі проведеного дослідження аналізувався вплив структури ТКМ, сценаріїв компрометації (табл. 2) та моделей блокування КЗ (15)–(19) на показники завантаженості мережі (12) та рівня мережної безпеки. Рівень мережної безпеки оцінювався за таким показником, як імовірність компрометації пакетів *k*-го потоку вздовж множини використаних шляхів

$$p_{E2E}^{k}=\sum_{s\in S^{k}}\frac{\lambda_{s}^{k}}{\lambda^{k}}p_{s}\ \text{ за умови }\ p_{s}=1-\prod_{E_{i,j}\in Path_{S}}(1-p_{i,j}),\qquad(20)$$

де S^{k} – множина шляхів (маршрутів), які застосовуються 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; $Path_{S}=\left\{E_{i,j}\right\}$ – це множина каналів зв'язку мережі, які утворюють у ній *s*-й шлях.

Отримані в межах запропонованої моделі маршрутні рішення спрямовані на зменшення завантаженості каналів зв'язку, які мають високу ймовірність компрометації, шляхом перенаправлення трафіку на більш безпечні канали. Це дозволило залежно від структури ТКМ, обраної моделі блокування КЗ (15)–(19) та сценарію компрометації знизити ймовірність компрометації пакетів (20) від 5–10 % до 20–25 %.

У **четвертому розділі** вперше запропоновано модель швидкої перемаршрутизації (Fast Reroute, FRR) із забезпеченням балансування навантаження на принципах Traffic Engineering (TE) та диференційованого обмеження трафіку (Traffic Policing, TP) у програмно-конфігурованих телекомунікаційних мережах. У межах моделі забезпечувався розрахунок двох типів змінних $x_{i,j}^{k}$ та $\bar{x}_{i,j}^{k}$, які визначали порядок маршрутизації за основними та резервними шляхами відповідно. Надалі параметри, які позначені «рискою», зберігають свій фізич-

ний зміст, але належать до характеристик резервних шляхів. На $\bar{x}_{i,j}^{k}$ накладалось обмеження, подібне до (1). *Новизною* моделі є модифікація умов збереження потоку, які враховують пріоритетне обмеження трафіку на границі мережі в разі 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. Зазначені умови для основного та резервного шляхів мають такий вигляд:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 0;\ k\in K,\ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = 1-\beta^{k};\ k\in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^{k} = \beta^{k} - 1;\ k\in K,\ R_i = d_k; \end{cases} \quad \begin{cases} \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^{k} = 0;\ k\in K,\ R_i \neq s_k, d_k; \\ \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^{k} = 1-\bar{\beta}^{k};\ k\in K,\ R_i = s_k; \\ \sum\limits_{j:E_{i,j}\in E} \bar{x}_{i,j}^{k} - \sum\limits_{j:E_{j,i}\in E} \bar{x}_{j,i}^{k} = \bar{\beta}^{k} - 1;\ k\in K,\ R_i = d_k; \end{cases} \quad (21)$$

де β^{k} та $\bar{\beta}^{k}$ є частками інтенсивності k-го потоку, який у разі реалізації політики ТР отримує відмову в обслуговуванні (обмежується) на границі мережі під час використання основного та резервного шляхів відповідно.

Використання розробленої моделі швидкої перемаршрутизації дозволяє реалізувати відомі схеми захисту елементів ТКМ:

- умови захисту каналу зв’язку $E_{i,j} \in E$:

$$0 \le \bar{x}_{i,j}^{k} \le \delta_{i,j}^{k}\ \text{, якщо}\ \delta_{i,j}^{k} = \begin{cases} 0, \text{ у разі захисту каналу зв'язку } E_{i,j}; \\ 1, \text{ в іншому випадку.} \end{cases} \quad (22)$$

- умови захисту вузла $R_i \in R$:

$$0 \le \bar{x}_{i,j}^{k} \le \delta_{i,j}^{k},\ R_j \in R_i^{*},\ j = \overline{1,m}, \quad (23)$$

де R_i^{*} – це множина маршрутизаторів, які є суміжними до R_i .

Модифіковані умови захисту пропускної здатності ТКМ із забезпеченням у ній балансування навантаження мали такий вигляд:

$$\sum_{k\in K} \lambda^{k} \cdot u_{i,j}^{k} \le \alpha \cdot \varphi_{i,j},\ E_{i,j} \in E\ \text{, якщо}\ x_{i,j}^{k} \le u_{i,j}^{k}\ \text{та}\ \bar{x}_{i,j}^{k} \le u_{i,j}^{k}, \quad (24)$$

де $u_{i,j}^{k}$ – це додаткові керуючі змінні, кожна з яких характеризує верхній поріг для значень маршрутних змінних $x_{i,j}^{k}$ та $\bar{x}_{i,j}^{k}$, а також відповідає обмеженням

$$0 \le u_{i,j}^{k} \le 1, \quad (25)$$

а керуюча змінна α відповідає умовам

$$0 \le \alpha \le \alpha_{TH}, \quad (26)$$

де α_{TH} – граничне значення верхнього порогу завантаженості каналів зв'язку мережі, величина якої попередньо задається на основі аналізу QoS-вимог.

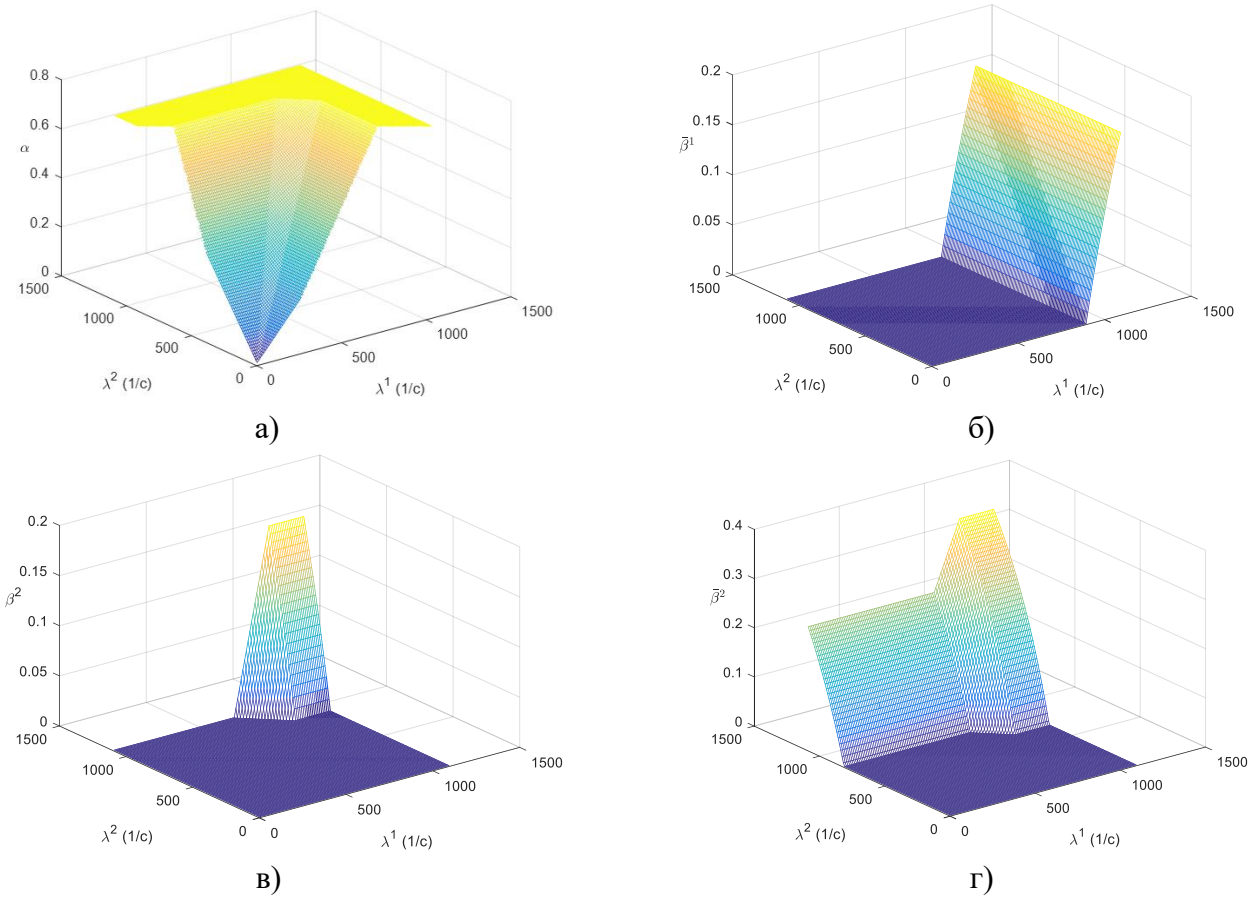
Критеріями оптимальності рішень завдання швидкої перемашрутизації з балансуванням навантаження та диференційованим обмеженням трафіку був мінімум таких цільових функцій:

$$J = \sum_{k \in K} w_k \cdot \beta^k + \sum_{k \in K} \bar{w}_k \cdot \bar{\beta}^k + c \cdot \alpha \to \min, \tag{27}$$

$$J = \sum_{k \in K} w_k \cdot (\beta^k)^2 + \sum_{k \in K} \bar{w}_k \cdot (\bar{\beta}^k)^2 + c \cdot \alpha \to \min, \tag{28}$$

де вагові коефіцієнти відповідали умові $w_z > \bar{w}_z > w_p > \bar{w}_p > \ldots > c$, якщо z-й пріоритет потоку є вищим за p-й пріоритет.

На множині мережних структур проведено дослідження процесів швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку. Результати дослідження підтвердили адекватність та ефективність запропонованих рішень із точки зору забезпечення відмовостійкості ТКМ в умовах відмов мережних елементів (рис. 2).



а) б) в) г)

Рис. 2. Результати дослідження для двох потоків пакетів: перший потік мав четвертий пріоритет, а другий – перший пріоритет, $\alpha_{TH} = 0,75$

Водночас в умовах перевантаження ТКМ для забезпечення заданого рівня завантаженості КЗ мережі (26) здійснювалося диференційоване обмеження по-

токів або на підставі абсолютних пріоритетів, коли використовувався критерій (27), або з відносних – коли застосовувався критерій (28). Мінімально обмежувалися високопріоритетні потоки, які передавалися за основними шляхами, а більш інтенсивно відкидалися пакети найменш пріоритетних потоків, що передавалися резервним маршрутом.

У цьому ж розділі запропоновано вдосконалення потокової моделі швидкої безпечної перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку на границі ТКМ. Фактично ця модель є поєднанням рішень, які представлені виразами (1), (12)–(20) та (21)–(28). Наукова новизна моделі полягає в забезпеченні захисту елементів мережі та її пропускної здатності в процесі реалізації швидкої перемаршрутизації та диференційованого обмеження трафіку на основі врахування ймовірності компрометації каналів зв'язку:

$$\sum_{k \in K} \lambda^k \cdot u_{i,j}^k \le \alpha v_{i,j} \varphi_{i,j}, \; E_{i,j} \in E, \tag{29}$$

де значення коефіцієнтів $v_{i,j}$ визначалися відповідно до виразів (13), (15)–(19). У запропонованій моделі для визначення вагових коефіцієнтів у критеріях (27) та (28) враховувалися не тільки пріоритет потоку пакетів, але і його вимоги до рівня мережної безпеки, які задавалася граничним значенням імовірності компрометації пакетів (20).

У межах моделі (1), (13), (15)–(29) завдання безпечної швидкої перемаршрутизації було представлено у вигляді задачі лінійного (27) або квадратичного (28) програмування, коли обмеженнями на маршрутні змінні були вирази (1), (21)–(26), (29). Результати дослідження підтвердили, що отримані в межах запропонованої моделі маршрутні рішення орієнтовані на зменшення завантаженості каналів зв'язку з високою ймовірністю компрометації шляхом перерозподілу трафіку для передавання пакетів більш безпечними каналами (маршрутами) мережі. Крім того, установлено, що на інтенсивність відкинутих на границі ТКМ пакетів впливали значення їхніх пріоритетів та вимоги до рівня безпеки.

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; 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 забезпечити розрахунок та застосування маршрутів із мінімальним ризиком інформаційної безпеки, забезпечивши цим максимальний рівень мережної безпеки пакетам, які передаються в 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 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.

4. Уперше запропоновано модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіку в програмно-конфігурованих телекому-

нікаційних 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.

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.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ 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**)

АНОТАЦІЯ

Шаповалова А. С. Потокові моделі безпечної та відмовостійкої маршрутизації з балансуванням навантаження в програмно-конфігурованих телекомунікаційних мережах. – Рукопис. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 – телекомунікаційні системи та мережі. – Харківський національний університет радіоелектроніки, Харків, 2021.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної задачі, 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. Удосконалено та досліджено потокову модель безпечної маршрутизації в телекомунікаційних мережах. Удосконалено та досліджено потокову модель безпечної маршрутизації з балансуванням навантаження на основі врахування параметрів мережної безпеки в програмно-конфігурованих телекомунікаційних мережах. Уперше запропоновано та досліджено модель швидкої перемаршрутизації із забезпеченням балансування навантаження на принципах Traffic Engineering та диференційованого обмеження трафіку в програмно-конфігурованих телекомунікаційних мережах. Удосконалено та досліджено потокову модель безпечної швидкої перемаршрутизації з балансуванням навантаження та диференційованим обмеженням трафіку на границі телекомунікаційної мережі.

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. – Manuscript. Dissertation for the Candidate of Technical Sciences degree in the specialty 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 novel-

ty 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.

АННОТАЦИЯ

Шаповалова А. С. Потоковые модели безопасной и отказоустойчивой маршрутизации с балансировкой нагрузки в программно-конфигурируемых телекоммуникационных сетях. – Рукопись. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекомму-

никационные системы и сети. – Харьковский национальный университет радиоэлектроники, Харьков, 2021.

Диссертация посвящена решению актуальной научно-прикладной задачи, которая заключается в обеспечении отказоустойчивости и сетевой безопасности в программно-конфигурируемых ТКМ, функционирующих в условиях отказов и компрометации сетевого оборудования, путем разработки и совершенствования соответствующих математических моделей маршрутизации. Усовершенствована и исследована потоковая модель безопасной маршрутизации в телекоммуникационных сетях. Усовершенствована и исследована потоковая модель безопасной маршрутизации с балансировкой нагрузки на основе учета параметров сетевой безопасности в программно-конфигурируемых телекоммуникационных сетях. Впервые предложена и исследована модель быстрой перемаршрутизации с обеспечением балансировки нагрузки на принципах Traffic Engineering и дифференцированного ограничения трафика в программно-конфигурируемых телекоммуникационных сетях. Усовершенствована и исследована потоковая модель безопасной быстрой перемаршрутизации с балансировкой нагрузки и дифференцированным ограничением трафика на границе телекоммуникационной сети.

Ключевые слова: потоковая модель, сетевая безопасность, отказоустойчивость, безопасная маршрутизация, быстрая перемаршрутизация, риск информационной безопасности, базовые метрики, критичность уязвимостей, балансировка нагрузки, дифференцированное ограничение трафика.

Підп. до друку 25.03.21. Формат 60×84 1/16. Спосіб друку – ризографія.
Умов.-друк. арк. 2,8. Тираж 100 прим.
Зам. № 2-812. Ціна договірна.

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ
61166, Харків, просп. Науки, 14