DOI 10.31891/2307-5732-2025-347-19
УДК 004.7

КРЕМІНЬ ІГОР
Луцький національний технічний університет
e-mail: igor.kremin@gmail.com
КРЕМІНЬ СЕРГІЙ
Луцький національний технічний університет
e-mail: sergiy.kremin@gmail.com
МІНДЗЯ ОЛЕКСАНДР
Луцький національний технічний університет
e-mail: olexandr.mindzia@gmail.com

ЗАХИСТ WEB РЕСУРСІВ ВІД DDOS АТАК ЗА ДОПОМОГОЮ CDN

Захист веб-ресурсів від DDoS-атак (розподілених атак відмови в обслуговуванні) є критично важливим питанням в інформаційній безпеці. Ці атаки можуть спричиняти значні фінансові втрати та підривати довіру користувачів. Сьогодні DDoS-атаки стають все більш складними та потужними, використовуючи великі обсяги шкідливого трафіку для перевантаження серверів та мережевої інфраструктури. Одним з ефективних методів захисту веб-ресурсів від таких атак є використання мережі доставки контенту, або CDN. CDN не лише оптимізує доставку контенту, але й розподіляє навантаження між декількома серверами, зменшуючи вплив DDoS-атак шляхом розподілу трафіку по своїй мережі.

У цій статті розглядається, як CDN можуть бути використані для захисту веб-ресурсів від DDoS-атак. Основна мета — дослідити методи CDN для фільтрації та обмеження шкідливого трафіку, забезпечення безперервної доступності контенту та покращення продуктивності ресурсів. CDN розподіляють вхідний трафік по своїй глобальній мережі серверів, допомагаючи уникнути перевантаження окремих серверів та ефективно протистояти масштабним атакам.

Ключові методи захисту CDN включають: Кешування на периферії (Edge Caching) — це зберігання статичного контенту на серверах, ближчих до користувачів, що зменшує затримку та знижує кількість запитів до основного сервера. Балансування навантаження (Load Balancing) — автоматичний розподіл трафіку між серверами CDN, що знижує ризик перевантаження будь-якої окремої точки. Географічний розподіл серверів — стратегічне розміщення серверів у різних регіонах для мінімізації затримок та забезпечення високої доступності контенту.

Крім того, CDN використовують заходи безпеки, такі як шифрування TLS/SSL для захисту передачі даних, веб-фаєрволи додатків (WAF) для захисту від атак на рівні додатків (наприклад, SQL-ін'єкцій та XSS), а також технології для виявлення аномального або шкідливого трафіку. Завдяки своїй розподіленій архітектурі, CDN можуть обмежувати доступ до цільових ресурсів, блокуючи підозрілий трафік на периферійних серверах.

Результати цього дослідження показують, що використання CDN може значно знизити ризик порушення роботи сервісу під час DDoS-атак, особливо при поєднанні з іншими методами захисту, такими як обмеження швидкості та аналіз трафіку. Хоча CDN забезпечують високий рівень захисту, вони не можуть повністю замінити спеціалізовані заходи кібербезпеки та повинні бути частиною ширшої стратегії безпеки.

Ключові слова: DDoS атака, CDN, захист web-ресурсів, Web Application Firewall (WAF), фільтрація трафіку.

KREMIN IGOR
KREMIN SERHII
MINDZIA OLEKSANDR
Lutsk National Technical University

PROTECTION OF WEB RESOURCES FROM DDOS ATTACKS USING CDN

Protecting web resources from DDoS attacks (Distributed Denial of Service attacks) is a crucial issue in information security. These attacks can cause significant financial losses and damage user trust. Today, DDoS attacks are becoming more complex and powerful, using large amounts of harmful traffic to overload servers and network infrastructure. One of the effective methods to protect web resources from such attacks is by using a Content Delivery Network, or CDN. A CDN not only optimizes content delivery but also spreads the load across multiple servers, reducing the impact of DDoS attacks by distributing traffic over its network.

This article examines how CDNs can be used to protect web resources from DDoS attacks. The main goal is to explore CDN methods for filtering and limiting harmful traffic, ensuring continuous content availability, and improving resource performance. CDNs distribute incoming traffic across their global server network, helping avoid overloading single servers and efficiently countering large-scale attacks.

Key CDN protection methods include: Edge Caching - This stores static content on servers closer to users, reducing delay and lowering requests to the main server. Load Balancing- This automatically distributes traffic across CDN servers, reducing the risk of any single point being overloaded. Geographic Server Distribution - Servers are strategically placed in different regions to minimize delays and ensure high content availability.

Additionally, CDNs use security measures such as TLS/SSL encryption to protect data transfers, Web Application Firewalls (WAFs) to guard against application-level attacks (like SQL injections and XSS), and technologies for detecting abnormal or harmful traffic. With their distributed architecture, CDNs can restrict access to targeted resources by blocking suspicious traffic at edge servers.

The results of this study show that using a CDN can significantly reduce the risk of service disruption during DDoS attacks, especially when combined with other protection methods, such as rate limiting and traffic analysis. While CDNs provide a strong level of protection, they cannot completely replace specialized cybersecurity measures and should be part of a broader security strategy.

Keywords: DDoS *attack, CDN, protection of web resources, Web Application Firewall (WAF), traffic filtering.*

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

DDoS-атаки є серйозною загрозою для сучасних web-сайтів та онлайн-сервісів, оскільки можуть зробити їх недоступними для користувачів та призвести до фінансових втрат. Стандартні методи захисту часто виявляються недостатньо ефективними через великий обсяг шкідливого трафіку, який генерують такі атаки. Одним з перспективних рішень є використання CDN (мереж доставки контенту), які можуть розподілити навантаження між багатьма серверами, знижуючи ризик перевантаження системи. Завдання дослідження полягає в аналізі механізмів CDN для захисту web-ресурсів від DDoS-атак.

Аналіз досліджень та публікацій

У сфері захисту web-ресурсів від DDoS-атак науковці досліджують різноманітні підходи, що включають використання CDN, брандмауерів для web-додатків, кешування та машинне навчання для виявлення аномалій у трафіку. Враховуючи зростаючу складність та інтенсивність DDoS-атак, особливий інтерес викликає роль CDN у забезпеченні стабільної роботи ресурсів шляхом розподілу навантаження та зниження ризику перевантаження серверів. У статті "Аналіз методів захисту від DDoS атак" [1] проведено огляд різних підходів до захисту, включаючи використання CDN для розподілу навантаження та фільтрації шкідливого трафіку. Дослідження «Anycast Agility: Network Playbooks to Fight DDoS» [2] аналізує ефективність використання технології Anycast у CDN для розподілу трафіку під час DDoS-атак, що дозволяє знизити ризик перевантаження серверів. У роботі «Mitigation of Random Query String DoS via Gossip» [3] розглядається роль кешування на периферії мережі (Edge Caching) у запобіганні перевантаження основного сервера шляхом зберігання статичного контенту на серверах, розташованих ближче до користувачів. Стаття «Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection» [4] обговорює підходи до виявлення аномалій у трафіку CDN за допомогою алгоритмів машинного навчання, що сприяє швидкому реагуванню на підозрілу активність.

Формулювання цілей статті

Метою дослідження є: вивчення можливостей використання CDN для захисту web-ресурсів від DDoS-атак, зокрема, аналіз механізмів, які дозволяють розподіляти навантаження, фільтрувати шкідливий трафік та забезпечувати безперебійну роботу ресурсів під час атак.

Виклад основного матеріалу

Незважаючи на ефективність CDN у захисті веб-ресурсів від DDoS-атак, існують аспекти, які потребують подальшого дослідження та вдосконалення. По-перше, CDN здебільшого використовуються для розподілу статичного контенту, що залишає певні типи динамічного контенту вразливими до перевантаження під час атак. Необхідно дослідити, як розширити можливості кешування для динамічного контенту без шкоди для його актуальності. По-друге, атаки, спрямовані на обхід CDN шляхом безпосереднього доступу до IP-адрес основного сервера, залишаються проблемою. Для зниження таких ризиків потрібні нові методи приховування та маскування IP-адрес оригінального сервера. Також CDN-мережі вимагають удосконалення алгоритмів виявлення аномалій у трафіку. Більшість сучасних підходів базуються на аналізі шаблонів поведінки, однак новітні DDoS-атаки стають дедалі складнішими та можуть імітувати звичайний трафік, що ускладнює виявлення аномалій.

Ці невирішені питання свідчать про необхідність розробки нових механізмів захисту для забезпечення безперервної роботи веб-ресурсів у контексті постійно еволюціонуючих кіберзагроз.

Метою DDoS-атак є суттєве сповільнення або зупинка легітимного трафіку в досягненні цільового призначення. Наприклад, це може означати заборону користувачеві отримати доступ до web-сайту, купити продукт або послугу, чи переглянути інформацію. Крім того, роблячи ресурси недоступними або знижуючи продуктивність, DDoS може призвести до зупинки бізнесу. Це може призвести до того, що клієнти не зможуть отримати доступ до електронної пошти, web-додатків або інших послуг [5].

DDoS-атаки можуть бути запущені з кількох причин:

- хактивізм – зловмисники можуть спрямувати DDoS-атаку проти компаній або web-сайтів, з якими вони мають філософські чи ідеологічні розбіжності.
- кібервійна – уряди можуть використовувати такі кіберзагрози, як DDoS, щоб завдати шкоди критичній інфраструктурі ворожої держави.
- вимагання – зловмисники часто використовують загрози DDoS, щоб вимагати гроші від компаній.
- розваги – багато атак здійснюються хакерами, які просто хочуть розважитися, сіючи хаос або експериментуючи з кіберзлочинністю.
- ділова конкуренція – бізнес може здійснити DDoS-атаку на іншу компанію, щоб отримати конкурентну перевагу.

Однією з типів атак на web ресурс може бути атака на перевищення можливого потоку прийому пакетів на інтерфейсі сервера. Є кілька варіантів, як можна цьому запобігати:

- захищати сервер,
- розподілити трафік та навантаження на декілька серверів.

DDoS-атака спрямована на перевантаження мережі величезними обсягами трафіку, блокуючи доступ до ресурсу-жертви. Це заважає реальним клієнтам використовувати додаток або сервіс, зупиняючи роботу сервісу. Об'ємні атаки здійснюються за допомогою ботнетів, що складаються з заражених пристроїв, які генерують шкідливий трафік [6].

Наведемо загальний план підходу до захисту web-ресурсу:

1. Оптимізація мережевих налаштувань,
2. Фільтрація трафіку,
3. Збільшення пропускної спроможності інтерфейсу,
4. Розподіл навантаження:
   - балансування трафіку,
   - масштабованість,
   - Anycast маршрутизація,
   - кешування статичного контенту.

Мережі доставки контенту CDN (Content Delivery Network) є розподілені мережі серверів, які працюють спільно для доставки web-контенту користувачам на основі їх географічного розташування [7]. Основна мета використання CDN полягає у покращенні продуктивності та надійності доставки контенту, а також у зменшенні затримок.

Основні аспекти доставки web-контенту за допомогою CDN:

1.Кешування на периферії [8]:

- CDN використовують сервери на периферії мережі (edge servers), які знаходяться ближче до кінцевих користувачів. Ці сервери кешують контент, що дозволяє користувачам завантажувати дані швидше, оскільки запити не потрібно надсилати до центрального дата-центру.
- оскільки вміст зберігається на серверах, що знаходяться ближче до користувачів, час затримки значно скорочується.

2.Балансування трафіку:

- CDN автоматично розподіляють трафік між різними серверами на основі поточного навантаження та доступності. Це запобігає перевантаженню та покращує загальний час відгуку.
- множинні сервери і дата-центри забезпечують високу доступність контенту навіть при збоях в окремих вузлах мережі.

3. Географічне розподілення серверів:

- сервери CDN розміщені по всьому світу, що забезпечує швидку доставку контенту користувачам, незалежно від їхнього розташування.
- CDN вибирають оптимальні маршрути передачі даних, що також сприяє зниженню затримок.

Використання CDN може значно підвищити рівень безпеки web-ресурсів за рахунок різних механізмів захисту.

Така система дозволяє впоратися з деякими DDoS-атаками за рахунок своєї архітектури [10]. Велика мережа CDN дозволяє точно визначати шкідливий трафік та його джерело, блокуючи його на усіх точках входу. Є можливість обробити підозрілий трафік, застосувавши CAPTCHA для перевірки чи клієнт є людиною.

Будь-яка атака спрямована на сервер на рівнях 1- 4 не дійде до атакованого сервера, тобто атака буде зустрінута на точках присутності CDN. Власнику сервера потрібно подбати про захист на рівнях 5 - 7 (рівні: сеансовий, представлення, прикладний). Сучасні CDN пропонують TLS/SSL шифрування як частину своєї інфраструктури, що забезпечує безпечну передачу даних від клієнта до CDN та від CDN до сервера.

Захист від DDoS атак на рівнях 5-7 моделі OSI.

Сеансовий рівень (Layer 5)

Атаки: перехоплення сеансів, фальшиві сеанси.

Можливий захист:

- TLS/SSL шифрування,
- сеансова аутентифікація,
- контроль тривалості сеансу

Рівень представлення (Layer 6)

Атаки: Шифрувальні атаки, експлойти форматів даних.

Можливий захист:

- алгоритми шифрування
- перевірка формату даних
- аналізатор шифрування

Прикладний рівень (Layer 7) [9]

Атаки: HTTP-flood, SQL-ін’єкції, XSS.

Можливий захист:

- Web Application Firewall (WAF)
- Rate limiting
- аналіз трафіку
- аналіз журналів
- оновлення програмного забезпечення

Використання CDN разом з іншими методами захисту на рівнях 5-7 дозволяє ефективно протистояти DDoS-атакам та забезпечувати безперебійну роботу web-ресурсів.

Основні методи захисту web-ресурсів з використанням CDN [10]:

1.Захист від DDoS атак:

- CDN можуть виявляти та блокувати DDoS-атаки (атаки на відмову в обслуговуванні), розподіляючи трафік по своїх серверах та використовуючи технології фільтрації для захисту від шкідливих запитів.
- CDN впроваджують фільтри та шлюзи безпеки, щоб виявляти та блокувати підозрілий трафік до того, як він досягне основного сервера.

2.Захист від SQL-ін'єкцій та XSS [11]:

- вбудовані в CDN WAF забезпечують захист від атак на web-програми, таких як SQL-ін'єкції та міжсайтовий скриптинг (XSS), шляхом аналізу та фільтрації вхідного трафіку.
- WAF також можуть виявляти та блокувати аномальну поведінку, таку як надто часті запити з однієї IP-адреси.

3. Шифрування трафіку [12]:

- CDN підтримують шифрування трафіку з використанням SSL/TLS, що забезпечує безпечну передачу даних між користувачами та серверами.
- CDN керують SSL-сертифікатами та забезпечують їх оновлення, що спрощує процес шифрування для власників web-ресурсів.

4. Контроль доступу та автентифікація:

- CDN надають інструменти для керування доступом до контенту, включаючи автентифікацію користувачів та обмеження доступу на основі IP-адрес або географічного положення.
- використання токенів для автентифікації запитів до контенту дозволяє обмежити доступ лише авторизованим користувачам.

Ці заходи роблять CDN потужним інструментом не тільки для прискорення доставки web-контенту, але й для захисту web-ресурсів від різних загроз.

CDN не є універсальним засобом захисту, оскільки зловмисники можуть впливати як на саму мережу доставки контенту (CDN), так і на сервер, що надає цей контент [13].

Основні механізми атак через CDN [14]:

– Зловмисники можуть виявити IP-адреси крайових серверів CDN за допомогою відомих технік, що дозволяє їм надсилати запити безпосередньо до цих серверів.

– Зловмисники можуть маніпулювати запитами, щоб направляти їх до бажаних крайових серверів, оминаючи алгоритми вибору CDN. Це дозволяє їм використовувати велику кількість серверів для розподілу атак.

– Додавання випадкових рядків запитів до URL дозволяє зловмисникам обходити cache CDN і змушувати крайові сервери завантажувати свіжий контент з оригінального сервера.

– Зловмисники можуть генерувати більший трафік, перериваючи з'єднання з крайовим сервером після відправлення запиту, тоді як CDN продовжує завантажувати контент з оригінального сервера.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

CDN забезпечує ефективний захист від DDoS-атак завдяки розподіленій архітектурі, яка дозволяє обробляти трафік на численних точках присутності. Це значно знижує ризик перевантаження основного сервера і забезпечує швидку доставку контенту користувачам навіть під час атак. Завдяки використанню методів, таких як кешування на периферії мережі (Edge Caching), балансування навантаження та Anycast маршрутизація, CDN здатний оперативно реагувати на підвищення обсягу трафіку і розподіляти його, знижуючи негативний вплив DDoS-атак.

Комбінація CDN з іншими засобами захисту на різних рівнях моделі OSI, включаючи шифрування TLS/SSL для забезпечення безпеки даних та брандмауери для захисту на рівні додатків, створює багаторівневий захист для web-ресурсів. Це дозволяє ефективно знизити ризики, пов'язані з DDoS-атаками, і гарантує безперебійну роботу сервісів.

Водночас, важливо забезпечувати додатковий захист і на серверах розміщення контенту, щоб уникнути можливих загроз, які можуть обійти CDN. Зокрема, це стосується налаштування правил доступу, обмеження частоти запитів та моніторингу аномальної активності.

Література

1. V. Bilko, I. Lavrovsky, A.Barom «Аналіз методів захисту від DDoS атак». [Електронний ресурс] : [веб-сайт]. – Режим доступу : https://journals.dut.edu.ua/index.php/dataprotect/article/view/2327/2226

DOI: 10.31673/2409-7292.2019.035763.

2. A S M Rizvi, L. Bertholdo, J. Ceron, J. Heidemann «Anycast Agility: Network Playbooks to Fight DDoS». [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://arxiv.org/pdf/2006.14058 – (Дата звернення: 10.09.2024).

3. S. Ferretti, V.Ghini «Mitigation of Random Query String DoS via Gossip». [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://arxiv.org/pdf/1109.4404 – (Дата звернення: 10.09.2024).

4. L.Yang, A.Moubayed, A.Shami, P.Heidari, A.Boukhtouta, A.Larabi, R.Brunner, S.Preda, D.Migault «Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection». [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://arxiv.org/pdf/2107.11514 – (Дата звернення: 10.09.2024).

5. Akamai Connected Cloud. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://www.akamai.com/glossary/what-is-ddos – (Дата звернення: 12.04.2024). – Назва з екрана.

6. Sectigo. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://www.sectigo.com/resource-library/how-does-a-ddos-attack-work – (Дата звернення: 12.04.2024). – Назва з екрана.

7. IEEE Communications Surveys & Tutorials (Volume: 23, Issue: 4, Fourthquarter 2021).

8. Edge-Cloud Computing for IoT Data Analytics: Embedding Intelligence in the Edge with Deep Learning July 2020.

9. Kapil Patel1, Prof. Rajni Ranjan Singh Makwana SQL Injection and HTTP Flood DDOS Attack Detection and Classification Based on Log Data. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://www.irjet.net/archives/V9/i5/IRJET-V9I5293.pdf – (Дата звернення: 12.04.2024).

10. How Cloudflare'S Architecture Can Scale to Stop the Largest Attacks, 2017. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks – (Дата звернення: 12.04.2024).

11. Bree Benesh, CDN + WAF: Enhancing and Protecting Your Website. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://www.amazee.io/blog/post/cdn-waf-enhancing-protecting-your-website – (Дата звернення: 12.09.2024).

12. CDN SSL/TLS | CDN security. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://www.cloudflare.com/learning/cdn/cdn-ssl-tls-security/ – (Дата звернення: 12.09.2024).

13. Content Delivery Network Security: A Survey. [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://ieeexplore.ieee.org/document/9466938/ – (Дата звернення: 12.04.2024).

14. Sipat Triukose, Zakaria Al-Qudah, and Michael Rabinovich. Content Delivery Networks: Protection or Threat? [Електронний ресурс] : [веб-сайт]. – Режим доступу: https://link.springer.com/chapter/10.1007/978-3-642-04444-1_23 – (Дата звернення: 12.04.2024).

References

1. V. Bilko, I. Lavrovsky, A.Barom «Analysis of DDoS Attack Protection Methods». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://journals.dut.edu.ua/index.php/dataprotect/article/view/2327/2226

DOI: 10.31673/2409-7292.2019.035763.

2. A S M Rizvi, L. Bertholdo, J. Ceron, J. Heidemann «Anycast Agility: Network Playbooks to Fight DDoS». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://arxiv.org/pdf/2006.14058 (Data zvernennia: 10.09.2024).

3. S. Ferretti, V.Ghini «Mitigation of Random Query String DoS via Gossip». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://arxiv.org/pdf/1109.4404 (Data zvernennia: 10.09.2024).

4. L.Yang, A.Moubayed, A.Shami, P.Heidari, A.Boukhtouta, A.Larabi, R.Brunner, S.Preda, D.Migault «Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection». [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://arxiv.org/pdf/2107.11514 (Data zvernennia: 10.09.2024)

5. Akamai Connected Cloud. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.akamai.com/glossary/what-is-ddos (Data zvernennia: 12.04.2024). – Nazva z ekrana.

6. Sectigo. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.sectigo.com/resource-library/how-does-a-ddos-attack-work (Data zvernennia: 12.04.2024). – Nazva z ekrana.

7. IEEE Communications Surveys & Tutorials (Volume: 23, Issue: 4, Fourthquarter 2021)

8. Edge-Cloud Computing for IoT Data Analytics: Embedding Intelligence in the Edge with Deep Learning July 2020

9. Kapil Patel1, Prof. Rajni Ranjan Singh Makwana SQL Injection and HTTP Flood DDOS Attack Detection and Classification Based on Log Data. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.irjet.net/archives/V9/i5/IRJET-V9I5293.pdf (Data zvernennia: 12.04.2024).

10. How Cloudflare'S Architecture Can Scale to Stop the Largest Attacks, 2017. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks (Data zvernennia: 12.04.2024).

11. Bree Benesh, CDN + WAF: Enhancing and Protecting Your Website. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.amazee.io/blog/post/cdn-waf-enhancing-protecting-your-website (Data zvernennia: 12.09.2024).

12. CDN SSL/TLS | CDN security. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://www.cloudflare.com/learning/cdn/cdn-ssl-tls-security/ (Data zvernennia: 12.09.2024).

13. Content Delivery Network Security: A Survey. [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://ieeexplore.ieee.org/document/9466938/ (Data zvernennia: 12.04.2024).

14. Sipat Triukose, Zakaria Al-Qudah, and Michael Rabinovich. Content Delivery Networks: Protection or Threat? [Elektronnyi resurs] : [veb-sait]. – Rezhym dostupu : https://link.springer.com/chapter/10.1007/978-3-642-04444-1_23 (Data zvernennia: 12.04.2024).