УДК 004.7

В. Ю. Зубок
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова
вул. Генерала Наумова, 15, 03164 Київ, Україна
тел. (+38044) 424-10-63; e-mail: vitaly.zubok@gmail.com

Поєднання традиційних методів і метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію

Однією із масштабних проблем кібербезпеки є запобігання перехопленню маршрутів у системі глобальної маршрутизації мережі Інтернет. Запропоновано класифікацію загроз, ідентифікацію та оцінку ризиків перехоплення маршруту за допомогою комбінованого підходу до відомих моделей STRIDE та DREAD. Зроблено формальний опис двовимірної моделі оцінки ризику, що дозволяє отримати кількісну оцінку ризику кожної із загроз, які притаманні глобальній маршрутизації у мережі Інтернет. Також, завдяки метричній функції, яка описує взаємне розташування вузлів у мережі Інтернет, установлено зв'язок між положенням вузла в мережі та ризиком перехоплення маршрутів до нього.

Ключові слова: *глобальна маршрутизація, перехоплення маршрутів, оцінка ризиків, кібербезпека.*

Вступ

«Перехоплення маршрутів» чи «крадіжка маршрутів» (route hijack) протягом 10 років набуло рис масштабної кіберзагрози [1]. Оскільки в сучасному світі Інтернет здебільшого є основою всіх інших телекомунікацій, атаки на глобальну маршрутизацію насправді можуть нести загрозу багатьом видам зв'язку та доставки інформації.

24 квітня 2018 року така атака була застосована до інфраструктурного IP-префікса широко відомого хмарного сервісу Amazon AWS, метою якого була фішингова атака на криптовалютний сервіс «MyEtherWallet» шляхом перенаправлення трафіка. 12 листопада 2018 року збій глобальної маршрутизації, що торкнувся сервісів G Suite, Google Пошук і Google Аналітика, стався завдяки невеликому нігерійському провайдеру за участю China Telecom та Ростелекому [2]. Пізніше цей інцидент фахівці визнали умисними діями [3]. У червні 2019 року такої самої атаки зазнав відомий сервіс мережевого захисту CloudFlare [4].

Мета дослідження

Оскільки повністю уникнути захоплення маршрутів неможливо, актуальною проблемою є зведення ризику до мінімуму. Спираючись на актуальні світові практики управління ризиками, мають бути запропоновані нові теоретичні підходи щодо виявлення та оцінки ризику захоплення маршрутів. Для цього необхідно на основі єдиного методичного підходу, викладеного в ISO Guide 73:2009 «Управління ризиками — словник», провести систематизацію та класифікацію загроз, що з'являються від атак на глобальну маршрутизацію [5]. Після цього етапу стане можливою розробка нових моделей оцінювання ризиків, які виникають унаслідок цих загроз.

Ідентифікація загроз

Модель STRIDE [6] дозволяє зробити наступний аналіз загроз від атак на глобальну маршрутизацію.

Загроза *підміни мережевих об'єктів* притаманна атакам на глобальну маршрутизацію, причому можливо використання трьох сценаріїв:

1) IP-адреси мережі жертви присвоюються іншим мережевим пристроям, що розташовані під керуванням зловмисника;

2) зловмисник анонсує IP-адреси жертви так, щоб новий хибний маршрут мав вищий пріоритет за істинний маршрут;

3) зловмисник набуває можливості створювати мережеву активність (навіть ініціювати та приймати повноцінні сеанси клієнт-сервер) з власних мережевих пристроїв, видаючи їх за пристрої жертви. Реалізація атаки за таким сценарієм лежить в основі інших загроз, наведених далі.

Загроза *модифікації даних*, або порушення цілісності даних, є реальною в разі, коли перехоплений зловмисником завдяки хибному анонсу трафік повертається зловмисником знову в Інтернет, щоб бути доставленим істинному одержувачу. Така атака може відбуватися з підміною мережевих об'єктів або без неї.

Загроза *відмови від авторства* також є можливою в ході атаки, разом із з підміною мережевих об'єктів.

Однією із найбільш суттєвих загроз є *розголошування інформації* унаслідок перехоплення трафіка. Порушення конфіденційності є можливим у разі виконання атаки методом перехоплення трафіка та повернення його в мережу, бо це часто є необхідною умовою з урахуванням особливостей побудови мережевих протоколів рівня застосувань.

Відмова в обслуговуванні є найбільш частим наслідком перехоплення маршрутів. Створення «чорної діри», в яку потрапляє частина трафіка, який адресовано мережі жертви, не потребує отримання та аналізу трафіка.

Загроза *підвищення рівня привілеїв*, на наш погляд, не властива атакам із захопленням префікса, оскільки керування глобальною маршрутизацією не має ієрархії повноважень.

Оцінка ризику методом DREAD

Ідентифікація загроз дозволяє нам визначити ризики, що пов'язані з переліченими загрозами, та оцінити їх. Однією з відомих і перевірених часом моделей оцінки ризиків є модель DREAD [7], назва якої є акронімом з факторів ризику.

Міра чи межа потенціального збитку (*Damage potential*) може бути дуже високою внаслідок того, що така впливає на всі аспекти інформаційної безпеки, як це буде показано далі.

Відтворюваність (*Reproducibility*), тобто можливість використати вразливість «типовими» засобами, які не потрібно розробляти під конкретну атаку, є також високою. Для проведення атаки з перехопленням маршруту використовуються стандартні засоби керування глобальною маршрутизацією.

Легкість організації атаки (*Exploitability*) визначається необхідними обставинами та кваліфікацією зловмисника. Попри те, що багато атак типу перехоплення маршруту відбуваються помилково через низьку кваліфікацію чи брак досвіду, все ж атаку може виконати лише професіонал з навичками та інструментами.

Коло користувачів, які опиняться під впливом перехоплення маршруту (*Affected users*), є потенційно надзвичайно великим і зазвичай перевищує кількість уражених від більш типових DDoS із використанням техніки виснаження ресурсів (resource exhaustion).

За показником складності виявлення (*Discoverability*) атаки перехоплення маршруту є такими, виявити які найпростіше. З перелічених інцидентів усі атаки та їхні джерела були виявлені протягом декількох годин. Проте лишається відомий інцидент з крадіжкою криптовалют у 2014, коли підміною маршрутів зловмисники досягали своїх цілей протягом чотирьох місяців.

Інтегральний ризик у методиці DREAD оцінюється за формулою

$$R = \frac{R_{Dam} + R_R + R_E + R_A + R_{Dis}}{5}, \tag{1}$$

де R з індексом — чисельні оцінки відповідних типів ризику.

У той же час, кожен R з індексом є функцією, яка пов'язує вірогідність настання певного наслідку в разі реалізації певної загрози. У [8] запропоновано поєднати методи STRIDE та DREAD для отримання двовимірної моделі безпеки для оцінки ризиків кібератак на глобальну маршрутизацію. Запропонований підхід дозволяє не тільки розрахувати інтегральний ризик за факторами методом DREAD, а й оцінити вагу кожної загрози з моделі STRIDE у формуванні ризику. Тобто, на прикладі оцінки ризику потенціального збитку (damage potential):

$$R_{Dam} = R^S_{Dam} + R^T_{Dam} + R^R_{Dam} + R^I_{Dam} + R^D_{Dam} + R^E_{Dam}. \tag{2}$$

Тепер запишемо формальне представлення інтегрального ризику запропонованого методу:

$$R = \frac{\sum^{STRIDE} R_{Dam} + \sum^{STRIDE} R_R + \sum^{STRIDE} R_E + \sum^{STRIDE} R_A + \sum^{STRIDE} R_{Dis}}{5}, \tag{3}$$

де R з індексом — чисельні оцінки відповідних типів ризику.

Приклад застосування формули (3) представлено у вигляді діаграми на рис. 1.

Тип загрози	R_{Dam}	R_R	R_E	R_A	R_{Dis}	Інтегральний ризик R
S	10	5	5	10	9	7,8
T	10	4	1	8	5	5,8
R	10	4	1	8	5	5,8
I	5	5	5	10	5	6
D	8	8	8	10	0	6,8
E	0	0	0	0	0	0
Сума по категоріях	43	26	20	46	24	**32.2**

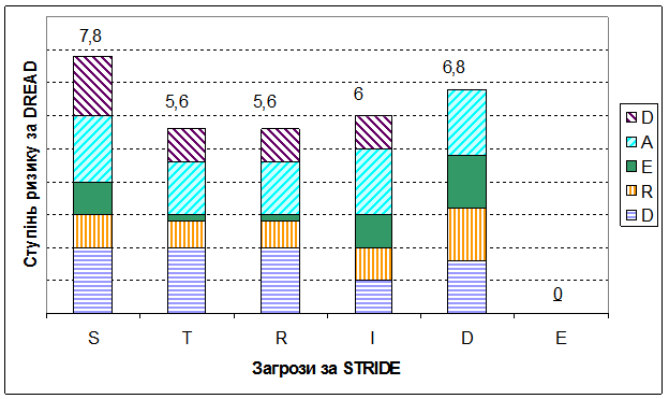

Рис. 1. Приклад оцінки загроз від атак на глобальну маршрутизацію за методом STRIDE за факторами ризику DREAD

Обґрунтування використання метричного підходу до оцінки ризику

Як відомо з принципів організації глобальної маршрутизації і протоколу BGP-4, основним транзитивним параметром, що характеризує привабливість маршруту, є довжина шляху (AS_PATH) [9]. Довжина шляху — це фактор, який дозволяє маршрутам до однакових префіксів конкурувати. Інтернет на цьому рівні являє собою незважений граф, вершинами якого є автономні системи. В загальному випадку граф є циклічним та обов'язково зв'язним. Математично цей граф можна представити або квадратною матрицею суміжності, або квадратною матрицею відстаней розмірності N, де N — кількість вузлів [10].

Якщо існує підмножина вузлів, об'єднана якоюсь сутністю, топологія цієї підмножини може розглядатись окремо. Назвемо цю підмножину цільовою групою вузлів. Такою групою можуть бути вузли-учасники будь-якої мережі обміну трафіком чи вузли-клієнти одного провайдера доступу до Інтернет.

Якщо зловмисник вдало провів перехоплення маршруту чи захоплення префікса, це означає, що для певної цільової групи вузлів маршрут до префікса жертви через вузол зловмисника став коротшим ніж інші природні маршрути, а отже — буде перехоплено трафік до цього префікса від згаданої групи вузлів.

Як уже згадувалось, у сучасній практиці для формалізації ризику широко використовують моделі, які пов'язують між собою ймовірність виникнення негативних подій і можливих збитків у результаті цих подій [5]. Визначимо ризик перехоплення трафіка R до певного префікса як добуток імовірності P такого перехоплення та збитку C, що пов'язані з цим перехопленням. Збиток є, в свою чергу, сумою збитків від перехоплення трафіка від кожного з вузлів у цільовій групі, тому:

$$R = P\sum_i C_i \,. \tag{4}$$

Якщо розподіл збитків між вузлами заздалегідь невідомий, виправданим буде вважати його однаковим для кожного вузла. Тоді збиток є пропорційним до кількості вузлів у цільовій групі. Тоді можливо оцінювати ризик як величину, пропорційну кількості вузлів N, що потрапили під вплив перехоплення:

$$R = NC \,. \tag{5}$$

Проаналізуємо, від чого залежить імовірність перехоплення трафіка P. Для цього необхідно звернутися до предметної області та зрозуміти, на які з перелічених раніше загроз та як саме може впливати фактор відстані.

Отже опишемо, завдяки яким маніпуляціям відбувається перехоплення маршруту. Атака класу BGP hijacking має кілька варіантів реалізації:

1) захоплення префікса, коли вузол анонсує як джерело адресний простір, що не належить йому. BGP віддасть перевагу маршруту, в якому кількість транзитних вузлів мереж між джерелом і одержувачем менша. Таким чином, цей маршрут буде конкурувати з істинним (рис. 2). Така атака може бути швидко виявлена, бо з точки зору «полісі» глобальної маршрутизації, наявність двох джерел в одного префікса є помилкою;

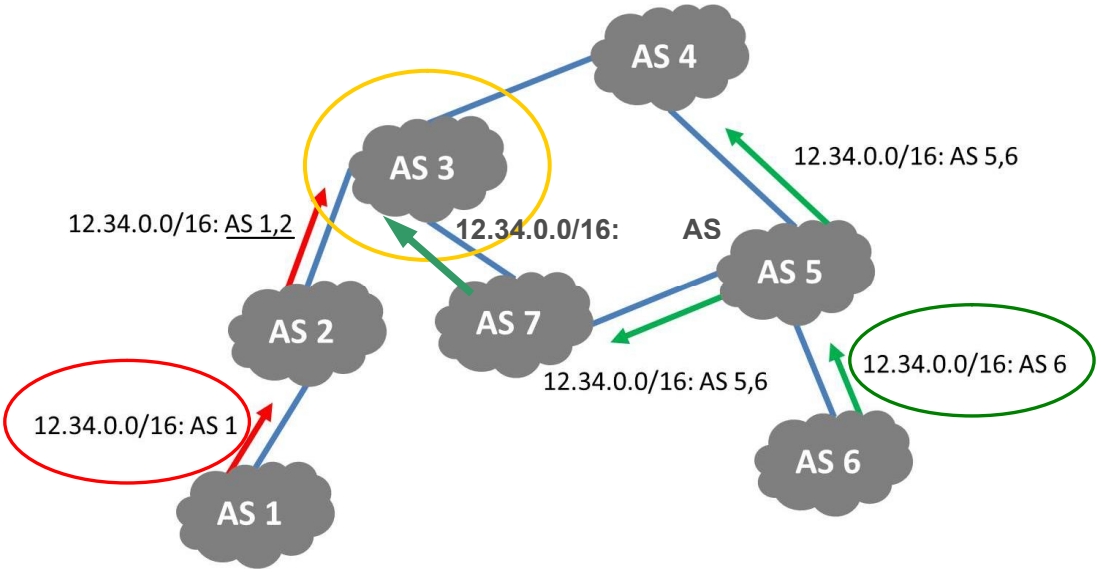

Рис. 2. Перехоплення маршруту шляхом пропонування коротшого шляху.
AS6 надсилає істинний анонс, AS1 надсилає хибний, який конкурує з істинним за критерієм коротшого шляху. Для AS3 хибний маршрут матиме перевагу через меншу довжину

2) захоплення маршруту, коли вузол ретранслює легально отриманий анонс «чужого» адресного простору, пропонуючи транзит через себе. Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, «джерело» не підмінюється, і виявити такий інцидент значно складніше;

3) захоплення нерозподіленого або невикористаного адресного простору. В цьому випадку анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету;

4) захоплення підмереж, коли анонсуються більш специфічні префікси, або так звана «деагрегація». IP-маршрутизація влаштована так, що «виграє» маршрут, в якому вказується більш специфічний префікс. На прикладі (рис. 2) адреса 12.34.128.1 входить і до префікса 12.34.0.0/16, і до 12.34.128.0/17, та останній — більш специфічний. Якщо істинний вузол анонсує префікс 12.34.0.0/16, а зловмисник — 12.34.128.0/17, з усіх маршрутизаторів, де присутні обидва анонси, трафік до 12.34.128.1 буде відправлено за хибним маршрутом. Таким чином, атакуючий «виграє», незважаючи на топологічну віддаленість (рис. 3).

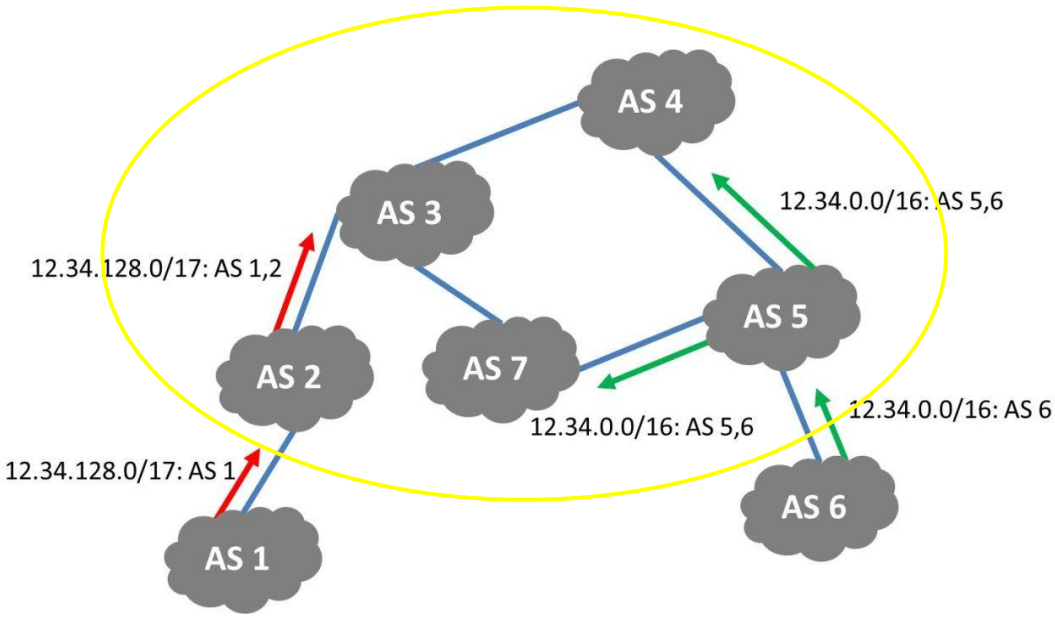

Рис. 3. Захоплення маршруту через анонсування більш специфічного префікса. AS6 надсилає істинний анонс, AS1 — більш специфічний і перехоплює трафік у глобальному масштабі

Як бачимо з пояснень до рис. 2, наведені вище випадки 1, 2, 3 пов'язані з обранням коротшого шляху, тобто залежні від відстані. Перехоплення означає, що маршрут до префікса жертви через вузол зловмисника став коротшим, ніж істинний маршрут. Існує поняття метричної розмірності графа (metric dimension) — такої мінімальної кількості вузлів графа, що положення інших вузлів може бути точно описано відстанями до перших. Відстань між вузлами як довжина найкоротшого маршруту для мережі Інтернет [11] — це функція

$$d(v,u) = \min_i \left(d(v,i) + d(i,u)\right). \tag{6}$$

З практичної точки зору це означає, що в разі перехоплення маршруту відстань (3) через фіктивний маршрут стане меншою, ніж через справжній маршрут. Маніпулювати довжиною шляху тим простіше, чим цей шлях довший (у довшому шляху посередині існує більше вузлів, через які можна анонсувати фіктивний

маршрут). Отже ймовірність перехоплення $P(v,u)$ між вузлами *v*, *u* збільшується для далеких вузлів і зменшується для близьких:

$$P(v,u) \sim d(v,u). \tag{7}$$

Отже ризик пов'язаний з кількістю вузлів, що можуть потрапити під вплив перехоплення і з відстанню до кожного з цих вузлів.

У роботі [6] представлено дослідження Інтернету з точки зору теорії складних мереж і показано зв'язок між середнім шляхом мережі, її ефективністю та вразливістю. Для кожного конкретного вузла *v* за відомими відстанями $d(v,i)$ можна визначити суму відстаней:

$$D_v = \sum_{i=1}^{|V|} d(v,i)\,. \tag{8}$$

Застосовуючи (7) до множини вузлів *V* з урахуванням (8), можна отримати залежність ризику перехоплення маршрутів до вузла *v* від його положення відносно інших вузлів:

$$R_v \sim \sum_{i=1}^{|V|} d(v,i)\,. \tag{9}$$

Таким чином, завдяки метричній функції, яка описує взаємне розташування вузлів у мережі Інтернет, встановлено зв'язок між положенням вузла в мережі та ризиком перехоплення маршрутів до нього.

Висновки

Для визначення стратегії поводження з ризиками атак на глобальну маршрутизацію запропоновано двовимірну модель оцінки ризиків на основі класифікації загроз і поєднання добре відомих моделей STRIDE та DREAD. Результат дозволяє отримати кількісну оцінку ризику кожної із загроз, притаманних глобальній маршрутизації у мережі Інтернет.

Також, завдяки метричній функції, яка описує взаємне розташування вузлів у мережі Інтернет, встановлено зв'язок між положенням вузла в мережі та ризиком перехоплення маршрутів до нього. Таке обґрунтування доводить необхідність урахування фактору відстані як третього виміру при загальній оцінці ризиків, що пов'язані з кібератаками на глобальну маршрутизацію.

1. Зубок В.Ю. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет. *Електрон. моделювання*. 2018. Т. 40. № 5. С. 67–76.

2. Internet Vulnerability Takes Down Google. URL: https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/ (дата звернення: 20.01.2019).

3. China Telecom's Internet Traffic Misdirection. URL: https://internetintel.oracle.com/blogsingle.html?id= China+Telecom%27s+Internet+Traffic+Misdirection (дата звернення: 15.01.2019).

4. The deep-dive into how Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Monday. URL: https://blog.cloudflare.com/the-deep-dive-into-how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-Monday/ (дата звернення: 29.05 2019).

5. Risk Management — Vocabulary (ISO Guide 73:2009, IDT): ДСТУ ISO Guide 73:2013. [Чинний від 2014-07-01]. Київ: Мінекономрозвитку України, 2014. 13 с. (Національні стандарти України).

6. Kohnfelder L., Garg P. The threats to our products. URL: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx (дата звернення: 21.02.2019).

7. *Howard M., LeBlanc D*. Writing Secure Code, 2nd ed. Microsoft Press, 2003, 768 p.

8. Зубок В.Ю. Оцінювання ризику кібератак на глобальну маршрутизацію. *Електрон. Моделювання*. 2019. Т. 41. № 2. С. 97–110.

9. Rekhter Y., Li T., and Hares S. A Border Gateway Protocol 4 (BGP-4). URL: https://tools.ietf.org/html/rfc4271 (дата звернення: 29.06 2018).

10. Зубок В. Практические аспекты моделирования изменений в топологии глобальных компьютерных сетей. *Реєстрація, зберігання і оброб. даних.* 2012. Т. 14. № 2. С.67-78.

11. Мохор В.В., Зубок В.Ю. Формування міжвузлових зв'язків в Інтернет з використанням методів теорії складних мереж. Київ: «Прометей», 2017. 175 с.

Надійшла до редакції 05.06.2019