МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

МАТЕРІАЛИ

XII Всеукраїнської науково-технічної конференції з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2024

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю [Електронний ресурс]. – Миколаїв : НУК, 2024. – 234 с.

У збірнику подано матеріали XII Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 004.056.5

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ОЦІНЮВАННЯ РИЗИКІВ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ

Автор: *Єсипенко А.О., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Актуальність захисту системи глобальної маршрутизації зумовлена зростанням обсягів даних, що передаються через Інтернет, поширенням онлайн-сервісів і практики зберігання інформації в хмарі або банках даних як окремими особами, так і організаціями, державними органами і соціальними групами. Кібербезпека передавання даних через Інтернет забезпечується тільки надійністю системи глобальної маршрутизації, що робить її привабливим об'єктом для зловмисників [1], який має низку переваг у застосуванні:

– дозволяє мати в раз успіху теоретично необмежений вплив на мережу і завдати шкоди у великих масштабах за рахунок ефекту ланцюгової реакції;

– вимагає менших витрат на організацію атаки порівняно з іншими видами розповсюджених кібератак;

– має передумови для успіху організації атак: уразливості у базових протоколах глобальної маршрутизаці, високу ймовірність наявності хоча б у одного провайдера недоліків налаштування роутерів, складність узгодження дій всіх провайдерів і операторів для успішної протидії, впровадження підтримуваних Інтернет-спільнотою взаємно узгоджених норм безпеки маршрутизації (англ. Mutually Agreed Norms for Routing Security, MANRS [1]) є добровільним для провайдерів і операторів.

Забезпечення надійності глобальної маршрутизації є особливо актуальним для галузі річкового та морського транспорту, оскільки:

– навігаційні системи, логістичні системи і системи відстеження вантажів передають і приймають дані через незахищене середовище;

– в цій галузі наявна велика кількість стейкхолдерів [2], які обмінюються інформацією через Інтернет, і інтереси яких мають бути враховані при ідентифікації та оцінюванні ризиків;

– водний транспорт відноситься до критичної інфраструктури, і порушення кібербезпеки може спричинити значну шкоду національній безпеці, нормальним умовам життєдіяльності і здоров'ю населення, соціальній сфері, державному суверенітету, економіці та екології [3];

– порушення кібербезпеки водного транспорту може мати негативний вплив на пов'язані з ним інші сектори критичної інфраструктури держави та зарубіжжя.

Розробці методів забезпечення безпеки маршрутизації присвячено роботи багатьох зарубіжних [1, 4, 5] і вітчизняних [6-10] науковців, однак на даний час на ринку відсутні засоби автоматизації, які дозволяли б ефективно впроваджувати MANRS, механізми та засоби протидії найбільш вагомим загрозам маршрутизації.

Метою даної роботи є розробка системи підтримки прийняття рішень (СППР) щодо оцінювання ризиків глобальної маршрутизації.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

− провести аналіз відкритих літературних джерел і визначити загрози інформаційній безпеці системи глобальної маршрутизації та особливості методів оцінювання асоційованих з ними ризиків;

− розробити основні алгоритми і структуру СППР щодо оцінювання ризиків глобальної маршрутизації.

Як показав проведений аналіз відкритих літературних джерел, загрозами глобальній маршрутизації є:

– викрадення префіксів або маршрутів;

– виток маршрутів;

– підробка IP адрес.

При цьому в системі глобальної маршрутизації з різною ймовірністю можуть виникати загрози, які за моделлю STRIDE [6] відносяться до наступних типів:

– відмова в обслуговуванні (D) – з дуже високою ймовірністю;

– підміна мережевих об'єктів (S) і розголошування інформації (I) – з високою ймовірністю;

– модифікація даних (T) і відмова від авторства (R) – із середньою ймовірністю;

– підвищення рівня привілеїв (E) – з нульовою ймовірністю.

Наслідки реалізації загроз глобальній маршрутизації можуть бути визначені і оцінені шляхом аналізу накопичених статистичних даних за методикою DREAD згідно з прийнятою бальною шкалою і в узагальненому вигляді на підставі визначеної долі ризиків різних категорій у сумарному ризику. За даними [6, 7]:

– потенційний збиток (D), відтворюваність (R) і область ураження (A) наслідки реалізації загроз глобальній маршрутизації оцінюються як високі;

– легкість організації атаки (E) – як середня;

– складність виявлення (D) може мати оцінки в діапазоні значень Висока-Середня-Низька.

Наслідки реалізації загроз глобальній маршрутизації можуть бути представлені у вигляді ієрархії:

рівень 1 – хибна інтерпретація або внесені випадково чи цілеспрямовано зміни в таблицю маршрутизації;

рівень 2 – несанкціонована модифікація напрямку трафіка;

рівень 3 – дії зловмисника, який отримав несанкціонований доступ до трафіка, із даними (наприклад, накопичення, аналіз, модифікація) і з самим трафіком (наприклад, блокування трафіку чи його частини);

рівень 4 – результати дій зловмисника на рівні 3 (наприклад, реалізація ddos-атаки, розсилка спаму, переадресація на фальсифікований сайт);

рівень 5 – наслідки реалізації загроз глобальній маршрутизації для автономних систем;

рівень 6 – наслідки для бізнес-процесів.

Отримані оцінки ризиків по категоріях моделі DREAD дозволяють обчислити інтегральний ризик, асоційований із загрозами моделі STRIDE. Проведений аналіз показав, що впорядковані за спаданням інтегрального ризику загрози моделі STRIDE можуть бути представлені у вигляді наступного списку:

1) підміна мережевих об'єктів (S);

2) відмова в обслуговуванні (D);

3) розголошування інформації (I);

4) модифікація даних (T) і відмова від авторства (R);

5) підвищення рівня привілеїв (E).

При оцінюванні ризиків глобальної маршрутизації слід враховувати їх особливості, визначені в [9]:

– джерелом загроз, з якими асоціюються ризики, зазвичай є суб'єкти глобальної маршрутизації (загрози типів A – цілеспрямована діяльність субєктів і D –випадкові помилки суб'єктів за ДСТУ ISO/IEC 27005:2023 [11]);

– загрози реалізуються через вразливості протоколів маршрутизації, налаштувань роутерів і недоліки організаційного забезпечення інформаційної безпеки;

– наслідки реалізації загроз є взаємопов'язаними і утворюють ієрархічну систему як за послідовністю так і за структурними складовими інформаційно-комунікаційних систем, де вони проявляються.

Узагальнений алгоритм оцінювання ризиків у розроблюваній СППР наведено на рис.1.

Алгоритм оцінювання узагальнених показників ризиків за оцінками ризиків R_{ij}, який застосовується на етапі «Кількісна оцінка ризику» рис.1 наведено на рис.2. При цьому оцінки ризиків R_{ij} представлені у вигляді матриці, в якій $i \in \{S, T, R, I, D, E\}$, $j \in \{Dam, R, E, A, Dis\}$. Узагальненими показниками ризиків є суми ризиків за категоріям моделей DREAD та STRIDE, загальний сумарний ризик, долі ризиків, що відповідають категоріям моделей DREAD та STRIDE, інтегральний інтегральний ризик для кожної і-ої загрози, який розраховується як $0,2\sum_j R_{ij}$. Оцінювання ризиків здійснюється за обраною шкалою, для котрої визначені одиниці вимірювання O, кількість діапазонів H, ліва і права границі кожного h-го діапазону ($\{(gl_h, gr_h)\}$, де h=1, 2, …, H), множина можливих якісних оцінок ризиків $\{Y_h\}$, в якій Y_h є лінгвістичними термами (наприклад, Нульовий, Дуже низький, Низький, Середній, Високий, Дуже високий). Ризики R_{ij} кількісно оцінюються експертним шляхом, а якісно – за наступними правилами: Y_1 , якщо $R_{ij} < gl_1$; Y_h, якщо $gl_h \le R_{ij} < gr_h$ і $h \ne 1$, $h \ne H$; Y_H, якщо $R_{ij} \ge gl_H$. Аналогічно визначаються якісні оцінки узагальнених показників ризиків.

Структура СППР, в якій реалізуються розроблені алгоритми, наведена на рис.3

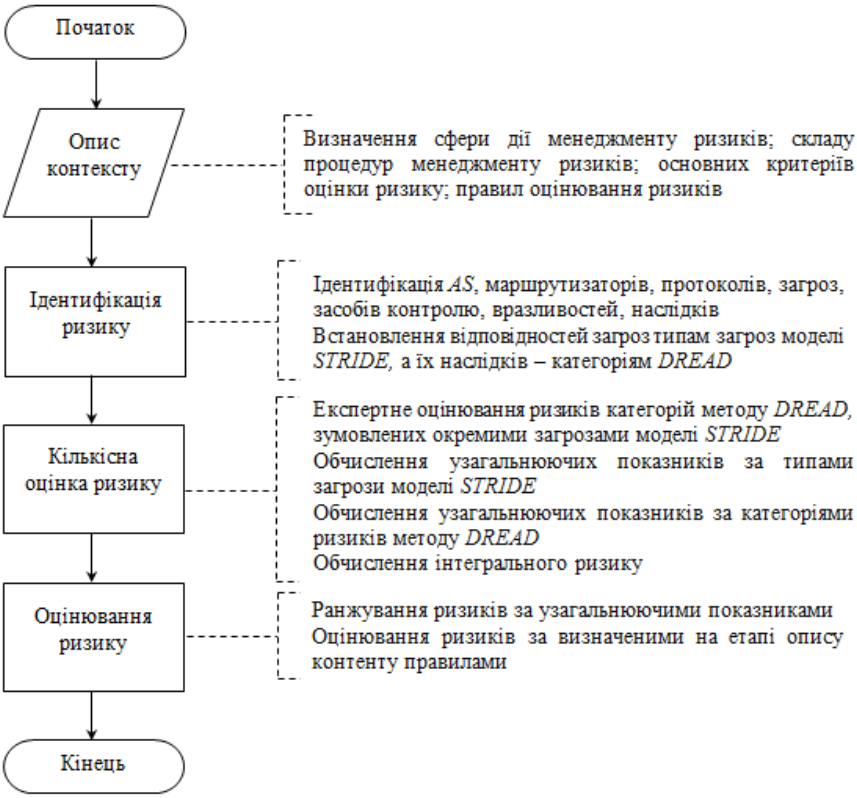

Рисунок 1 – Узагальнений алгоритм оцінювання ризиків

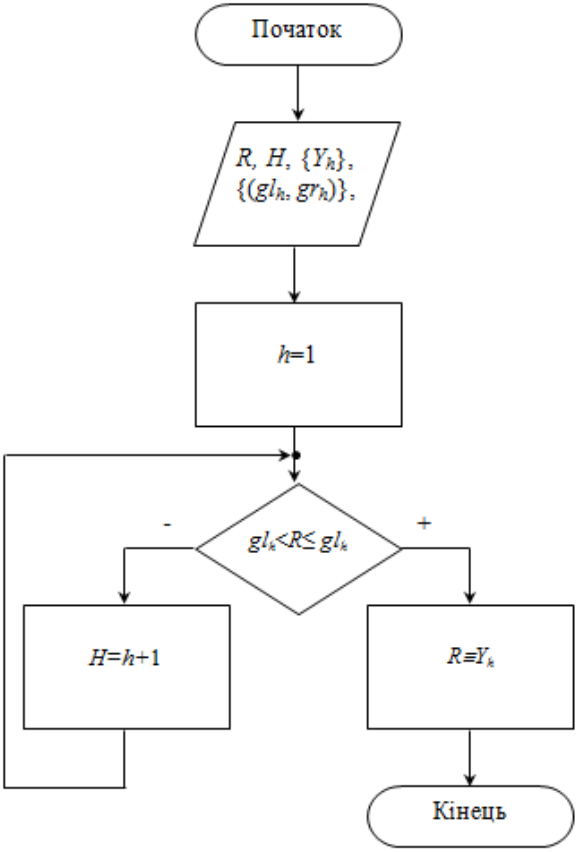

Рисунок 2 – Алгоритм оцінювання узагальнених показників ризиків

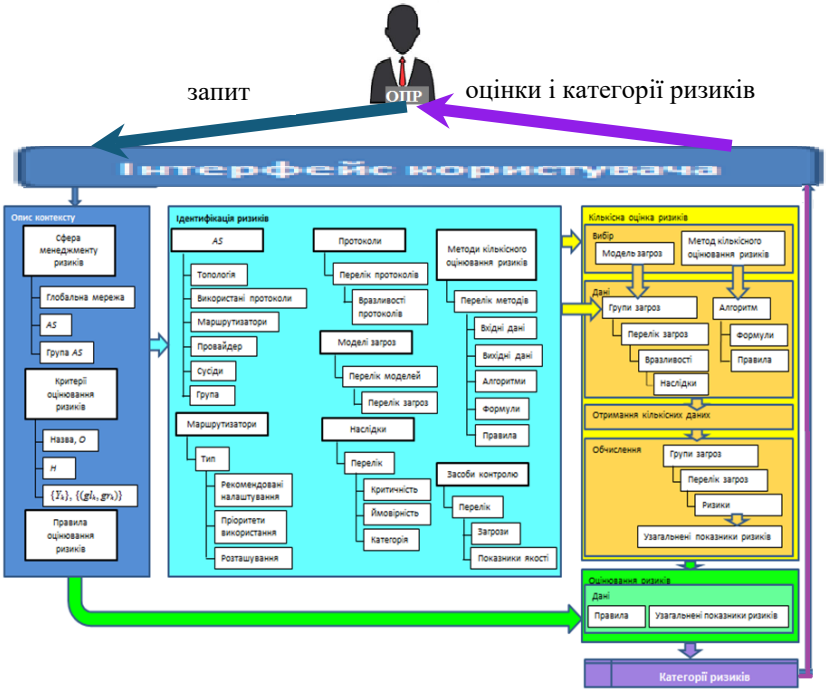

Рисунок 3 – Структура СППР

Висновки

В даній роботі проведено аналіз відкритих літературних джерел і визначені загрози інформаційній безпеці системи глобальної маршрутизації та особливості методів оцінювання асоційованих з ними ризиків, розроблено базові алгоритми і структуру СППР щодо оцінювання ризиків глобальної маршрутизації загрози

Список літератури:

1. MANRS: Protect the Internet URL: https://www.manrs.org/

2. IAPH Cybersecurity Guidelines for Ports and Port Facilities. URL: https://sustainable worldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf

3. Про критичну інфраструктуру. Закон України URL: https://zakon.rada. gov.ua/laws/ show/1882-20#Text

4. Jiajia L., Yih-Chun H., Mingwei X., Jianping W. BGP with BGPsec: Attacks and Countermeasures. IEEE Network. 2019. Vol. 33. Issue 4. PP. 194-200. URL: https://ieeexplore.ieee. org/document/8594708

5. Lakshmanan R. Researchers Uncover New BGP Flaws in Popular Internet Routing Protocol Software. URL: https://thehackernews.com/2023/05/ researchers-uncover-new-bgp-flaws-in.html

6. Зубок В.Ю. Оцінювання ризиків глобальної маршрутизації. Електронне моделювання. 2019. Т.41. №2. С.97-109. URL: https://www.emodel. org.ua/images/em/41-2/Zubok.pdf

7. Зубок В.Ю. Мохор В. В. Кібербезпека топології INTERNET: монографія. К.: ІПМЕ ім. Г.Є.Пухова, 2022. 191 с. URL: https://ipme.kiev.ua/wp-content/uploads/2022/07/ Zubok_ Mokhor_Kiberbezpeka_ Topologii_Internet.pdf

8. Патент України №107617 H04L 12/00, МПК (2016.01). Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки / Снігуров А.В., Чакрян В.Х.; власник Харківський національний університет радіоелектроніки. – № u201600667; заявл. 27.01.2016; опубл. 10.06.2016, бюл. № 11

9. Турти М.В. Загрози глобальній маршрутизації в сучасному кіберпросторі. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК, 2023. С.83-92. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

10. Чакрян В.Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. Кваліфікаційна наук. праця на правах рукопису. Дисертація на здобуття наук. ступеня канд. техн. наук (доктора філософії) за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Харківський нац. ун-т радіоелектроніки, Харків, 2017. URL: https://nure.ua/wp-content/uploads/2018/Dissertation /diss_Chakryan.pdf

11. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2024

XII Всеукраїнська науково-технічна конференція
з міжнародною участю

12–13 грудня 2024 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич