Doi: https://doi.org/10.15407/emodel.42.05.111
УДК 004.7

В.Ю. Зубок, канд. техн. наук
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Україна, 03164, Київ-164, вул. Генерала Наумова, 15,
тел. (+38044) 4241063, e-mail: vitaly.zubok@gmail.com

Нові метрики для ризикорієнтованого підходу до протидії атакам на глобальну маршрутизацію в Інтернеті

Вразливості системи глобальної маршрутизації зумовлюють великі ризики інформаційної безпеки, які потребують аналізу топології Інтернет, суб'єктів, об'єктів та процесів глобальної маршрутизації. Запропоновано нові метрики для оцінки ризику перехоплення маршрутів, базовані на топологічних характеристиках мережі.

К л ю ч о в і с л о в а: кібербезпека, глобальна маршрутизація, перехоплення маршрутів, поводження з ризиками, метрика довіри.

Маршрутизацією в комп'ютерних мережах називається процес пересилання логічно адресованого пакета від джерела в сторону пункту призначення через проміжні вузли. Система маршрутизації — це процеси, правила і протоколи. Інтернет створений і розвивається як об'єднання комп'ютерних мереж. В Інтернеті розрізняють дві системи маршрутизації: внутрішню (внутрішньомережеву, intra-domain) і зовнішню, (глобальну, міжмережеву, inter-domain). Для глобальної маршрутизації розроблені і діють по всій мережі єдині правила і протоколи обміну інформацією. Суб'єктом глобальної маршрутизації є так звана автономна система (AS). Це комп'ютерна мережа або сукупність мереж під загальним управлінням.

В останні роки все частіше відбуваються інциденти з глобальною маршрутизацією, які перетворюються на нову масштабну кіберзагрозу [1]. Кібератаки на глобальну маршрутизацію в Інтернеті використовуються для несанкціонованої зміни шляхів пересилання пакетів з метою перехоплення інформації, дестабілізації роботи мережі або її частини, порушення доступу до певних інформаційних ресурсів тощо. Такі атаки називаються «перехоплення маршруту» і «витік маршруту».

«Викрадення маршруту», чи «викрадення префіксу», — це явище, при якому AS нелегітимно оголошує себе джерелом маршруту (route origin) замість справжнього джерела. «Витік маршруту» означає, що AS нелегітимно, з порушенням політики маршрутизації, пропонує маршрути до чужих префіксів через себе. Ці нелегітимні маршрути забруднюють таблиці маршрутизації BGP, спотворюють шляхи проходження мережевого трафіку та впливають на конфіденційність, цілісність та доступність IP-комунікацій. Вони зумовлені вразливістю системи глобальної маршрутизації і, перш за все, недостатньою захищеністю єдиного протоколу глобальної маршрутизації BGP-4.

Механізми згаданих кібератак спрямовані на нав'язування суб'єктам глобальної маршрутизації помилкового уявлення про топологію мережі при відсутності механізмів валідації цієї інформації в протоколі BGP-4. Проблема відома більше 25 років, але завершення розробки нового протоколу глобальної маршрутизації, здатного вирішити завдання валідації маршруту, і його широке впровадження є завданням далекої перспективи. Пропоновані наразі зовнішні стосовно протоколу методики усунення вразливостей BGP-4 недостатньо широко впроваджені і в жодному разі не забезпечують повної захищеності маршрутів.

BGP-інциденти з глобальною маршрутизацією — це результат не тільки помилки новачка або зловмисної активності атакуючого, але й нездатність великих операторів підтримувати в належному стані фільтри маршрутів. Проблему давно усвідомлено і низка міжнародних фахівців намагається внести свій внесок [2] у поліпшення технічної складової Інтернету і здійснює ініціативу щодо внесення змін до протоколу BGP в рамках міжнародної організації IETF (Internet Engineering Task Force — Інженерної ради Інтернету). Розширення BGP дозволить надати механізм для автоматичного виявлення BGP-перехоплень і запобігання їх поширенню. Але для реалізації цього завдання знадобляться роки навіть в разі повного успіху і за сприйняття професійним співтовариством. Для того щоб система стала ефективною, потрібно змінювати саме протокол, а також відповідні зміни повинні бути впроваджені значним числом операторів в світі.

Отже, актуальною є проблема підвищення захищеності інформації при міжмережевому обміні. Метою дослідження є розвиток методології аналізу та вдосконалення топології міжмережевих зв'язків глобальної комп'ютерної мережі Інтернет, що знижують можливості нав'язування помилкового уявлення про її топологію [3].

Обґрунтування ризикорієнтованого підходу. Сучасне управління інформаційною безпекою базоване на управлінні ризиками. Ризик кількісно прийнято подавати як добуток суми збитку від реалізації певної

загрози на ймовірність реалізації цієї загрози [4, 5]. В інформаційній безпеці на ризик впливає багато факторів. Для ризику, пов'язаного з вразливостями глобальної маршрутизації в комп'ютерній мережі Інтернет, важливим фактором є топологія. Аналізуючи топологію, можна оцінити ризик. Синтезуючи нову топологію, можна управляти цим ризиком. Кількісна оцінка ризику, пов'язаного з глобальною маршрутизацією, може бути важливим критерієм оцінки ефективності топології міжмережевих зв'язків Інтернет.

З цією метою на основі єдиного методичного підходу [4, 5] проведено систематизацію та класифікацію загроз від атак на глобальну маршрутизацію, а також запропоновано підхід до оцінювання ризиків, що виникають внаслідок цих загроз. Критерієм ефективності топології проти атак на глобальну маршрутизацію є оцінка ризику як міри захищеності інформації [4].

Формальна модель глобальної маршрутизації. Як відомо, маршрутизація в складових мережах — процес мережевого рівня. Особливістю і важливою перевагою маршрутизації в Інтернеті і в мережах, що функціонують за протоколами TCP/IP, є спосіб вирішення складної обчислювальної задачі пошуку оптимального маршруту. Ефективність досягається за допомогою двох спеціальних прийомів:

1. Розподіл обчислень методом покрокового прийняття рішення про направлення передачі пакета. Кожен вузол мережі приймає рішення виходячи виключно з власних даних, наявних на момент прийняття рішення. Такими даними є список активних мережевих інтерфейсів, локальні метрики (правила, переваги, пов'язані з політикою маршрутизації), таблиця маршрутизації, створена з адміністративно заданих правил, інформації від сусідніх пристроїв, статусу мережевих інтерфейсів тощо.

2. Зменшення розмірності адресного простору за допомогою його агрегування в підмережі (subnets) з використанням так званих мережевих префіксів в форматі «адреса_мережі/довжина_мережевої_маски». Таблиця маршрутизації на жодному пристрої Інтернет не містить маршруту до всіх адрес, а лише до мережевих префіксів. Маршрут до конкретної адреси в загальному випадку стає відомий тільки безпосередньо в фізичному сегменті мережі, до якого підключений пристрій з цією адресою. Для успішної взаємодії з усіма іншими пристроями достатньо знати мережеву адресу вузла (маршрутизатора), через який можна вийти за межі своєї підмережі.

Глобальна маршрутизація є, в деякому сенсі, метамаршрутизацією, де обмін інформацією про маршрути відбувається не на мережевому, а на прикладному рівні за протоколом BGP-4. Підмережі адміністративно об'єднані в AS. У кожної AS є не менше одного прикордонного маршру-

тизатора (border router). Необхідною компонентою прикордонного маршрутизатора є програмний або програмно-апаратний сервер маршрутів. Для того щоб підмережа стала доступною для мережевого префіксу, прикордонний маршрутизатор повинен повідомити (анонсувати) її префікс сусідам. При цьому він вказує ідентифікатор своєї AS, що є джерелом маршруту (origin). Наступний прикордонний маршрутизатор при подальшій передачі анонса додає ідентифікатор своєї AS, формуючи так званий шлях (AS path). Зрештою, на підставі прийнятих BGP-системою рішень складається таблиця маршрутизації мережевого рівня для кожного маршрутизатора, що входить в AS.

Дві головних властивості — визначення маршруту тільки на один крок вперед і агрегація адреси в префікси — притаманні і глобальній маршрутизації. Обидві ці властивості експлуатуються при атаках на маршрутизацію. BGP-система може задати тільки наступний крок (next hop), покладаючись на дані, отримані від інших систем. Зловмисник, який отримав управління одним з прикордонних маршрутизаторів, може постачати в сусідні AS хибну інформацію про маршрути. Захоплений маршрутизатор може бути переконфігурований так, щоб при анонсі певного префікса (префікса жертви атаки) змінити origin, видалити або скоротити AS path.

У деяких випадках атакуючий прикордонний маршрутизатор анонсує префікс жертви, навіть не перебуваючи на шляху проходження анонса від легітимного джерела. Інколи захоплена BGP-система анонсує адресний простір жертви дрібнішими префіксами. Така атака з деагрегацією є найгіршим випадком для жертви, бо маршрути до більш специфічних префіксів є безумовно пріоритетними.

Для виявлення атак з перехоплення маршрутів та дослідження масштабів впливу на топологію, а також подальшої оцінки ризиків необхідно мати модель мережі Інтернет на рівні глобальної маршрутизації, що базується на BGP-зв'язках. Для визначення необхідних якостей нової моделі було формалізовано поняття маршрутизації.

Спочатку зроблено формальний опис перелічених раніше мережевих об'єктів та процесів:

мережева адреса та адресний простір A як безперервна множина унікальних адрес a —

$$A = \{a_1, a_2, a_3, \ldots a_{|A|} : a_i \neq a_j,\ \{i, j\} \leq |A|\}, \quad a \in p \subset A;$$

мережевий префікс p як послідовність адрес, кратна ступеню двійки, та вкладеність префіксів один в одного —

$$p_i = 2^{j-i} p_j, \quad i \leq j, \quad 0 \leq \{i, j\} \leq \log_2 |A|;$$

маршрут m як послідовність вузлів до місця призначення —

$$m(p) := (v_p, e_p);$$

відносини між префіксом та маршрутом, а саме перевага маршрутів дрібніших підмереж —

$$p_j \subset p_i \Rightarrow m(p_j) \subset m(p_i);$$

маршрутизація —

$$\begin{aligned} p(a) &= \{\min_j(p_j) : a \in p \subset A,\ 0 < j \le |A|\}, \\ \pi_v(p) &= \{\min_j(p_j) : a \in p \subset A,\ 0 < j \le |A|\}. \end{aligned} \quad (1).$$

Маршрутизацію в (1) подано як двоетапний процес. На першому етапі відбувається вибір в базі маршрутів префікса найменшої підмережі (more specific prefix), в яку може входити IP-адреса, вказана в заголовку пакета як місце призначення (destination address). На другому етапі відбувається вибір шляху, тобто найкоротшого маршруту до префікса. Перехоплення, витік маршруту, в будь-якому випадку означають, що механізм атаки спрямований на другу частину системи (1) і справжній маршрут або не досягає місця призначення, або конкурує на ньому з хибним маршрутом і може бути не прийнятий як найкращий. Серед відомих інцидентів таких — переважна кількість.

Перехоплення маршруту з деагрегацією префіксу спрямовано на першу частину системи (1), тобто підміну префікса більш специфічним. Якщо це відбувається, легітимні маршрути не можуть конкурувати з хибними, тому що система (1) вже вирішується стосовно іншого мережевого префіксу.

Нехай as_a — вузол, що є джерелом анонсу маршруту, а as_b — вузол, де наразі приймається рішення про вибір маршруту:

$$as_a, as_b \in AS : as_a \neq as_b.$$

Залежно від топології міжмережевих зв'язків, помилкові маршрути будуть мати певний ареал поширення. Оскільки нормальна BGP-система анонсує тільки маршрути, визнані нею кращими, то в певній множині AS, віддалених від захопленої BGP-системи далі, ніж атакована, легітимні анонси природним чином виграють. Але за межами якогось радіуса буде перемагати хибний анонс.

Перша складова ризику — ймовірність настання збитку — є багатофакторною компонентою, але з викладеного вище можна зробити обґрунтований висновок про те, що для довільно обраного вузла as_b ймо-

вірність P (likelihood) того, що в разі перехоплення маршруту переможе хибний маршрут, зростає разом з відстанню між вузлами $d\,(as_a, as_b)$:

$$P\,(as_a, as_b) \sim d\,(as_a, as_b). \qquad (2)$$

Розглянемо другий аспект ризику, а саме розмір збитку (losses), який є багатофакторною компонентою, як і ймовірність шкоди. Можна обґрунтовано припустити, що для власника інформаційного активу, який взаємодіє з Інтернет (наприклад, веб-ресурсу) і наражається на ризик у зв'язку з глобальною маршрутизацією (власника ризику), збиток зростає разом зі зростанням кількості $as_b \in \overline{AS}_b$, де переміг хибний маршрут:

$$as_b \in \overline{AS}_b : as_b \notin AS_b;\ AS_b \cup \overline{AS}_b = AS.$$

В загальному випадку сума збитків по конкретних вузлах $as_b \in \overline{AS}_b$, в яких переміг хибний маршрут, має вигляд

$$L = \sum_{i}^{|\overline{AS}_b|} L_i,$$

де

$$|\,\overline{AS}_b\,| \sim D : D = \sum_{i}^{|AS|} d\,(as_a, as_i).$$

Це дозволяє порівнювати потенційний збиток при моделюванні різних топологій. Різниця збитку вузла as_a за двох різних топологій міжмережевих зв'язків, що порівнюються має вигляд

$$\Delta L = L_2 - L_1 \Rightarrow \Delta L \sim \sum_{i}^{|AS|} d_2\,(as_a, as_i) - \sum_{i}^{|AS|} d_1\,(as_a, as_i).$$

Важливо зазначити, що нема достовірної можливості передбачити, де буде джерело хибного маршруту. З цієї та низки інших причин власник ризику (risk owner) u, який є і власником потенційно перехопленого префіксу, не може достовірно передбачити перебіг та результат вибору маршруту в довільному вузлі v. Оцінка однією стороною суб'єктивної ймовірності виконання певної дії на іншій стороні, в якій зацікавлена перша, але ще не може її побачити, є одним з визначень поняття довіри [6], яке можна використати.

Суб'єктом довіри є вихідний вузол u, об'єктом — вузол v, предметом довіри — прийняття в v істинного маршруту до префіксу, що належить u. Оскільки довіра є оцінкою ймовірності, враховуючи (2) як метрику довіри (trust metrics) вузла v, запишемо співвідношення середньої від-

стані між суб'єктом довіри *u* та іншими вузлами, обрахованої по вихідних зв'язках, та відстані від *u* до конкретного вузла *v*, що є об'єктом довіри:

$$T_u^v = \frac{\sum_i^{|AS|} d\,(u,i)}{d\,(u,v)(|AS|-1)},\ \{i,\ u, v\} \in AS,\ u \neq v,\ u \neq i.$$

Тут T_u^v — метрика довіри *v* за оцінкою *u*, де *u* і *v* — суб'єкт і об'єкт довіри; *i*, *u*, *v* — автономні системи мережі; *AS* — множина всіх автономних систем мережі Інтернет. На множині вузлів *AS* було введено відношення порядку за метрикою довіри: $T_i^u \leq T_j^u$, де *i*, *j* — автономні системи.

Для суб'єкта довіри як власника ризику важливість вибору істинного маршруту на вузлі *v* пов'язана з кількістю вихідних зв'язків у ньому та кількістю власних префіксів, для яких він є джерелом маршруту. Це тому, що відповідно до (2) ці фактори прямо впливають на збиток. Отже, на множині вузлів AS запропоновано ввести відношення порядку за сумою кількості вихідних зв'язків та анонсованих префіксів, яка отримала назву «значущість» (significance):

$$S_v^u = |\pi_v(p)|,$$

де S_v^u — значущість вузла *v* за оцінкою *u*; $|\pi_v(p)|$ — кількість отриманих від BGP-системи вузла *u* маршрутів, що пролягають через *v*. Відношення порядку за метрикою значущості на множині всіх автономних систем AS:

$$S_i^u \leq S_j^u,\ (i, j, u) \in AS.$$

Запровадження відношення порядку за двома метриками дозволяє власникові ризику сформувати двовимірну модель безпеки глобальної маршрутизації в Інтернеті, в основі якої лежить розподіл вузлів мережі Інтернет за зростанням ризику, бо дозволяє виразити ризик *R* через довіру як оцінку ймовірності та значущість як оцінку потенційних збитків. Дві метрики утворюють ризикоорієнтовану модель міжмережевих зв'язків, яка основана на розподілі вузлів в просторі (R, T, S), де *R* — ризик, *T* — довіра і *S* — значущість:

$$R^u = \frac{\sum_{i \neq u}^{|V|-1} S_i^u T_i^{u-1}}{|V|-1}.$$

Тут $T_i^{u^{-1}}$ — «антидовіра», ймовірність настання збитку.

Адекватність моделі. Розглянемо основні властивості цієї моделі. За даними проекту CAIDA Інтернет наразі налічує понад 80000 автономних систем, понад 800000 префіксів, декількасот тисяч зв'язків між AS, середня відстань між AS — від чотирьох до п'яти, максимальна (діаметр) — 10. Метрика довіри теоретично може набувати таких значень: $0 < T_v^u \le (|AS| - 1)$, $\left\langle T_u^v \right\rangle = 1$. На практиці з урахуванням середньої відстані та діаметру мережі Інтернет метрика довіри може набувати значень від 0,1 до п'яти. Значення більше за одиницю означає метрику довіри до вузлів від *u* до *v* більшу, ніж в середньому до інших вузлів, і навпаки.

Метрика значущості теоретично лежить в межах $1 \le S_u^v < |AS|$. Зважаючи на результати багатьох досліджень Інтернету, переважна більшість автономних систем анонсують лише один мережевий префікс і не є транзитними, тобто мають значущість S_u^v=1. А загалом розподіл вихідного ступеню має степеневий (power-law) характер і в окремих *AS* він сягає декількох тисяч. Проте в деяких формаціях, наприклад мережах обміну трафіком, зв'язки щільнійші. Отже, пошук і аналіз зв'язків *AS* з S_u^v>1 — важливий етап поводження з ризиками.

Таким чином, результати досліджень свідчать про те, що ризикорієнтована модель глобальної маршрутизації, основана на розподілі вузлів за метриками довіри та значущості, є адекватною для відображення характеристик вузлів з точки зору власника ризику.

Висновки

Сучасне управління інформаційною безпекою базовано на управлінні ризиками. Ідентифікація ризиків, пов'язаних з кібератаками на глобальну маршрутизацію в Інтернеті, свідчить про зв'язок ризику та топології міжмережевих зв'язків. Ранжування мережевих вузлів за метрикою довіри та метрикою значущості, пов'язані з ймовірністю настання ризику та масштабом потенційного збитку, дозволяє власникові ризику створити двовимірну модель розподілу вузлів мережі Інтернет за зростанням ризику і приймати рішення стосовно поводження з ризиками з використанням цієї моделі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Sermpezis P., Kotronis V., Dainotti A., Dimitropoulos X.* A survey among network operators on BGP prefx hijacking // ACM SIGCOMM Computer Communication Review, 2018, 48(1), pp. 64—69.
2. *Reuter A., Bush R., Cunha I. et al*. Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering// Ibid, 2018, 48(1), pp. 19—27.

3. *Зубок В.Ю.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електрон. моделювання, 2018, **40**, № 5, с. 67—76.
4. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. ISO/IEC JTC 1/SC 27. Feb. 2018.
5. ISO Guide 73:2009. Risk management — Vocabulary, ISO/TMBG, Nov. 2009.
6. *Mui L., Mohtashemi M., Halberstadt A*. A computational model of trust and reputation // System Sciences, 2002, pp. 2431—2439.

Отримано 03.09.2020

REFERENCES

1. Sermpezis, P., Kotronis, V., Dainotti, A. and Dimitropoulos, X. (2018), “A survey among network operators on BGP prefx hijacking”, *ACM SIGCOMM Computer Communication Review*, Vol. 48, no. 1, pp. 64-69.
2. Reuter, A., Bush, R. and Cunha, I. (2018), “Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering”, *ACM SIGCOMM Computer Communication Review*, Vol. 48, no. 1, pp. 19-27.
3. Zubok, V. (2018), “Determining the ways of counteraction to cyberattacks on the Internet global routing”, *Elektronne modelyuvannya*, Vol. 40, no. 5, pp. 67-76.
4. (2018), ISO/IEC 27000:2018, Information technology. Security techniques. Information security management systems. Overview and vocabulary.
5. (2009), ISO Guide 73:2009. Risk management, ISO/TMBG.
6. Mui, L., Mohtashemi, M. and Halberstadt, A. (2002) “A computational model of trust and reputation”, *System Sciences*, pp. 2431-2439.

Received 03.09.2020

V.Yu. Zubok

NEW METRICS FOR ASSESSMENT THE RISKS
OF THE INTERNET ROUTE HIJACK CYBERATTACS

Possibility of dynamic routes change between nodes which are not physically connected is a key feature of the Internet routing. One of the most significant problems deriving from weaknesses of the exterior gateway protocol BGP-4 is route leaks and route hijacks. None of proposed and partially implemented upgrades and add-ons like MANRS and RPKI can not deliver reliable defense against those types of attacks. Estimating the risks of route hijack requires quantitative measurement of the impact of an attack on the routing distortion, and therefore, the loss of information security breach. In this paper, we will use the knowledge of the features of the Internet topology. Then we will find the relationship between topology and routing vulnerability. As a conclusion, we will try to obtain a method for quantifying information risk using a formal global routing model and trust metrics.

K e y w o r d s: cybersecurity, global routing, route hijack, risk management, trust metrics.

ЗУБОК Віталій Юрійович, канд. техн. наук, докторант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1994 р. закінчив Київський політехнічний інститут. Область наукових досліджень — глобальні інформаційні мережі, Інтернет, теорія складних мереж, кібербезпека.