УДК 004.7

В.В. Мохор, Київ
В.Ю. Зубок, Київ

ДОСЛІДЖЕННЯ ЗВ'ЯЗКУ МІЖ ТОПОЛОГІЄЮ ТА РИЗИКОМ ВНАСЛІДОК КІБЕРАТАК НА ГЛОБАЛЬНУ МАРШРУТИЗАЦІЮ

Abstract. Cyber incidents with global routing, known as a route hijacking, lead to blocking, redirecting or distorting network traffic of millions of users and network devices. In the absence of rapid prospects for replacing the existing BGP-4 protocol globally, it is necessary to propose approaches that could be applied at the level of a large operator, industry, region, and to reduce the potential damage from attacks on global routing. This paper proposes the theoretical framework for identification and evaluation of security risks from intercepting a route through the explore of the links topology between Internet Autonomous Systems. As a conclusion, it is claimed that there is a definite relation between security risk and node position in the network. This fact opens the ways to reduce risks from route hijacking by optimizing links topology.

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

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 досягнення цілі або мети. Проте, оскільки таке поняття ризику неможливе у знеособленому сенсі, важливо насамперед визначити, хто є зацікавленою стороною (stakeholder) в оцінюванні ризику. 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

© В.В. Мохор, В.Ю. Зубок

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.

Ризик має аналізуватись у контексті оточення, яке поділяється на зовнішнє та внутрішнє. До внутрішнього оточення спробуємо віднести внутрішню політику маршрутизації, а до 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.

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. Результат ідентифікації повинен бути структурованим та охоплювати чотири елементи – джерела виникнення; події, що виникнуть; причини цих подій; наслідки подій. Для ідентифікації 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.

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:

$$R = P\sum_i C_i \ . \qquad (1)$$

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:

$$R = NC \ . \qquad (2)$$

Метричний підхід до визначення ризику. Проаналізуємо, від чого залежить ймовірність перехоплення трафіку P. 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:

$$d(v,u) = \min_i \left(d(v,i) + d(i,u)\right). \qquad (3)$$

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 (в 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 та зменшується для близьких:

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

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:

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

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

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

Висновок. 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. Це дає в подальшому можливість сформулювати задачу керування ризиками для певного вузла від перехоплення маршрутів як задачу пошуку для нього найбільш ефективної топології зв'язків.

1. *Зубок В.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електронне моделювання. – К., 2018. Т.40, № 5.

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., Li T. and Hares S.* A Border Gateway Protocol 4 (BGP-4). [Електронний ресурс]. – Режим доступу: 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. 2012., **14**, № 2, С.67-78.

5. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments // NIST Special Publication 800-30, 2012. – 95 pages.

6. *Мохор В.В., Зубок В.Ю.* Формування міжвузлових зв'язків в Інтернет з використанням методів теорії складних мереж // К.:«Прометей», 2017. – 175 с.

Поступила 27.08.2018р.