DOI: https://doi.org/10.15407/emodel.42.06.108
УДК 004[413.3+738.5.057.4]

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

Побудова та візуалізація нової ризикорієнтованої моделі глобальної маршрутизації в комп'ютерній мережі Інтернет

Описано методологію пошуку ефективної топології міжмережевих зв'язків для захисту від атак на глобальну маршрутизацію. Критерієм ефективності є оцінка ризику як міра захищеності інформації. Запропоновано методику пошуку необхідних міжмережевих зв'язків за допомогою побудови моделі розподілу Інтернет-вузлів за метриками довіри та значущості, що характеризують ризик від атак типу перехоплення маршруту. Візуалізований результат моделювання наглядно демонструє практичні шляхи зниження ризику.

К л ю ч о в і с л о в а: кібербезпека, ризикорієнтована модель, глобальна маршрутизація, перехоплення маршрутів, метрика довіри.

В роботах [1, 2] описано проблеми безпеки інформації при міжмережевому обміні в Інтернеті та показано топологію зв'язків між інтернет-вузлами, якими є автономні системи (AS), і ризиком перехоплення маршруту до певної підмережі. При цьому існує зв'язок з обома компонентами ризику: з вірогідністю перехоплення і з потенційними розмірами збитку.

Розглянемо метрику довіри вузла u до вузла v, тобто співвідношення середньої відстані між вузлом — суб'єктом довіри u — та іншими вузлами, обрахованої за вихідними зв'язками, та відстанню від u до конкретного вузла v, що є об'єктом довіри. Найвищий рівень довіри з точки зору власника ризику має його власний вузол, оскільки він є суб'єктом глобальної маршрутизації та анонсує принаймні один префікс. Це має бути враховано у формулі метрики. Однак $d(u, u) = 0$. Отже, вагу метрики довіри доводиться інвертувати, а саме нижча метрика означає вищу

© Зубок В.Ю., 2020

довіру. Покажемо, що це матиме позитивні наслідки:

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

Тут T_u^v — метрика довіри v за оцінкою u, де u і v — суб'єкт і об'єкт довіри; $d\,(u, v)$ — відстань між вузлами u та v; i, u, v — автономні системи мережі; AS — множина всіх автономних систем мережі Інтернет, на якій було введено відношення порядку за метрикою довіри: $T_i^u \le T_j^u$, де $i, j — AS$, $u = v \Leftrightarrow T_u^v = 0$.

Масштаб збитку в разі появи на вузлі v хибного маршруту залежить від кількості підмереж, що маршрутизуються через цей вузол, бо їхній трафік, адресований перехопленим префіксам, буде уражено. Для оцінки масштабу збитку запропоновано метрику значущості, що пов'язана з кількістю підмереж, які отримують маршрути за посередництва вузла v. Оскільки немає практичних засобів отримання даних від кожної підмережі Інтернету для з'ясування, чи не надходять до неї маршрути за посередництва певної AS, пропонується спрощена метрика значущості, а саме за підрахунком анонсованих цією AS мережевих префіксів, які можна спостерігати в таблицях глобальної маршрутизації:

$$S_v^u = |\,\pi_v\,|, \qquad (2)$$

де S_v^u — значущість вузла v за оцінкою u; $|\,\pi_v\,|$ — кількість видимих в BGP-системі вузла u маршрутів, що пролягають через v чи виходять безпосередньо від нього. Певним чином це характеризує кількість мереж, для яких ця AS є провайдером чи партнером [3].

Відомо, що мережеві префікси мають різну довжину і описують різну кількість мережевих адрес. Так, наприклад, префікс довжиною 24 біти означає, що мережа налічує 256 адрес, 23 біти — 512 адрес, 22 біти — 1024 адреси тощо [4]. Отже, префікси нерівнозначні і мають різну вагу. Для визначення метрики значущості пропонується модифікувати формулу (2) для підрахунку не кількості, а сумарної ваги w_π анонсованих префіксів, яка розраховується за довжини префікса $l\,(\pi)$:

$$w_\pi = 2^{24-l(\pi)}. \qquad (3)$$

Згідно з (3) мережевий префікс довжиною 24 біти (256 адрес) враховується із вагою 1, а наприклад, префікс 19 біт (8192 адреси) — з вагою 32. Автономна система, що анонсує 32 мережеві префікси з 256 адресами, матиме таку саму метрику значущості, як АС, яка анонсує один префікс з 8192 адресами.

Крім того, слід зазначити, що для цільового вузла v інші вузли мережі також мають певну метрику довіри. Так, ступінь впливу маршруту, отриманого від вузла-провайдера, матиме найбільший вплив, бо до провайдера відстань найменша. При розрахунку метрики значущості S_v^u відстань між мережевим префіксом та вузлом, через який проходить анонс цього префікса, має бути врахована.

Пропонується при розрахунку значущості враховувати кожен префікс π_v із зменшувальним коефіцієнтом $(1+\delta)^{-1}$, що залежить від відстані δ між джерелом цього префікса та вузлом v, значущість якого розраховується. Тоді мережевий префікс, для якого v є джерелом маршруту ($\delta = 0$), враховується з коефіцієнтом 1. Якщо джерелом є, наприклад, сусідній з v вузол, то $(1+\delta)^{-1} = 0{,}5$. Тоді метрика значущості набуде такого вигляду:

$$S_v^u = \sum_{\pi} w_\pi (1+\delta_\pi)^{-1} = \sum_{\pi} 2^{24-l(\pi)} (1+\delta_\pi)^{-1}, \qquad (4)$$

де δ_π – відстань між джерелом префіксу та вузлом v.

Запровадження відношення порядку за двома метриками дозволяє власникові ризику чисельно оцінити ризик перехоплення маршруту на кожному цільовому вузлі. Дві метрики утворюють ризикоріентовану модель міжмережевих зв'язків, яка основана на розподілі вузлів в просторі (R, T, S), де R — ризик, T — довіра, S – значущість:

$$R_v^u = T_v^u S_v^u. \qquad (5)$$

При цьому сукупний ризик від перехоплення маршрутів по всіх цільових вузлах має вигляд

$$R^u = \sum_{i \neq u}^{|AS|-1} R_i^u. \qquad (6)$$

Отже, отримано двовимірну модель безпеки глобальної маршрутизації в Інтернеті, в основі якої лежить розподіл вузлів мережі Інтернет за зростанням ризику, де ризик виражений через довіру як оцінку ймовірності та значущість як оцінку потенційних збитків. Важливо зазначити, що картина розподілу вузлів за ризиком, складена за цією моделлю, є суб'єктивною, тому що її створено за оцінкою власника ризику — вузла u. Можливе узагальнення і спроба подати водночас всі моделі для всіх вузлів мережі у вигляді сукупної метамоделі ризику наразі здаються позбавленими перспективи практичного застосування.

Методика отримання даних для розрахунку метрик довіри та значущості. В [5, гл.1] наведено методики дослідження топології Інтер-

нету та з'ясовано, що найбільш повну і актуальну інформацію про зв'язки між AS можна отримати, дослідивши глобальні таблиці маршрутизації, які формуються в результаті взаємодії AS по протоколу маршрутизації BGP-4. Для реалізації цієї методики дослідження необхідно мати безпосередній доступ до такої інформації, яка є відкритою. Проте шляхи її оперативного отримання в повному обсязі обмежені. Необхідно мати безпосередній доступ до маршрутизатора, що або являє собою BGP-шлюз для певної автономної системи, або є посередником при обміні маршрутами. Це завдання може вирішити уповноважений мережевий адміністратор.

Іншим способом отримання інформації є отримання таблиць через так звані сервери-«дзеркала» (looking glass). По суті, сервер-дзеркало діє як обмежений за функціями портал доступу до функцій маршрутизатора в режимі «тільки читання» (тобто дозволяє лише отримувати інформацію і не дозволяє вносити зміни, наприклад, в таблиці маршрутизації чи правила фільтрації анонсів). Здебільшого сервер-дзеркало є веб-інтерфейсом до команд маршрутизатора. Програмне забезпечення для реалізації цих функцій не є стандартизованим, але є загально прийнятий перелік функцій, які може виконувати такий сервер. Зазвичай, ці сервери належать Інтенет-провайдерам чи центрам керування мережами (network operation centre (NOC)). До типових функцій сервера looking glass належить, зокрема, отримання записів з BGP-таблиці стосовно певного префіксу.

Оцінка метрик має відбуватись з позиції власника ризику. Це означає, що для отримання даних він має користуватись власними таблицями маршрутизації або засобами, що дають доступ до таблиць маршрутизації провайдерів – операторів, які надають власникові ризику послуги доступу до мережі Інтернет.

Методика розрахунку ризику. Двовимірна модель (6) має бути забезпечена за даними BGP-системи, а саме на множині отриманих маршрутів. Незалежно від формату BGP-таблиці вона міститиме наступні дані стосовно кожного маршруту: мережевий префікс, довжина префіксу, атрибут as_path, який в кожному маршруті має вигляд послідовності ідентифікаторів AS зліва направо від найближчого сусіда власника ризику до кінцевого вузла, тобто джерела префіксу. Відстань d в (1) обраховується за as_path зліва направо, а відстань δ у (4) — справа наліво. Крім того, необхідно знати ідентифікатор AS власника ризику.

А л г о р и т м розрахунку.

Попередні кроки:

1. Визначення ідентифікатора AS власника ризику (вузол u).
2. Отримання повної BGP-таблиці для вузла u.

3. Формування списку видимих AS з отриманої BGP-таблиці за атрибутами as_path.

4. За списком видимих AS кожна з них по черзі призначається вузлом *v*, після чого виконується розрахунок метрики.

Розрахунок метрики значущості вузла v:

1. Отримання переліку перфіксів π_v, які містять *v* в as_path.

2. Визначення довжини $l(\pi_v)$ для кожного префікса π_v.

3. Визначення за as_path джерела кожного префікса π_v.

4. Визначення за as_path відстані δ між *v* та джерелом префікса для кожного префікса π_v.

5. Розрахування метрики значущості S_v^u згідно з (4).

Розрахунок метрики довіри вузла v:

1. З повного списку атрибутів as_path розрахування середнього шляху від *u* до інших видимих AS за раніше складеним списком.

2. Для кожного *v* зі списку AS пошук найкоротшої відстані між *u* та *v* з повного списку атрибутів as_path.

3. Розрахунок середньої відстані від *v* серед видимих AS [5, гл.3].

4. Розрахунок метрики довіри *u* до *v* відповідно до (1).

Розрахунок ризику для вузла u:

1. По всій множині AS для вузла *u* розрахунок сумарного ризику перехоплення маршруту за формулою (6).

Розрахунок ризику для AS8258. За наведеною методикою обраховано ризик перехоплення маршуту до префікса 195.64.224.0/22, джерелом якого є AS8258. Для цього з прикордонних маршрутизаторів AS8258 отримано BGP-таблицю маршрутизації і виконано розрахунки метрики значущості та метрики довіри. З BGP надійшла інформація про 811143 мережевих префікса. В маршрутах були присутні ідентифікатори 68803 автономних систем. Серед маршрутів виявлено 101000 унікальних шляхів, тобто послідовностей AS в маршруті.

Після розрахунку метрики значущості *S* перелік AS було впорядковано за зменшенням значення *S*. З'ясовано, що таке впорядкування має експоненційний розподіл з «важким хвостом» AS, що мають мінімальну значущість. Так, 10841 з 68803 AS мають метрику значущості 1 та менше, тому що анонсують один мережевий префікс довжиною 24 біта або взагалі лише зустрічаються у шляхах одного чи двох префіксів, що належать іншим AS.

Для подальшого аналізу відібрано 1000 AS з максимальною метрикою значущості (рис. 1). В цій групі $1557 \le S_v^u \le 786647$. З урахуванням такої розрядності було підсилено вагу метрики довіри в оцінці ризику через зміну формули ризику (5), а саме введенням експоненти довіри:

$$R_v^u = 10^{T_v^u} S_v^u. \qquad (7)$$

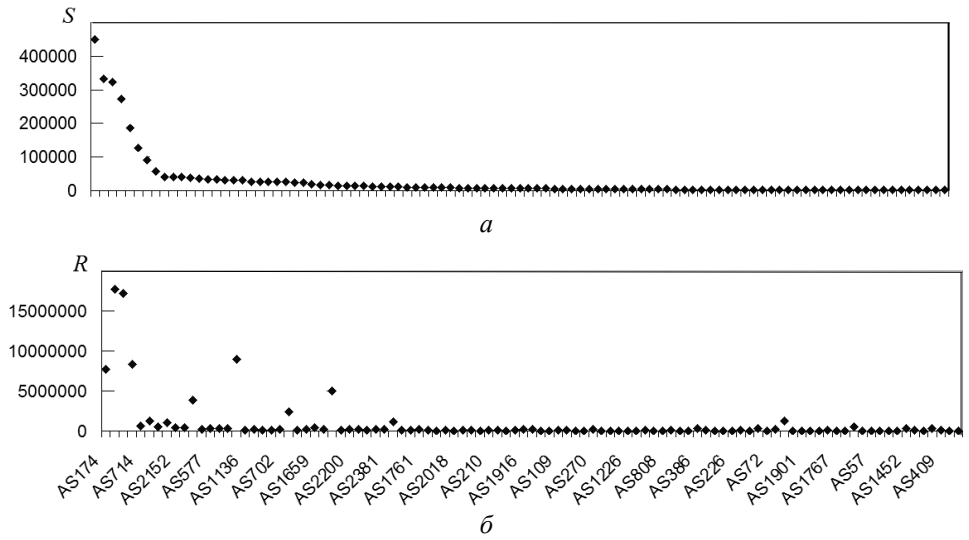

Рис. 1. Графіки розподілу за зменшенням значущості серед 100 AS з максимальною метрикою значущості

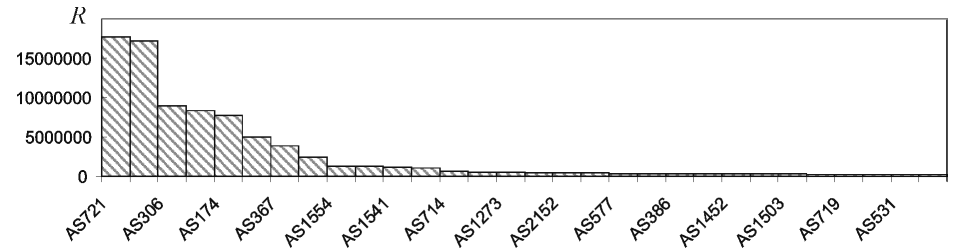

Рис. 2. Візуалізація сумарного ризику по впорядкованих за ризиком вузлах мережі

Для впорядкованої за S_v^u множини AS розраховано метрику довіри відповідно до (1) та ризик відповідно до (7). На рис. 1, *б*, на прикладі 100 вузлів з найвищою значущістю показано, як метрика довіри впливає на початкове значення вузлів (рис. 1, *а*).

Обробляння ризику. Впорядкування вузлів за зменшенням ризику (рис. 2) уможливлює зручний спосіб зниження рівня ризику. Сумарний ризик від перехоплення маршруту можна візуалізувати як площу заштрихованої фігури. Зменшення її площі відповідає зниженню ризику. Є очевидним, що зниження ризику можливе через вплив на метрики довіри певних вузлів: чим вище значущість вузла, тим вагоміше вплив на ризик.

Вплив на довіру можливий через зменшення відстані до вузла. На практиці це означає, що серед вузлів з високим ризиком необхідно шукати ті, з якими фізично та економічно можливо побудувати BGP-взає-

модію, зменшивши таким чином відстань до одиниці. Якщо побудову прямого зв'язку ускладнено, можна шукати вузол-посередник, з яким побудова з'єднання здатна забезпечити відстань 2 до одного чи декількох значущих вузлів. Отже, пошук оптимальної комбінації з'єднань є NP-складною задачею, але існують методи, які забезпечують її часткові чи приблизні рішення [5].

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. Застосування до мережевих вузлів метрики довіри та метрики значущості, які 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 з пошуку найбільш ефективної топології міжмережевих зв’язків, використовуючи ризик для оцінки цієї ефективності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Зубок В.Ю.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електрон. моделювання, 2018, 40, № 5, с. 67—76.
2. *Зубок В.Ю.* Формальний опис об’єктів і процесів глобальної маршрутизації у мережі Інтернет для оцінки впливу кібератак на маршрутизацію // Реєстрація, зберігання і обробка даних, 2019, **21**, № 4, с. 67—74. – DOI: 10.35681/1560-9189.2019.21.4.199409
3. *Dimitropoulos X., Riley G.*Modeling Autonomous–System Relationships // 20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06). Singapore, 2006. DOI: 10.1109/PADS.2006.26
4. *Fuller V., Li T.* Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. Електронний ресурс. Режим доступу: https://tools.ietf.org/html/rfc4632 (Доступно: 11.10.2019).
5. *Мохор В., Зубок В.* Формування міжвузлових зв’язків в Інтернет з використанням методів теорії складних мереж. Київ: Прометей, 2017, 175с.

Отримано 05.10.2020

REFERENCES

1. Zubok, V.Yu. (2018), “Determining the ways of counteraction to cyber attacks on the Internet global routing”, *Elektronne modelyuvannya*, Vol. 40, № 5, pp. 67-76.
2. Zubok, V.Yu. (2019), “A formal description of the Internet global routing objects and processes for global routing cyber attacks impact assessment”, *Reyestratsiya, zberihannya i obrobka danykh*, Vol. 21, № 5, pp. 67-74. DOI: 10.35681/1560-9189.2019.21.4.199409.
3. Dimitropoulos, X., Riley, G. (2006), “Modeling Autonomous–System Relationships”, *20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06)*, Singapore, May 24-26, 2006. DOI: 10.1109/PADS.2006.26.

4. Fuller, V., Li, T. (2006), “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan”, available at: https://tools.ietf.org/html/rfc4632 (accessed: November 10, 2019).
5. Mokhor, V., Zubok, V. (2017), *Formuvannia mizhvuzlovikh zviazkiv v Internet z vikoristanniam metodiv teorii scladnikh merezh* [Interconnection of the Internet nodes using methods of the complex networks theory], Prometey, Kyiv, Ukraine.

Received 05.10.2020

V.Yu. Zubok

CONSTRUCTION AND VISUALIZATION OF A NEW RISK-ORIENTED MODEL OF GLOBAL ROUTING IN THE INTERNET

In this paper the methodology of searching effective internetwork links topology for defending the global routing is developed. The risk as a measure of information security is used for criteria of topological efficiency. In a framework of risk-based approach a methodology of searching required network links by constructing a node distribution model by trust metrics and significance metrics, which characterize the risk of route hijack. Visualized result of modeling graphically demonstrates practical ways to risk mitigation.

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

ЗУБОК Віталій Юрійович, канд. техн. наук, ст. наук. співр. 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.