УДК 004.056 DOi 10.30837/ bi.2024.1(100).07

Г. А. Плєхова[1], С. М. Неронов[2], М. В. Костікова[3], С. О. Кашкевич[4]

[1]ХНАДУ, м. Харків, Україна, plehovaanna11@gmail.com, ORCID iD: 0000-0002-6912-6520

[2]ХНАДУ, м. Харків, Україна, sernikner@gmail.com, ORCID iD: 0000-0003-2381-1271

[3]ХНАДУ, м. Харків, Україна, kmv_topaz@ukr.net, ORCID iD: 0000-0001-5197-7389

[4]НАУ, м. Харків, Україна, svitlana.kashkevych@npp.nau.edu.ua, ORCID iD: 0000-0002-4448-3839

УДОСКОНАЛЕННЯ МОДЕЛІ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Наразі розгортання таких мережних архітектур, як програмно-конфігуровані мережі (Software-Defined Networking, SDN), стикається з новими загрозами кібербезпеці, які вимагають розробку та дослідження нових спеціалізованих рішень щодо підвищення рівня мережної безпеки. Незважаючи на високу відкритість і можливості програмованості, архітектура SDN замінює традиційну мережу, проте збільшує кількість потенційних мережних атак, що призводить до нових проблем безпеки.

Зростаючий інтерес до SDN та широкому розгортанню програмно-конфігурованих мереж різних типів дозволяють виявляти їхні недоліки в процесі боротьби із загрозами кібербезпеці. Очевидно, що питання безпеки тісно пов'язані з характеристиками самих SDN мереж. Крім того, проблеми безпеки в SDN можна розділити на основі трьох рівнів: площини даних, площини управління та площини застосунків.

Водночас серед об'єктів атак можуть бути пристрої різних рівнів SDN. Отже, відповідно до багаторівневої архітектури SDN можна класифікувати загрози безпеці на рівнях передачі даних, управління та застосунків. Зі свого боку, площина даних складається з комутаторів та інших мережних пристроїв і головним чином відповідає за обробку даних, їх пересилання, відкидання, а також збір статистики. Функціонування площини даних відбувається на основі правил потоків, що надаються контролером мережі. Тоді як основними причинами проблем безпеки є власне архітектура SDN, зовнішні шкідливі атаки, недостатність контролю доступу та засобів шифрування.

На сьогоднішній день важливе місце у комплексі засобів підвищення мережної безпеки, у тому числі мереж SDN, відводиться протоколам маршрутизації, які потребують системної та скоординованої взаємодії одночасно множини мережних елементів – SDN-комутаторів, і контролерів мережі під час формування (розрахунку) шляхів і правил потоків, вздовж яких має забезпечуватися необхідний рівень безпеки за обраними показниками або критеріям.

В роботі проведена аналіз того як модифікувати маршрутні метрики таким чином, щоб отримувана модель набула властивостей безпечної QoS-маршрутизації. Показано що удосконалення моделі та вибір маршруту потрібно обирати з урахуванням базових метрик критичності вразливостей, і пропускної здатності каналів зв'язку, що складають цей маршрут.

МОДЕЛЬ, МАРШРУТИЗАЦІЯ, ВРАЗЛИВІСТЬ, БЕЗПЕКА, МЕТРИКА, ДЕЦЕНТРАЛІЗОВАНІ СХОВИЩА ДАННИХ, СТИСНЕННЯ ЗОБРАЖЕНЬ

G. A. Pliekhova, S. M. Neronov, M. V. Kostikova, S. O. Kashkevich. Improvement of the secure routing model in software-configured networks. Currently, the deployment of such network architectures as Software-Defined Networking (SDN) is facing new cyber security threats that require the development and research of new specialized solutions to increase the level of network security. Despite its high openness and programmability, the SDN architecture replaces the traditional network, but it increases the number of potential network attacks, which leads to new security problems.

The growing interest in SDN and the widespread deployment of software-configured networks of various types allow identifying their shortcomings in the process of combating cyber security threats. Obviously, security issues are closely related to the characteristics of SDN networks themselves. Furthermore, security issues in SDN can be divided based on three layers: data plane, control plane, and application plane.

At the same time, devices of different SDN levels can be among the objects of attacks. Therefore, according to the multilayer architecture of SDN, security threats can be classified at the data transmission, management and application layers. For its part, the data plane consists of switches and other network devices and is mainly responsible for data processing, forwarding, discarding, and collecting statistics. The data plane functions on the basis of flow rules provided by the network controller. While the main causes of security problems are the SDN architecture itself, external malicious attacks, insufficient access control and encryption tools.

Today, an important place in the complex of means of increasing network security, including SDN networks, is given to routing protocols, which require the systematic and coordinated interaction of a number of network elements at the same time – SDN switches and network controllers during the formation (calculation) of paths and flow rules, along which the required level of security must be ensured according to selected indicators or criteria.

The paper analyzes how to modify route metrics in such a way that the resulting model acquires the properties of secure QoS routing. It is shown that the improvement of the model and the choice of the route should be chosen taking into account the basic metrics of the criticality of vulnerabilities and the bandwidth of the communication channels that make up this route.

MODEL, ROUTING, VULNERABILITY, SECURITY, METRICS, DECENTRALIZED DATA STORAGE.

Вступ

Головною метою використання NFV (Network function virtualization) є необхідність використовувати стандартні технології віртуалізації для консолідації апаратного забезпечення та віртуалізації мережних функцій у блоки, які можна об'єднувати для створення наскрізних комунікаційних послуг. Це може бути реалізовано для будь-якої функції площини

управління або площини даних у середовищі як проводових, так і безпроводових мереж. Національна база даних вразливостей та загальна система оцінки вразливостей.

Розглянемо більш детально сферу технічних вразливостей. Видатним ресурсом є національна база даних про вразливості NIST – National Vulnerability Database (NVD), і відповідна загальна система оцінки вразливостей – Common Vulnerability Scoring System (CVSS), описана в NISTIR 7946, Посібник із впровадження CVSS. NVD – це вичерпний список відомих технічних вразливостей систем, апаратного та програмного забезпечення. CVSS забезпечує відкриту структуру для передачі характеристик вразливостей. CVSS визначає вразливість як помилку, недолік, слабкість або відкритість програми, системного пристрою чи сервісу, що може призвести до збою конфіденційності, цілісності чи доступності.

Отже, модель CVSS намагається забезпечити повторювані та точні вимірювання, одночасно дозволяючи користувачам переглядати базові характеристики вразливості, які використовуються для створення числових оцінок. CVSS надає загальну систему вимірювання для галузей промисловості, організацій та урядів, які вимагають точних і послідовних оцінок використання вразливостей та їхнього впливу.

Розуміння CVSS дозволяє оцінити широкий спектр вразливостей, які впливають на системи. Крім того, систематизована схема для оцінки вразливостей у CVSS є корисною для розробки подібного системного підходу до інших вразливостей, таких як ті, що пов'язані з організаційними питаннями, політикою та процедурами, а також фізичною інфраструктурою. На сьогоднішній день CVSS широко прийнятий і використовуваний підхід. Наприклад, використання CVSS рекомендується для кількісного розрахунку рівня вразливості мережного обладнання.

Кожен запис NVD містить наступну інформацію:

– унікальний словниковий ідентифікатор вразливостей і ризиків – Common Vulnerabilities and Exposure (CVE);

– опис вразливості;

– посилання на веб-сайти та інші посилання з інформацією, пов'язаною з вразливістю;

– метрики CVSS.

1. Мета та постановка задачі

Метою роботи є розв'язання задачі, яка спрямована на розгляд категорії вразливостей, використання національної бази даних вразливостей та загальної системи оцінки вразливостей, метрики загальної системи оцінки вразливостей виходячи з проведеного аналізу стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання. Також приділено увагу використанню існуючої методики розрахунку метрик маршрутизації на основі базових метрик критичності вразливостей.

Таким чином бажаючи удосконалити математичну модель безпечної маршрутизації з урахуванням базових метрик критичності вразливостей в роботі [1] розроблено та досліджено модель безпечної маршрутизації з балансуванням навантаження в мережах на основі SD-WAN. Технологічне завдання безпечної маршрутизації з балансуванням навантаження було сформульовано у формі оптимізаційної задачі з квадратичним критерієм оптимальності. Така форма критерію дозволяє збалансувати частки потоків, що передаються в мережі.

Перспективним в моделі [1] представляється те, що використовується комбінована метрика під час розрахунку мультишляху:

$$f_{i,j}^{\text{комб}} = f_{i,j}^{OSPF} + f_{i,j}^{SEC}, \qquad (1)$$

де $f_{i,j}^{OSPF}$ – метрика, обрана за аналогією з протоколом OSPF, яка відповідає за те, щоб розраховуваний маршрут містив у собі найбільш продуктивні канали зв'язку

$$f_{i,j}^{OSPF} = \frac{10^8}{c_{i,j}}, \qquad (2)$$

де $c_{i,j}$ – пропускна здатність відповідного каналу зв'язку; $f_{i,j}^{SEC}$ – метрика, заснована на параметрі мережної безпеки – ймовірності компрометації каналу зв'язку

$$f_{i,j}^{SEC} = \frac{10^8}{R} p_{i,j}. \qquad (3)$$

При цьому R є співвідношенням між ваговими коефіцієнтами метрик продуктивності та мережної безпеки:

$$R = \frac{w^{OSPF}}{w^{SEC}}, \; w^{SEC} = \frac{w^{OSPF}}{R} = \frac{10^8}{R}. \qquad (4)$$

Результати моделювання показали, що досліджуване навантаження на канал зв'язку (а саме частка потоку, що передається, оскільки використовувалась стратегія багатошляхової маршрутизації) зменшується із збільшенням ймовірності компрометації каналу. Аналіз результатів дослідження також виявив значення співвідношення R метрик мережної безпеки та продуктивності, коли модель найбільш чутлива до погіршення ймовірності компрометації каналів зв'язку та мережі загалом.

2. Аналіз публікацій

Представлена в [1] модель безпечної маршрутизації з балансуванням навантаження з адитивною комбінованою метрикою враховує продуктивність і безпеку мережі, дозволяє ефективніше використовувати наявні мережні ресурси, але також враховує ймовірність компрометації каналів зв'язку під час прийняття маршрутних рішень. Отже, в роботі [2] розроблено проактивне рішення щодо забезпечення мережної безпеки, а саме метод безпечної маршрутизації повідомлень шляхами, що перетинаються. Новизна цього методу полягає в тому, що допускається використання шляхів, які перетинаються. Вони також становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку. Крім того, основу методу складає оптимізаційний процес вибору множини

композитних шляхів і балансування ними частин повідомлення, що передається, із забезпеченням допустимих значень його ймовірності компрометації. Проведені числові дослідження довели працездатність та ефективність запропонованого методу, тобто його використання в межах наведених розрахункових прикладів дозволило знизити ймовірність компрометації повідомлень, що передаються, в середньому від 5 – 10% до 25 – 50% з огляду на можливості використання композитних шляхів [2].

Другий метод, розроблений і запропонований в [2], пов'язаний з необхідністю оперативного розрахунку та зміни множини шляхів, що використовуються для передачі частин конфіденційних повідомлень, у разі зміни стану мережі, викликаної порушенням рівня безпеки. Тому підходи та механізми щодо швидкої перемаршрутизації з локальним чи глобальним захистом елементів мережі можуть розглядатися як реалізація реактивного підходу щодо забезпечення безпечної маршрутизації [2]. Отже, в [2] було розроблено та досліджено метод безпечної швидкої перемаршрутизації повідомлень у мережі, який орієнтує на реалізацію як проактивної, так і реактивної безпечної маршрутизації конфіденційних повідомлень.

Сутність методу безпечної швидкої перемаршрутизації (Secure Fast ReRoute, S-FRR) полягає в тому, що порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, тобто основного мультишляху, призводить до використання попередньо розрахованою множиною резервних композитних шляхів для багатошляхової передачі частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації. Крім того, метод передбачає реалізацію захисту або основного мультишляху загалом, або одного чи декількох заздалегідь заданих композитних шляхів, що містить основний мультишлях [2].

Застосування методу S-FRR дозволило в режимі реального часу забезпечити задані значення показника мережної безпеки, а саме ймовірності компрометації повідомлень, що передаються, навіть в умовах динамічної зміни стану мережі (ймовірності компрометації каналів і шляхів) на підставі розрахунку й оперативного переходу на використання резервних композитних шляхів за умови багатошляхової передачі частин конфіденційного повідомлення [2].

Підсумовуючи, можна зробити висновок, що розроблені в [2] методи безпечної маршрутизації можуть рекомендуватися до використання як основа нових мережних протоколів безпечної маршрутизації та безпечної швидкої перемаршрутизації для багатошляхової передачі частин конфіденційного повідомлення із заданими вимогами щодо граничної ймовірності його компрометації в мережі.

Алгоритми маршрутизації з урахуванням параметрів ризику інформаційної безпеки розглянуті у роботах [3] пропонується під час вибору маршруту в ІКМ враховувати ризики інформаційної безпеки. Це забезпечується шляхом відповідного формування маршрутних метрик, коли в них сумісно з показниками якості обслуговування враховується показник ризику інформаційної безпеки елементів мережі. Цей підхід дозволяє динамічно вибрати найбільш безпечний маршрут потоків, що передаються в умовах активних атак і в разі пасивного аналізу ризиків у системі маршрутизації.

Так, у [3] запропоновано використовувати параметр ризику інформаційної безпеки у формулі розрахунку метрики протоколу EIGRP для маршрутизації трафіка найбільш безпечними шляхами в мережі. Метод пропонує розраховувати ризик на основі двох параметрів: ризик, який розраховується на основі стандарту NIST CVSS, і ризик, який розраховується на основі формули для ступеня вразливості вузла з теорії живучості інформаційних систем. Це дозволяє враховувати інформаційну безпеку маршрутизованих пакетів і структурну цілісність мережі. Також у [3] розроблено модифікований алгоритм балансування навантаження між шляхами, який дозволяє розвантажити найефективніший вузол маршрутизації під час атаки «відмова в обслуговуванні» (DoS). Результати дослідження довели, що запропонований підхід ефективний під час запобігання порушенню інформаційної безпеки маршрутизованих пакетів і забезпечення безпеки найефективніших вузлів маршрутизації в мережі, які дозволяють ефективно маршрутизувати довірений трафік, коли мережа піддається DoS-атаці або бракує критичних системних ресурсів.

Потокові моделі маршрутизації на основі базових метрик критичності вразливостей у роботах [4, 5] пропонуються потокові моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку мережі, а задача безпечної маршрутизації також сформульована як оптимізаційна. У моделі [4] для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку мережі та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених вразливостей. Запропонований авторами підхід до формування маршрутних метрик може бути використаний під час комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування.

Безпечна маршрутизація на основі SPREAD включає відомий підхід щодо застосування механізмів SPREAD (Secure Protocol for Reliable dAta Delivery) та H-SPREAD (Hybrid Secure Protocol for

Reliable dAta Delivery) та їх розвиток запропоновано у роботах [2, 3], що націлені на посилення безпечної передачі та маршрутизації секретних повідомлень у MANET (рис. 1). Основною ідеєю є те, що конфіденційне повідомлення розділяється на декілька фрагментів – частин, які потім передаються від відправника до отримувача множиною шляхів, що не перетинаються. Таким чином, що навіть якщо деяка кількість фрагментів повідомлення буде скомпрометовано, то секретне повідомлення загалом залишиться нескомпрометованим [2, 6]. Отже, в [2, 6] було запропоновано загальну математичну модель для створення та реконструкції фрагментів секретного повідомлення, оптимальний розподіл його частин за декількома шляхами з урахуванням параметра мережної безпеки, а також підходи щодо розрахунку мультишляху в безпроводових мережах MANET.

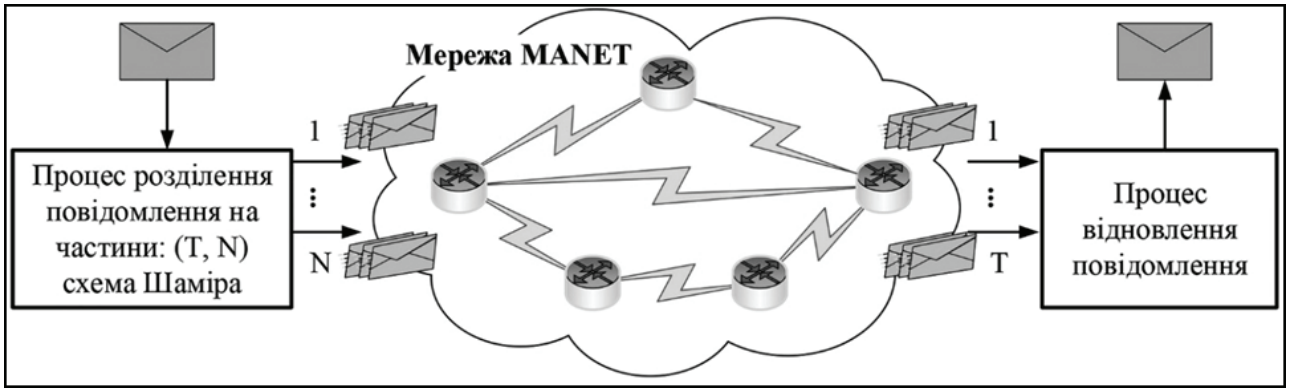

Рис. 1. Загальна архітектура роботи механізму SPREAD

Відмічається, що у порівнянні з проводовими мережами забезпечення безпеки в MANET пов'язано з виявленням і запобіганням множини наявних вразливостей та атак [2]. Перш за все, радіоканали більш сприйнятливі до атак пасивного прослуховування й активного втручання в сигнали та здійснення завад. Крім того, більшість протоколів маршрутизації MANET припускають, що взаємодія між вузлами для здійснення передачі пакетів є довірчою. Таким чином, передача даних стає більш вразливою щодо несанкціонованого доступу, підміни даних, а також атак типу «відмова в обслуговуванні» (Denial of Service, DoS). Також відсутність фіксованої інфраструктури та централізованого управління ускладнює застосування більшості традиційних рішень щодо забезпечення мережної безпеки.

Численні дослідження застосування механізму SPREAD та його модифікацій дозволяє знизити ймовірність компрометації секретного повідомлення, що передається, завдяки ускладненню завдання зловмисника: йому необхідно скомпрометувати не один маршрут, яким передається нерозділене повідомлення, а всі шляхи, якими передаються його фрагменти [2, 6]. Згідно з [2] під компрометацією повідомлення розуміється подія, пов'язана з несанкційним доступом до його вмісту.

Для забезпечення безпечної маршрутизації повідомлення в мережі під час застосування механізму SPREAD необхідно вирішити такі завдання [3, 6]:

1. Розрахувати множини маршрутів, що не перетинаються, між заданими вузлами «відправник» і «отримувач».

2. Розділити конфіденційне повідомлення, що передається, на множину частин відповідно до обраної схеми Шаміра.

3. Розподілити множини фрагментів повідомлення між множиною маршрутів, визначених на першому кроці.

Отже, ймовірність компрометації маршруту (шляху) багато в чому залежить від кількості вузлів і каналів зв'язку, що його складають, і від параметрів їх безпеки, тобто кожен елемент мережі (вузол, канал) шляху може бути скомпрометований з певною ймовірністю [2, 6]. У загальному випадку шляхи для передачі частин розділеного відповідно до схеми Шаміра [2, 6] повідомлення, можуть мати різні рівні безпеки, що визначаються ймовірністю компрометації. Доведено, що у межах відомих рішень, присвячених реалізації механізму SPREAD, не враховуються параметри безпеки (зокрема ймовірність компрометації) цих шляхів [2]. Крім того, подібні рішення орієнтовані на використання лише шляхів, що не перетинаються. Це негативно впливає на ефективність використання доступного мережного ресурсу.

Проактивні та реактивні методі безпечної маршрутизації повідомлень шляхами, що перетинаються також розглядаються у [2] запропоновано використання особливого класу шляхів, що перетинаються, які зі свого боку можуть формувати композитні шляхи та містять відповідно мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку мережі. Такий підхід щодо вибору шляхів орієнтує на зниження ймовірності компрометації конфіденційних (секретних) повідомлень, які передаються в комунікаційній мережі.

Отже, в роботі [2] розроблено проактивне рішення щодо забезпечення мережної безпеки, а саме метод безпечної маршрутизації повідомлень шляхами, що перетинаються. Новизна цього методу полягає в тому, що допускається використання шляхів, які

перетинаються. Вони також становлять основу композитних шляхів і містять мережні фрагменти з послідовним та (або) паралельним з'єднанням каналів зв'язку. Крім того, основу методу складає оптимізаційний процес вибору множини композитних шляхів і балансування ними частин повідомлення, що передається, із забезпеченням допустимих значень його ймовірності компрометації. Проведені числові дослідження довели працездатність та ефективність запропонованого методу, тобто його використання в межах наведених розрахункових прикладів дозволило знизити ймовірність компрометації повідомлень, що передаються, в середньому від 5 – 10% до 25 – 50% з огляду на можливості використання композитних шляхів [2].

Другий метод, розроблений і запропонований в [2], пов'язаний з необхідністю оперативного розрахунку та зміни множини шляхів, що використовуються для передачі частин конфіденційних повідомлень, у разі зміни стану мережі, викликаної порушенням рівня безпеки. Тому підходи та механізми щодо швидкої перемаршрутизації з локальним чи глобальним захистом елементів мережі можуть розглядатися як реалізація реактивного підходу щодо забезпечення безпечної маршрутизації [2]. Отже, в [2] було розроблено та досліджено метод безпечної швидкої перемаршрутизації повідомлень у мережі, який орієнтує на реалізацію як проактивної, так і реактивної безпечної маршрутизації конфіденційних повідомлень.

Сутність методу безпечної швидкої перемаршрутизації (Secure Fast ReRoute, S-FRR) полягає в тому, що порушення вимог мережної безпеки, викликаного підвищенням ймовірності компрометації одного або множини композитних шляхів, тобто основного мультишляху, призводить до використання попередньо розрахованою множиною резервних композитних шляхів для багатошляхової передачі частин конфіденційного повідомлення із забезпеченням заданих значень ймовірності його компрометації. Крім того, метод передбачає реалізацію захисту або основного мультишляху загалом, або одного чи декількох заздалегідь заданих композитних шляхів, що містить основний мультишлях [2].

Застосування методу S-FRR дозволило в режимі реального часу забезпечити задані значення показника мережної безпеки, а саме ймовірності компрометації повідомлень, що передаються, навіть в умовах динамічної зміни стану мережі (ймовірності компрометації каналів і шляхів) на підставі розрахунку й оперативного переходу на використання резервних композитних шляхів за умови багатошляхової передачі частин конфіденційного повідомлення [2].

Підсумовуючи, можна зробити висновок, що розроблені в [2] методи безпечної маршрутизації можуть рекомендуватися до використання як основа нових мережних протоколів безпечної маршрутизації та безпечної швидкої перемаршрутизації для багатошляхової передачі частин конфіденційного повідомлення із заданими вимогами щодо граничної ймовірності його компрометації в мережі.

Алгоритми маршрутизації з урахуванням параметрів ризику інформаційної безпеки розглянуті у роботах [3] пропонується під час вибору маршруту в IKM враховувати ризики інформаційної безпеки. Це забезпечується шляхом відповідного формування маршрутних метрик, коли в них сумісно з показниками якості обслуговування враховується показник ризику інформаційної безпеки елементів мережі. Цей підхід дозволяє динамічно вибрати найбільш безпечний маршрут потоків, що передаються в умовах активних атак і в разі пасивного аналізу ризиків у системі маршрутизації.

Запропоновано використовувати параметр ризику інформаційної безпеки у формулі розрахунку метрики протоколу EIGRP для маршрутизації трафіка найбільш безпечними шляхами в мережі. Метод пропонує розраховувати ризик на основі двох параметрів: ризик, який розраховується на основі стандарту NIST CVSS, і ризик, який розраховується на основі формули для ступеня вразливості вузла з теорії живучості інформаційних систем. Це дозволяє враховувати інформаційну безпеку маршрутизованих пакетів і структурну цілісність мережі. Розроблено модифікований алгоритм балансування навантаження між шляхами, який дозволяє розвантажити найефективніший вузол маршрутизації під час атаки «відмова в обслуговуванні» (DoS). Результати дослідження довели, що запропонований підхід ефективний під час запобігання порушенню інформаційної безпеки маршрутизованих пакетів і забезпечення безпеки найефективніших вузлів маршрутизації в мережі, які дозволяють ефективно маршрутизувати довірений трафік, коли мережа піддається DoS-атаці або бракує критичних системних ресурсів.

Потокові моделі маршрутизації на основі базових метрик критичності вразливостей у роботах [4, 5] пропонуються потокові моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку мережі, а задача безпечної маршрутизації також сформульована як оптимізаційна. У моделі [4] для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку мережі та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених вразливостей. Запропонований авторами підхід до формування маршрутних метрик може бути використаний під час комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування.

3. Виклад основного матеріалу

Таким чином пропонуємо використання методики розрахунку метрик маршрутизації на основі базових метрик критичності вразливостей відповідно до результатів, отриманих у роботах [4, 5, 7–9] , виявлено, що одним з ефективних засобів забезпечення захисту мереж є попереднє оцінювання ризику інформаційної безпеки (РІБ). Процес оцінювання РІБ спрямований на запобігання використання відомих вразливостей, потенційно наявних у мережі, що захищається [9]. Зі свого боку РІБ може розраховуватися за допомогою використання зазначених у рекомендації NIST CVSS v3 [8, 10] метрик критичності вразливостей: базових, часових і метрик середовища користувачів.

У межах запропонованого у [4] та удосконаленого у [9] рішення для розрахунку вагових коефіцієнтів $w_{i,j}$, що використовувались у процесі отримання маршрутних рішень, обрано базові метрики, які характеризують наявні вразливості елементів мережі та дозволяють оцінити ризик інформаційної безпеки мережі загалом, а не для окремих випадків компрометації мережних елементів, на відміну від часових метрик і метрик середовища.

В роботах [4, 9] введено наступні позначення:

– $U = \left\{U_i^q; q = \overline{1,Q}, i = \overline{1,m}\right\}$ – множина вразливостей, виявлених на вузлах (маршрутизаторах) мережі;

– U_i^q – q -та вразливість на i -му вузлі мережі;

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

– BS_i^q – показник критичності q -ї вразливості на i -му вузлі мережі, що розраховується за допомогою базових метрик системи оцінювання вразливостей відповідно до NIST CVSS v3 [8, 11] та характеризує умовні збитки від використання вразливості U_i^q зловмисником;

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

У [12] зазначено наступний вираз для розрахунку ризику інформаційної безпеки від використання наявних вразливостей на i -му вузлі мережі:

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

Згідно з рекомендацією NIST [8, 10], збитки щодо базових метрик вразливостей на вузлах мережі розраховуються як

$$BS_i^q = \left(0{,}6 \cdot \mathrm{Imp}_i^q + 0{,}4 \cdot \mathrm{Ex}_i^q - 1{,}5\right) \cdot f\left(\mathrm{Imp}_i^q\right), \quad (6)$$

де Imp_i^q – потенційний збиток від використання q -ї вразливості зловмисником на i -му вузлі мережі; Ex_i^q – складність використання q -ї вразливості зловмисником на i -му вузлі мережі; $f\left(\mathrm{Imp}_i^q\right)$ – функція від потенційного збитку в разі використання q -ї вразливості зловмисником на i -му вузлі мережі.

Тоді як потенційний збиток від використання вразливості можна отримати таким чином [7, 9]:

$$\mathrm{Imp}_i^q = 10{,}41\left[1 - \left(1 - Conf_i^q\right) \cdot \left(1 - Int_i^q\right) \cdot \left(1 - v_i^q\right)\right], \quad (7)$$

де $Conf_i^q$ – збитки від порушення конфіденційності інформації, що передається мережею та не може бути отримана неавторизованим, наприклад, зовнішнім, користувачем (зловмисником); Int_i^q – збитки від порушення цілісності мережі, що характеризуються модифікацією, зміною та руйнуванням інформації неавторизованим користувачем (зловмисником); Av_i^q – збитки від порушення доступності мережного ресурсу у випадку використання q -ї вразливості на i -му вузлі мережі.

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

Відповідно до [8, 10], у кожній із цих метрик збитки від використання вразливості можуть бути:

– відсутніми із значенням 0;

– частковими із значенням 0,275;

– повними із значенням 0,66.

Значення метрик $Conf_i^q$, Int_i^q та Av_i^q наведено в табл. 1.

Таблиця 1

Значення показників для розрахунку базових метрик вразливостей елементів мережі [4, 9]

Значення	Опис	Числова характеристика
Збиток конфіденційності $Conf_i^q$		
Відсутній (В)	Можливість порушення конфіденційності інформації відсутня	0,000
Частковий (Ч)	Існує значне, однак обмежене розголошення конфіденційної інформації	0,275
Повний (П)	Існує повне розкриття конфіденційної інформації	0,660
Збиток цілісності Int_i^q		
Відсутній (В)	Можливість порушення цілісності інформації відсутня	0,000
Частковий (Ч)	Існує можливість часткової модифікації даних або системних файлів	0,275

Значення	Опис	Числова характеристика
Повний (П)	Існує можливість модифікації будь-яких даних вузла	0,660
Збиток доступності Av_i^q		
Відсутній (В)	Можливість порушення доступності ресурсу відсутня	0,000
Частковий (Ч)	Існує можливість зниження продуктивності або виведення з ладу деяких функцій вузла	0,275
Повний (П)	Існує можливість повного виведення вузла з ладу	0,660

Крім того, складність використання вразливості отримується як [6, 8]:

$$\mathrm{Ex}_i^q = 20 \cdot Ac_i^q \cdot Au_i^q \cdot AcV_i^q, \qquad (8)$$

де Ac_i^q – показник системи оцінки вразливості, що характеризує складність отримання доступу (вектор доступу); Au_i^q – показник системи оцінки вразливості, що відповідає за вимоги до автентифікації; AcV_i^q – показник системи оцінки вразливості, який відображає спосіб використання q-ї вразливості на i-му вузлі мережі, що за фізичним змістом характеризується «віддаленістю» зловмисника, тобто кількістю пристроїв та/або обмежень доступу, через які зловмисник може досягнути i-го вузла мережі для здійснення атаки.

Зазначені показники є базовими метриками [8], які характеризують загальну складність реалізації атаки у використанні тієї чи іншої вразливості на i-му вузлі мережі (табл. 2).

Таблиця 2

Значення показників системи оцінки вразливості, які характеризують складність використання вразливостей [4, 9]

Значення	Опис	Числова характеристика
Вектор доступу Ac_i^q		
Потрібен локальний доступ (Л)	Зловмисникові потрібен безпосередній фізичний доступ до об'єкта, на якому розташована вразливість	0,395
Можливий доступ із суміжної мережі (СмМ)	Зловмисникові потрібен доступ у межах однієї локальної мережі (одного широкомовного домену) до вразливого об'єкта	0,646
Можливий доступ із будь-якої мережі (М)	Зловмисник може використовувати вразливість віддалено з будь-якої ділянки мережі, зокрема з допомогою інтернету	1,000
Вимоги до автентифікації Au_i^q		
Множинна (М)	Зловмисник повинен зробити більше ніж одну процедуру автентифікації для експлуатації вразливості вузла	0,450
Одинична (О)	Зловмиснику досить один раз автентифікуватися для експлуатації вразливості вузла	0,560
Відсутня (В)	Зловмисникові не потрібно проходити процедуру автентифікації для експлуатації вразливості вузла	0,704
Збиток доступності Av_i^q		
Складна (Ск)	Існує низка жорстких обмежень доступу до вузла. Наприклад, експлуатація вразливості вузла можлива тільки в дуже короткий проміжок часу або вимагає застосування соціальної інженерії, коли зловмисника може бути опізнано	0,350
Середня (Ср)	Існують деякі обмеження доступу до вузла. Наприклад, підключення до вразливого пристрою можливе тільки з певних вузлів або вразливий пристрій має функціонувати з нестандартними налаштуваннями	0,610
Легка (Л)	Немає особливих умов доступу до вразливості вузла. Наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на множині вузлів мережі	0,710

Згідно з [4, 9] функція від потенційного збитку $f\left(\mathrm{Imp}_i^q\right)$ приймає значення 0, якщо збитку немає, тобто $f\left(\mathrm{Imp}_i^q\right) = 0$. Тоді розглядатиметься випадок, коли потенційний збиток наявний $\left(\mathrm{Imp}_i^q \neq 0\right)$, і в подальших розрахунках використовувалось $f\left(\mathrm{Imp}_i^q\right) = 1{,}176$ [3, 7].

Отже, для розрахунку ризику інформаційної безпеки за умови компрометації каналу зв'язку $E_{i,j} \in E$, що виходить з i-го вузла, використовується наступний вираз [9, 12]:

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

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

Якщо компрометація каналу зв'язку $E_{i,j} \in E$ відбувається тільки через використання вразливостей на i-му вузлі, то ризики інформаційної безпеки вузла та каналу зв'язку тотожно рівні [9]:

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

Більше того, розрахунок вагових коефіцієнтів $w_{i,j}$ ґрунтується на тому, що компрометація каналу зв'язку $E_{i,j} \in E$ відбуватиметься внаслідок компрометації i-го вузла мережі.

Далі відповідно до виразів (9) – (10) значення вагових коефіцієнтів $w_{i,j}$, що можуть у подальшому слугувати метриками маршрутизації, обчислюються наступним чином [4, 9]:

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

Таким чином можливо удосконалення існуючої моделі безпечної маршрутизації з урахуванням базових метрик критичності вразливостей.

Висновки

В роботі проведена аналіз того як модифікувати маршрутні метрики таким чином, щоб отримувана модель набула властивостей безпечної QoS-маршрутизації. Показано що удосконалення моделі та вибір маршруту потрібно обирати з урахуванням базових метрик критичності вразливостей, і пропускної здатності каналів зв'язку, що складають цей маршрут. В подальших роботах планується провести удосконалення математичної моделі безпечної маршрутизації з урахуванням базових метрик критичності вразливостей та розв'язати технологічну задачу, яку буде сформульовано як оптимізаційну з квадратичною цільовою функцією, коли оптимальний маршрут обирався відповідно до комбінованої метрики на основі базових метрик критичності вразливостей і пропускної здатності каналів зв'язку, що складають цей маршрут.

Список літератури:

[1] Yeremenko O., Persikov M., Lemeshko V., Altaki B. Research and development of the secure routing flow-based model with load balancing. Проблеми телекомунікацій. 2021. № 2(29). С. 3–14. URL: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf.

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

[3] 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: https://doi.org/10.1109/INFCOM.2004.1354662.

[4] 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. C. 707–714.

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

[6] 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: https://doi.org/10.1109/TVT.2006.877707.

[7] Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine. P. 207–217. URL: http://ceur-ws.org/Vol-2917/paper19.pdf.

[8] Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, 2018. 800 p.

[9] CVSS v3.1 Specification Document. FIRST – Forum of Incident Response and Security Teams. URL: https://www.first.org/cvss/v3.1/specification-document.

[10] Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : монографія / О. В. Лемешко, О. С. Єременко, М. О. Євдокименко та ін. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1.

[11] Abedin M., Nessa S., Al-Shaer E., Khan L. Vulnerability analysis For evaluating quality of protection of security policies. Quality of Protection (QoP): Proceedings of the 2nd ACM Workshop, 2006. P. 49–52. DOI: https://doi.org/10.1145/1179494.1179505.

[12] CVSS v3.0 User Guide. FIRST – Forum of Incident Response and Security Teams. URL: https://www.first.org/cvss/v3.0/user-guide.

Надійшла до редколегії 7.05.2024