УДК 621.391

МЕТОД ПРОЄКТУВАННЯ КІБЕРСТІЙКОЇ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ

О.В. Лемешко, О.С. Єременко, В.О. Куренко, М.А. Фукс
Харківський національний університет радіоелектроніки

Abstract *– The proposed method for designing a cyber-resilient information and communication network (ICN) is based on solving an optimization problem related to the mutually coordinated calculation of various control variables responsible for choosing the network topology; the order of connecting access networks to ICN core routers; determining the characteristics of the equipment used in terms of its performance and security level; determining the order of routing packet flows. The method assumes that the locations of the probable placement of network routers are known in advance. Due to the synthesized mathematical model, the method provides not a sequential but a simultaneous solution to the primary design tasks, which significantly affects the level of efficiency of the final solutions. The mathematical model on which the developed design method is based is mostly linear. Only the conditions for preventing the overloading of communication links (router interfaces) are non-linear. The cyber resilience of design solutions is ensured by the fact that in the objective function to be minimized, the weighting coefficients, along with cost and quality of service indicators, should also consider network (information) security indicators – the compromise probability or information security risks of network equipment. This will make it possible to synthesize a network with specified or predicted cyber resilience indicators. Prospects for further research in this area are related to the introduction of a mathematical model and a method for designing conditions for ensuring guaranteed quality of service, which will allow only the requirements for the level of cyber resilience to be taken into account at the level of the optimality criterion. On the other hand, an attempt to move to a linear version of the conditions for preventing communication link overload is a certain direction of model improvement, which will somewhat reduce the computational complexity of calculations related to the determination of a large number of control variables.*

Анотація *– В основу запропонованого методу проєктування кіберстійкої інфокомунікаційної мережі (ІКМ) покладено розв'язання оптимізаційної задачі, пов'язаної з взаємопогодженим розрахунком різнотипних керуючих змінних, які відповідають за вибір топології мережі; порядок підключення мереж доступу до маршрутизаторів ядра ІКМ; визначення характеристик використаного обладнання з погляду його продуктивності та рівня безпеки; визначення порядку маршрутизації потоків пакетів. Метод припускає, що місця ймовірного розміщення маршрутизаторів мережі попередньо відомі. Завдяки синтезованій математичній моделі, метод забезпечує не послідовне, а одночасне розв'язання основних проєктних задач, що істотно впливає на рівень ефективності кінцевих рішень. Математична модель, на якій базується розроблений метод проєктування, є здебільшого лінійною. Нелінійними є лише умови запобігання перевантаження каналів зв'язку (інтерфейсів маршрутизаторів) мережі. Кіберстійкість проєктних рішень забезпечується тим, що у цільовій функції, яка підлягала мінімізації, вагові коефіцієнти наряду з вартісними показниками та показниками якості обслуговування, мають також враховувати показники мережної (інформаційної) безпеки – імовірності компрометації або ризики інформаційної безпеки мережного обладнання. Це дозволить синтезувати мережу із заданими або прогнозованими показниками кіберстійкості. Перспективи подальших досліджень у цьому науковому напрямку пов'язані із введенням у структуру математичної моделі та методу проєктування умов забезпечення гарантованої якості обслуговування, що дозволить на рівні критерію оптимальності враховувати лише вимоги щодо рівня кіберстійкості. З іншого боку, певним напрямком вдосконалення моделі є спроба перейти до лінійного варіанту умов запобігання перевантаження каналів зв'язку, що дозволить дещо знизити обчислювальну складність розрахунків, пов'язаних із визначенням великої кількості керуючих змінних.*

Вступ

Як показав проведений аналіз [1-5], сучасні інфокомунікаційні мережі (ІКМ), апаратне та програмне забезпечення (АПЗ) комунікаційних пристроїв та серверного обладнання все частіше стають об'єктом кібератак з метою компрометації інформації, зниження рівня якості обслуговування (Quality of Service, QoS) або взагалі блокування надання мережею базових сервісів шляхом організації атак на комунікаційну інфраструктуру. Для цього зловмисники використовують уже відомі та нові вразливості, які все ще залишаються неусуненими у процесі оновлення АПЗ мережного обладнання. Проте всебічне виявлення вразливостей та їхнє оперативне

усунення – це лише локальний засіб підвищення рівня кіберстійкості ІКМ. Більш системним вбачається напрямок щодо забезпечення заданого рівня кіберстійкості ІКМ ще на етапі її проєктування. Тобто варто, щоб обґрунтування вибору топології мережі, комунікаційного обладнання та його програмного забезпечення відбувалося зокрема з урахуванням показників інформаційної та мережної безпеки.

Проблема проєктування ІКМ практично завжди формулюється в оптимізаційному вигляді, є дуже складною (рис. 1) з погляду традиційно високої розмірності та зазвичай нелінійності та багатокритеріальності [6-12]. Велика кількість керуючих змінних обумовлена необхідністю детально врахувати ключові особливості окремих задач проєктування. Багатокритеріальність проблеми напряму пов'язана з необхідністю покращення множини різнотипних показників ефективності ІКМ, які охоплюють як аспекти якості обслуговування, так і мережної безпеки. Нелінійність зумовлена тим, що основні показники QoS та мережної безпеки, на досягнення яких орієнтуються при проєктуванні ІКМ зазвичай нелінійно залежать від характеристик мережного трафіка та параметрів самої мережі. Додатковим фактором складності може також вважатись динамічний характер процесу проєктування [13] за необхідності врахування його багатоетапності у часі, пов'язаного з етапним (наприклад, щоквартальним) фінансуванням та/або поступовим введенням в експлуатацію мережних потужностей.

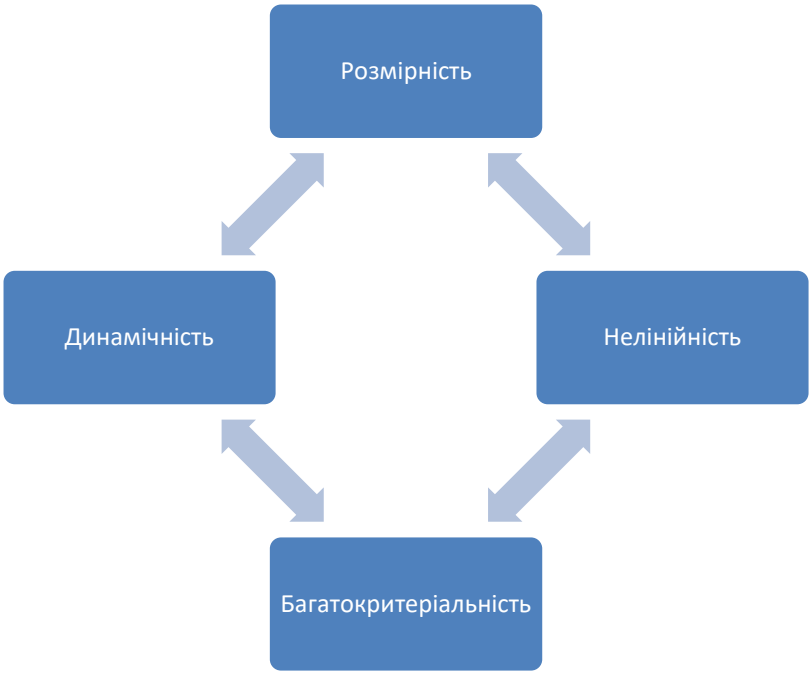

Рис. 1. Фактори складності проблеми проєктування ІКМ

З метою системного врахування перерахованих факторів і зниження складності подальших розрахунків у процесі отримання кінцевих рішень дослідники та проектувальники постійно працюють у напрямку вдосконалення існуючих і розробки нових математичних моделей і методів проєктування ІКМ. Одним з напрямків

зниження складності проблеми проєктування, наприклад, розглядається її декомпозиція на окремі задачі проєктування, які пропонується розв'язувати послідовно [14-18] (рис. 2). Як правило, виділяються задачі щодо вибору місцезнаходження комунікаційних і керуючих вузлів (комутаторів, маршрутизаторів, контролерів); вибору топології мережі; визначення типу характеристик використаного обладнання (конфігурація, продуктивність, рівень мережної безпеки); визначення порядку розподілу (маршрутизації) трафіка в ІКМ. Це дозволяє значно знизити розмірність проблеми, об'єм розрахунків, але негативно впливає на оптимальність кінцевих рішень, оскільки проєктні задачі розв'язуються досить автономно одна від одної. Проте інколи такий варіант являється єдиним доступним, особливо коли не вдається в межах однієї математичної моделі адекватно описати взаємозв'язок перелічених задач та їхніх рішень.

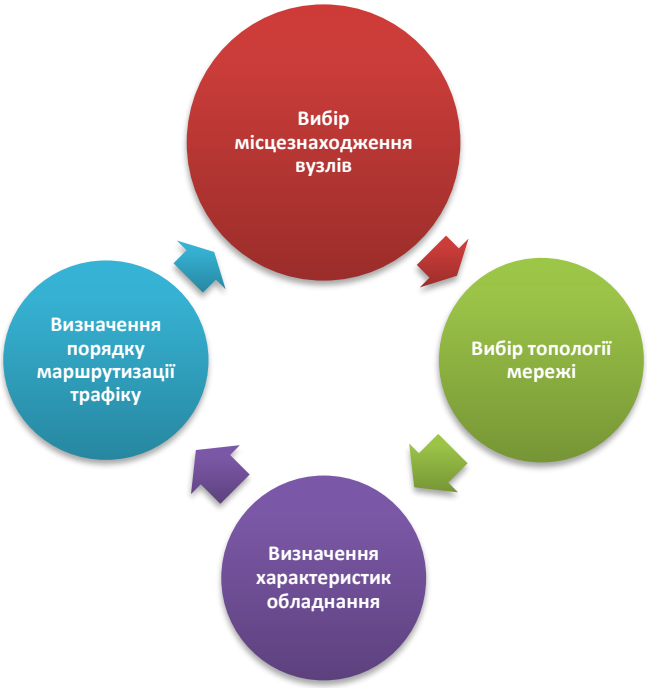

Рис. 2. Варіант декомпозиції проблеми проєктування ІКМ на окремі задачі

Для того щоб не втратити адекватність при математичному описі ІКМ та значно не погіршити оптимальність проєктних рішень, важливо мати у своєму розпорядженні ефективні математичні моделі та методи проєктування мереж, які б повно та взаємопов'язано враховували аспекти QoS та мережної безпеки, щоб забезпечити вимоги щодо рівня кіберстійкості ІКМ. Тому метою даної статті є розробка математичної моделі та методу проєктування кіберстійкої ІКМ, в межах яких оптимізується використання доступного мережного обладнання, пов'язані з його ціною, комплектацією, продуктивністю (пропускною здатністю) та рівнем мережної безпеки (компрометації, ризику інформаційної безпеки тощо). В межах запропонованих рішень буде здійснена спроба забезпечити взаємопогоджене

оптимізоване розв'язання задач вибору топології, характеристик мережного обладнання та каналів зв'язку, а також розподілу (маршрутизації) трафіка.

I. Математична модель проєктування кіберстійкої інфокомунікаційної мережі

З метою побудови математичної моделі кіберстійкої ІКМ введемо до розгляду граф $G=(M,L)$, у якому:

$M=R\bigcup V$ – множина вершин графа, яка математично описує мережі доступу (МД) та ядро ІКМ ($R\bigcap V=\varnothing$);

$R=\left\{R_i, i=\overline{1,m}\right\}$ – вершини графа *G*, які моделюють місця можливого розташування маршрутизаторів ядра мережі;

$m=\left|R\right|$ – загальна кількість таких місць розташувань;

$R^{+}\subset R$ – підмножина вершин, що моделюють місця можливого розташування приграничних маршрутизаторів ядра мережі;

$R^{-}\subset R$ – підмножина вершин, що моделюють місця можливого розташування транзитних маршрутизаторів ядра мережі;

$V=\left\{V_j, j=\overline{1,v}\right\}$ – вершини графа *G*, які моделюють мережі доступу ІКМ;

$v=\left|V\right|$ – загальна кількість мереж доступу в ІКМ;

$L=E\bigcup W$ – множина дуг графа, яка математично описує зв'язки між маршрутизаторами та мережами доступу в ІКМ ($E\bigcap W=\varnothing$);

$E=\left\{E_{i,j}, i,j=\overline{1,m}, i\neq j\right\}$ – множина дуг графа *G*, які моделюють імовірні канали зв'язку (КЗ) між маршрутизаторами ядра мережі;

$W=W^{+}\bigcup W^{-}$ – множина дуг графа *G*, які моделюють імовірні лінії зв'язку (*ЛД*) між мережами доступу та маршрутизаторами ядра мережі;

$W^{+}=\left\{W^{+}_{i,j}, i=\overline{1,v}, j=\overline{1,m^{+}}\right\}$ – множина дуг, що описують лінії доступу, які з'єднують мережі доступу та приграничні маршрутизатори

$W^{-}=\left\{W^{-}_{i,j}, i=\overline{1,m^{+}}, j=\overline{1,v}\right\}$ – множина дуг, що описують лінії доступу, які з'єднують приграничні маршрутизатори ІКМ та мережі доступу.

Як приклад, на рис. 3 представлено граф ІКМ, яка складається з чотирьох мереж доступу та максимально з дев'яти маршрутизаторів ядра мережі. Ймовірні лінії доступу та канали зв'язку на рис. 3 представлені штриховими лініями.

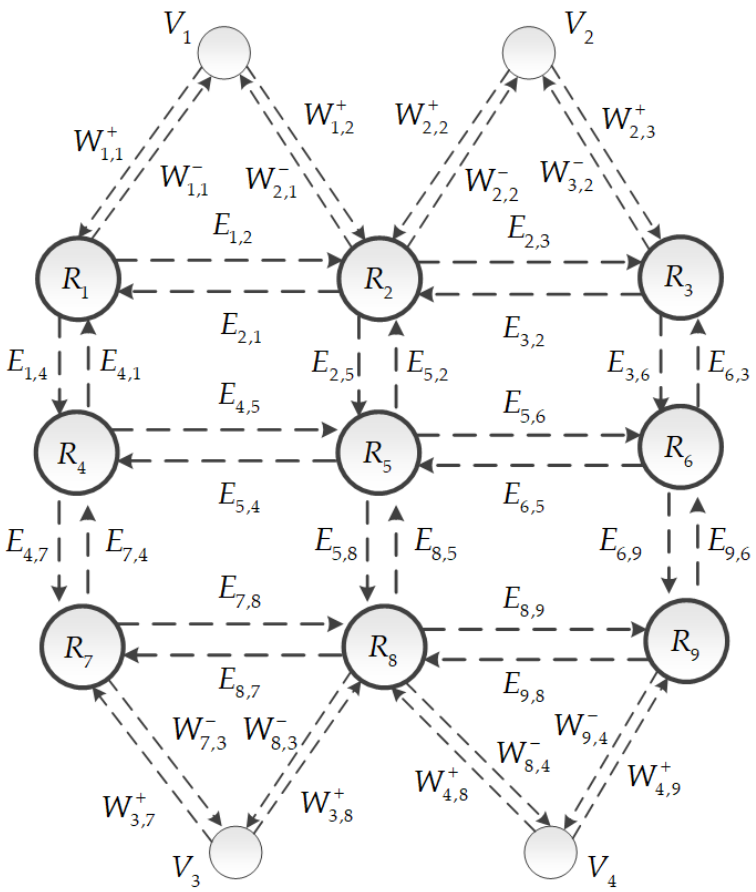

Рис. 3. Приклад графа $G=(M,L)$

Нехай при проєктуванні ІКМ доступні до використання різнотипні маршрутизатори, на кожному з яких можуть бути інстальовані модулі з інтерфейсами різних видів. У загальному випадку маршрутизатори та інтерфейси можуть мати різні вартісні та функціональні характеристики:

T – загальна кількість типів маршрутизаторів, доступних до використання при проєктуванні ІКМ. На тип маршрутизатора можуть впливати назва вендора, серія, модель, версія встановленої операційної системи (ОС) тощо;

S – загальна кількість видів інтерфейсів, які можуть застосовуватись на маршрутизаторах ІКМ. Вид інтерфейсу зазвичай визначається технологіями канального та фізичного рівнів, які він підтримує, наприклад, Gigabit Ethernet або Fast Ethernet на основі використання крученої пари або оптичного кабелю;

$\varphi^s_{i,j}$ – пропускна здатність каналу зв'язку між i-м та j-м маршрутизаторами (тобто маршрутизаторами, що знаходяться у місцях R_i та R_j), які використовують інтерфейси s-го виду (Мбіт/с).

Позначимо через K множину потоків пакетів, що циркулюють в ІКМ. Тоді нехай K^+_i – множина потоків, що надходять до ядра ІКМ від мережі доступу V_i; K^-_i – множина потоків, що виходять з ядра ІКМ до мережі доступу V_i; V^k_s – мережа

доступу, яка є джерелом k-го потоку пакетів; V_s^k – мережа доступу, яка є отримувачем пакетів k-го потоку; λ^k – середня швидкість пакетів k-го потоку, з якою вони генеруються на термінальних пристроях МД тим чи інших мережним додатком.

Для розв'язання задачі топологічного синтезу введемо множину керуючих булевих змінних

$$q_{t,j} \in \{0;1\},\ (t=\overline{1,T},\ j=\overline{1,m}). \tag{1}$$

Змінна $q_{t,j}$ дорівнює 1, якщо у j-му місці розташування встановлюється маршрутизатор t-го типу, або ж дорівнює 0 у іншому випадку.

У одному і тому ж місці може працювати лише один маршрутизатор певного типу, тому має місце така умова:

$$\sum_{t=1}^{T} q_{t,j} \le 1,\ (j=\overline{1,m}). \tag{2}$$

Множину змінних (1) доповнює ще одна множина змінних

$$q_{t,j}^s \in \{0;1\},\ (t=\overline{1,T},\ j=\overline{1,m},\ s=\overline{1,S}). \tag{3}$$

Змінна $q_{t,j}^s$ дорівнює 1, якщо на маршрутизаторі t-го типу, який встановлюється у j-му місці розташування, оснащений модулем з інтерфейсом s-го виду. У іншому випадку ця ж змінна приймає значення 0. Визначення змінних (2) пов'язана з розв'язанням задачі щодо вибору характеристик каналів зв'язку між маршрутизаторами ІКМ.

Виходячи з фізичного сенсу змінних (1) та (2) на них накладаються такі умови:

$$q_{t,j}^s \le q_{t,j}\ (t=\overline{1,T},\ j=\overline{1,m},\ s=\overline{1,S}). \tag{4}$$

Тобто на маршрутизаторі можуть бути інстальовані певні інтерфейсні модулі лише у випадку, коли цей маршрутизатор використовується в топології ІКМ. Крім того варто врахувати обмежені можливості реальних маршрутизаторів щодо кількості інстальованих інтерфейсних модулів, що досягається забезпеченням виконання таких обмежень:

$$\sum_{s=1}^{S} q_{t,j}^s \le N_t\ (t=\overline{1,T},\ j=\overline{1,m}), \tag{5}$$

де N_t – сумарна кількість модулів, на які розрахований маршрутизатор t-го типу.

Для подальшого розв'язання задачі маршрутизації (розподілу трафіка) в ІКМ вводяться маршрутні змінні $x_{i,j}^k$, кожна з яких характеризує частку k-го потоку в каналі

зв'язку, представленого дугою $E_{i,j}$. У разі реалізації в ІКМ одношляхової маршрутизації потоків на маршрутні змінні накладаються такі обмеження:

$$x_{i,j}^{k} \in \{0;1\}, \tag{6}$$

а при використанні багатошляхової маршрутизації:

$$0 \le x_{i,j}^{k} \le 1. \tag{7}$$

Нехай множина змінних $y_{i,j}^{k}$ та $z_{j,i}^{k}$ будуть трактуватися як змінні доступу. Змінна доступу $y_{i,j}^{k}$ визначає частку *k*-го потоку, що протікає в лінії доступу, представленій дугою $W_{i,j}^{+}$ [19-22]. Змінна доступу $z_{j,i}^{k}$ характеризує частку *k*-го потоку, що протікає в лінії доступу, представленій дугою $W_{j,i}^{-}$. Розрахунок цих змінних відбувається з метою розв'язання задачі топологічного синтезу ІКМ при визначенні порядку комутації мереж доступу до маршрутизаторів ІКМ. У більш широкому сенсі ці ж змінні можуть визначати порядок балансування навантаження, яке надходить від мереж доступу на ці ж маршрутизатори. Тобто, якщо мережа доступу взаємодіє лише з одним із приграничних маршрутизаторів ІКМ, то на змінні доступу накладаються обмеження виду

$$y_{i,j}^{k} \in \{0;1\} \text{ та } z_{j,i}^{k} \in \{0;1\}. \tag{8}$$

У випадку можливості підключення мережі доступу одночасно до декількох маршрутизаторів з подальшим використанням протоколів VRRP, HSRP або GLBP [19-22], на ці ж змінні накладаються умови, аналогічні до (7):

$$0 \le y_{i,j}^{k} \le 1 \text{ та } 0 \le z_{i,j}^{k} \le 1. \tag{9}$$

Для забезпечення збереження потоку пакетів на рівні доступу ІКМ на відповідні керуючі змінні накладаються додаткові умови-обмеження:

$$\sum_{R_j \in R_p^{+}} y_{p,j}^{k} = 1, \; V_p = V_s^{k}; \tag{10}$$

$$\sum_{R_j \in R_h^{+}} z_{j,h}^{k} = 1, \; V_h = V_d^{k}. \tag{11}$$

Умови збереження потоку на рівні маршрутизаторів ІКМ мають наступний вигляд [19-22]:

$$\begin{cases} \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k - \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = 0; \;\; k\in K,\, R_i \in R^-; \\ \sum\limits_{j:E_{i,j}\in E} x_{i,j}^k = y_{p,i}^k; \;\; k\in K,\, R_i \in R^+,\, V_p = V_s^k; \\ \sum\limits_{j:E_{j,i}\in E} x_{j,i}^k = z_{i,h}^k; \;\; k\in K,\, R_i \in R^+,\, V_h = V_d^k. \end{cases} \tag{12}$$

Система рівнянь (12) зв'язує між собою керуючі змінних різних типів, які відповідають за розподіл потоків пакетів на різних рівнях ІКМ. З метою погодження рішень щодо топологічного синтезу та маршрутизації вводяться умови запобігання перевантаження каналів зв'язку:

$$\sum_{k\in K} \lambda^k x_{i,j}^k \le \sum_{s=1}^{S}\sum_{t=1}^{T}\sum_{d=1}^{T} q_{t,i}^s q_{d,j}^s \varphi_{i,j}^s \,. \tag{13}$$

Фізичний зміст умов (10) полягає у тому, щоб інтенсивність потоку пакетів, яка направляється на той чи інший інтерфейс (канал), не перевищувала його пропускну здатність. У загальному випадку суміжні маршрутизатори можуть бути як однотипними, так і різнотипними. Проте вид інтерфейсу, який використовується на суміжних маршрутизаторах, має бути обов'язково однаковим, щоб забезпечити апаратну та протокольну сумісність обладнання.

II. Вибір критерію оптимальності проєктних рішень

Важливу роль при оптимізаційному формулюванні проблеми проєктування ІКМ відіграє вид і форма критерію оптимальності. Його зміст має погоджуватися з фізикою процесу та орієнтувати на застосування ефективних обчислювальних методів розрахунку множини керуючих змінних $q_{t,j}$, $q_{t,j}^s$, $x_{i,j}^k$, $y_{i,j}^k$ та $z_{j,i}^k$ за наявності обмежень (1)-(13). При цьому варто врахувати, що обмеження (1)-(12) носять лінійний характер, а умови (13) є нелінійними.

У даній роботі пропонується до використання наступна цільова функція, яку доцільно у процесі розрахунків мінімізувати:

$$J = \sum_{i=1}^{m}\sum_{t=1}^{T} g_{t,i} q_{t,i} + \sum_{i=1}^{m}\sum_{t=1}^{T}\sum_{s=1}^{S} g_t^s q_{t,i}^s + \sum_{k\in K}\sum_{E_{i,j}\in E} \lambda^k \left(g_{i,j}^{k,x} x_{i,j}^k + g_{i,j}^{k,y} y_{i,j}^k + g_{i,j}^{k,z} z_{i,j}^k \right), \tag{14}$$

де $g_{t,j}$ – умовна вартість використання t-го типу маршрутизатора у j-му місці розташування ($t=\overline{1,T}$, $j=\overline{1,m}$); g_t^s – умовна вартість використання на маршрутизаторі t-го типу інтерфейсу s-го виду ($t=\overline{1,T}$, $s=\overline{1,S}$); $g_{i,j}^{k,x}$ – маршрутна

метрика каналу, представленого дугою $E_{i,j}$; $g_{i,j}^{k,y}$ – метрика лінії доступу, представленого дугою $W_{i,j}^{+}$; $g_{i,j}^{k,z}$ – метрика лінії доступу, представленого дугою $W_{i,j}^{-}$

Для забезпечення врахування рівня кіберстійкості використаного при проєктуванні ІКМ обладнання вагові коефіцієнти $g_{t,j}$, g_t^s, $g_{i,j}^{k,x}$, $g_{i,j}^{k,y}$ та $g_{i,j}^{k,z}$ повинні наряду з вартісними показниками та показниками якості обслуговування, також враховувати показники мережної безпеки. Так, наприклад, у найпростішому випадку коефіцієнти $g_{t,j}$ повинні напряму залежати від імовірності компрометації *t*-го типу маршрутизатора (p_t). Коефіцієнти g_t^s мають додатково залежати від показників мережної безпеки каналів зв'язку, які б враховували тип використаного фізичного середовища при передачі сигналів. Тому що зрозуміло, що технічний захист інформації, яка передається оптичним або радіоканалом, може суттєво відрізнятись.

Більш системним є підхід, коли вагові коефіцієнти $g_{t,j}$ та g_t^s враховують не тільки частковий показник мережної безпеки – ймовірність компрометації маршрутизатора чи каналу, але й більш загальний показник – ризик інформаційної безпеки (РІБ). РІБ є складним показником, який досить повно враховує багато аспектів, що впливають на рівень безпеки елемента мережі, наприклад, маршрутизатора. На значення ризику інформаційної безпеки впливає тип апаратного забезпечення, тип та версія використаного програмного забезпечення, кількість та рівень критичності виявлених вразливостей та ймовірності їхньої реалізації тощо [23-25]. Вагові коефіцієнти $g_{i,j}^{k,x}$, $g_{i,j}^{k,y}$ та $g_{i,j}^{k,z}$ у цільовій функції (14) можуть опосередковано враховувати вимоги того чи іншого потоку до рівня компрометації пакетів при їхній передачі в ІКМ. По аналогії з маршрутними метриками використання вагових коефіцієнтів $g_{i,j}^{k,x}$, $g_{i,j}^{k,y}$ та $g_{i,j}^{k,z}$ (14) як функцій від показників мережної безпеки, дозволить першочергово використовувати більш безпечні маршрути в ІКМ.

Знаходження балансу між вартісними показниками, показниками QoS та показниками мережної та інформаційної безпеки при визначенні вагових коефіцієнтів у цільовій функції (14) є самостійною досить складною задачею. Якщо при постановці задачі допустимий ліміт на об'єм фінансування при проєктуванні кіберстійкої ІКМ є відомою величиною (*C*), то модель (1)-(14) можна доповнити умовою

$$\sum_{i=1}^{m}\sum_{t=1}^{T} c_{t,i} q_{t,i} + \sum_{i=1}^{m}\sum_{t=1}^{T}\sum_{s=1}^{S} c_t^s q_{t,i}^s \le C, \tag{15}$$

де $c_{t,j}$ – це фактична вартість використання *t*-го типу маршрутизатора у *j*-му місці розташування ($t=\overline{1,T}$, $j=\overline{1,m}$); c_t^s – фактична вартість використання на маршрутизаторі *t*-го типу інтерфейсу *s*-го виду ($t=\overline{1,T}$, $s=\overline{1,S}$). Тоді у виразі (14)

вагові коефіцієнти $g_{t,j}$ та g_t^s будуть за залишковим принципом враховувати виключно показники якості обслуговування, перш за все, продуктивність маршрутизаторів та пропускну здатність каналів (інтерфейсів), а також рівень їхньої мережної (інформаційної) безпеки.

Висновки

Таким чином, у основу запропонованого методу проєктування кіберстійкої ІКМ покладено розв'язання оптимізаційної задачі, пов'язаної з розрахунком керуючих змінних $q_{t,j}$, $q_{t,j}^s$, $x_{i,j}^k$, $y_{i,j}^k$ та $z_{j,i}^k$ шляхом мінімізації цільової функції (14) за наявності обмежень (1)-(13) та (15). Метод припускає, що місця ймовірного розміщення маршрутизаторів мережі попередньо відомі. Ґрунтуючись на єдиному математичному описі (1)-(15), метод проєктування охоплює погоджене, а не послідовне розв'язання задач, пов'язаних з вибором топології мережі; порядку підключення мереж доступу до маршрутизаторів ядра ІКМ; визначення характеристик використаного обладнання з погляду його продуктивності та рівня безпеки; визначення порядку маршрутизації потоків пакетів.

Кіберстійкість проєктних рішень забезпечується тим, що у цільовій функції (14) вагові коефіцієнти $g_{t,j}$, g_t^s, $g_{i,j}^{k,x}$, $g_{i,j}^{k,y}$ та $g_{i,j}^{k,z}$ наряду з вартісними показниками та показниками якості обслуговування, мають також враховувати показники мережної (інформаційної) безпеки – ймовірності компрометації або ризики інформаційної безпеки мережного обладнання. Це дозволить синтезувати мережу із заданими або прогнозованими показниками кіберстійкості.

Перспективи подальших досліджень у цьому науковому напрямку пов'язані із введенням у структуру математичної моделі (1)-(15) та методу проєктування умов забезпечення гарантованої якості обслуговування [26], що дозволить на рівні формування вагових коефіцієнтів $g_{t,j}$, g_t^s, $g_{i,j}^{k,x}$, $g_{i,j}^{k,y}$ та $g_{i,j}^{k,z}$ враховувати лише вимоги щодо рівня кіберстійкості. З іншого боку, певним напрямком вдосконалення моделі (1)-(15) є спроба перейти до лінійного варіанту умов запобігання перевантаження каналів зв'язку (13), що дозволить дещо знизити обчислювальну складність розрахунків, пов'язаних з визначенням великої кількості керуючих змінних. Обчислювальна складність рішень для проблеми проєктування є важливим, але некритичним моментом, оскільки розрахунок керуючих змінних необхідно проводити не у реальному масштабі часу.

Список літератури

1. *European Union Agency for Cybersecurity (ENISA), Lella, I., Theocharidou, M., Magonara, E., Malatras, A. et al.* (2024), ENISA Threat Landscape 2024, 131 p. **DOI**: https://doi.org/10.2824/0710888.

2. *European Union Agency for Cybersecurity (ENISA), Mattioli, R., Malatras, A.* (2024), Foresight Cybersecurity Threats For 2030 – Update 2024: Extended report, 37 p. **DOI**: https://doi.org/10.2824/349493.

3. *European Union Agency for Cybersecurity (ENISA), Tsekmezoglou, E., Lella, I., Malatras, A. et al.* (2023), ENISA Threat Landscape for DoS Attacks: January 2022 to August 2023, 33 p. **DOI**: https://doi.org/10.2824/859909.

4. *Rak, J.* (2020), Guide to Disaster-Resilient Communication Networks, 1st edition, Springer, 813 p.

5. *Mohammed, S.A., Ralescu, A.L.* (2023), Future Internet Architectures on an Emerging Scale—A Systematic Review. Future Internet, 15, 166. https://doi.org/10.3390/fi15050166.

6. *Tache, M.D., Păscuțoiu, O., Borcoci, E.* (2024), Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization. Applied Sciences, 14, 5967. https://doi.org/10.3390/app14145967.

7. *Лемешко, О. В., Поповський, В. В., Лошаков, В. А. та ін., за ред. Поповського В. В.* (2010), Багатоканальний електрозв'язок та телекомунікаційні технології: підручник у 2-х ч. Ч. 1. Харків: ТОВ "Компанія СМІТ", 470 с.

8. *Лемешко, О. В., Лошаков, В. А., Поповський, В. В. та ін.; за заг. ред. проф. Поповського В. В.* (2010), Багатоканальний електрозв'язок та телекомунікаційні технології: підручник у 2-х частинах. Ч. 2. Харків: ТОВ "Компанія СМІТ", 482 с.

9. *Лемешко, О. В., Єременко, О. С., Невзорова, О. С.* (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

10. *Лемешко, О. В., Єременко, О. С., Євдокименко, М. О., Шаповалова, А. С., Слейман, Б.* (2022), Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах: Монографія. Х.: ХНУРЕ, 198 с. **DOI**: https://doi.org/10.30837/978-966-659-378-1.

11. *Bezruk, V.M., Bukhanko, A.N., Chebotaryova, D., Varich, V.V.* (2012), "Multicriteria optimization in telecommunication networks planning, designing and controlling", Open Book "Telecommunications Networks – Current Status and Future Trends", Dr. Jesús Ortiz (Ed.), P. 251–274. **URL**: https://cdn.intechopen.com/pdfs/33213/intech-multicriteria_optimization_in_telecommunication_networks_planning_designing_and_controlling.pdf.

12. *Kozdrowski, S., Wnuk, K.* (2022), "Application of nature inspired algorithms to multi-objective optimization of new generation network problem", Proceedings of the Genetic and Evolutionary Computation Conference Companion, P. 336–339. **DOI**: https://doi.org/10.1145/3520304.3529085.

13. *Lemeshko, O., Sterin, V.* (2013), "Design and structural-functional optimization transport telecommunication network", Proceedings of the 2013 12th International Conference on the Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), Lviv, UKraine, 19-23 February, P. 208-210.

14. *Chen, M., Wang, S., Ou, Z.* (2023), "Solving the Multi-tasking Robust Optimization on Networks via Structural Reconstructions using a Multi-factor Evolutionary Algorithm", Proceedings of the 2023 International Conference on Communications, Computing and Artificial Intelligence (CCCAI), Shanghai, China, 23-25 June, P. 35–41. **DOI**: https://doi.org/10.1109/CCCAI59026.2023.00015.

15. *Galimberti, E., Bonchi, F., Gullo, F., Lanciano, T.* (2020), "Core Decomposition in Multilayer Networks", ACM Transactions on Knowledge Discovery from Data (TKDD), No. 14, P. 1–40. **DOI**: https://doi.org/10.1145/3369872.

16. *Hewitt, M., Rei, W., Wallace, S.W.* (2021), "Stochastic Network Design", in: Crainic, T.G., Gendreau, M., Gendron, B. (eds) Network Design with Applications to Transportation and Logistics, Springer, Cham, P. 283–315. **DOI**: https://doi.org/10.1007/978-3-030-64018-7_10.

17. *Єременко, О. С.* (2019), "Огляд теоретичних рішень щодо безпечної маршрутизації в інфокомунікаційних мережах", Проблеми телекомунікацій, No. 1(24). С. 3–23. **DOI**: https://doi.org/10.30837/pt.2019.1.01.

18. *Єременко, О. С., Євдокименко, М. О.* (2018), "Огляд теоретичних рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах", Проблеми телекомунікацій, No. 1(22), С. 25–42. **DOI**: https://doi.org/10.30837/pt.2018.1.02.

19. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Zhuravlova, A., Kruhlova, A., Lemeshko, V.* (2021), "Research of improved traffic engineering fault-tolerant routing mechanism in SD-WAN", Proceedings of the 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 26-28 August, P. 187-190. **DOI**: https://doi.org/10.1109/UKRCON53503.2021.9575272.

20. *Lemeshko, O., Yeremenko, O., Mersni, A., Yevdokymenko, M., Persikov, M., Kruhlova, A.* (2023), "Analysis of Proactive Models of Fault-Tolerant Routing under Load Balancing and Border Routers Availability", Proceedings of the 2023 17th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), Jaroslaw, Poland, 22-25 February, P. 28–31, **DOI**: https://doi.org/10.1109/CADSM58174.2023.10076525.

21. *Лемешко, О.В., Круглова, А.О., Крепко, А.В.* (2022), "Порівняльний аналіз проактивних рішень з відмовостійкої маршрутизації в інфокомунікаційній мережі", Проблеми телекомунікацій, No. 2(31), С. 3–22. **DOI**: https://doi.org/10.30837/pt.2022.2.01.

22. *Лемешко, О.В., Круглова, А.О., Журавльова, А.С., Лемешко, В.О.* (2020), "Вдосконалена модель балансування навантаження в інфокомунікаційній мережі. Проблеми телекомунікацій", No. 2(27), С. 56–67. **DOI**: https://doi.org/10.30837/pt.2020.2.05.

23. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Baranovskyi, O.* (2022), "Complex Investigation of the Compromise Probability Behavior in Traffic Engineering Oriented Secure Routing Model in Software-Defined Networks", in Klymash, M., Beshley, M., Luntovskyy, A. (eds) Future Intent-Based Networking, Lecture Notes in Electrical Engineering, Vol. 831, Springer, Cham, P. 145–160. **DOI**: https://doi.org/10.1007/978-3-030-92435-5_8.

24. *Євдокименко, М.О., Шаповал, М.М., Крепко, А.В.* (2020), "Потокова модель маршрутизації з балансуванням навантаження на принципах Traffic Engineering з врахуванням ризиків інформаційної безпеки", Проблеми телекомунікацій, No. 2(27), С. 32–42. **DOI**: https://doi.org/10.30837/pt.2020.2.03.

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

26. *Lemeshko, O., Papan, J., Yeremenko, O., Yevdokymenko, M., Segec, P.* (2021), "Research and Development of Delay-Sensitive Routing Tensor Model in IoT Core Networks", Sensors, No. 21, 3934. **DOI**: https://doi.org/10.3390/s21113934.