УДК 621.391

ОГЛЯД ТЕОРЕТИЧНИХ РІШЕНЬ ЩОДО БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

О.С. ЄРЕМЕНКО
Харківський національний університет радіоелектроніки

Abstract *– In this article, an overview of theoretical solutions for secure routing in infocommunication networks (ICNs) ranging from empirical solutions to system optimization approaches has been provided. Due to the fact that network security solutions must be complex in terms of both organizational and technical aspects, the implementation of all available technological and protocol means used at different levels of the OSI model should be implemented in practice. An important place in this set of means is taken precisely by the technological solutions of the Network Layer, namely routing protocols. The analysis has shown that proactive solutions related to the use of threshold cryptography, which is widely used to enhance network security in ICN, have great potential. At the same time, in multipath secure routing, it is promising to use not only disjoint paths but also a special class of overlapping paths, which form the basis of composite paths and contain network fragments with serial and/or parallel connection of network communication links. However, the use of proactive network security solutions in ICN should be complemented by appropriate reactive means when the network remains operational, even with the local compromise of its elements, such as paths, that require the development of new mathematical models and methods for secure fast rerouting.*

Анотація *– В статті представлено огляд теоретичних рішень щодо безпечної маршрутизації в інфокомунікаційних мережах (ІКМ). Як показав аналіз, великий потенціал мають проактивні рішення із застосуванням порогової криптографії. При цьому при багатошляховій безпечній маршрутизації перспективним представляється використання не тільки шляхів, що не перетинаються, а й особливого класу шляхів, що перетинаються. Проте використання проактивних рішень має бути доповнене відповідними реактивними засобами, коли мережа зберігає працездатність навіть при локальній компрометації її елементів, що вимагає розробки нових або вдосконалення існуючих математичних моделей і методів безпечної швидкої перемаршрутизації.*

Аннотация *– В статье представлен обзор теоретических решений по безопасной маршрутизации в инфокоммуникационных сетях (ИКС). Как показал анализ, большой потенциал имеют проактивные решения с применением пороговой криптографии. При этом при многопутевой безопасной маршрутизации перспективным представляется использование не только непересекающихся путей, но и особого класса пересекающихся. Однако использование проактивных решений должно быть дополнено соответствующими реактивными средствами, когда сеть сохраняет работоспособность даже при локальной компрометации ее элементов, что требует разработки новых или усовершенствования существующих математических моделей и методов безопасной быстрой перемаршрутизации.*

Вступ

Як показав проведений аналіз [1-16], вибір тих чи інших мережних технології при побудові мультисервісних інфокомунікаційних мереж (ІКМ) залежить від ступеня задоволення *комплексу вимог*, що продиктовані всіма учасниками інформаційно-комунікаційного процесу – користувачами, операторами зв'язку та виробниками різноманітного телекомунікаційного обладнання та програмного забезпечення [10]. Основною вимогою, що висувається до ІКМ, є виконання її основної функції – надання користувачам широкого переліку послуг зв'язку із забезпеченням заданого рівня якості обслуговування, відмовостійкості та безпеки.

Суцільний комплекс вимог до сучасних ІКМ можна узагальнити наступним чином [10]:

– забезпечення широкого спектру градацій *якості обслуговування користувачів*, підтримка класів обслуговування;

– висока *продуктивність* ІКМ, заснована на ефективному використанні мережних ресурсів (канальних, буферних, обчислювальних, програмних та інформаційних);

– *надійність* ІКМ як на експлуатаційному рівні (*відмовостійкість*), так і на рівні доставки пакетів (імовірність доставки);

– висока *масштабованість*, тобто здатність ІКМ зберігати в заданих границях показники своєї ефективності в умовах зростання розміру мережі, кількості користувачів, послуг, що досягається сегментацією ІКМ і використанням ієрархічної структурної та функціональної побудови;

– підтримка комплексних апаратно-програмних рішень щодо *мережної безпеки*, яка має забезпечуватися на всіх рівнях надання послуги.

Відповідно до проведеного аналізу [10, 12-14, 17-24], однією з найважливіших задач, яка регламентується стандартами побудови інфокомунікаційних систем і мереж, є завдання реалізації функцій мережної безпеки. Згідно зі стандартом ITU-T X-805 [25], в архітектурі безпеки (рис. 1) інфокомунікаційної мережі можна умовно виділити наступні площини:

– **функціональні площини безпеки**:
- *контролю* (для передачі службової інформації з метою моніторингу стану ресурсів системи);
- *управління* (для передачі службової інформації з метою поточного управління ресурсами системи);
- *користувача* (для передачі інформації);

– **рівні безпеки**:
- *інфраструктури*, яка складається з елементів системи (каналів зв'язку, каналоутворюючої апаратури, маршрутизаторів, серверів тощо);
- *сервісів* (послуг), які надаються кінцевим користувачам інфокомунікаційною мережею та провайдерами;
- *додатків*, які приймають участь у комунікаційному процесі та генерують трафік користувачів, який циркулює в мережі.

У відповідності до цих площин і рівнів, формуються модулі захисту ІКМ, які характеризуються наступними параметрами: управління доступом; автентифікація; збереженість інформації; конфіденційність даних; безпека зв'язку; цілісність даних; доступність; секретність.

Відповідно до вимог стандартів ITU, забезпечення інформаційної безпеки здійснюється в рамках трьох рівнів: безпеки інфраструктури, безпеки сервісів і безпеки додатків (рис. 1) [25]. При цьому ефективність роботи верхніх двох рівнів цілком і повністю визначається ефективністю функціонування засобів рівня безпеки інфраструктури, основним завданням якого є забезпечення безпеки на рівні мережних елементів (комутаторів, маршрутизаторів, серверів), каналів зв'язку та маршрутів у цілому, які з них складаються.

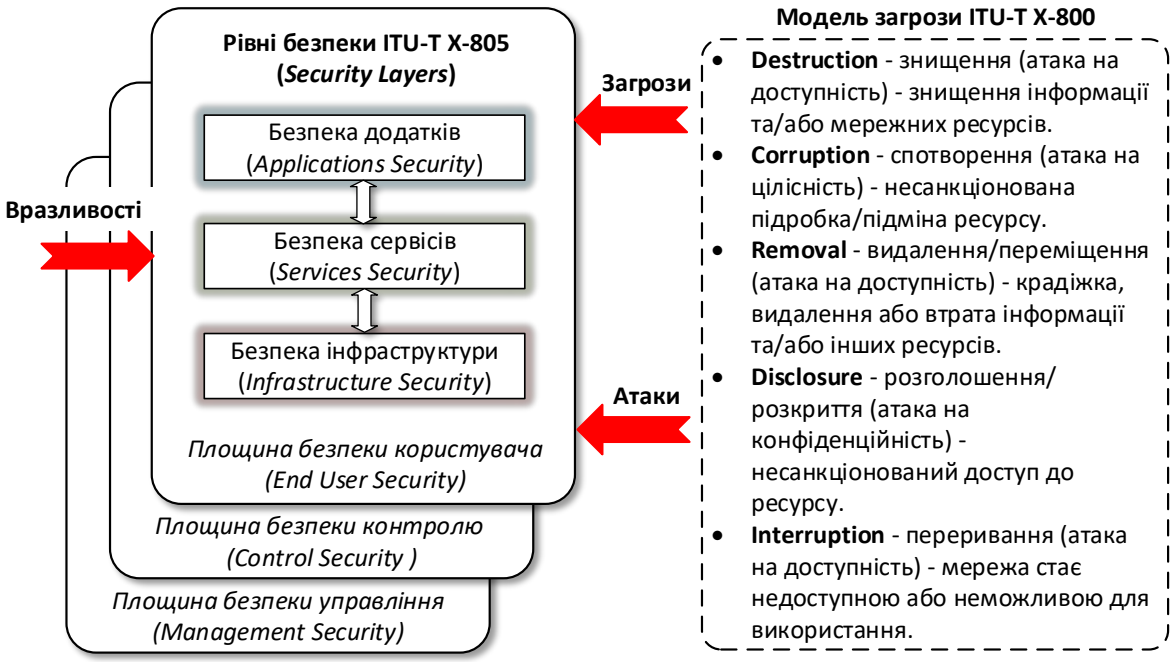

Рис. 1. Архітектура безпеки відповідно до стандарту ITU-T X-805

Якщо розглядати забезпечення мережної безпеки з точки зору рівнів моделі взаємодії відкритих систем (Open Systems Interconnection, OSI) і стандарту ISO 7498-1, а також архітектури безпеки згідно з ISO 7498-2 [26-28], то сервіси безпеки повинні забезпечуватися протоколами відповідних рівнів моделі OSI. У свою чергу безпека на мережному рівні повинна підтримуватися і забезпечуватися також протоколами маршрутизації.

До засобів забезпечення мережної безпеки, як правило, відносять автентифікацію; криптографічний захист; системи аналізу та аудиту; виконання політик безпеки; використання міжмережних екранів; застосування систем виявлення та протидії атакам; управління трафіком і контроль доступу [29, 30].

I. Загальна характеристика засобів мережної безпеки в ІКМ

Важлива роль при управлінні трафіком у ході конфігурування мережного обладнання відводиться задачам формування списків доступу (Access Control List, ACL) [17, 18, 29]. Списки доступу можна використовувати для контролю над потоками пакетів, їх ідентифікації, для обмеження поширення оновлень маршрутизації, проте однією з найбільш важливих причин використання списків доступу є забезпечення мережної безпеки. Списки доступу входять до функціональних можливостей «брандмауера» (міжмережного екрану, Firewall) маршрутизаторів, які часто розташовані між LAN і WAN мережами. Можна також використовувати списки доступу на маршрутизаторах, розташованих між двома мережами, для управління трафіком при вході або виході з певної мережі.

ACL дозволяють фільтрувати мережний трафік шляхом заборони або дозволу передачі пакетів, що надходять на вхідні та/або вихідні інтерфейси маршрутизатора.

В ході фільтрації трафіка маршрутизатор перевіряє кожен пакет і приймає рішення про те, передати його або відкинути, ґрунтуючись на ACL. Тоді як при розподілі канального ресурсу ІКМ у ході конфігурування механізмів PQ, CQ, CBWFQ і LLQ за допомогою посилань на ACL можна конкретизувати, яким саме пакетам (потокам) виділяється та чи інша черга та пропускна здатність інтерфейсу.

Крім того, якщо стандартні ACL використовуються для фільтрації пакетів виключно на основі IP-адреси джерела трафіка на мережному рівні моделі OSI, то розширені ACL можуть оперувати інформацією про ймовірного відправника та/або одержувача пакетів, що належить мережному та транспортному рівням моделі OSI: IP-адреси, номери портів транспортних протоколів TCP та UDP, значення полів пріоритету пакетів тощо.

Основним недоліком технологій фільтрації трафіка, заснованих на використанні ACL, є те, що їх налаштування на маршрутизаторі здійснюється вручну адміністратором мережі, як правило, в режимі командного рядку. Це, з одного боку, негативно позначається на оперативності реакції на можливі загрози безпеці мережі та комутаційного обладнання, а з іншого, встановлює пряму залежність між рівнем підготовки, досвіду та кваліфікації адміністраторів мережі в цілому та рівнем її безпеки. Крім того, при виході з ладу мережного обладнання на відновлення раніше налаштованих списків доступу можуть знадобиться тижні, тому, наприклад, у SDN-мережах ACL, як правило, зберігаються на серверах мережної операційної системи, а в перспективі задачі формування та коригування ACL мають бути автоматизовані.

Ключову роль в забезпеченні мережної безпеки також відіграють криптографічні засоби захисту інформації, які широко реалізуються в сучасних ІКМ. Наприклад, при пороговій криптографії на стороні відправника конфіденційне повідомлення (секрет) розбивається на декілька частин, які в загальному випадку мають доставлятись отримувачу незалежно одна від одної. При цьому повідомлення може бути дешифровано лише за наявності у отримувача більш ніж заданої порогової кількості його частин. Таким чином, при використанні порогової криптографії зловмисник має скомпрометувати не менше порогової кількості частин повідомлення. Слід відмітити, що порогова криптографія вважається однією з найбезпечніших криптосистем і використовується в сучасних рішеннях, наприклад, таких як RSA (алгоритм Рівеста-Шаміра-Алдемана), криптосистема Пейє, криптосистема Дамгорда-Юрика, схема Ель-Гамаля, алгоритм електронного цифрового підпису з використанням еліптичних кривих [31-33].

Концепція порогової криптографії широко використовується та має різні застосування при побудові сучасних інфокомунікаційних мереж і знаходить реалізацію в технологіях хмарних обчислень, механізмах автентифікації, управління ключами, технології Інтернету речей (Internet of Things, IoT), мобільних самоорганізованих мережах (Mobile Ad hoc Network, MANET), сенсорних мережах, електронних цифрових підписах, додатках електронного голосування, візуальній криптографії тощо (табл. 1) [32].

Таблиця 1. Області застосування різних порогових схем при побудові ІКМ

Область застосування	Схема порогового розділення секрету	Переваги використання
Хмарні обчислення	Схема Шаміра	Зменшення кількості ключів; забезпечення конфіденційності приватних даних; безпечне та надійне зберігання даних; безпечна передача даних.
Автентифікація	Схема Шаміра, криптосистема Пейє	Швидка групова автентифікація користувачів; стійкість до масиву атак, масштабованість, гнучкість; легковагова, масштабована групова автентифікація в IoT; анонімна автентифікація в IoT.
Ad-Hoc мережі	Схема Шаміра, порогова криптографія на основі еліптичних кривих (ECC)	Стійкість до сертифікатів фальшивих відкритих ключів, захист від вразливостей, спричинених шкідливими вузлами; високий рівень безпеки, доступний сервіс керування ключами.
Електронний цифровий підпис	Схема Шаміра, схема Шаміра з криптосистемою Ель-Гамаля	Відстежуваність підписів, множина політик підпису; відсутність потреби в довіреній третій стороні.
Електронне голосування	Схема Шаміра, схема Асмута-Блума, криптосистема Пейє	Зменшення порушення цілісності даних, відсутність потреби в довіреній третій стороні; надійність, конфіденційність; підтримка множинного та нульового вибору, ієрархічність; використання властивості гомоморфності.
Цифрова обробка зображень	Схема Шаміра	Безпечна передача зображення через незахищені мережі.

Схеми розділення секрету (secret sharing schemes) можна класифікувати наступним чином [33]:

– проактивне розділення секрету;

– динамічне розділення секрету;

– розділення секрету з можливостями вето;

– робастне розділення секрету;

– поліноміальне розділення секрету;

– схеми, засновані на китайській теоремі про остачі (Chinese Remainder Theorem, CRT);

– анонімне розділення секрету;

– розділення секрету на основі систематичних блокових кодів;

– розділення секрету у вигляді «чорного ящику» (black box secret sharing);

– візуальне розділення секрету.

Так, наприклад, схема Шаміра відноситься до схем поліноміального розділення секрету, тоді як схема Асмута-Блума базується на використанні теореми CRT. У схемі візуального розділення секрету візуальне зображення виступало як конфіденційне повідомлення.

Слід відзначити, що багатошляхова маршрутизація потоків пакетів і конфіденційних даних за шляхами, що не перетинаються, також сприяє підвищенню безпеки на мережному рівні. В цьому контексті до прикладів забезпечення мережної безпеки можна віднести концепцію безпечної маршрутизації, наприклад, за допомогою механізму SPREAD [34-38]. Це рішення засновано на багатошляховій доставці частин конфіденційного повідомлення, які сформовано відповідно до схеми Шаміра. При цьому, чим більше шляхів буде використано та чим менше вони будуть перетинатись, тим з меншою ймовірністю компрометації повідомлення буде доставлено адресату. Подібні особливості, в свою чергу, накладають додаткові вимоги на використовувані математичні моделі та методи маршрутизації в ІКМ.

В залежності від часу реакції на можливу компрометацію каналів зв'язку та фрагментів мережі для забезпечення заданого рівня мережної безпеки на практиці можуть застосовуватися як проактивні, так і реактивні засоби, які повинні взаємно доповнювати один одного. Проактивні засоби застосовуються, як правило, на етапі запобігання компрометації повідомлень або мінімізації ймовірності її виникнення [34-38]. Реактивні засоби використовуються тоді, коли безпека даних, що передаються, вже порушена і мережними засобами важливо оперативно відновити необхідний рівень безпеки.

II. Аналіз проактивних методів і механізмів безпечної маршрутизації в ІКМ

У роботі [39] було запропоновано новий евристичний підхід щодо безпечної міждоменної маршрутизації *Secure Multi-Party Computation* (*SMPC*). При цьому міждоменна маршрутизація передбачає координацію між взаємно «недовірливими» сторонами, що призводить до виникнення вимог, відповідно до яких *Border Gateway Protocol* (*BGP*) забезпечує автономність, гнучкість та конфіденційність шляхом розподіленого виконання рішень на основі політик під час процесу ітеративного обчислення маршруту. Цей підхід має слабку збіжність і робить планування та забезпечення відмовостійкості складним завданням. У зв'язку з цим в [39] запропоновано принципово інший підхід до обчислення міждоменного маршруту на основі SMPC, який забезпечує кращу гарантію конфіденційності, ніж BGP, і дозволяє розгортати нові парадигми політик.

У роботі [40] отримав подальшого розвитку алгоритм безпечної оверлейної маршрутизації на основі схеми ймовірнісного передрозподілу ключів, яка набула широкого застосування в безпроводових мережах. Запропоновано масштабоване рішення для мереж високої розмірності з кількістю вузлів більше тисячі, засноване на детерміністському алгоритмі на основі алгоритму Дейкстри (Deterministic Dijkstra-

based Algorithm, DDA), який дозволяє розраховувати оптимальні безпечні шляхи в оверлейних безпроводових мережах при часовій складності, значно нижчій ніж в оригінальному алгоритмі. Також у [40] запропоновано відповідну апроксимацію для знаходження шляху, близького до оптимального, з точністю до 1% у порівнянні з DDA.

У роботах [34, 35] представлено та досліджено механізми *SPREAD* (*Secure Protocol for Reliable dAta Delivery*) та *H-SPREAD* (*Hybrid Secure Protocol for Reliable dAta Delivery*) посилення безпечної передачі повідомлень у MANET (рис. 2). Основна ідея полягає в тому, щоб розділити конфіденційне повідомлення на кілька фрагментів – частин, а потім передавати ці частини від відправника до одержувача за множиною шляхів, що не перетинаються, так, щоб навіть якщо певна кількість частин повідомлення буде скомпрометована, секретне повідомлення в цілому залишається нескомпрометованим. Запропоновано загальну архітектуру системи: математичну модель для створення та реконструкції частин повідомлення, оптимальний розподіл його частин за декількома шляхами з точки зору безпеки, а також підходи щодо розрахунку мультишляху в мережах MANET.

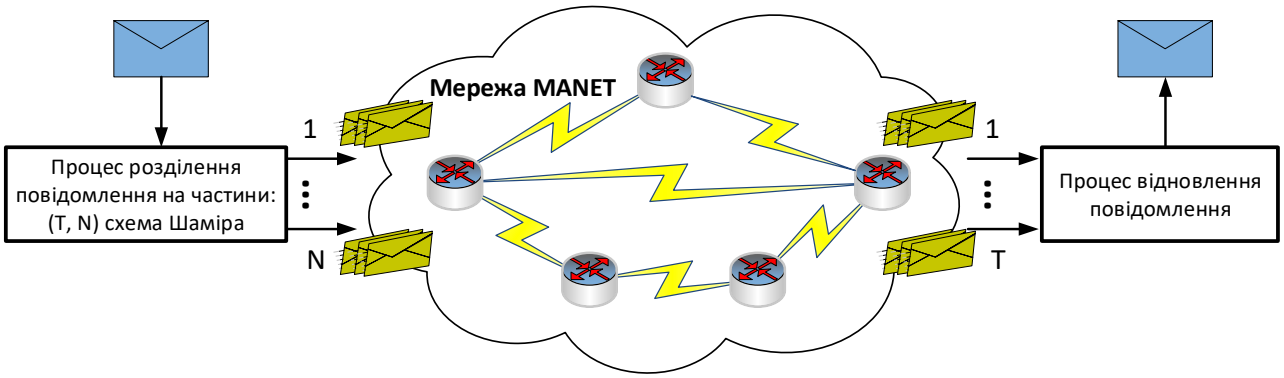

Рис. 2. Загальна архітектура роботи механізму SPREAD

У порівнянні з проводовими мережами забезпечення безпеки в MANET пов'язано з виявленням і запобіганням множини існуючих уразливостей та атак [41]. Радіоканали більш сприйнятливі до атак як пасивного прослуховування, так і активного втручання в сигнали та здійснення завад. По-друге, більшість протоколів маршрутизації в MANET припускають довірчі взаємодії між вузлами для здійснення передачі пакетів. Залежність від такої взаємодії робить передачу даних більш уразливою щодо несанкціонованого доступу, підміни даних та атакам типу «відмова від обслуговування». По-третє, відсутність фіксованої інфраструктури та централізованого управління ускладнює застосування більшості традиційних рішень щодо забезпечення мережної безпеки.

В результаті застосування механізму SPREAD вдається знизити ймовірність компрометації переданого повідомлення, тому що помітно ускладнюється завдання зловмисника: йому необхідно скомпрометувати не один маршрут, по якому передається нерозділене повідомлення, а всі шляхи, по яких передаються його частини.

При цьому під компрометацією повідомлення розуміється подія, пов'язана з несанкціонованим доступом до його вмісту.

При забезпеченні безпечної маршрутизації повідомлення в мережі відповідно до механізму SPREAD необхідно вирішити такі завдання [34, 35]:

1. Розрахунок множини маршрутів, що не перетинаються, між заданими вузлами відправник та одержувач.
2. Розділення конфіденційного повідомлення, що передається, на множину частин відповідно до обраної схеми Шаміра.
3. Розподіл множини частин повідомлення між множиною маршрутів, визначених у ході вирішення першого завдання.

Варто окремо відзначити, що ймовірність компрометації шляху багато в чому залежить як від числа складових його вузлів і каналів зв'язку, так і від параметрів їх безпеки, тобто кожен елемент (вузол, канал) шляху може бути скомпрометований з певною ймовірністю. У загальному випадку шляхи, які використовуються для передачі частин розділеного відповідно до схеми Шаміра [34, 35, 38] повідомлення, можуть мати різні значення ймовірності компрометації. На жаль, у рамках відомих рішень, присвячених реалізації механізму SPREAD, не враховуються параметри безпеки (зокрема ймовірність компрометації) цих шляхів. Крім того, подібні рішення орієнтовані на використання лише шляхів, які не перетинаються, що негативно впливає на ефективність використання доступного мережного ресурсу.

В роботах [42, 43] пропонується в ході вибору маршруту в ІКМ враховувати ризики інформаційної безпеки. Це забезпечується шляхом відповідного формування маршрутних метрик, коли в них сумісно з QoS-показниками враховуються і показники ризику інформаційної безпеки елементів системи маршрутизації. Даний підхід дозволяє динамічно вибрати найбільш безпечний маршрут потоків, що передаються, як в умовах активних атак, так і при пасивному аналізі ризиків у системі маршрутизації.

Одним із ефективних проактивних засобів забезпечення заданого рівня мережної безпеки, як було сказано раніше, є багатошляхова маршрутизація конфіденційних повідомлень, розділеного на частини відповідно до схеми Шаміра, з балансуванням кількості таких частин за маршрутами, що не перетинаються [34, 35, 38]. Тоді як у [44, 45] пропонується використання особливого класу шляхів, що перетинаються, які складають основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі. Це дозволило знизити ймовірність компрометації конфіденційних повідомлень, які передаються в ІКМ [44].

Як показав проведений аналіз [34-38, 42, 43], можливість аналітичного розрахунку ймовірності компрометації повідомлення, що передається в мережі, багато в чому визначається особливостями структурної побудови ІКМ і типами використовуваних маршрутів. Як відомо, множину шляхів у мережі можна умовно розділити на дві підмножини: підмножина шляхів, що не перетинаються, та підмножина шляхів, які допускають вузловий або канальний перетин [46-49].

Слід відмітити, що в разі використання шляхів, що перетинаються, процедура числової оцінки ймовірності компрометації повідомлення, яке передається, помітно ускладнюється, а в ряді випадків стає неможливою (в аналітичному вигляді) [35]. У зв'язку з цим у [44] було вирішено актуальну задачу пошуку компромісного рішення, пов'язаного з визначенням такого класу маршрутів, що перетинаються, для яких можливо в аналітичному вигляді розрахувати, а отже і контролювати ймовірність компрометації конфіденційного повідомлення, що передається.

В цьому контексті було додатково введено ще два типи шляхів: простий і композитний. Простий шлях завжди утворений послідовним з'єднанням каналів зв'язку мережі, а композитні шляхи являють собою більш складні структурні форми, що включають в себе перетин простих шляхів. У зв'язку з цим введено наступні позначення:

Константи

$\tilde{M}$ — кількість використовуваних композитних шляхів, що не перетинаються, які можуть використовуватися при маршрутизації частин повідомлення;

$\tilde{M}_i$ — кількість фрагментів в i-му композитному шляху, які можуть бути скомпрометовані ($i = \overline{1, \tilde{M}}$);

M_i — кількість каналів зв'язку в i-му композитному шляху, які можуть бути скомпрометовані ($i = \overline{1, \tilde{M}}$);

p_i^j — ймовірність компрометації j-го каналу зв'язку i-го композитного шляху ($i = \overline{1, \tilde{M}}$, $j = \overline{1, M_i}$).

Кількісні показники

$\tilde{p}_i^j$ — ймовірність компрометації j-го фрагмента i-го композитного шляху ($i = \overline{1, \tilde{M}}$, $j = \overline{1, \tilde{M}_i}$);

$\tilde{p}_i$ — ймовірність компрометації i-го композитного шляху ($i = \overline{1, \tilde{M}}$);

$\tilde{P}_{msg}$ — ймовірність компрометації повідомлення в цілому при його передачі частинами за композитними шляхами.

Змінні

n_i — цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним шляхом ($i = \overline{1, \tilde{M}}$).

Для того щоб забезпечувалася можливість формулювання в аналітичному вигляді виразу для розрахунку ймовірності компрометації композитного шляху в ході безпечної маршрутизації, він повинен містити два типи фрагментів, що складаються з послідовного рис. 3 а) або з паралельного з'єднання каналів зв'язку рис. 3 б). На рис. 3 в) наведено приклад композитного шляху з послідовним з'єднанням двох фра-

гментів мережі. Перший фрагмент представлений паралельним з'єднанням каналів зв'язку, а другий – послідовним.

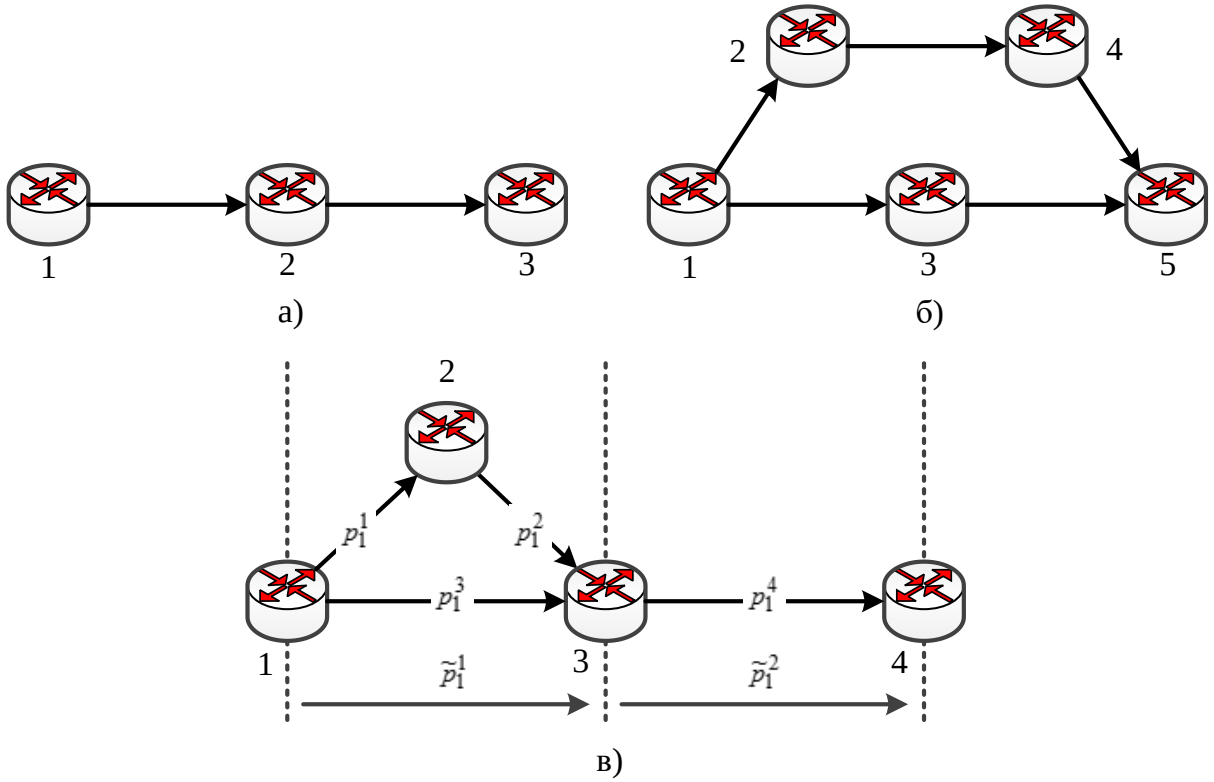

Рис. 3. Приклади типів фрагментів і композитного шляху: послідовне з'єднання каналів зв'язку (а), паралельне з'єднання каналів зв'язку (б), композитний шлях (в)

Таким чином, у загальному випадку ймовірність компрометації i-го композитного шляху, що складається з $\tilde{M}_i$ фрагментів, може бути розрахована відповідно до наступного виразу:

$$\tilde{p}_i = 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^{\,j}) . \qquad (1)$$

У разі, якщо для доставки повідомлення використовується єдиний композитний шлях, то ймовірність компрометації даного повідомлення визначається ймовірністю компрометації цього композитного шляху. В більш загальному випадку, коли частини повідомлення передаються за множиною композитних шляхів, що не перетинаються, для розрахунку ймовірності компрометації повідомлення необхідно використовувати такий вираз:

$$\tilde{P}_{msg} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i , \qquad (2)$$

за умови забезпечення заданого рівня мережної безпеки $P_{msg} \le \gamma_P$.

У загальному випадку один композитний шлях може містити кілька послідовно з'єднаних фрагментів з паралельним з'єднанням каналів зв'язку. Позначимо через h_i

максимальне число паралельно з'єднаних каналів зв'язку за всіма фрагментами i-го композитного шляху. Тоді має місце умова

$$h_i \le n_i \le T-1,\ (i=\overline{1,\tilde{M}}\ ), \tag{3}$$

а її виконання дозволить таким чином розподілити частини повідомлення за паралельно з'єднаними каналами мережних фрагментів композитних шляхів, щоб в кожному з них передавалося ненульове число таких частин повідомлення та були справедливі вирази (1) і (2).

Крім того, за аналогією з [34, 35] має бути введена умова з урахуванням композитного характеру використовуваних шляхів:

$$N-n_i<T\ ,\ (i=\overline{1,\tilde{M}}\ ). \tag{4}$$

У зв'язку з цим в основу запропонованого в [44] методу безпечної маршрутизації частин повідомлення, яке передається за множиною шляхів, що перетинаються, може бути покладено розв'язання оптимізаційної задачі, пов'язаної з використанням критерію оптимальності

$$\min_{n_i}\prod_{i=1}^{\tilde{M}}\tilde{p}_i(n_i)\,, \tag{5}$$

що гарантує мінімізацію ймовірності компрометації переданого повідомлення. Крім того, на керуючі змінні залежно від використовуваної схеми Шаміра накладаються обмеження (1), (3) або (4), а також умова

$$\sum_{i=1}^{\tilde{M}} n_i = N\,. \tag{6}$$

Сформульована оптимізаційна задача відноситься до класу задач нелінійного цілочисельного програмування (Nonlinear Integer Programming), тому що змінні, які підлягають розрахунку, є цілочисельними, а критерій оптимальності (5) є нелінійним.

Запропонований у [44, 45] метод безпечної маршрутизації повідомлень за множиною шляхів, що перетинаються, є засобом проактивного підходу щодо поліпшення рівня мережної безпеки. Це визначається тим, що на основі постійного аналізу стану мережі, її структури та параметрів безпеки каналів зв'язку, а також в ході оптимального балансування частин конфіденційних повідомлень за шляхами, що перетинаються, реалізуються всі доступні можливості для того, щоб максимально знизити ймовірність компрометації даних, які передаються.

Новизна методу [44, 45] полягає в тому, що він, по-перше, допускає використання шляхів, що перетинаються, які складають основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку, а по-друге, заснований на оптимізації процесу вибору множини композитних шляхів і балансування за ними частин повідомлення, що передається, із забезпеченням

допустимих значень його ймовірності компрометації. Проведений аналіз у [44, 45] показав, що використання запропонованого методу в рамках поданих розрахункових прикладів дозволяє знизити ймовірність компрометації переданих повідомлень у середньому від 5-10% до 25-50% з огляду на можливості використання композитних шляхів, які є одним з підкласів шляхів, що перетинаються.

III. Метод безпечної швидкої перемаршрутизації повідомлень за композитними шляхами: проактивний і реактивний підходи

З метою розширення функціональних можливостей засобів безпечної маршрутизації, важливо щоб запропонований метод реалізував принципи не тільки проактивного, але і реактивного підходу. Іншими словами, в структурі методу безпечної маршрутизації важливо передбачити процедури оперативної реакції на можливі порушення рівня мережної безпеки [44]. В даний час протоколи маршрутизації реагують на можливі зміни стану мережі в масштабі часу десятків секунд, що не є прийнятним з точки зору необхідного рівня мережної безпеки.

У зв'язку з цим все частіше на практиці застосовуються методи та протоколи швидкої перемаршрутизації, в ході яких попередньо розраховуються два типи шляхів: основний і резервний. При цьому використання окремо кожного типу шляхів повинно приводити до задоволення вимог щодо рівня мережної безпеки. Тоді при відмові основного шляху повідомлення практично миттєво (із затримкою в десятки мілісекунд) будуть передаватись з використанням резервних маршрутів. Очевидно, що основний і резервний маршрути не повинні перетинатися за елементами мережі, які скомпрометовані (маршрутизаторами, каналами зв'язку або маршрутами в цілому) [6-8, 20-24].

Тоді в рамках безпечної швидкої перемаршрутизації (Secure Fast ReRouting, S-FRR) використання множини основних шляхів відноситься до рішень проактивного підходу щодо забезпечення заданого рівня мережної безпеки, а застосування резервних шляхів відповідає вимогам реактивного підходу. При цьому в рамках запропонованого в [44] методу розрахунок множини основних і резервних шляхів повинен здійснюватися максимально злагоджено для підвищення ефективності кінцевих рішень.

Поділ шляхів на основні та резервні має на увазі, що частини повідомлення будуть передаватися не за всіма доступними композитними та простими шляхами, а лише за їх обмеженою кількістю, але з виконанням вимог щодо ймовірності компрометації. З огляду на те, що для підвищення рівня мережної безпеки повідомлень, що передаються, необхідно реалізувати багатошляхову маршрутизацію їх частин, то як основні та резервні будуть виступати не окремі композитні або прості шляхи, а утворені ними мультишляхи. При цьому до складу як основного, так і резервного мультишляху можуть входити кілька композитних та (або) простих шляхів.

В ході розрахунку резервного мультишляху пропонується реалізувати наступні дві схеми захисту основного мультишляху:

– схема захисту основного мультишляху в цілому, при якій основний і резервний мультишляхи не перетинаються ні за вузлами, ні за каналами;
– схема захисту окремого шляху (композитного або простого) основного мультишляху, при якій резервний мультишлях не повинен містити канали та вузли шляху, який захищається.

Реалізація кожної зі схем захисту націлена на відновлення заданого рівня мережної безпеки за рахунок відмови від основного мультишляху та переходу до використання резервного мультишляху. У зв'язку з цим були уточнені раніше та введені додаткові позначення [44]:

Кількісні показники

$\tilde{p}_i^{pr}$ — ймовірність компрометації i-го композитного або простого шляху основного мультишляху ($i = \overline{1, \tilde{M}}$);

$\tilde{p}_i^{b}$ — ймовірність компрометації i-го композитного або простого шляху резервного мультишляху ($i = \overline{1, \tilde{M}}$);

$\tilde{P}_{msg}^{pr}$ — ймовірність компрометації повідомлення в цілому при його передачі частинами за композитними або простими шляхами основного мультишляху;

$\tilde{P}_{msg}^{b}$ — ймовірність компрометації повідомлення в цілому при його передачі частинами за композитними або простими шляхами резервного мультишляху.

Змінні

n_i — цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним або простим шляхом, що входить до складу основного мультишляху ($i = \overline{1, \tilde{M}}$);

$\overline{n}_i$ — цілочисельна змінна, яка характеризує кількість частин повідомлення, що передаються за i-м композитним або простим шляхом, що входить до складу резервного мультишляху ($i = \overline{1, \tilde{M}}$).

Відповідно до введених позначень для розрахунку ймовірності компрометації повідомлення, яке передається частинами за множиною композитних шляхів, необхідно за аналогією з формулою (2) використовувати відповідно вирази

$$\tilde{P}_{msg}^{pr} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^{pr} \quad \text{і} \quad \tilde{P}_{msg}^{b} = \prod_{i=1}^{\tilde{M}} \tilde{p}_i^{b} . \tag{7}$$

Варто відзначити, що ймовірності компрометації мережних фрагментів $\tilde{p}_i^{pr}$ і $\tilde{p}_i^{b}$ є функціями від кількості частин повідомлення, що передаються ними, тобто від n_i й $\overline{n}_i$. Тоді з урахуванням (1) мають місце умови

$$\tilde{p}_i^{pr} = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), n_i > 0; \\ 1, n_i = 0, \end{cases} \text{ і } \tilde{p}_i^b = \begin{cases} 1 - \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), \bar{n}_i > 0; \\ 1, \bar{n}_i = 0. \end{cases} \quad (8)$$

Системи (8) можуть бути записані як:

$$\tilde{p}_i^{pr} = 1 - H_0(n_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j) \text{ і } \tilde{p}_i^b = 1 - H_0(\bar{n}_i) \prod_{j=1}^{\tilde{M}_i} (1 - \tilde{p}_i^j), \quad (9)$$

де H_0 – функція Хевісайда, яка з урахуванням виразу (8) розраховується наступним чином

$$H_0(n) = \begin{cases} 0, n = 0; \\ 1, n > 0. \end{cases}$$

Умова (6) з огляду на реалізацію S-FRR доповнюються виразом

$$\sum_{i=1}^{\tilde{M}} \bar{n}_i = N. \quad (10)$$

В свою чергу, для захисту основного мультишляху, за аналогією з [50], необхідно забезпечити виконання наступної умови:

$$\sum_{i=1}^{\tilde{M}} n_i \bar{n}_i = 0. \quad (11)$$

При необхідності захисту окремого i-го композитного шляху важливо забезпечити виконання умови

$$n_i \bar{n}_i = 0, \quad (12)$$

яка також є нелінійною (білінійною).

Для того, щоб при використанні і основного, і резервного мультишляху виконувалися вимоги щодо ймовірності компрометації повідомлення, яке за ними передається, вводиться за аналогією з (2) наступна умова:

$$P_{msg}^{pr} \le P_{msg}^b \le \gamma_P. \quad (13)$$

Тоді в основу розроблюваного методу S-FRR може бути покладено рішення оптимізаційної задачі нелінійного цілочисельного програмування (Nonlinear Integer Programming) з критерієм оптимальності

$$J = \sum_{i=1}^{\tilde{M}} \tilde{p}_i n_i + \sum_{i=1}^{\tilde{M}} \tilde{p}_i \bar{n}_i \quad (14)$$

і обмеженнями, представленими умовами (3), (4), (6), (10), (11), (12) і (13). При цьому обмеження (11)-(13) є нелінійними, а змінні, що розраховуються, n_i і $\bar{n}_i$ носять цілочисельний характер. У критерії (14) значення $\tilde{p}_i$, розраховані відповідно до виразів

(1), є вартісними ваговими коефіцієнтами. Цим забезпечується безпечна маршрутизація в мережі, коли максимальна кількість частин повідомлення буде передаватися за шляхом з мінімальною ймовірністю компрометації. Навпаки, за шляхом з найвищою ймовірністю компрометації передаватиметься мінімальна кількість частин повідомлення або не буде передано жодної.

Отже, запропонований в [44] метод безпечної швидкої перемаршрутизації повідомлень в мережі орієнтує на реалізацію як проактивної, так і реактивної безпечної маршрутизації конфіденційних повідомлень, новизна якого полягає в тому, що в разі порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, що входять в основний мультишлях, багатошляхова передача частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації буде здійснюватися вже за заздалегідь розрахованою множиною резервних композитних шляхів, реалізуючи захист або основного мультишляху в цілому, або одного чи декількох заздалегідь заданих композитних шляхів, що входять в основний мультишлях.

IV. Загальні рекомендації щодо практичної реалізації методів безпечної швидкої перемаршрутизації

Загальна архітектура організації безпечної швидкої перемаршрутизації (S-FRR), в основу якої покладено метод, описаний в розділі 3, що реалізує проактивну та реактивну безпечну маршрутизацію конфіденційних повідомлень, представлено на рис. 4. Функціональні блоки, пов'язані з реалізацією даного методу, показано у відповідній архітектурі приграничних маршрутизаторів інфокомунікаційної мережі.

Дані з блоку моніторингу та аналізу рівня мережної безпеки (ймовірності компрометації каналів зв'язку), а також блоку моніторингу топологічних характеристик ІКМ і пропускної здатності каналів зв'язку поступають на блок формування множини шляхів (простих або композитних), а потім на блок розрахунку ймовірності компрометації отриманих шляхів (9). Проактивний характер рішень обумовлений розрахунком множини композитних шляхів, що утворюють основний мультишлях, за яким передаються частини конфіденційного повідомлення, отримувані в результаті фрагментації за схемою Шаміра у відповідному блоці.

В рамках запропонованого в [44] методу S-FRR закладено можливість захисту як основного мультишляху в цілому – умови захисту мультишляху (11), так і одного або декількох заданих композитних шляхів, що входять в основний мультишлях – умови захисту шляху (12). За формування подібних умов у пропонованій архітектурі відповідають окремі блоки (рис. 4). Далі інформація з розглянутих блоків поступає до блоку оптимізації процесу безпечної швидкої перемаршрутизації (14). Цей блок відповідає за визначення множини основних і резервних шляхів, а також балансування частин конфіденційних повідомлень за ними з виконанням умов захисту елементів ІКМ.

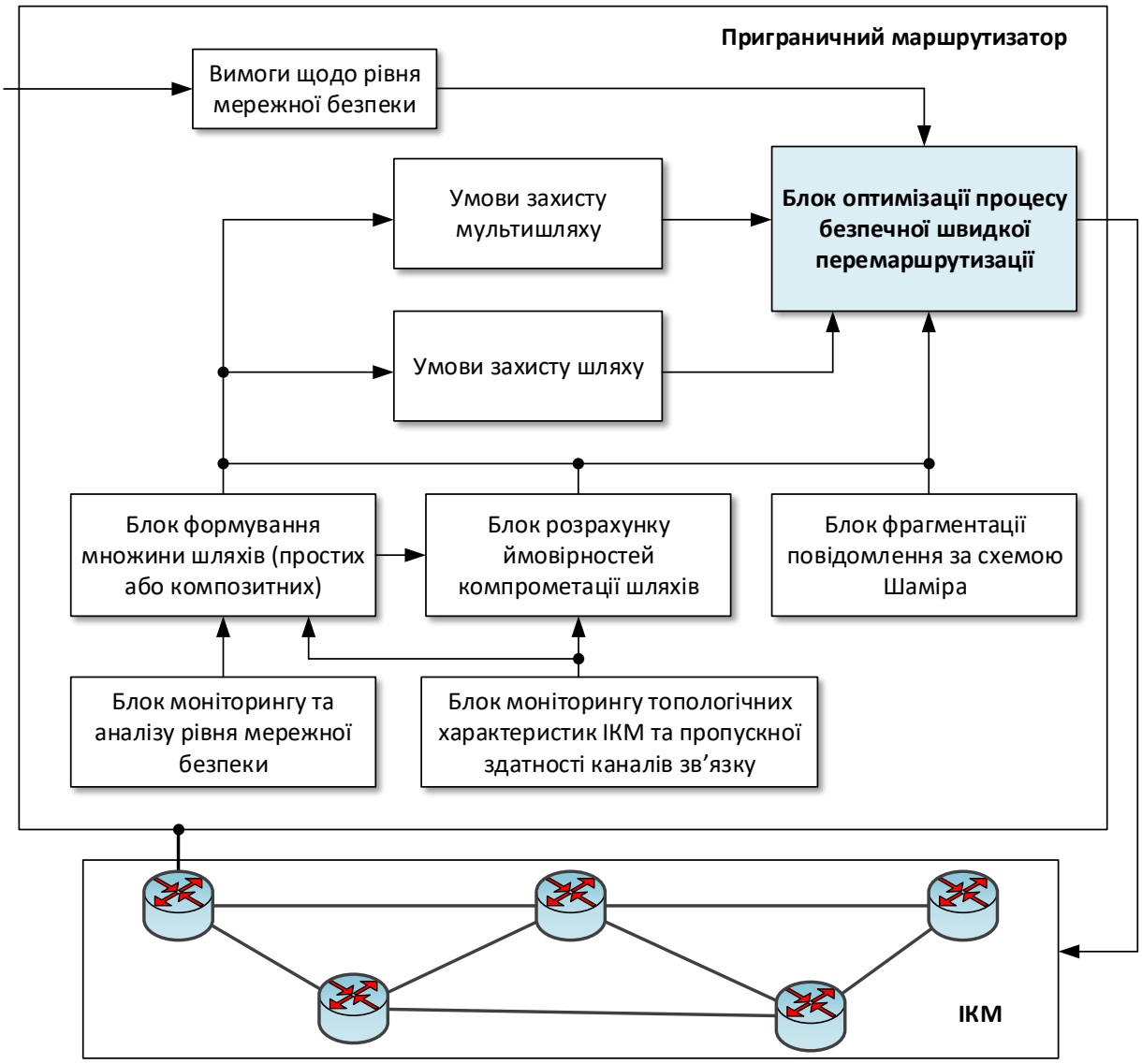

Рис. 4. Узагальнена архітектура безпечної швидкої перемаршрутизації

У разі порушення вимог щодо мережної безпеки (13), викликаного, наприклад, підвищенням імовірності компрометації одного або множини композитних шляхів, що входять в основний мультишлях, повідомлення будуть передаватися за попередньо розрахованою множиною резервних композитних шляхів, реалізуючи принципи реактивного підходу до забезпечення заданого рівня мережної безпеки. Слід відмітити, що реалізація розробленого методу S-FRR дозволяє в реальному часі забезпечувати задані значення ймовірності компрометації повідомлень (7), що передаються, в умовах динаміки змін стану ІКМ, наприклад, рівня загроз, а відповідно й імовірностей компрометації каналів, шляхів та ІКМ у цілому на підставі розрахунку та переходу на використання резервних композитних шляхів (мультишляхів) при багатошляховій передачі частин конфіденційного повідомлення.

Висновки

У зв'язку з тим, що рішення щодо забезпечення мережної безпеки повинні носити комплексний характер, стосуючись як організаційних, так і технічних аспектів, то на практиці варто забезпечити реалізацію всіх доступних засобів – технологічних і протокольних, які використовуються на різних рівнях моделі OSI. Слід відмітити, що важливе місце в цьому комплексі засобів відводиться саме технологічним рішенням мережного рівня OSI, а саме протоколам маршрутизації, які потребують системної та скоординованої взаємодії одночасно множини мережних елементів – маршрутизаторів, серверів маршрутів, мережних контролерів тощо в ході формування (розрахунку) шляхів, вздовж яких би забезпечувався необхідний рівень мережної безпеки за обраними показниками або критеріями.

На теперішній час у напрямку безпечної маршрутизації проведено значну кількість теоретичних досліджень, починаючи від найпростіших емпіричних варіантів рішень до системних оптимізаційних підходів. Як показав проведений аналіз, значний потенціал мають проактивні рішення, пов'язані з застосуванням порогової криптографії, яка достатньо широко використовується з метою підвищення мережної безпеки в ІКМ. Зокрема, ефективним вбачається підхід щодо реалізації багатошляхової безпечної маршрутизації за шляхами, що не перетинаються. До таких рішень відносить механізм SPREAD/H-SPREAD, який дозволяє максимально ускладнити завдання зловмисника щодо компрометації конфіденційного повідомлення, розділеного на частини за допомогою схеми Шаміра. При цьому ці частини (фрагменти) передаються в мережі за шляхами, що не перетинаються.

Встановлено, що перспективним також представляється використання не тільки шляхів, що не перетинаються, а й особливого класу шляхів, що перетинаються, які складають основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі. Використання такого типу мультишляхів дозволяє не тільки покращити показники мережної безпеки (ймовірність компрометації переданих повідомлень), а й підвищити продуктивність мережі в цілому.

Проте використання проактивних рішень забезпечення мережної безпеки в ІКМ на практиці має бути доповнене і відповідними реактивними засобами. Так, мережа має зберігати працездатність навіть при локальній компрометації її елементів, наприклад, вузлів, каналів та навіть шляхів. При зміні стану мережі, викликаного порушенням рівня безпеки конфіденційних повідомлень, що передаються в ІКМ, важливо визначити оперативний порядок зміни множини шляхів, які використовуються для передачі його частин. Тому рішення щодо швидкої перемаршрутизації із локальним чи глобальним захистом елементів ІКМ можуть розглядатися як реалізація реактивного підходу щодо забезпечення безпечної маршрутизації. Крім того, важливим представляється розробка відповідних алгоритмів розрахунку композитних маршрутів. Все вищезазначене вимагає розробки нових або вдосконалення існуючих математичних моделей і методів безпечної маршрутизації та швидкої пере-

маршрутизації, які можуть бути покладені в основу нових мережних протоколів для безпечної передачі конфіденційних даних із заданими вимогами щодо граничної ймовірності їх компрометації в мережі.

Список літератури:

1. *Hutchison D., Galis A., Gavras, A.* The Future Internet-LNCS 7858. Springer-Verlag Berlin Heidelberg. 2013. 401 p. DOI: 10.1007/978-3-642-38082-2.

2. *Chaparadza R., Wodczak M., Meriem T.B., De Lutiis P., Tcholtchev N., Ciavaglia L.* Standardization of resilience & survivability, and autonomic fault-management, in evolving and future networks: an ongoing initiative recently launched in ETSI. Design of Reliable Communication Networks (DRCN) 2013: Proceedings of the 9th International Conference. Budapest, Hungary, 4-7 March, 2013. IEEE, 2013. P. 331-341.

3. Quality of service regulation manual. 2017. ITU. 176 p. URL: https://www.itu.int/pub/D-PREF-BB.QOS_REG01-2017.

4. *Matsubara D., Egawa T., Nishinaga N., Kafle V.P., Shin M.K., Galis A.* Toward future networks: A viewpoint from ITU-T. IEEE Communications Magazine. 2013. Vol. 51, No. 3. P.112-118.

5. *Barona López L.I., Valdivieso Caraguay Á.L., Sotelo Monge M.A., García Villalba L.J.* Key technologies in the context of future networks: operational and management requirements. Future Internet. 2017. Vol. 9, No. 1. P. 1-15. DOI: https://doi.org/10.3390/fi9010001.

6. *Cholda P., Tapolcai J., Cinkler T., Wajda K., Jajszczyk A.* Quality of resilience as a network reliability characterization tool. IEEE network. 2009. Vol. 23, No. 2. P. 11-19. DOI: 10.1109/MNET.2009.4804331.

7. *Tipper D.* Resilient network design: challenges and future directions. Telecommunication Systems. 2014. Vol. 56, No. 1. P. 5-16. DOI: 10.1007/s11235-013-9815-x.

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

9. *Mauthe A., Hutchison D., Cetinkaya E.K., Ganchev I., Rak J., Sterbenz J.P., Gunkelk M., Smith P., Gomes T.* Disaster-resilient communication networks: Principles and best practices. Resilient Networks Design and Modeling (RNDM) 2016: Proceedings of the 8th International Workshop. Halmstad, Sweden, 13-15 September, 2016. IEEE, 2016. P. 1-10. DOI: 10.1109/RNDM.2016.7608262.

10. Телекомунікаційні системи та мережі. Структура та основні функції [Електронний ресурс] / *В. В. Поповський та ін.* Т. 1. Харків: СМІТ, 2011. Режим доступу: http://www.znanius.com/3534.html.

11. *Лемешко О. В., Євсеєва О. Ю.* Конспект лекцій з дисципліни «Алгоритми управління та адаптації в ТКС» для студентів денної форми навчання спеціальності 7.092401 – Телекомунікаційні системи та мережі. Харків: ХНУРЕ, 2008. 164 с.

12. *Поповский В. В., Персиков А. В.* Защита информации в телекоммуникационных системах. В 2-х т. Харьков: СМИТ, 2006.

13. *Поповский В. В., Персиков А. В.* Основы криптографической защиты информации в телекоммуникационных системах. В 2-х т. Харьков: СМИТ, 2010.

14. *Ленков С. В., Перегудов Д. А., Хорошко В. А.* Методы и средства защиты информации. Киев: Арий, 2008. 464 с.

15. *Stallings W.* Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud.1st Edition. Pearson Education Inc., 2016. 510 p.

16. *Monge A. S., Szarkowicz K. G.* MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services. 1st ed. O'Reilly Media, 2016. 920 p.

17. *Schneier B.* Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company, 2015. 398 p.

18. *Stallings W.* Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2016. 768 p.

19. *Новиков С. Н.* Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи. М.: Горячая линия – Телеком, 2015. 128 с.

20. *Björck F., Henkel M., Stirna J., Zdravkovic J.* Cyber resilience–fundamentals for a definition. New Contributions in Information Systems and Technologies. 2015. Vol. 353. Springer, Cham. P. 311-316. DOI: https://doi.org/10.1007/978-3-319-16486-1_31.

21. *Fink G. A., Griswold R. L., Beech Z. W.* Quantifying cyber-resilience against resource-exhaustion attacks. Resilient Control Systems (ISRCS) 2014: Proceedings of the 7th International Symposium, Denver, CO, USA, 19-21 August, 2014. IEEE, 2014. P. 1-8. DOI: 10.1109/ISRCS.2014.6900093.

22. *Choras M., Kozik R., Bruna M.P.T., Yautsiukhin A., Churchill A., Maciejewska I., Eguinoa I., Jomni A.* Comprehensive approach to increase cyber security and resilience. Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24-27 August, 2015. IEEE, 2015. P. 686-692. DOI: 10.1109/ARES.2015.30.

23. *Musman S.* Assessing prescriptive improvements to a system's cyber security and resilience. Systems Conference (SysCon) 2016: Proceedings of the Annual IEEE Conference. Orlando, FL, USA, 18-21 April, 2016. IEEE, 2016. P. 1-6. DOI: 10.1109/SYSCON.2016.7490660.

24. *Galinec D., Steingartner W.* Combining cybersecurity and cyber defense to achieve cyber resilience. Informatics 2017: Proceedings of the IEEE 14th International Scientific Conference. Poprad, Slovakia, 14-16 November, 2017. IEEE, 2017. P. 87-93. DOI: 10.1109/INFORMATICS.2017.8327227.

25. ITU-T X-805. Security architecture for systems providing end-to-end communications. October 2003. 28 p. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en.

26. ISO 7498-1:1994 Information technology – Open Systems Interconnection –Basic Reference Model: The Basic Model. International Standard ISOIEC, 74981, 1994. 59 p.

27. ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989, 32 p.

28. ITU-T X-800. Security architecture for Open Systems Interconnection for CCITT applications. March 1991. 48 p. URL: https://www.itu.int/rec/T-REC-X.800-199103-I.

29. *Santos O., Kampanakis P., Woland A.* Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. 1 edition. Cisco Press, 2016. 368 p.

30. *Al-Kuwaiti M., Kyriakopoulos N., Hussein S.* A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. IEEE Communications Surveys & Tutorials. 2009. Vol. 11, No. 2. P. 106-124. DOI: 10.1109/SURV.2009.090208.

31. *Kaur R., Kashmira P., Meena K., Mohapatra A. K.* Survey on Different Techniques of Threshold Cryptography. Journal of Electronics and Communication Engineering (IOSR-JECE). 2017. P. 114-119.

32. *Venukumar V., Pathari V.* A survey of applications of threshold cryptography – proposed and practiced. Information Security Journal: A Global Perspective. 2016. Vol. 25, No. 4-6. P.180-190. DOI: 10.1080/19393555.2016.1251996.

33. *Sarma K. S., Lamkuche H. S., Umamaheswari S.* A Review of Secret Sharing Schemes. Research Journal of Information Technology. 2013. Vol. 5. P.67-72. DOI: 10.3923/rjit.2013.67.72.

34. *Lou W., Kwon Y.* H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. IEEE Transactions on Vehicular Technology. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.

35. *Lou W., Liu W., Fang Y.* SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Hong Kong, China, 7-11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.

36. *Alouneh S., En-Nouaary A., Agarwal A.* A Multiple LSPs Approach to Secure Data in MPLS Networks. Journal of Networks. 2007. Vol. 2, No. 4. P. 51–58. DOI: 10.4304/jnw.2.4.51-58.

37. *Alouneh S., Agarwal A., En-Nouaary A.* A Novel Path Protection Scheme for MPLS Networks using Multi-path Routing. Computer Networks: The International Journal of Computer and Telecommunications Networking. 2009. Vol. 53, No. 9. P. 1530–1545. DOI: 10.1016/j.comnet.2009.02.001.

38. *Кулаков Ю. А., Лукашенко В. В., Левчук А. В.* Безопасная многопутевая маршрутизация в беспроводных сетях большой размерности. Захист інформації. 2011. Том 13, №2(51). С. 5–10. DOI: 10.18372/2410-7840.13.2018.

39. *Gupta D., Segal A., Panda A., Segev G., Schapira M., Feigenbaum J., Rexford J., Shenker S.* A new approach to interdomain routing based on secure multi-party computation. Hot Topics in Networks: Proceedings of the 11th ACM Workshop. October, 2012. ACM, 2012. P. 37-42. DOI: 10.1145/2390231.2390238.

40. *Gharib M., Yousefizadeh H., Movaghar A.* Secure Overlay Routing for Large Scale Networks. IEEE Transactions on Network Science and Engineering. 2018. Vol. 1. P. 1-12. DOI: 10.1109/TNSE.2018.2812830.

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

42. *Снегуров А. В., Чакрян В. Х.* Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности. Системи управління, навігації та зв'язку. 2012. №4(24). С. 105-110.

43. *Snihurov A., Chakrian V.* Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters. Scholars Journal of Engineering and Technology. 2015. Vol. 3, No. 8. P. 707-714.

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

45. *Еременко А. С.* Методика расчета вероятности компрометации сообщения при использовании пересекающихся маршрутов с последовательно-параллельной или комбинированной структурой. Наукові записки Українського науково-дослідного інституту зв'язку. 2015. №6(40). С. 64–71.

46. *Gomes T., Martins L., Ferreira S., Pascoal M., Tipper D.* Algorithms for determining a node-disjoint path pair visiting specified nodes. Optical Switching and Networking. 2017. Vol. 23. P. 189-204. DOI: https://doi.org/10.1016/ j.osn.2016.05.002.

47. *Myslitski K., Rak J., Kuszner Ł.* Toward fast calculation of communication paths for resilient routing. Networks. 2017. Vol. 70, No. 4. P. 308-326. DOI: https://doi.org/10.1002/net.21789.

48. *Natarajan M.* Graph Theory Algorithms for Mobile Ad Hoc Networks. Informatica – An International Journal of Computing and Informatics. 2012. Vol. 36. P. 185–200.

49. *Suurballe J. W.* Disjoint paths in a network. Neworks. 1974. Vol. 4, No. 2. P. 125–145.

50. *Lemeshko O., Romanyuk A., Kozlova H.* Design schemes for MPLS Fast ReRoute. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) 2013: Proceedings of the 12th International Conference. Polyana Svalyava, Ukraine, 19-23 February, 2013. IEEE, 2013. P. 202–203.