*УДК 621.391*

# МЕТОДИКА РОЗРАХУНКУ ЙМОВІРНОСТІ КОМПРОМЕТАЦІЇ КОНФІДЕНЦІЙНИХ ПОВІДОМЛЕНЬ ПРИ БЕЗПЕЧНІЙ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ШЛЯХІВ, ЯКІ ПЕРЕТИНАЮТЬСЯ

О.В. Лемешко, О.С. Єременко, М.О. Євдокименко, Т.М. Коваленко
*Харківський національний університет радіоелектроніки*

***Abstract*** *– The work presents and investigates the method of calculating the probability of confidential message compromise during secure routing in infocommunication networks, fragments of which are transmitted by intersecting paths. In comparison with existing approaches, in particular with the well-known SPREAD method, which allows the routing of confidential message fragments only by disjoint paths, the proposed solution makes it possible to achieve more efficient usage of network and cyber resources when solving the secure routing problem. The methodology is based on a mathematical model for calculating the compromise probability of fragmented messages. It was improved to enable its application in networks with a more complex structure, where routing paths are represented not only by the series-parallel connection of links but also bridges may be present. The effectiveness of the presented solution regarding secure routing was evaluated by the indicator of the confidential message compromise probability using the mechanism of its fragmentation according to Shamir's scheme. At the same time, unlike the well-known SPREAD approach, the presented technique does not require the preliminary calculation of the paths through which message fragments are transmitted, simplifying its implementation in practice. The analysis of the proposed method confirmed its higher efficiency compared to the SPREAD method, while the lower the values of the network link compromise probability, the greater the gain in terms of the message compromise probability, even in a small network with a small number of nodes, links, and only one bridge. The proposed technique is implemented as software prototypes of secure routing protocols in MATLAB and Python environments.*

*Анотація – У роботі представлено та досліджено методику розрахунку ймовірності компрометації конфіденційних повідомлень при їх безпечній маршрутизації в інфокомунікаційних. У порівнянні з існуючими підходами, зокрема з відомим методом SPREAD, який дозволяє маршрутизацію фрагментів конфіденційного повідомлення лише шляхами, які не перетинаються, запропоноване рішення дозволяє досягти більш ефективного використання мережних та кіберресурсів під час вирішення задачі безпечної маршрутизації. В основу методики покладено математичну модель розрахунку ймовірності компрометації фрагментованого повідомлення, яку було вдосконалено з метою можливості її використання у мережах з більш складною структурою, де шляхи представлені не лише послідовно-паралельним з'єднанням каналів, але й можуть включати «містки». Ефективність представленого рішення щодо безпечної маршрутизації оцінювалася за показником ймовірності компрометації конфіденційно повідомлення з використанням механізму його фрагментації за схемою Шаміра. При цьому, на відміну від відомою підходу SPREAD, представлена методика не вимагає попереднього розрахунку множини шляхів, якими передаються фрагменти повідомлення, що спрощує її реалізацію на практиці. Аналіз запропонованої методики підтвердив її більш високу ефективність у порівнянні із методом SPREAD, при цьому чим нижчими були значення ймовірності компрометації каналів зв'язку мережі, тим більший досягався виграш щодо ймовірності компрометації повідомлення – навіть у невеликій мережі з невеликою кількістю вузлів, каналів і лише одним «містком». Запропонована методика реалізована у вигляді програмних прототипів протоколів безпечної маршрутизації у середовищах MATLAB та Python.*

## Вступ

З огляду на зростаючий рівень кіберзагроз у сучасних інформаційних і телекомунікаційних системах і мережах однією з найактуальніших задач на сьогодні є розвиток та вдосконалення існуючих методів і технологій забезпечення інформаційної

безпеки. Інфокомунікаційні системи та мережі є складними багаторівневими об'єктами, де на кожному рівні існують свої окремі завдання, які вирішуються в межах протоколів відповідного рівня. Одним з цих завдань у сучасних інфокомунікаційних системах, безперечно, є завдання забезпечення інформаційного захисту. Відповідно до вимог стандартів Міжнародного союзу телекомунікацій (International Telecommunication Union, ITU), розрізняють три основні рівні забезпечення інформаційної безпеки мереж: безпека інфраструктури, безпека послуг і безпека додатків [1, 2]. Безпека інфраструктури має на увазі забезпечення безпеки на рівні мережних елементів (комутаторів, маршрутизаторів, серверів), на рівні каналів зв'язку та на рівні шляхів (маршрутів), які складаються з вузлів та каналів. Водночас рівень інфраструктури є фундаментальним для двох верхніх рівнів, тому ефективність методів забезпечення інформаційної безпеки на рівні інфраструктури визначає, наскільки ефективним буде захист від кіберзагроз на рівні послуг і додатків.

Реалізація розроблених методів і механізмів захисту інформації має забезпечуватися відповідними протоколами на кожному з рівнів семирівневої моделі OSI [1-4]. Так, наприклад, на мережному рівні ці завдання мають вирішуватися за допомогою протоколів маршрутизації. Як показано у роботах [2, 5-9] за допомогою засобів маршрутизації може здійснюватися безпечна доставка різної конфіденційної інформації, зокрема сеансових ключів, інформації про аутентифікацію, критично важливих даних користувачів тощо. Таким чином, методи безпечної маршрутизації є одними з ключових механізмів забезпечення інформаційної безпеки на рівні інфраструктури та безпосередньо впливають на показники захищеності та кіберстійкості інфокомунікаційних мереж (ІКМ) [10-14].

Необхідно зазначити, що під час розробки ефективних методів безпечної маршрутизації потрібно враховувати рівень захищеності елементів мережі, який оцінюється за допомогою такого важливого показника, як імовірність компрометації. Під компрометацією мається на увазі факт несанкціонованого доступу до інформації, а також наявність підозри щодо такого несанкціонованого доступу [2, 15]. Залежно від часу реакції на можливу компрометацію каналів зв'язку і фрагменти мережі розрізняють проактивні та реактивні засоби, зокрема пов'язані з рішеннями маршрутизації. Проактивні засоби використовуються зазвичай на етапі запобігання компрометації передачі повідомлень або з метою мінімізації ймовірності її виникнення [14]. Реактивні засоби використовуються в тих випадках, коли безпеку даних, що передаються, було порушено, і необхідно швидко відновити заданий рівень безпеки, наприклад, шляхом зміни маршруту на інший, більш безпечний.

Багатошляхова маршрутизація, під час якої відбувається розбиття повідомлень на частини, з подальшою передачею від джерела до отримувача фрагментів повідомлення різними шляхами, є прикладом проактивного підходу. Якщо виникає порушення рівня безпеки повідомлення, що передається, набір шляхів і порядок розподілу фрагментів повідомлень цими шляхами перераховуються відповідно до змін у стані ІКМ, водночас відбувається балансування фрагментів повідомлення між різними шляхами [15]. Ефективність конкретних протокольних рішень, що реалізують подібні

методи, визначається перш за все порядком розрахунку шляхів та в значній мірі залежить від покладених в його основу математичних моделей. У статті розглянуто існуючі математичні рішення та запропоновано вдосконалену математичну модель та методику, які дозволяють вирішувати задачу безпечної маршрутизації повідомлень у мережі зі складною топологією, яку неможливо звести лише до паралельно-послідовного типу з'єднання у структурі каналів зв'язку ІКМ.

## I. Огляд існуючих моделей і методів безпечної маршрутизації конфіденційних повідомлень шляхом їх фрагментованої передачі

Одним із напрямів забезпечення необхідного рівня інформаційної безпеки в ІКМ є реалізація механізму, заснованого на використанні багатошляхової маршрутизації повідомлення, попередньо розділеного на частини за схемою Шаміра [2, 15]. Внаслідок використання такої схеми можна зменшити ймовірність компрометації повідомлення, оскільки для цього зловмиснику необхідно скомпрометувати всі шляхи, якими передаються частини розділеного повідомлення.

У відомих дослідженнях інших авторів [15, 16] було розглянуто підхід до розробки та вдосконалення механізму безпечної маршрутизації SPREAD. Цей механізм передбачає:

- розрахунок набору маршрутів, що не перетинаються, між заданими вихідним і кінцевим вузлами;
- поділ конфіденційного повідомлення, що передається, на кілька фрагментів за обраною схемою Шаміра;
- розподіл фрагментів повідомлення по маршрутах, які не перетинаються.

У загальному випадку зловмиснику може бути відома схема поділу повідомлення на фрагменти, але компрометація цього конфіденційного повідомлення буде можливою лише, якщо будуть скомпрометовані всі маршрути, які використовуються для його доставки. Тому рівень інформаційної безпеки визначається кількістю шляхів, які використовуються для доставки фрагментів повідомлення, та рівнем їх безпеки.

Проте, як показав проведений аналіз [15-17], можливість розрахунку ймовірності компрометації повідомлення, що передається в мережі, багато в чому визначається структурними властивостями мережі та тим, які типи шляхів використовуються. Набір шляхів у мережі можна розділити на два типи: шляхи, що не перетинаються, і шляхи, що перетинаються, тобто мають спільні вузли/канали [2, 18]. Шляхи, що не перетинаються, мають спільними лише вузол-джерело та вузол-отримувач повідомлення. Шляхи, що перетинаються, завжди мають хоча б один спільний вузол і/або канал зв'язку. Якщо вони мають спільні канали, вони називаються шляхами, що перетинаються каналами. Якщо ж шляхи мають спільні вузли, вони називаються шляхами, що перетинаються вузлами.

Математична модель, покладена в основу методу безпечної маршрутизації за шляхами, які не перетинаються, SPREAD є найпростішою. Під час розрахунку

ймовірності компрометації повідомлення, що передається частинами з використанням шляхів, що не перетинаються, передбачається, що компрометація елементу (вузла, каналу) шляху призведе до компрометації всіх фрагментів повідомлення, які передаються через цей елемент мережі [15, 17].

Перевагами методу SPREAD є те, що у разі використання для передачі частин конфіденційного повідомлення набору шляхів, що не перетинаються, процес розрахунку ймовірності його компрометації в мережі значно спрощується, однак необхідно попередньо розрахувати множину подібних шляхів. З іншого боку, обмеження доступних рішень лише набором шляхів, що не перетинаються, може призвести до того, що рішення поставленої задачі щодо забезпечення заданого рівня безпеки за таких умов не може бути знайдене. І хоча в мережі з такою самою топологію теоретично воно може існувати, якщо розглядати шляхи, що перетинаються, проте процедура розрахунку ймовірності компрометації повідомлення, запропонована у методі SPREAD, в цьому разі значно ускладнюється, й іноді знаходження такого рішення в аналітичній формі стає неможливим [2, 15-17].

Під час забезпечення високого рівня мережної безпеки та якості обслуговування варто враховувати, що сучасні інфокомунікаційні мережі є гетерогенними системами з досить складною та неоднорідною (нерегулярною) топологією. Тому між заданою парою маршрутизаторів ІКМ зазвичай існує декілька шляхів, які мають досить різні характеристики як щодо пропускної здатності, затримок і втрат пакетів, так і ймовірності компрометації. Проте використання при безпечній маршрутизації лише маршрутів, які не перетинаються, залишає поза увагою деякі вузли та канали, які мають певний мережний і кіберресурс. Нехтувати такими ресурсами, особливо в умовах складних та інтенсивних кіберзагроз, недоцільно.

В роботах [19, 20] було запропоновано метод забезпечення безпечної маршрутизації шляхами, що перетинаються. Під час розробки математичної моделі, покладеної в основу представленого методу, було введене поняття «композитного» шляху, який є більш складною структурною формою, що містить фрагменти мережі з послідовним та/або паралельним з'єднанням каналів мережі. Такий підхід дозволив сформулювати задачу пошуку набору шляхів, що перетинаються, у формі оптимізаційної задачі цілочисельного нелінійного програмування. Основою методу є оптимізація процесу вибору набору композитних шляхів і балансування між ними частин повідомлення, що передається, таким чином, щоб було забезпечено зазначений рівень імовірності компрометації повідомлення. Водночас множина змінних для обчислення, що характеризують кількість переданих частин повідомлення в композитному шляху, є цілими числами, а критерій оптимізації, пов’язаний з обчисленням імовірності компрометації повідомлення, та обмеження є нелінійними функціями.

Запропонований у роботах [19, 20] метод дозволяє знайти розв’язання задачі безпечної багатошляхової маршрутизації з урахуванням маршрутів, що перетинаються, для яких можна аналітично розрахувати, а отже, контролювати ймовірність компрометації повідомлення. Проте цей метод має деякі обмеження

щодо рівня структурної складності ІКМ, у якій його можна використати, та передбачає маршрутизацію за шляхами, які мають лише послідовно-паралельне з'єднання каналів зв'язку.

Проведений аналіз у роботах [19, 20] показав, що використання запропонованого рішення в межах наведених розрахункових прикладів дозволив у порівнянні з механізмом SPREAD знизити ймовірність компрометації переданих повідомлень залежно від розміру ІКМ у середньому від 5–10 % до 25–50 %. У цій роботі запропоновано подальший розвиток описаних рішень, представлений у вигляді методу безпечної маршрутизації конфіденційних повідомлень за маршрутами з довільним характером перетинання в ІКМ та проведено його порівняльний аналіз з класичним рішенням SPREAD.

## II. Методика розрахунку ймовірності компрометації конфіденційних повідомлень, які фрагментовано передаються за шляхами, які перетинаються

Для опису математичної моделі розрахунку ймовірності компрометації конфіденційних повідомлень буде використовуватись система позначень, яку наведено в табл. 1.

Для розрахунку ймовірності компрометації $i$-го шляху, що складається з $M_i$ елементів, у роботах [19, 21] використовувалась наступна формула:

$$p_i = 1-\left(1-p_i^1\right)\left(1-p_i^2\right)\ldots\left(1-p_i^{M_i}\right) = 1-\prod_{j=1}^{M_i}\left(1-p_i^j\right). \quad (1)$$

При цьому змінні $n_i$ ($i=\overline{1,M}$) мають відповідати такій умові [19, 21]:

$$\sum_{i=1}^{M} n_i = N. \quad (2)$$

У разі використання схеми Шаміра з параметрами $T<N$ повинні виконуватись умови [19, 21]:

$$N-T+1 \le n_i \le T-1, \ (i=\overline{1,M}). \quad (3)$$

При використанні схеми без надмірності, тобто коли $T=N$ виконуються такі умови [19, 21]:

$$1 \le n_i \le T-1, \ (i=\overline{1,M}). \quad (4)$$

*Таблиця* 1. Система позначень

| Позначення | Опис |
|---|---|
| $G=(R,E)$ | Граф мережі |
| $R=\left\{R_i; i=\overline{1,m}\right\}$ | Множина вершин (маршрутизаторів) |
| $E=\left\{E_{i,j}; i,j=\overline{1,m}; i\neq j\right\}$ | Множина дуг (каналів зв'язку) |
| $V$ | Кількість каналів у мережі |
| $s$ | Вихідний вузол |
| $d$ | Кінцевий вузол |
| $M$ | Кількість шляхів, що не перетинаються |
| $M_i$ | Кількість каналів в $i$-му шляху, які можуть бути скомпрометовані ($i=\overline{1,M}$) |
| $\tilde{M}$ | Кількість шляхів, які перетинаються та можуть бути використаними для фрагментованої передачі конфіденційного повідомлення |
| $p^j$ | Імовірність компрометації $j$-го каналу ІКМ ($j=\overline{1,V}$) |
| $q^j$ | Імовірність події, що $j$-й канал ІКМ не буде скомпрометовано ($j=\overline{1,V}$) |
| $p_i^j$ | Ймовірність компрометації $j$-го каналу $i$-го шляху ($i=\overline{1,M}$, $j=\overline{1,M_i}$) |
| $(T,N)$ | Параметри схеми Шаміра |
| $N$ | Загальна кількість фрагментів, на які розбивається повідомлення за схемою Шаміра |
| $T$ | Мінімальна кількість фрагментів, необхідних для відновлення надісланого повідомлення ($T\leq N$) |
| $p_i$ | Імовірність компрометації $i$-го шляху ($i=\overline{1,M}$) |
| $P_{msg}$ | Імовірність компрометації всього повідомлення за його фрагментарної передачі у мережі |
| $n_i$ | Цілочисельна змінна, що характеризує кількість фрагментів повідомлення, переданих $i$-м шляхом ($i=\overline{1,M}$) |

У разі використання фрагментації повідомлення за схемою Шаміра з подальшою передачею $N$ фрагментів повідомлення $M$ шляхами, які не перетинаються, ймовірність компрометації конфіденційного повідомлення можливо розрахувати за формулою [19, 21]:

$$P_{msg}=\prod_{i=1}^{M}p_i\,. \tag{5}$$

Крім того, для кожного каналу зв'язку ІКМ буде справедливою наступна умова:

$$p^j + q^j = 1,\ (j = \overline{1,V}). \quad (6)$$

Однак, у разі безпечної маршрутизації шляхами, що перетинаються, події, пов'язані з компрометацією шляхів, стають сумісними, тобто формула (5) для розрахунку ймовірності компрометації повідомлення використовуватись не може. Тоді, в межах логіко-ймовірнісного підходу [22, 23] елементи мережі, за якими перетинаються маршрути, можна представити у вигляді так званих «містків» або «перемичок». Наприклад, для структури ІКМ, представленої на рис. 1, при передачі конфіденційного повідомлення між $R_1$ і $R_4$ «містком» виступає канал між маршрутизаторами $R_2$ і $R_3$. Цей «місток» з'єднує два маршрути, які не перетинаються: $R_1 \to R_2 \to R_4$ та $R_1 \to R_3 \to R_4$.

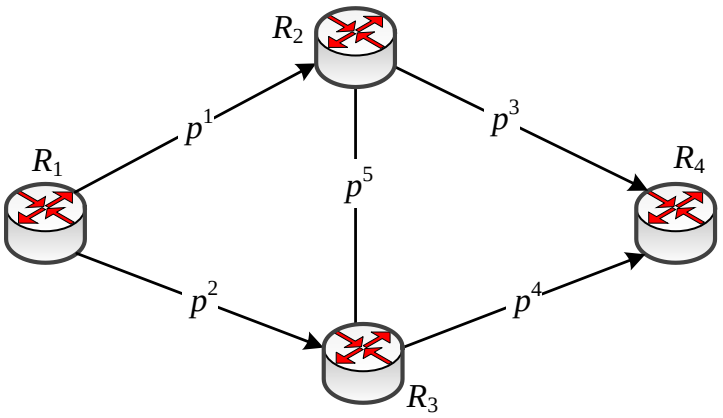


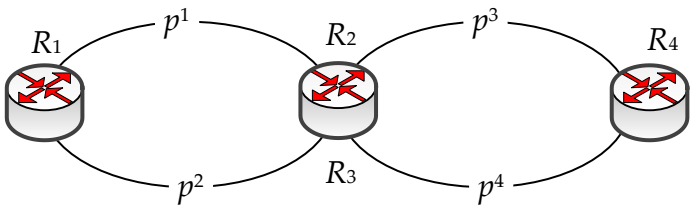

*Рис.* 1. Досліджуваний фрагмент структури ІКМ

Структура ІКМ з «містком» між $R_2$ і $R_3$ залежно від крайніх значень імовірності компрометації каналу $E_{2,3}$ може набувати варіанти з'єднань, які наведені на рис. 2. Тобто, якщо канал $E_{2,3}$ абсолютно безпечний ($p^5 = 0$), то структура ІКМ може бути представленою варіантом, показаним на рис. 2, а. У випадку компрометації цього ж каналу ($p^5 = 1$) структура ІКМ може бути описана топологією, наведеною на рис. 2, б. Тоді вираз для ймовірності компрометації повідомлення, яке передається між $R_1$ і $R_4$, буде записано на основі формули для обчислення повної ймовірності компрометації мережі, наведеної на рис. 1:

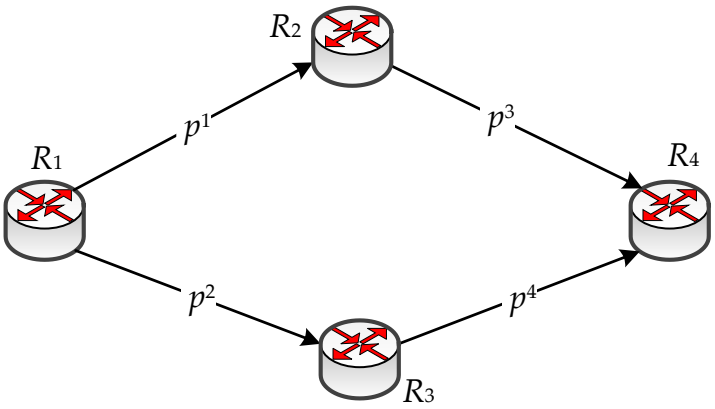
$$P_{msg} = q^5(1-(1-p^1p^2)(1-p^3p^4)) + p^5(1-q^1q^3)(1-q^2q^4). \quad (7)$$

З метою проведення подальшого порівняльного аналізу визначимо ймовірність компрометації повідомлення, яке передається за двома шляхами, що не перетинаються (рис. 2, б):

$$P_{msg} = (1-q^1q^3)(1-q^2q^4). \quad (8)$$




а) $p^5 = 0$, $q^5 = 1$




б) $p^5 = 1$, $q^5 = 0$

*Рис.* 2. Варіанти з'єднань маршрутизаторів ІКМ залежно від крайніх значень імовірності компрометації каналу $E_{2,3}$

## III. Дослідження рівня безпеки ІКМ, в якій використовуються шляхи, що перетинаються

У роботі проведено дослідження з метою оцінки виграшу щодо рівня безпеки ІКМ від використання безпечної маршрутизації за шляхами, що перетинаються, у порівнянні з рішенням SPREAD. На рис. 3 показано залежність імовірностей компрометації повідомлення (7) і (8) від імовірностей компрометації каналів зв'язку ІКМ (рис. 1), які в межах даного прикладу вважались однаковими. З наведених графіків можна зробити висновок, що за наявності перетинання шляхів, імовірність компрометації повідомлення буде нижчою, ніж у разі передачі фрагментів повідомлення шляхами, що не перетинаються.

Числові значення такого виграшу для структури мережі, наведеної на рис. 1, представлено на рис. 4. З отриманих результатів розрахунків можна зробити висновок, що найбільше зниження ймовірності компрометації повідомлення $P_{msg}$ за рахунок використання «містка» спостерігається при малих значеннях імовірності компрометації каналів і досягає 45% при мінімальних її значеннях.

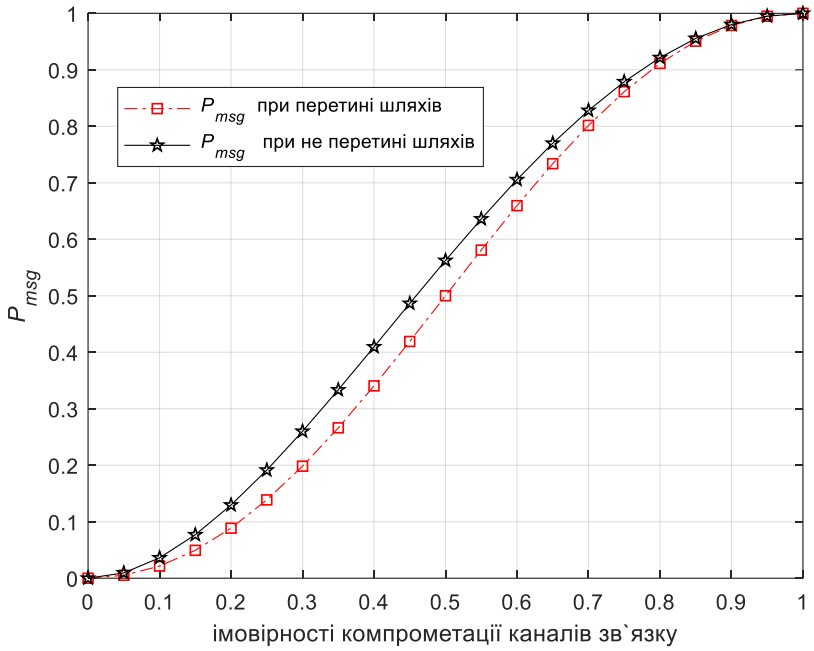



*Рис.* 3. Залежність імовірності компрометації повідомлення (7) та (8) від імовірностей компрометації каналів зв'язку ІКМ

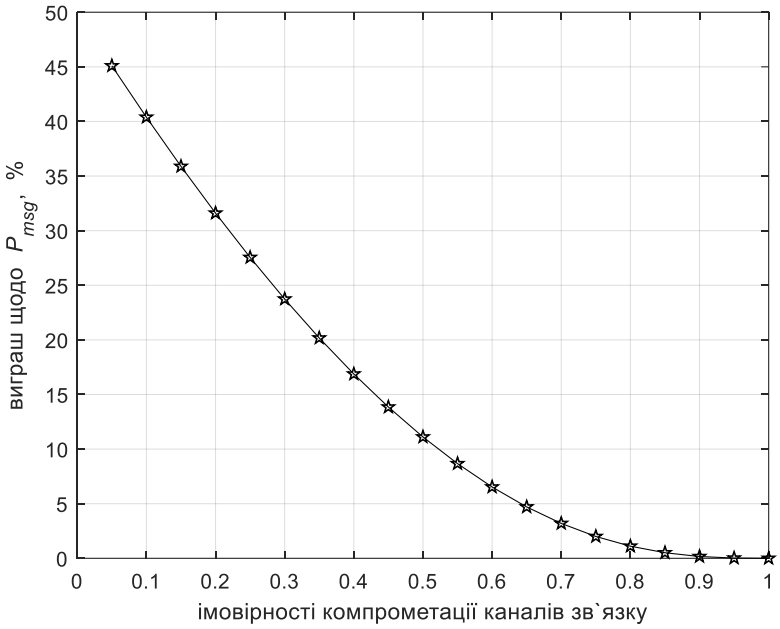



*Рис.* 4. Виграш від використання шляхів, які перетинаються, для структури мережі, наведеної на рис. 1

З метою дослідження впливу ймовірності компрометації окремих каналів на виграш у ймовірності компрометації повідомлення за рахунок використання шляхів, що перетинаються, було досліджено залежність виграшу щодо $P_{msg}$ від імовірності компрометації каналу $E_{2,3}$ ($p^5$) за умови, коли ймовірність компрометації всіх інших

каналів ІКМ є однаковою. Результати цього дослідження наведено на рис. 5, де показано, як змінюється значення виграшу, якщо ймовірність компрометації каналу $E_{2,3}$ ($p^5$) збільшується у межах від 0 до 1. Розрахунки було проведено для значень імовірностей компрометації всіх інших каналів ІКМ $p^j = 0,2;\ 0,4;\ 0,6$ та $0,8$, $j \neq 5$.

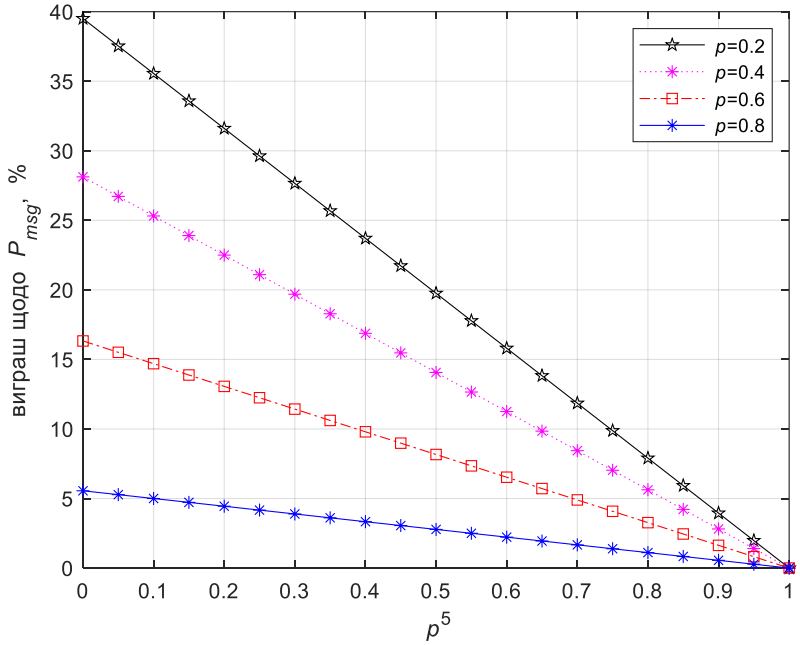



*Рис.* 5. Залежність виграшу щодо значень ймовірності компрометації повідомлення від ймовірності компрометації каналу $E_{2,3}$ ($p^5$) для різних значень ймовірностей компрометації інших каналів мережі

З наведених графіків видно, що найбільший виграш (найбільше зниження ймовірності компрометації повідомлення $P_{msg}$) від використання маршрутизації фрагментованого повідомлення шляхами, що перетинаються, у порівнянні з маршрутизацією шляхами, що не перетинаються, також має місце при малих значеннях ймовірності компрометації каналу $E_{2,3}$ ($p^5$). Така сама залежність спостерігається й щодо ймовірностей компрометації інших каналів ІКМ: чим нижча ця ймовірність, тим більший виграш щодо ймовірності компрометації повідомлення $P_{msg}$ досягається за рахунок використання «містка».

Таким чином, навіть для невеликої за кількістю вузлів структури ІКМ (рис. 1) з мінімальним числом каналів та одним «містком» використання шляхів, які перетинаються, дозволяє значно знизити ймовірність компрометації конфіденційного повідомлення. При зміні ймовірності компрометації каналів у діапазоні від 0,05 до 0,7 вдавалось знизити ймовірність компрометації повідомлення $P_{msg}$ від 3,2% до 45%.

## Висновки

У статті запропоновано методику розрахунку ймовірності компрометації конфіденційних повідомлень при безпечній маршрутизації з використанням шляхів, що перетинаються. У межах запропонованої методики використовується формула повної ймовірності компрометації повідомлення з урахуванням рівня мережної безпеки «містків» у структурі мережі. Крім того, у порівнянні з відомим раніше механізмом SPREAD представлена методика не вимагає попереднього розрахунку множини шляхів, що не перетинаються, що спрощує її реалізацію на практиці.

В межах проведеного дослідження розробленої методики було показано, що використання шляхів, що перетинаються, забезпечує більш низькі значення ймовірності компрометації фрагментованого повідомлення у порівнянні із відомим методом SPREAD, який дозволяє використовувати під час маршрутизації лише такі шляхи, що не мають перетинів. Застосування при безпечній маршрутизації шляхів, які перетинаються, призводить до більш ефективного використання пропускної здатності мережі та її кіберресурсу.

Відповідно до виконаних розрахунків виграш щодо ймовірності компрометації конфіденційного повідомлення за рахунок використання навіть одного «містка» може досягати 45% у порівнянні з відомим методом SPREAD. Так, наприклад, якщо ймовірність компрометації каналів ІКМ дорівнює 0,2, то виграш за рахунок використання «містків» складає трохи більше 30%, але якщо ймовірність компрометації каналів ІКМ знижується до 0,05, то цей виграш зростає вже до 45%.

Незважаючи на те, що в представленій моделі розрахунку ймовірності компрометації повідомлення розглядається тільки ймовірність компрометації каналів мережі, рівень мережної безпеки вузлів (маршрутизаторів) також може буде врахований без зміни змісту запропонованої моделі – шляхом представлення вузлів мережі віртуальними мережними каналами, через які також проходять повідомлення під час маршрутизації.

Вдосконалену математичну модель реалізовано у вигляді програмних прототипів протоколів безпечної маршрутизації у середовищах MATLAB та Python. Ці прототипи можуть бути використані під час розробки перспективних протоколів маршрутизації, що підтримують метрики безпеки для подальшого використання в традиційних і програмно-конфігурованих мережах з метою підвищення рівня їх кібербезпеки.

Напрямки подальших досліджень у сфері безпечної маршрутизації в ІКМ передбачають розробку більш досконалих математичних моделей і методів, пов'язаних з урахуванням не лише ймовірності компрометації каналу, але й інших показників мережної безпеки, наприклад, оцінки вразливостей та ризиків інформаційної безпеки.

## Список літератури

1. *ITU-T* (2003), X-805: Security architecture for systems providing end-to-end communications, Geneva, 28 p.

2. *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

3. *ISO* (1989), 7498–2:1989: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 32 p.

4. *ITU-T* (1991), X-800: Security architecture for Open Systems Interconnection for CCITT applications, Geneva, 48 p.

5. *Stallings, W.* (2016), Cryptography and Network Security: Principles and Practice, 7th edn. Pearson, London.

6. *Schneier, B.* (2015), Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, 1st edn. WW Norton & Company, New York.

7. *Cisco Networking Academy* (2014), Routing Protocols Companion Guide, 1st edn. Cisco Press.

8. *Santos, O., Kampanakis, P., Woland, A.* (2016), Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP, 1st edn. Cisco Press

9. *Wang, M., Liu, J., Mao, J., Cheng, H., Chen, J.* (2016), "NSV-GUARD: constructing secure routing paths in software defined networking", Proceedings of the 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom), P. 293–300.

10. *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), No. 1, Metz, France, 18-21 September, P. 117-122. **DOI**: https://doi.org/10.1109/IDAACS.2019.8924294

11. *Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Shapovalova, A., Lemeshko, V., Persikov, M.* (2021), "Analysis of Secure Routing Processes Using Traffic Engineering Model", Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22-25 September, P. 951-955. **DOI**: https://doi.org/10.1109/IDAACS53288.2021.9660980

12. *Lemeshko, O., Yeremenko, O., Shapovalova, A., Hailan, A. M., Yevdokymenko, M., Persikov, M.* (2021), "Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach," Proceedings of the 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2021, Lviv, Ukraine, 22-26 February, P. 23-26. **DOI**: https://doi.org/10.1109/CADSM52681.2021.9385253

13. *Chhaytli A., Persikov M.* (2021), "Providing cyber resilience in software-defined networks by secure routing means", Infocommunication technologies and electronic engineering, No.1(1), P. 11-19. **DOI**: https://doi.org/10.23939/ictee2021.01.011

14. *Almerhag, I. A., Almarimi, A. A., Goweder, A. M., Elbekai, A. A.* (2010), "Network security for QoS routing metrics", Proceedings of the 2010 International Conference on Computer and Communication Engineering (ICCCE), P. 1–6.

15. *Lou, W., Liu, W., Zhang, Y., Fang, Y.* (2009), "SPREAD: improving network security by multipath routing in mobile ad hoc networks", Wirel. Netw., No. 15(3), P. 279–294.

16. *Alouneh, S., Agarwal, A., En-Nouaary, A.* (2009) "A novel path protection scheme for MPLS networks using multi-path routing", Comput. Netw. No. 53(9), P. 1530–1545.

17. *Yeremenko, O. S., Ali, A. S.* (2015) "Secure multipath routing algorithm with optimal balancing message fragments in MANET", Radioelectron. Inform. No. 1(68), P. 26–29.

18. *Yeremenko, O.* (2015), "Enhanced flow-based model of multipath routing with overlapping by nodes paths", Proceedings of the 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), P. 42-45.

19. *Yeremenko, O., Lemeshko, O., Persikov, A.* (2018), "Secure Routing in Reliable Networks: Proactive and Reactive Approach", Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655. **DOI**: https://doi.org/10.1007/978-3-319-70581-1_44

20. *Yeremenko O., Lemeshko O., Persikov A.* (2017), "Enhanced method of calculating the probability of message compromising using overlapping routes in communication network", Proceedings of the 2017 XIIth International Scientific and Technical Conference Computer Sciences and Information Technologies (CSIT), P. 87-90.

21. *W. Lou W., Liu W, Fang Y. (2004),* "SPREAD: enhancing data confidentiality in mobile ad hoc networks", IEEE INFOCOM 2004, vol. 4, P. 2404-2413. **DOI**: https://doi.org/10.1109/INFCOM.2004.1354662

22. *Boesch, F. T.* (1988), "A survey and introduction to network reliability theory", Proceedings of the IEEE International Conference on Communications, - Spanning the Universe, No. 2, P. 678-682. **DOI**: https://doi.org/10.1109/ICC.1988.13649

23. *Pai, K.-J., Chang, R.-S., Wu, R.-Y., Chang, J.-M.* (2019), "Three Completely Independent Spanning Trees of Crossed Cubes with Application to Secure-Protection Routing", Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), P. 1358-1365. **DOI**: https://doi.org/10.1109/HPCC/SmartCity/DSS.2019.00189