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) 424 10 63, e-mail: vitaly.zubok@gmail.com

Результати формування ефективної топології зв'язків в комп'ютерній мережі Інтернет на основі оцінок захищеності системи глобальної маршрутизації

Вирішено актуальну науково-практичну проблему підвищення рівня захищеності топології глобальної комп'ютерної мережі Інтернет від кібератак на систему глобальної маршрутизації. Описано застосування методики пошуку ефективної топології міжмережних зв'язків в Інтернеті для захисту від атак на систему глобальної маршрутизації, де критерієм ефективності топології є оцінка ризику як міра захищеності інформації. Наведено практичні результати застосування методики для різних за масштабом та географією суб'єктів глобальної маршрутизації. Візуалізований результат моделювання показує практичні шляхи підвищення захищеності топології міжвузлових зв'язків від кібератак типу перехоплення маршруту.

К л ю ч о в і с л о в а: кібербезпека, захищеність топології Інтернет, глобальна маршрутизація, перехоплення маршрутів.

Постановка задачі. В роботах [1, 2] описано проблеми безпеки інформації при міжмережевому обміні в Інтернеті в результаті вразливості системи глобальної маршрутизації. Існуючі методи на даний час не здатні забезпечити надійний захист ані системи глобальної маршрутизації в цілому, ані окремих маршрутів. Підвищення рівня захищеності топології глобальної комп'ютерної мережі Інтернет від кібератак на систему глобальної маршрутизації залишається актуальною науково-прикладною проблемою. В цих роботах показано, що топологія зв'язків між інтернет-вузлами, якими є автономні системи (АС), і ризик кібератаки типу перехоплення маршруту пов'язані між собою. При цьому існує зв'язок з обома компонентами ризику: вірогідністю перехоплення і потенційними розмірами збитку.

Запропонована загальна модель оцінки захищеності топології Інтернет, в якій використано нові метрики для Інтернет-вузлів, а саме метрика

© Зубок В.Ю., 2021

значущості та метрика довіри, має наступний вигляд:

$$R_v^u = \frac{\sum_i^{|V|} d(u, i)}{d(u, v)(|V| - 1)} \sum_p^{|P|} 2^{24-l(p)} (1 + \delta_p)^{-1}, \quad (1)$$

де R_v^u — ризик перехоплення на узлі v маршруту, джерелом якого є вузол u ; V — множина вузлів, до якої входять v та u ; $d(u, v)$ — топологічна відстань між u та v ; P — множина мережових префіксів, маршрут до яких пролягає крізь v ; $l(p)$ — довжина мережового префіксу $p \in P$; δ_p — відстань від v до джерела мережового префіксу p .

Методику отримання вхідних даних для ризиканалізу глобальної комп'ютерної мережі Інтернет або її певного сегменту описано у роботі [2]. Модель (1) має бути забезпечена даними з BGP-системи вузла u , названого AS власника ризику, ідентифікатор якого необхідно знати. Незалежно від формату BGP-таблиця містить наступні дані стосовно кожного маршруту: мережовий 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.

Для забезпечення моделі необхідними даними можливе використання різноманітних джерел. Перше джерело — це власні таблиці глобальної маршрутизації, які отримують безпосередньо з апаратно-програмних систем, задіяних у виконанні протоколу глобальної маршрутизації BGP-4 [3]. Дані містять «вигляд» Інтернету з однієї точки спостереження — AS власника ризику. Друге джерело даних — проект інформаційної служби маршрутизації (Routing Information Service (RIS)), який збирає та зберігає дані маршрутизації в Інтернеті. Дані надаються Інтернет-спільноті для пошуку та усунення проблем, пов'язаних з глобальною маршрутизацією, і є загальнодоступними. RIS використовує віддалені колектори маршрутів (RRC), які підтримуються регіональними інтернет-реєстрами [4] на багатьох точках обміну Інтернет-трафіком (IXP). RRC взаємодіють з місцевими операторами для збору інформації про маршрутизацію. Зібрані дані скидаються за допомогою сервера BGP і зберігаються в архіві довічно [5].

Наявність моделі та доступність вихідних даних для її застосування дає можливість проводити ризик-аналіз захищеності топології глобальної комп'ютерної мережі Інтернет. Після завершення аналізу на наступному етапі необхідно розробити методику вдосконалення міжмережових зв'язків з метою підвищення рівня захищеності топології глобальної комп'ютерної мережі Інтернет від кібератак на систему глобальної маршрутизації.

Рис. 1. Блок-схема процедури оцінки ризику перехоплення маршруту: БОТГМ — блок обробки таблиць глобальної маршрутизації, в який входять МЗТГМ — модуль збору вхідних даних таблиць глобальної маршрутизації, МВП та МВШ — модулі виділення префіксів та унікальних шляхів; БРМЗ — блок визначення метрики значущості, у який входять МОШ — модуль обробки шляхів та МРМЗ — модуль розрахунку; БРМД — блок визначення метрики довіри, до складу якого входять МРСШ — модуль розрахунку середнього коротшого шляху в мережі, МРКШ — модуль розрахунку коротшого шляху до цільового вузла, МРМД — модуль обчислення метрики довіри; БВВ — блок впорядкування вузлів, до складу якого входять МРР — модуль розрахунку ризику та МС — модуль сортування

На рис. 1 наведено функціональну схему процедури оцінки ризику перехоплення маршруту, яка є складовою методики моделювання ефективної топології. Методика вдосконалення міжмережових зв'язків для підвищення рівня захищеності топології глобальної комп'ютерної мережі Інтернет від кібератак на систему глобальної маршрутизації включає наступне:

- отримання з відкритих джерел даних про топологію Інтернет на рівні анонсів префіксів;
- визначення групи вузлів, яким перехоплення маршруту спричинить збиток;
- розрахунок метрик довіри та значущості для цільової групи вузлів;
- розрахунок поточного ризику і порівняння його із заданим;
- пошук найпривабливіших вузлів для скорочення шляху до них, моделювання скорочення шляху та повторний розрахунок метрик довіри та значущості;
- повторний розрахунок поточного ризику і порівняння його із заданим.

Рис. 2. Схема реалізації методики моделювання ефективної топології зв'язків

На рис. 2 наведено гібридну схему реалізації методики підвищення рівня захищеності топології зв'язків, на якій позначено інформаційний актив 1, підключений до Інтернет-вузла AS1 — власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора). AS1 разом з вузлами {AS2, AS3, AS4 ... ASn} входить до мережі Інтернет 2. Дані про глобальну маршрутизацію 3, отримані на вузлі AS1, передають до блоків розрахунку метрики значущості 4 та розрахунку метрики довіри 5. Результати розрахунку метрик обробляють в блоці розрахунку ризику перехоплення маршруту 6 та у впорядкованому вигляді виводять на дисплей 7, наприклад у вигляді графіка або таблиці.

Під час моделювання ефективної топології зв'язків для зниження ризику до блоку розрахунку метрики довіри подається нова топологія міжмережових зв'язків, що містить нові зв'язки. Враховуючи нові зв'язки, розраховують метрику довіри та ризик, який порівнюється із заданим.

Результати експериментальних досліджень. Експерименти було проведено на реальних даних глобальної таблиці маршрутизації, отриманих від декількох різних AS. Практичні дослідження на реальній таблиці маршрутизації показали, що запропонована методика здатна характеризувати топологію зв'язків стосовно ризику перехоплення маршруту. Отримано розподіл вузлів за метрикою значущості, визначено розподіл метрики довіри та показано її вплив на ризик.

Ризики перехоплення на окремих вузлах можна підсумувати і отримати інтегральний ризик для всієї мережі. На останньому етапі отримано емпіричне підтвердження того, що мінімальні зміни в топології, запроваджені власником інформаційного активу для підвищення рівня захищеності від атак типу перехоплення маршруту, здатні суттєво вплинути на ризик перехоплення маршруту. Вибір нової топології є складною комбінаторною задачею, для розв'язання якої вже існує багато точних та наближених методів.

Було проведено експериментальне моделювання підвищення рівня захищеності AS8258 від ризику атак перехоплення маршруту. Для цього безпосередньо з маршрутизатора AS8258 отримано таблицю глобальної маршрутизації, в якій міститься інформація про маршрути до всіх доступних на той момент мережових префіксів. Кожен маршрут містить мережовий префікс та шлях (as_path). За шляхами було складено список видимих AS, що належать множині V в моделі (1).

Для кожного вузла $v \in V$ виконано розрахунок метрики значущості. При цьому для кожного v отримано множину мережових префіксів P , до яких в AS8258 маршрути пролягають через v . Для кожного префіксу $p \in P$ визначено його джерело та відстань між джерелом та v , а також визначено вагу кожного префіксу. Для кожного вузла $v \in V$ виконано розрахунок метрики довіри. З повного списку атрибутів as_path розраховано середній шлях від AS8258 до інших видимих AS за раніше складеним списком. Для кожного v зі списку AS знайдено коротший шлях від AS8258 серед усіх шляхів, наявних в таблиці глобальної маршрутизації. Зрештою, для кожного вузла v зроблено розрахунок сумарного ризику перехоплення маршруту за формулою (1), а також розраховано сумарний ризик:

$$R^u = \sum_{i \neq u}^{|V|-1} R_i^u. \quad (2)$$

Розподіл вузлів за метрикою значущості S та за метрикою довіри T для 50 вузлів з найвищою метрикою значущості наведено на рис. 3, а розподіл ризику перехоплення маршруту R — на рис. 4. В результаті підрахунку отримано наступне: сумарний ризик (2) для перших 50 вузлів з найвищою значущістю $R^u = 1,698 \cdot 10^6$. Далі проведено впорядкування вузлів за ризиком і виділено три вузли, що мають найвищий ризик. Це вузли AS721, AS209, AS306, через які проходить велика кількість коротших шляхів до інших мереж. З цими вузлами у AS8258 відсутній безпосередній зв'язок, тож вони є концентраторами ризику перехоплення маршруту.

Рис. 3. Розподіл вузлів за метрикою значущості S (а) та за метрикою довіри T (б)

Рис. 4. Діаграма розподілу ризику перехоплення маршруту R серед 50 вузлів з найвищою метрикою значущості

Відповідно до методики вдосконалення топології (див. рис. 2) на вхід модуля 5 (розрахунок метрики довіри) має бути передано модифіковану таблицю глобальної маршрутизації, відповідно до якої між AS8258 та трьома концентраторами ризику існує безпосередній зв'язок. Проте в результаті предметного аналізу концентраторів ризику встановлено, що один з трьох, а саме AS306, належить Департаменту Оборони США. Тому можливість встановлення прямої BGP-взаємодії з ним для звичай-

Рис. 5. Діаграма розподілу ризику перехоплення маршруту серед 100 вузлів з найвищою метрикою значущості для старої топології R_1 та нової топології R_2

ного українського Інтернет-провайдера є дуже сумнівною. З урахуванням цього замість AS306 для моделювання обрано наступний за ризиком вузол — AS701. В результаті отримано нові метрики довіри до вказаних вузлів та розраховано нові ризики по всіх вузлах. Результат наведено на рис. 5.

Візуальне та арифметичне порівняння рядів даних R_1 та R_2 свідчить про те, що запровадження окремих змін у топології зв'язків AS8258 здатно зменшити ризик перехоплення маршруту. Точний розрахунок показав, що сумарний ризик (2) для нової топології склав $R'' = 8,6 \cdot 10^5$, тобто R_2 на 50 % нижче за R_1 . Отже, знайдено топологію зв'язків AS8258, яка на 50 % більше захищена від кібератак типу перехоплення маршруту завдяки впровадженню лише трьох нових з'єднань. Пояснення такого суттєвого впливу полягає в тому, що кожне нове з'єднання породжує велику кількість нових доступних маршрутів.

Було проведено наступний практичний експеримент. У топології сучасного Інтернету відіграють дуже важливу роль мережі обміну трафіком чи біржі трафіка (Internet Exchange Points, IXPs) [6]. Ідея їх заснування — додержуватися чітко визначених процедур підключення та правил взаємодії між мережами учасників. Наразі в Європі функціонує багато мереж обміну трафіком, які мають різну кількість учасників та різні обсяги трафіка. Вони мають різні процедури підключення, а головне — різну політику маршрутизації та взаємодії між учасниками. Але кожна з них здійснює свій вплив на топологію зв'язків між автономними системами в Інтернеті.

В класичній мережі обміну трафіком є послуга вільного обміну маршрутами, або публічного пірінгу. Однією з «класичних» мереж обміну трафіком є Українська мережа обміну трафіком (UA-IX), заснована в 2001 р. Наприкінці 2000 років вона перестала бути монопольною мере-

Рис. 6. Діаграма розподілу ризику перехоплення маршрутів AS8258 на основі аналізу 50 вузлів з таблиці маршрутизації публічного пірінгу в UA-IX R_1 та після злиття з таблицею DTEL-IX R_2

жею обміну трафіком, коли з'явилась мережа Digital Telecom IX (DTEL-IX). Інтернет-провайдер AS8258 є учасником мережі UA-IX, але не є учасником DTEL-IX. За допомогою моделювання присутності AS8258 в вільному обміні маршрутами DTEL-IX проведено аналіз очікуваного підвищення рівня захищеності маршрутів AS8258 від перехоплення. Для проведення аналізу отримано таблицю маршрутів з публічного пірінгу DTEL-IX та виконано її злиття з раніше отриманою з вузла AS8258 таблицею маршрутів публічного пірінгу в мережі UA-IX. В таблиці публічного пірінгу UA-IX знайдено 7647 унікальних шляхів, DTEL-IX — 21534. Після злиття в сумарній таблиці отримано 25768 унікальних шляхів.

На рис. 6 наведено діаграму ризику перехоплення маршрутів AS8258 на основі аналізу 50 вузлів з таблиці маршрутизації публічного пірінгу в UA-IX (ряд R_1) та на основі аналізу 50 вузлів з таблиці маршрутизації, отриманої внаслідок злиття з DTEL-IX (ряд R_2).

Ризик перехоплення маршруту для початкової топології становить $R'' = 8,14 \cdot 10^5$. Моделювання приєднання AS8258 до обміну маршрутами в DTEL-IX фактично є додаванням лише одного зв'язку, а в результаті для AS8258 стали доступними майже 20 тисяч нових маршрутів. Це вплинуло на середню відстань до AS8258 в мережі і відповідно на метрику довіри. Ризик зменшився майже відносно кожного вузла, а сумарний ризик для нової топології становить $R'' = 4,24 \cdot 10^5$, тобто вдвічі менше за початковий.

Висновки

Методику формування топології комп'ютерної мережі Інтернет на основі оцінок ризику кібератак на глобальну маршрутизацію розроблено на ос-

нові запропонованої моделі [2] оцінки захищеності топології Інтернет від атак на систему глобальної маршрутизації. Методика складається з двох етапів: розрахунку оцінок ризику перехоплення маршруту та моделювання змін топології. Результати емпіричних досліджень свідчать про ефективність запропонованої методики стосовно підвищення захищеності топології зв'язків певного вузла Інтернет від кібератак, вектором яких є перехоплення маршруту до мережевих префіксів, що належать цьому вузлу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Зубок В.Ю. Аналіз захищеності Інтернет-вузлів від кібератак типу перехоплення маршруту // Реєстрація, зберігання і обробка даних, 2020, **22**, № 3, с. 58—67.
2. Зубок В.Ю. Побудова та візуалізація нової ризикорієнтованої моделі глобальної маршрутизації в комп'ютерній мережі Інтернет // Електрон. моделювання, 2020, **42**, № 6, с. 108—115. DOI:10.30525/978-9934-588-79-2-1.7
3. Rekhter Y., Li T., Hares S. A Border Gateway Protocol 4 (BGP-4). [Електронний ресурс] Режим доступу: <https://tools.ietf.org/html/rfc4271>. Дата доступу: жовт.21, 2020.
4. MERIT. List of Routing Registries. Електронний ресурс] Режим доступу: <http://www.irr.net/docs/list.html>. Дата звернення: жовтень, 21, 2020.
5. Stoves S. Visibility of IPv4 and IPv6 Prefix Lengths in 2019. [Електронний ресурс] Режим доступу: https://labs.ripe.net/Members/stephen_stowes/visibility-of-prefix-lengths-in-ipv4-and-ipv6. Дата звернення: жовтень, 21, 2020.
6. Zubok V. Worldwide Internet Service Providers in Ukrainian Internet Exchange: Threats and Opportunities // CEUR workshop Processing. [Електронний ресурс] Режим доступу <http://ceur-ws.org/Vol-1813/>. Дата доступу: жовтень, 21, 2020.

Отримано 16.12.2020

REFERENCES

1. Zubok, V. (2020), "Analysis of the Internet Nodes Security from route hijack cyber attacks", *Reyestratsiya, zberihannya i obrobka danykh*, Vol. 22, № 3, pp. 58-67.
2. Zubok, V. (2020), "Construction And Visualization Of A New Risk-Oriented Model Of Global Routing In The Internet ", *Elektronne modelyuvannya*, Vol. 42, № 6, pp. 108-115, DOI:10.30525/978-9934-588-79-2-1.7.
3. Rekhter, Y., Li, T. and Hares, S. (2006), A Border Gateway Protocol 4 (BGP-4), available at: <https://tools.ietf.org/html/rfc4271> (accessed: October 21, 2020).
4. MERIT. List of Routing Registries, available at: <http://www.irr.net/docs/list.html> (accessed: October 21, 2020).
5. Stoves, S. (2019), Visibility of IPv4 and IPv6 Prefix Lengths in 2019, available at: https://labs.ripe.net/Members/stephen_stowes/visibility-of-prefix-lengths-in-ipv4-and-ipv6 (accessed: October 21, 2020).
6. Zubok, V. (2018), "Worldwide Internet Service Providers in Ukrainian Internet Exchange: Threats and Opportunities". *CEUR workshop Processing*, Ukraine, Kryvyi Rih, Vol. 1813, available at: <http://ceur-ws.org/Vol-1813/> (accessed: October 21, 2020).

Received 16.12.2020

V.Yu. Zubok

EMPIRICAL RESULTS OF FORMING AN EFFECTIVE
TOPOLOGY IN THE INTERNET BASED ON THE GLOBAL
ROUTING SYSTEM SECURITY ASSESSMENTS

The method of searching for an effective topology of interconnections for protection against cyber attacks on global routing is described, where the criterion of efficiency of the links topology is risk assessment as a measure of information security. The practical results of the application of the methodology for different in scale and geography subjects of global routing are presented. The visualized simulation result clearly demonstrates practical ways to increase the security of the internodal topology from cyberattacks such as route hijack.

K e y w o r d s: cybersecurity, Internet topology security, global routing, route hijack.

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.