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 ВИБОРУ ЗАСОБІВ ЗАХИСТУ ВІД DDOS-АТАК

Автор: *Садалюк Є.О., магістрантка, 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 даної роботи зумовлена тим, що стрімкий розвиток апаратно-програмних засобів в галузі ІТ призводить до появи нових загроз у кіберпросторі, удосконалення кібератак і відповідних засобів протидії. Джерелами суттєвої долі кіберризиків протягом тривалого часу залишаються DoS і DDoS-атаки [1-3]. Розробці засобів виявлення і запобігання цим атакам, присвячено багато наукових робіт наукових робіт [4-8], а на ринку наявний ряд різноманітних засобів протидії [1, 2, 9-11], які суттєво різняться за функціональними та експлуатаційними властивостями. Вибір засобу захисту від DoS і DDoS-атак для конкретного середовища функціонування внаслідок цього є складною задачею, для пришвидшення розв'язку якої і уникання помилок доцільно застосовувати засоби автоматизації.

Метою даної роботи є озробка системи підтримки прийняття рішень щодо вибору засобів захисту від DDoS-атак.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– визначити параметри наявних на ринку засобів захисту від DDoS-атак (ЗЗDDoSA);

– визначити критерії прийняття рішень щодо вибору ЗЗDDoSA;

– розробити основні алгоритми і структуру системи прийняття рішень (СППР) щодо вибору ЗЗDDoSA.

Наявні на ринку ЗЗDDoSA можуть бути орієнтовані на захист від атак, здійснюваних по відомим алгоритмам, і від новітніх, невідомих на момент створення ЗЗDDoSA, атак, різне середовище функціонування і можуть розповсюджуватися на різних умовах та протидіяти DDoS різними способами. Тому при виборі ЗЗDDoSA необхідно приймати до уваги типи сучасних DDoS-атак, класифікація яких наведена на рис.1 і їх можливі наслідки для певної галузі застосування, зокрема для водного транспорту [7].

Рисунок 1 – Класифікація DDoS-атак

Вибір ЗЗDDoSA має здійснюватися після ідентифікації, аналізу, оцінювання та обробки ризиків, проведених згідно ISO/IEC 27005:2022 або відповідним Державним стандартом України [12], тобто після того як на етапі обробки ризиків буде прийняте рішення щодо необхідності зниження ризиків, асоційованих із DDoS-атаками, і визначене місце розташування ЗЗDDoSA в інформаційно-комунікаційній системі.

В розроблюваній СППР формування множини альтернативних варіантів ЗЗDDoSA можна здійснити за наступними критеріями, які віддзеркалюють параметри наявних на ринку ЗЗDDoSA:

– критерії придатності, які визначають область захисту, підтримувану операційну систему і протоколи, спосіб маршрутизації, спосіб підключення до мережі провайдера, місце розташування відносно мережевого екрану, рівнь виявлення атак, схему підключення, пропускну здатність, можливість додавання сигнатур інших розробників і користувачів;

– ресурсні критерії, які визначають наявність необхідного обсягу пам’яті, документації, персоналу з достатнім рівнем кваліфікації, фінансових ресурсів для придбання, впровадження і підтримки в процесі експлуатації ЗЗDDoSA, можливості співпрацювати із їх виробниками і розповсюджувачами, умови розпосвюдження;

– функціональні критерії, які визначають типи DDoS-атак і їх кількість, яка може бути виявлена ЗЗDDoSA; рівні моделі OSI і їх кількість, на яких може працювати засіб захисту; метод аналізу трафіку; характер реакції на виявлені атаки і виконувані дії; придатність для роботи у багатопоточному режимі, обміну даними з іншими інформаційно-комунікаційними системами і додатками, визначення прихованих даних і аномальних даних, відновлення TCP потоку і HTTP web-сторінки, декодування протоколу і відображення в додатку шару протоколу, оцінювання критичності трафіку для бізнесу; наявність сповіщення знаходження і мережевої комунікаційної матричної мапи; відкритість коду; Libpcap основа, UDP трафік; орієнтований обсяг оброблюваної інформації;

– якісні критерії, які визначають кількості використовуваних сигнатур і шаблонів нормального стану; ефективність виявлення і протидії DDoS-атакам певного типу; зручність використання, оновлення сигнатур і шаблонів нормального стану; адаптовність налаштувань під вимоги користувача, наявність декількох інтерфейсів, зручність інтерфейсу користувача; підтримку розробником налаштування та експлуатації ЗЗDDoSA.

Визначені вище критерії (або вибірка критеріїв) на першому етапі можуть використовуватися для формування множини альтернативних варіантів ЗЗDDoSA за умовою наявності у ЗЗDDoSA певних властивостей, а на другому – для визначення пріоритетів альтернативних варіантів ЗЗDDoSA за методом аналізу ієрархій з врахуванням важливості кожного критерію [13] і формування множини рекомендованих ЗЗDDoSA з максимальними пріоритетами, яка надається особі, що приймає остаточне рішення. Узагальнений алгоритм вибору ЗЗDDoSA наведений на рис.2, а структура СППР – на рис.3.

Специфіка захисту від DDoS-атак у морській галузі полягає у наявності великої кількості зацікавлених у безпеці об'єктів сторін (у тому числі з різних країн) і залежності життєздатності окремих об'єктів інформаційної діяльності (наприклад, суден) від їх кіберстійкості [14]. За захист морської галузі від кібератак відповідають Уряди та окремі компанії. При цьому уряди часто підтримують порти, а компанії беруть на себе відповідальність за власні судна.

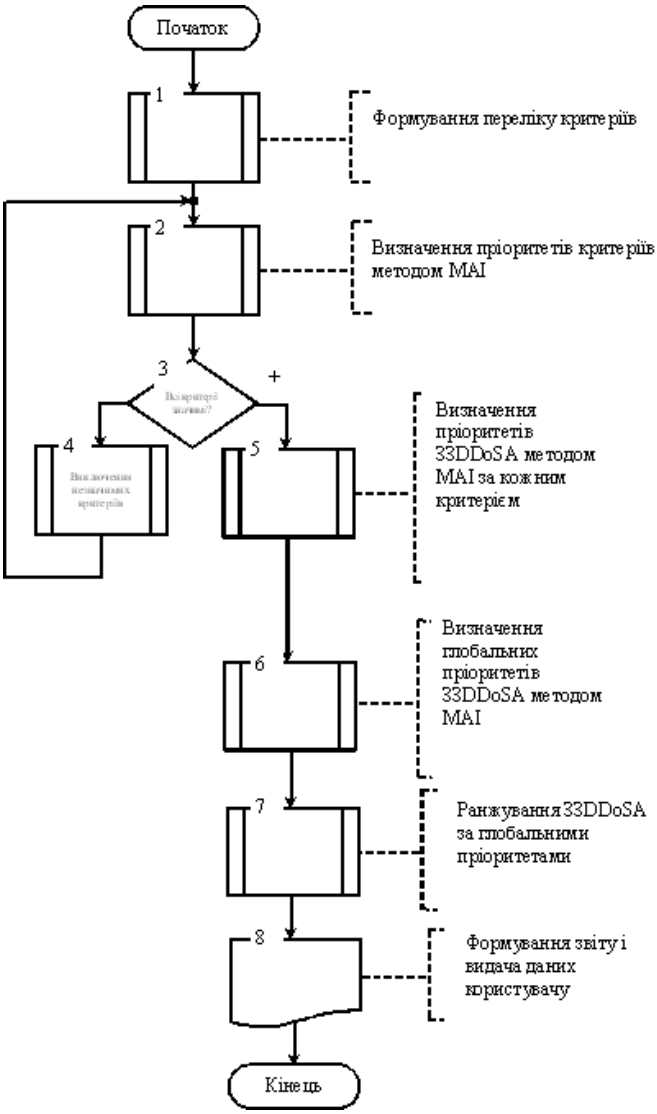

Рисунок 2 – Узагальнений алгоритм вибору 33DDoSA

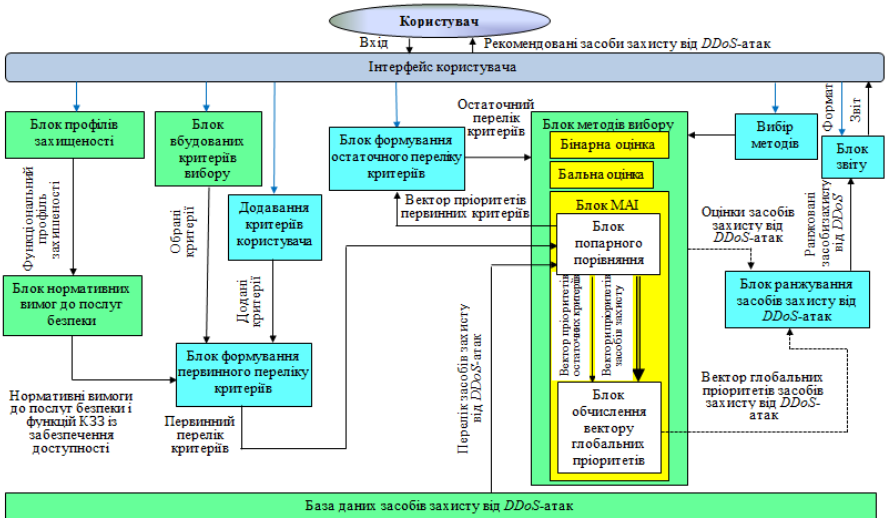

Рисунок 3 – Структура СППР

Компанії повинні мати можливість визначати вразливі місця системи захисту та усувати їх, щоб запобігти кібератакам. Це означає підтримувати системи в актуальному стані, використовувати найкраще програмне забезпечення для захисту від зловмисних програм, а також створювати та використовувати протоколи безпеки.

Роботодавці також відповідають за навчання працівників і інформування їх про ризики та ознаки кібератак. Працівники повинні знати, як безпечно використовувати технології та як дотримуватися протоколів безпеки. Компанії повинні регулярно оцінювати стан своєї кібербезпеки та за потреби вносити оновлення.

При виборі ЗЗDDoSA слід враховувати, що відшкодувати збитки після кібератаки за судовим рішенням дуже складно, оскільки не завжди зрозуміло, хто ініціював атаку. Реальною підставою для подання позову та відшкодування збитків може бути виявлена недбалість персоналу або недоліки проектування чи експлуатації системи захисту, виявлення зв'язків інцидентів кібербезпеки із порушеннями контрактів або нормативних актів [15].

Висновки.

В даній роботі визначені параметри наявних на ринку засобів захисту від DDoS-атак і критерії прийняття рішень щодо їх вибору, розроблені основні алгоритми і структура СППР щодо вибору засобів захисту від DDoS-атак.

Список літератури:

1. DDoS-атаки – растущая угроза онлайн-сервисам. URL: https:// ictn e ws.uz/28/03/2023/ddos/

2. Обзор первого квартала 2023 года: отчет StormWall о DDoS-атаках. URL: https://stormwall.pro/otchet-o-ddos-atakah-stormwall-pervyj-kvarta l-2023

3. Садалюк Є.О. Актуальні питання захисту інформації в комп'ютерних мережах. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали IX Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2021. С.184-187. URL: https://nuos.edu.ua/wp-content/uploads/2022/06/SPIBT-2021_materiali.pdf

4. Anthony D. Wood and John A. Stankovic A Taxonomy for Denial-of-Servi ce Attacks in Wireless Sensor Networks. URL: https://www.cs.virginia.edu/~stankovic/psfi les/computer02-dos.pdf

5. Jenniefer A., Raybin J. Techniques for Identifying Denial of Service Attack in Wireless Sensor Network. *Survey International Journal of Advanced Research in Computer and Communication Engineering*. Vol.3. Issue 6. 2014. URL: https: //arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf

6. Александер М., Корченко О., Карпінський М., Одарченко Р. Дослідження вразливостей сенсорних підмереж архітектури інтернету речей до різних типів атак. *Безпека інформації*. 2016. Том 22. №1. С.12-19. URL: https://dspace.nau. edu.ua/bitstream/NAU/36403/1/10448-26997-1-SM.pdf

7. Садалюк Є.О. Наслідки DDoS-атак на водний транспорт. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2023. С.215-217. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

8. Юрченко Ю.Ю., Куцолабський В.П. Сенсорні мережі загального використання URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/2918 3/8940. pdf?sequence=3&isAllowed=y

9. Smurf attack. URL: https://en.wikipedia.org/wiki/Smurf_attack

10. Спам-атака на телефон. URL: https://promov.one/spam-ataka-na-telefon/

11. Управління ключами в інформаційній системі. URL: http://pidruchniki.com/13410927/informatika/upravlinnya_klyuchami_informatsiyniy_siste mi.

12. 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

13. Катренко А.В. Системний аналіз об"єктів та процесів комп'ютеризації: Навчальний посібник. – Львів : Новий Світ-2000", 2003. – 424 с.

14. Зубков А.П. Критерії прийняття рішень щодо обробки ризиків об'єктів морської інфраструктури. *Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю*. Миколаїв: НУК, 2023. С.175-181. URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf

15. Веремчук В.С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. *Вісник Одеського Національного ун-ту. Серія: Правознавство*. 2024. Т.26. Випуск 1(38). С.112-117. https://journals.visnyk-onu.od.ua/index.php/law/article/view/472/462

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