Дячук О.Ю., ст. викладач
Колощук М.С., асистент
Макаревич С.О., здобувач
Цимбалюк І. І., здобувач
Державний університет «Житомирська політехніка»

МЕТОДИ ЗАХИСТУ ВІД BGP-HIJACKING
В ЕПОХУ ГІБРИДНИХ ЗАГРОЗ

BGP-hijacking є серйозною загрозою для глобальної мережевої безпеки, особливо в контексті гібридної війни, де кіберзагрози поєднуються з військовими операціями, економічним тиском та інформаційними атаками. Ефективний захист вимагає комплексного підходу, який включає аутентифікацію BGP-оголошень, використання штучного інтелекту (ШІ) для виявлення атак, нормативні заходи та підготовку фахівців у сфері кібербезпеки.

Оскільки протокол BGP не має вбудованої аутентифікації маршрутних оголошень, це створює вразливість для атак, таких як підміна маршрутів (BGP-hijacking). Щоб мінімізувати ці ризики, впроваджуються сучасні механізми захисту, серед яких найпоширенішими є RPKI, BGPsec і ROV.

RPKI (Resource Public Key Infrastructure) – криптографічний механізм для перевірки права власності на IP-адреси. Він дозволяє підписувати BGP-оголошення за допомогою цифрових сертифікатів, що значно знижує ймовірність маніпуляцій із маршрутною інформацією [1].

BGPsec – це розширення BGP, яке додає криптографічний захист маршрутної інформації. Воно забезпечує аутентифікацію кожного етапу маршруту, ускладнюючи несанкціоновані зміни. Основними викликами є високе навантаження на обладнання та складність імплементації.

ROV (Route Origin Validation) працює у зв'язці з RPKI та блокує оголошення від автономних систем, які не мають підтвердженого права на певний IP-префікс. Незважаючи на ефективність, компрометація ключової інфраструктури може спричинити масштабні проблеми в глобальній маршрутизації.

Фільтрація маршрутів це ще один важливий механізм захисту від BGP-hijacking. Вона дозволяє інтернет-провайдерам контролювати, які маршрути приймаються та передаються їхньою мережею, запобігаючи поширенню несанкціонованих або шкідливих оголошень. Одним із найефективніших підходів є використання суворих політик фільтрації, де оператори мережі приймають маршрути лише від перевірених джерел, зокрема через списки дозволених префіксів (whitelisting). Це значно знижує ризик підміни маршрутів і мінімізує вплив потенційних атак. Також застосовується чорний список (blacklisting) для блокування підозрілих або вже відомих зловмисних автономних систем. Завдяки такому підходу можна оперативно реагувати на загрози та захищати критичні мережеві інфраструктури.

Крім вище зазначених механізмів велику роль відіграє ШІ, який активно використовується для аналізу аномалій у маршрутизації. Наприклад, нейромережі можуть навчатися на історичних даних про нормальну роботу мережі та виявляти відхилення, які можуть свідчити про потенційні атаки [2].

Одним із важливих підходів є прогнозування атак. Використовуючи методи машинного навчання, можливо аналізувати великі обсяги BGP-даних і виявляти загрози ще до того, як вони завдадуть шкоди.

На практиці вже існують ефективні рішення, які застосовують ШІ для моніторингу та захисту BGP-маршрутизації. Наприклад, ARTEMIS автоматично виявляє спроби BGP-HIJACKINGта допомагає операторам швидко реагувати на атаки [1].

Оскільки BGP-hijacking є серйозною загрозою, освітнім установам варто розширювати навчальні програми, включаючи теми, пов'язані з BGP, у курси з мережевої безпеки. Лабораторні роботи з використанням Cisco Packet Tracer, GNS3 та інших симуляторів дають студентам змогу практично вивчати атаки та методи захисту. Аналіз реальних кейсів та участь у CTF-змаганнях сприяють глибшому розумінню загроз та способів їх нейтралізації.

Крім аудиторних занять, важливу роль відіграє стажування у центрах реагування на кіберінциденти (CERT) та кібербезпекових лабораторіях.

Ще одним перспективним напрямом є розробка відкритих платформ для моделювання BGP-атак, які дозволять студентам та дослідникам експериментувати з різними сценаріями загроз.

Зростання кількості автономних систем (AS) ускладнює контроль маршрутизації. До того ж автоматизація атак за допомогою ШІ дозволяє зловмисникам швидше знаходити вразливості та здійснювати більш витончені атаки.

Хмарні сервіси (AWS, Google Cloud, Azure) є особливо вразливими до BGP-атак, оскільки будь-яке порушення їхньої роботи може призвести до значних фінансових та репутаційних втрат [3].

Серед перспективних методів захисту можна виділити:

1. Децентралізовану аутентифікацію на основі блокчейн-технологій.
2. Активне застосування ШІ для моніторингу BGP-трафіку.
3. Міжнародну співпрацю між провайдерами, державними установами та організаціями, що займаються кібербезпекою.
4. Юридичну відповідальність для інтернет-провайдерів, які нехтують належними стандартами безпеки [4].

BGP-хайджекінг залишається серйозною загрозою для стабільності інтернету, особливо в умовах кіберконфліктів та зростаючої залежності від цифрових технологій. Існуючі методи захисту, зокрема криптографічна аутентифікація та автоматизований моніторинг, значно знижують ризики, але потребують подальшого вдосконалення. У майбутньому розвиток штучного інтелекту дозволить не лише виявляти атаки, а й передбачати їх, а впровадження децентралізованих систем верифікації на основі блокчейну може створити більш надійну модель маршрутизації. Важливу роль також відіграватиме міжнародна співпраця та оновлення

нормативної бази, що зобов’яже провайдерів дотримуватися високих стандартів безпеки. Поєднання технологічних рішень, регулювання та освітніх ініціатив допоможе сформувати більш стійку та захищену інтернет-інфраструктуру.

Список використаних джерел:

1. Monitor, Detect, Mitigate: Combating BGP Prefix Hijacking in Real-Time with ARTEMIS / P. Sermpezis та ін. Networking and Internet Architecture. 2016. URL: https://arxiv.org/abs/1609.05702 (дата звернення: 15.03.2025).
2. Shapira T., Shavitt Y. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding. NetAI '20: Proceedings of the Workshop on Network Meets AI & ML. 2020. С. 35–41. URL: https://dl.acm.org/doi/10.1145/3405671.3405814 (дата звернення: 15.03.2025).
3. Shepardson D. White House asks agencies to step up internet routing security efforts. Reuters. URL: https://www.reuters.com/world/us/white-house-asks-agencies-step-up-internet-routing-security-efforts-2024-09-03/ (дата звернення: 15.03.2025).
4. Rundle J. White House Takes Aim at Internet Security. The Wall Street Journal. URL: https://www.wsj.com/articles/white-house-takes-aim-at-internet-security-78103a69 (дата звернення: 15.03.2025).
5. Zubok V. Y. Поєднання традиційних методів і метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію. Реєстрація, зберігання і обробка даних. 2019. Т. 21, № 2. С. 41–48. URL: https://doi.org/10.35681/1560-9189.2019.21.2.180256 (дата звернення: 20.03.2025).