Метричний підхід до оцінки ризику кібератак на глобальну маршрутизацію

Віталій Зубок[1]

[1] Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова Національної академії наук України, Київ, Україна
vitaly.zubok@gmail.om

Анотація. Одією з масштабних проблем кібербезпеки є запобігання перехопленню маршрутів в системі глобальної маршрутизації мережі Інтернет. На основі сучасної світової практики поводження з ризиками пропонуються теоретичні засади ідентифікації та оцінки ризиків перехоплення маршруту через дослідження топології зв'язків між автономними системами мережі Інтернет для подальшого формулювання задачі обробки ризиків як задачі про топологію.

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

1 Актуальність

Людство розбудовує Інтернет понад 30 років, та понад 20 років активно користується його можливостями. Сімейство мережевих протоколів TCP/IP є найбільш вдалим експериментом з побудови потужної, надійної, незалежної від фізичної середи передачі телекомунікаційної мережі. Але переваги Інтернет у певній мірі є її недоліками. Ці недоліки відчутні кожному користувачеві, насамперед, в разі втрати зв'язку з мережею чи окремими її частками, чи в незадовільній пропускній спроможності між користувачем інформації та підмережею, в якій розташований необхідний інформаційний ресурс. Зазвичай, пересічний користувач чи навіть чимале підприємство не може вплинути на розподіл ресурсів мережі поза межами зони своєї відповідальності.

Це відбувається, насамперед, через те, що Інтернет як телекомунікаційна мережа не має центру планування та керування. Централізація стосується лише деяких операцій, таких як розподіл адресного простору та керування системою доменних імен верхнього рівня.

Топологія мережі не є визначеною чи навіть типовою, кількість та структура вузлів також не є константами. Важливою особливістю Інтернет була та є можливість динамічної зміни маршрутів передачі пакетів між вузлами, які фізично не поєднані. Для такої маршрутизації використовується у якості стандартного єдиний „міжвузловий" протокол маршрутизації та правила оформлення політик маршрутизації. Наявність фізичного підключення між мережевим обладнанням в Інтернеті є необхідною, але не достатньою умовою

CEUR-WS.org/Vol-2318/paper21.pdf

для наявності зв‘язку. Пов‘язаність (наявність зв‘язків) між вузлами Інтернет визначається наявністю взаємодії між групами мережевого обладнання. З точки зору цієї прикордонної взаємодії, вузлом мережі мі будемо називати групу маршрутизаторів, які спільна політика маршрутизації об‘єднує в автономну систему. Під автономною системою (autonomous system, AS) ми розуміємо групу IP-мереж, які належать одному чи декільком операторам, та мають єдину чітко визначену політику маршрутизації. Автономні системи між собою обмінюються роутинговою інформацією з використанням протоколів зовнішньої маршрутизації (exterior routing protocol, EGP). В сучасному Інтернеті протоколом взаємодії між автономними системами є BGP-4 (Border Gateway Protocol, version 4)

Добре відомі недоліки цього єдиного протоколу глобальної маршрутизації в мережі Інтернет призводять до несанкціонованих змін в глобальній таблиці маршрутизації і, як наслідок, зміни маршруту проходження мережевого трафіку. Колись ці інциденти носили характер випадкової помилки конфігурації, але є впевненість, що протягом п’яти років зросла частка ворожих дій, тобто атак, для реалізації яких використовувалося перехоплення маршрутів [1]. Зокрема, відомі такі випадки успішної атаки на сектор криптовалют та підозри про атаку на фінансовий сектор:

- лютий 2008 р. — «захоплення» сервісу YouTube, що трапилось через дії пакістанських провайдерів, які виконували завдання свого уряду по блокуванню контенту в цьому сервісі;
- лютий-березень 2014 р. — перехоплення трафіку до майнінгових пулів криптовалют Bitcoin, Dogecoin, HoboNickels та Worldcoin через передачу фальсифікованих анонсів;
- квітень 2017 р. — перехоплення Ростелекомом маршрутів через анонсування протягом деякого часу значної кількості префіксів, які належали міжнародним платіжним системам та фінансовим сервісам;
- серпень 2017 р. — перехоплення трафіку Google багатьох операторів в Японії внаслідок технічної помилки конфігурування маршрутизаторів (за поясненням винуватця);
- грудень 2017 р. — перехоплення трафіку Google, Facebook, VK.com та інших відомих контент-провайдерів оператором з Хабаровська.

Захоплення маршруту (BGP hijacking) призводить до перетягування трафіку, призначеного для захопленої мережі, який зазвичай потім відкидається. Така стратегія має назву створення «чорної діри» (blackholing). Таким чином відбувається DoS-атака на всі сервіси мережі. У цю категорію потрапляє більшість помилок конфігурації. Якщо атака анонсує фрагмент нерозподіленого адресного простору (нічиї мережі), вона може бути використана для короткострокової генерації не просто трафіку, а для доставки шкідливого контенту, тобто елементарно — для розсилки спаму.

Інший варіант стратегії – перенаправлення трафіку. Трафік йде не в «чорну діру», а перехоплюється і аналізується. Іноді атака ще більш глибока, і перехоплений трафік не тільки не йде в «чорну діру» і аналізується, але після

перехоплення повертається знову в Інтернет, щоб бути доставленим істинному одержувачу. Таку атаку важче виявити. Метою може бути не тільки підслуховування, але і модифікація переданих даних. У більш витонченому вигляді захоплення маршруту може бути спрямоване на захоплення деякого інформаційного ресурсу, наприклад веб-сайту, з наданням користувачам підробленого сайту.

В роботі [1] пригорнуто увагу до масштабу загроз, пов'язаних з атаками на Інтернет-маршрутизацію.

Викладені факти доводять необхідність всебічного аналізу даної проблемної області з метою пошуку методів зменшення впливу таких атак, які матимуть важливе значення для кіберзахисту як на корпоративному рівні, так і на рівні критичної інфраструктури держав. Один із напрямків визначено як необхідність запобігання перехопленню маршрутів до власних префіксів. Напрямок дослідження сформульовано як задачу пошуку найбільш ефективної топологічної організації зв'язків на рівні глобальної маршрутизації в мережі Інтернет, що забезпечить мінімізацію втрат від перехоплення маршруту в межах певної цільової групи вузлів. Метою даної роботи є визначення зв’язку між топологією та ризиком перехоплення маршруту.

2 Аналіз механізмів перехоплення маршруту

Аналіз механізмів проведення атаки в залежності від її цілей. Атака класу BGP hijacking має кілька варіантів реалізації:

- Захоплення префіксу, коли вузол анонсує у якості джерела адресний простір що йому не належить. При виборі маршруту BGP віддасть перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем. Цей маршрут конкуруватиме з істинним (рис.1). Така атака може бути швидко виявлена, бо з точки зору глобальної маршрутизації, наявність двох джерел в одного префікса є помилкою.
- Захоплення маршруту, в якому 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.

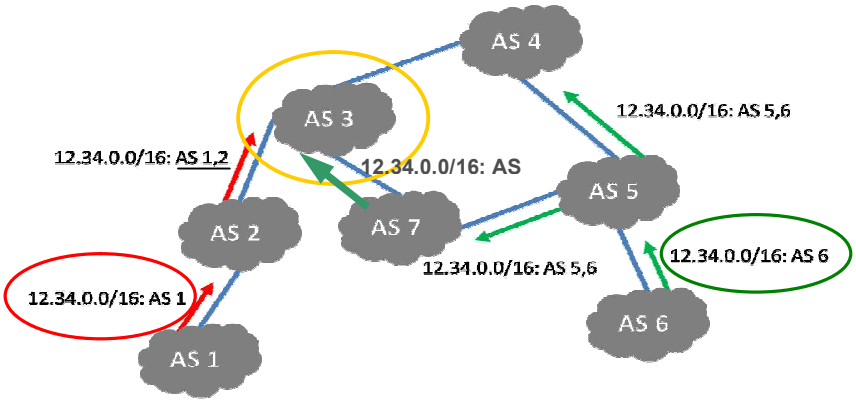

Рис.1. Перехоплення маршруту вибором коротшого шляху:

AS6 надсилає істинний анонс; AS1 – хибний, який конкурує з істинним за критерієм коротшого шляху; для AS3 хибний маршрут матиме перевагу через меншу довжину.

- Захоплення під мереж через анонсування більш специфічні префікси. При виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру захоплення має глобальний ефект (рис.2).
- Захоплення нерозподіленого або невикористаного адресного простору. Анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.
- Перенаправлення трафіку. Трафік доставляється коректному одержувачу, але передається шляхом, відмінним від істинного.

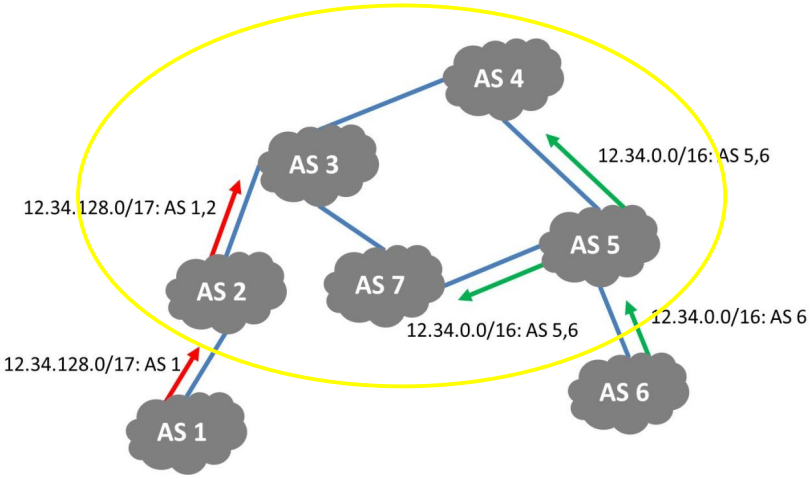

Рис.2. Захоплення маршруту через анонсування більш специфічного префіксу:

AS6 надсилає істинний анонс; AS1 – більш специфічний та перехоплює трафік в глобальному масштабі.

Одним з основних завдань системи розподілу адресного простору Інтернет є забезпечення унікальності розподілених ресурсів в глобальному масштабі. Використання в глобальному Інтернеті одного і того ж адресного простору кількома мережами призводить до порушення функціонування цих мереж, оскільки система маршрутизації Інтернет діє за принципом: кожний кінцевий пристрій має унікальну адресу. Для контролю за глобальним розподілом понад 20 років тому було введено в експлуатацію кілька баз даних Інтернет-маршрутів (Internet Routing Registry (IRR)), якими опікуються п'ять авторизованих регіональних реєстрів, що уповноважені виконувати розподіл IP-адрес і номерів автономних систем. Але якість інформації, що розміщена у цих джерелах, є суттєво різною. Чим менші об'єкти реєстрації (мережі, маршрути і та ін.), та чим ближче вони до кінцевого користувача, тим менше довіри до того, що наведені дані дійсно відображають поточну політику маршрутизації суб'єктів, до яких ці дані мають відношення.

Іншою проблемою є те, що достовірність даних неочевидна для третіх осіб. Найчастіше перевірка достовірності перетворюється в детективне розслідування з залученням різних джерел. Для валідації джерел анонсів розроблено та адаптовано інфраструктуру публічних ключів для ресурсів (RPKI). Але це вирішує лише питання авторизації внесення змін в IRR та валідації інформації про приналежність мережевих префіксів. Залишається проблемою добровільність реєстрації та актуалізації даних в IRR і, як наслідок, – відсутність повноти та достовірності даних, необов'язковість імплементації даних IRR для конфігурації маршрутизаторів та погана масштабованість процесу такої побудови.

Отже, на даний час відсутні перспективи впровадження в світовому масштабі нового, більш захищеного протоколу глобальної маршрутизації.

3 Ризик перехоплення маршруту в термінах та визначеннях міжнародних стандартів

В сучасній світовій практиці поводження з ризиками існує основа єдиного методичного підходу до сприйняття документів, які регламентують різні аспекти діяльності. Такою основою є настанови ISO Guide 73:2009 "Risk Management – Vocabulary", які тлумачать зміст відповідних термінів [2]. Головним є поняття ризику, яке надано як вплив невизначеності на досягення цілі або мети. Проте, оскільки таке поняття ризику неможливе у знеособленому сенсі, важливо насамперед визначити, хто є зацікавленою чи причетною стороною (stakeholder) в оцінюванні ризику. В загальному визначенні розуміється «будь-який індивід, група або організація, які можуть впливати на ризик, піддаватися впливу або відчувати себе підданим впливу ризику». Зазвичай, до причетних сторін відносяться клієнти та контрагенти, внутрішньо корпоративні групи (персонал, менеджмент), неурядові організації, державні структури, ЗМІ. Але в

даній роботі такою стороною є суб'єкт глобальної маршрутизації, оскільки в наслідок можливого перехоплення маршруту саме він отримає збитки.

Ризик може матеріалізуватись як настання потенційно можливих подій та (або) наслідків цих подій. Значення ризику можна виразити як поєднання подій (і їхніх наслідків) із вірогідністю їх настання. Такою подією вважатимемо свідомі чи несвідомі дії третіх сторін, які призвели до такого наслідку, як несанкціонована поява в мережі альтернативних, більш пріоритетних маршрутів.

Оцінювання ризику потребує, серед іншого, його ідентифікації. Оскільки ризик обумовлений особливостями зовнішнього і внутрішнього середовища, розглядаються всі можливі джерела ризику, а також наявна інформація про сприйняття ризику (усвідомлення ризику) причетними сторонами, як внутрішніми по відношенню до компанії, так і зовнішніми. Особливі вимоги висуваються до якості інформації (максимально можливий рівень повноти, точності і тимчасової відповідності при наявних ресурсах на її отримання) та її джерел. Ризик має аналізуватись у контексті оточення, яке поділяється на зовнішнє та внутрішнє. До внутрішнього оточення спробуємо віднести внутрішню політику маршрутизації, а о зовнішнього оточення – весь процес глобальної маршрутизації в цілому, який полягає у відносинах зацікавленої сторони з усіма іншими суб'єктами глобальної маршрутизації. Ці відносини матеріалізуються, зокрема, в обміні маршрутами по протоколу BGP-4 та в інтерпретації (сприйнятті) глобальної таблиці маршрутизації. Результат ідентифікації повинен бути структурованим та охоплювати чотири елементи – джерела виникнення; події, що виникнуть; причини цих подій; наслідки подій. Для ідентицікації ризику перехоплення маршруту зробимо опис цього ризику на основі дослідження відомих тактик та стратегій таких атак перехоплення маршрутів [1] та узагальнимо цю інформацію.

Отже:

- джерелами виникнення ризику обов'язково є інші суб'єкти глобальної маршрутизації;
- події, виникнення яких спричинює ризик, це несанкціоновані зміни в глобальній таблиці маршрутизації чи її інтерпретації на інших суб'єктах глобальної маршрутизації;
- наслідками цих подій є несанкціонована зміна напрямку проходження мережевого трафіку.

4 Загальний підхід до оцінки ризику перехоплення маршруту

Як відомо з принципів організації глобальної маршрутизації та протоколу BGP-4, основним транзитивним параметром, що характеризує привабливість маршруту, є довжина шляху (AS_PATH) [3]. 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 [4].

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 префіксу, 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 префіксу від згаданої групи вузлів.

Як вже 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 трафіку R до певного префіксу як добуток ймовірності P такого перехоплення та збитку C, пов'язаних з цим перехопленням. Збиток є в свою чергу сумою збитків від перехоплення трафіку від кожного з вузлів в цільовій групі, тому:

$$R = P\sum_i C_i \quad . \tag{1}$$

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

$$R = NC\,. \tag{2}$$

5 Метричний підхід до визначення ризику

Проаналізуємо, від чого залежить ймовірність перехоплення трафіку Р. 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 [6] - це функція:

$$d(v,u) = \min_i \big(d(v,i) + d(i,u)\big). \tag{3}$$

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

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

$$P(v,u) \sim d(v,u). \qquad (4)$$

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

В роботі [6] представлено дослідження Інтернету з точки зору теорії складних мереж та було 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 :

$$D_v = \sum_{i=1}^{|V|} d(v,i) \qquad (5)$$

Застосовуючи (4) до множини вузлів *V*, з урахуванням (5) можна отримати залежність ризику перехоплення маршрутів до вузла *v* від його положення відносно інших вузлів:

$$R_v \sim \sum_{i=1}^{|V|} d(v,i). \qquad (6)$$

Таким чином, ми встановили зв'язок між положенням вузла в мережі та ризиком перехоплення маршрутів до нього. Для цього використано метричну функцію, яка описує взаємне розташування вузлів в мережі Інтернет.

6 Висновок

Розуміння принципів функціонування протоколу глобальної маршрутизації і практичних завдань, які стоять при побудові взаємодії з Інтернет, а також механізмів кібератак на маршрутизацію, надає можливість пошуку вирішення задачі мінімізації втрат від перехоплення маршруту з використанням найбільш ефективної топологічної організації зв'язків на рівні глобальної маршрутизації мережі Інтернет.

В даній роботі у відповідності до настанов ISO Guide 73:2009 "Risk Management – Vocabulary", які тлумачать зміст відповідних термінів у сфері поводження з ризиками, було запропоновано визначення зацікавлених сторін в оцінці ризику. Також було описано шляхи визначення (ідентифікації) ризику, тобто джерела виникнення ризику, безпосередні події, що свідчать про ризик, причини цих подій, а також перелік небажаних подій, пов'язаних з наслідками можливого перехоплення маршрутів.

З використанням метричної функції для мережі Інтернет, яка представлена у вигляді графа, встановлено зв'язок між положенням вузла в мережі та ризиком перехоплення маршрутів до нього. Цей підхід до оцінки ризику дає в подальшому можливість сформулювати задачу керування ризиками для певно го вузла від перехоплення маршрутів як задачу пошуку для нього найбільш ефективної топології зв'язків.

References

1. Зубок, В: Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет. Електронне моделювання 55(40), 10-15 (2016).
2. 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).
3. Rekhter, Y. and Li, T. and Hares, S.: A Border Gateway Protocol 4 (BGP-4). https://tools.ietf.org/html/rfc4271. Дата доступу: 29 червня, 2018 р.
4. Зубок, В.: Практические аспекты моделирования изменений в топологии глобальных компьютерных сетей. Реєстрація, зберігання і обробка даних 2(14), 67-78 (2012).
5. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 (2012).
6. Мохор, В. та Зубок, В.: Формування міжвузлових зв'язків в Інтернет з використанням методів теорії складних мереж. К.:«Прометей», 2017. – 175с.

Metric Approach to Risk Evaluation of Cyberattacks on Global Routing

Vitalii Zubok[1]

[1] Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
vitaly.zubok@gmail.com

Abstract. One of the most significant problems of cybersecurity is route hijacking counteraction in the Internet global routing system. Attacking global routing is capable of harming millions of network devices (and also users) with much less effort than the well-known DDoS or Ransomware attacks. Avoiding of minimizing this risk is an actual problem. Relying on actual world practices of risk management, in this paper author offers some new theoretical approaches of identification and evaluation of route hijacking risk in the way of

exploring links and relations between the Internet autonomous. On a first step, we have proceeded through ISO Guide 73:2009 "Risk Management – Vocabulary" to tie-up to the commonly used methodical approach for risk management. Thus, it was proposed to determine all global routing participants as the stakeholders of this risk assessment. While one of the most widely used definitions of risk is collating some events (and their consequences) with their probability, so we propose to describe the risk as deeds of another party which leaded to unauthorized appearance of alternative routes with more priority. Also for risk identification we offer such approach in context of sources, events and consequences (damage): risk sources are owned by global Internet routing participants; hazardous events are unauthorized or erroneous changes in global routing table or its incorrect perception at other parties; and the 'damage' is unwanted change of way of network traffic.

Using earlier offered metric function of the Internet (3) we can see and specify clear relation between distance between two nodes and risk of route hijacking. The more distance between two autonomous systems, the more is risk of successful intrusion in global routing for their mutual traffic distortion. The same way we can measure the distance (i.e. evaluate the risk of route hijacking) between one node and a group of some other nodes (5). In the conclusion we emphasize that such approach opens a way to further formulation of route hijacking risk management problem in terms of topology tasks.

Keywords: Global Routing, Route Hijacking, Risk Evaluation, Cybersecurity