doi:https://doi.org/10.15407/emodel.41.05.059

УДК 004.7

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

Особливості моделі порушника при аналізі атак на глобальну маршрутизацію в Інтернеті

Запропоновано модель порушника безпеки інформації. Через аналіз загроз та методів проведення атак на глобальну маршрутизацію встановлено, що джерелом таких загроз є зовнішні порушники. Наведено класифікацію таких порушників та розроблено неформальну модель порушника безпеки.

К л ю ч о в і с л о в а: глобальна маршрутизація, перехоплення маршрутів, модель загроз, модель порушника безпеки інформації, кібербезпека.

Однією з масштабних проблем кібербезпеки є запобігання перехопленню маршрутів в системі глобальної маршрутизації мережі Інтернет. Атаки з використанням впливу на глобальну маршрутизацію найчастіше призводять до порушення доступності, а також можуть бути інструментом порушення і конфіденційності, і цілісності.

Перехоплення маршрутів, або крадіжка маршрутів (route hijack), протягом 10 років набуло рис масштабної кіберзагрози [1]. Оскільки в сучасному світі Інтернет здебільшого є основою всіх телекомунікацій, атаки на глобальну маршрутизацію можуть нести загрозу багатьом видам зв'язку та доставки інформації. Щороку відбувається декілька значних інцидентів, пов'язаних з такими атаками. Так, 24 червня 2019 року, протягом декількох годин відбувалось перехоплення маршрутів до найвідомішого сервісу захисту від мережевих атак CloudFlare. Перехоплення було через відсутність достатньої фільтрації BGP-анонсів у американського телекомоператора Verizon. «Постраждалими» визначено 2400 автономних систем, які отримали хибні маршрути [2]. 24 липня 2019 року, та ж сама проблема призвела до втрати багатьох BGP-зв'язків в мережі обміну трафіком

AMS-IX. Проблемний тікет NOC24X7-46889 пояснював, що хтось у мережі проанонсував більш специфічний префікс, частину мережі для інтерфейсів підключення учасників (peering LAN). Навіть в межах однієї мережі вирішення цієї проблеми потребувало дві годин.

Атаки з використанням впливу на глобальну маршрутизацію найчастіше призводять до порушення доступності, а також можуть бути інструментом порушення конфіденційності і цілісності. Оскільки повністю уникнути захоплення маршрутів неможливо через вади протоколу BGP-4 та масштаб мережі Інтернет, актуальною проблемою є мінімізація ризиків. У зв'язку з цим виконано аналіз загроз від атак на глобальну маршрутизацію [3]. У даному випадку пропонується аналіз моделі порушника безпеки інформації.

Будемо використовувати такі терміни та скорочення:

автономна система (AS) — група IP-мереж, які належать одному чи декільком операторам, та мають єдину чітко визначену політику маршрутизації [4];

анонс — повідомлення протоколу BGP-4, який містить мережевий префікс та атрибути шляху:

BGP-4 — протокол глобальної маршрутизації, за допомогою якого AS обмінюються маршрутами;

власна ІТС — інформаційно-телекомунікаційна система, для захисту якої розробляється модель порушника;

маршрут — запис в таблиці маршрутизації, який містить мережевий префікс та спеціальні атрибути (напрямок, шлях, вага та ін.);

префікс (мережевий префікс) — безперервна множина IP-адрес, описана у вигляді безкласової нотації;

реєстр маршрутів (RR) — Інтернет-ресурс, якому мережеві адміністратори повідомляють дані про взаємодію між AS.

Модель порушника — традиційний підхід. Модель порушника — це всебічна структурна характеристика порушника, яка є частиною моделі загроз та використовується під час розроблення політики безпеки інформації [5]. Сукупність типових критеріїв для класифікації порушника та розробки неформального опису (неформальної моделі) порушника наведено в табл. 1.

Порушник є джерелом загрози. Відповідно до локалізації джерела загрози поділяються на внутрішні та зовнішні. До зовнішніх належать загрози, джерело яких перебуває поза межами власної мережі. Внутрішні загрози реалізуються в межах контрольованої зони через керування мере-

жевими пристроями, які є частиною власної ІТС. Відповідно до цього розрізняють два види порушників: зовнішній та внутрішній.

Зовнішній порушник — це порушник, який діє із зовнішнього, відносно власної мережі, боку. У цій моделі він розглядається як особа, що не має доступу до керування пристроями власної ІТС, і не є її авторизованим користувачем. Зовнішній порушник має можливість реалізувати загрозу інформації, тільки впливаючи на інформацію з боку інших автоматизованих систем (які не входять до складу власної ІТС).

Категорії осіб, які можуть бути зовнішніми порушниками:

сторонні особи, що перебувають за межами контрольованої території вузлів власної ІТС;

відвідувачі;

представники організацій, які взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності.

Внутрішній порушник — це порушник, який діє зсередини власної ІТС. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки власної ІТС. Внутрішній порушник має можливість реалізувати загрозу інформації і може бути як авторизованим користувачем, так і неавторизованим.

Категорії осіб, які можуть бути внутрішніми порушниками:

технічний персонал, що обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС;

персонал, який обслуговує технічні засоби (інженери, техніки);

системний адміністратор;

адміністратор безпеки;

користувачі.

Потенційним порушником безпеки інформації є особа, яка помилково, внаслідок необізнаності, або цілеспрямовано, за злим наміром або без

Таблиця 1. **Класифікація порушника за основними характеристиками**

Компетенція	Оснащеність	Мотивація (мета)	Повноваження в системі
Початківець з частковими знаннями	Має звичайні користувацькі засоби	Навмисні дії	Віддалене виконання фіксованого набору дій
Спеціаліст із знаннями	Має спеціальні програмні та апаратні засоби	Ненавмисні дії	Віддалене керування функціями, зміна конфігурації
Професіонал із знаннями та досвідом	Має змогу виготовляти (розробляти) власні інструменти		Віддалене створення та запуск власних функцій
			Фізичний доступ до обладнання

нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення конфіденційності, цілісності та доступності інформації.

Враховуючи особливості обробки інформації з глобальної маршрутизації власної ІТС, визначено такі категорії потенційних порушників:

адміністратори власної ІТС (системний адміністратор, адміністратор мережі, адміністратор безпеки);

користувачі власної ІТС;

технічний персонал, що обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС;

представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності;

сторонні особи, що перебувають за межами контрольованої території вузлів власної ІТС.

Це типовий перелік осіб, які можуть впливати на функціонування власної ІТС.

У табл. 2 наведено специфікації моделі порушника за мотивами здійснення порушень, рівнем кваліфікації та обізнаності щодо власної ІТС, показником можливостей використання засобів власної ІТС для реалізації загроз, за часом та місцем дії. Потенційний рівень загрози (можливі збитки) позначено так: 1 — незначний (низький); 2 — нижче середнього; 3 — середній; 4 — вище середнього; 5 — значний (високий).

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Модель порушника, яку побудовано з урахуванням особливостей власної ІТС (що забезпечує певне виконання технологічних процесів створення об'єкту захисту), технологій обробки інформації, категорій персоналу та користувачів, визначається сукупністю характеристик, наведених у табл. 2. Сукупність цих характеристик визначає профіль можливостей порушника.

Модель порушника з урахуванням особливостей атак на глобальну маршрутизацію. Проаналізуємо всі категорії порушників, які можуть створити обставини (чи сприяти таким обставинам), що призведуть до перехоплення маршрутів, шляхом моделювання їхніх повноважень та можливих дій (табл. 3).

Без урахування особливостей атак на глобальну маршрутизацію найвищий рівень небезпеки отримав би внутрішній порушник. Проте Інтернет є IP-мережею, що складається з понад 60000 автономних систем (AS). Кожна AS обмінюється маршрутами принаймні з однією іншою AS (це є запорукою зв'язності мережі). Відсутність надійних засобів забезпечення

Таблиця 2. **Категорії та специфікації порушників**

Позначення	Категорія та специфікація	Потенційний рівень загрози
П1	Системний адміністратор власної ІТС	5
П2	Відвідувачі	2
П3	Технічний персонал, що обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС	3
П4	Персонал, який обслуговує технічні засоби (інженери, техніки)	3
П5	Представники організацій, які взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності	3
П6	Сторонні особи, що перебувають за межами контрольованої території вузлів власної ІТС	2
	За мотивом порушення	
М1	Безвідповідальність (недбалість)	3
М2	Корисна цілеспрямованість	5
	За рівнем кваліфікації та обізнаності	
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами системи	1
К2	Має навички щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем та практичними навичками роботи з засобами, які реалізовано у власній ІТС	4
К4	Володіє знаннями щодо функціонування засобів та механізмів захисту, які використовуються в ІТС	5
	За можливостями використання засобів ІТС	
З1	Має фізичний доступ до програмно-апаратних засобів, але не є авторизованим користувачем ІТС	1
З2	Має можливість запуску фіксованого набору завдань (програм), які реалізують заздалегідь передбачені функції обробки інформації	3
З3	Має можливість керувати функціонуванням елементів ІТС, тобто конфігурує програмне забезпечення	5
З4	Не має фізичного доступу	1
	За часом дії	
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час).	4
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	3
	За місцем дії	
Д1	Усередині будівлі та приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів	5
Д3	З інших об’єктів ІТС, в тому числі каналів зв’язку	2

цілісності та доступності інформації про маршрути саме за межами власної ІТС є причиною атак на глобальну маршрутизацію.

Розглянемо узагальнену схему інформаційних потоків, які виникають між суб'єктами глобальної маршрутизації (див. рисунок). Адміністратори кожної AS зобов'язані розміщувати інформацію про взаємодію з іншими AS в базі даних (БД) RR. Незважаючи на те, що ця вимога є суто адміністративною, деякі адміністратори часто спираються на неї при конфігуруванні BGP-фільтрів.

У роботі [3] описано, у який спосіб проводяться атаки на глобальну маршрутизацію, а саме:

захоплення префіксу, коли вузол анонсує у якості джерела адресний простір, який йому не належить: при виборі маршруту BGP віддасть

Таблиця 3. **Моделювання дій порушника відносно атак на глобальну маршрутизацію**

Тип порушника	Можливості порушника	Можливі дії
Адміністратори ІТС	Мережевий доступ до обладнання власної ІТС Знання з налаштувань СЗІ Керування функціями, зміна конфігурації обладнання, зокрема маршрутизаторів Розуміння системи аудиту (реєстрації дій в системі)	Припинення глобальної маршрутизації адресного простору власної ІТС або його частки Внесення некоректних даних стосовно маршрутизації в RR Втрата (розголошення) атрибутів доступу до RR
Користувачі власної ІТС	Мережевий доступ до обладнання власної ІТС	Злам слабкої автентифікації обладнання власної ІТС та отримання повноважень адміністратора
Технічний персонал, що обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС	Фізичний доступ до приміщень та обладнання власної ІТС	Несанкціонована комутація, вмикання, вимикання пристроїв, підключення до них носіїв інформації
Представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності	Доступ до апаратного та програмного забезпечення обладнання власної ІТС	Отримання даних про налаштування апаратного та програмного забезпечення обладнання власної ІТС Внесення несанкціонованих змін до програмного забезпечення власної ІТС
Сторонні особи, що перебувають за межами контрольованої території вузлів власної ІТС	Ніяких особливих можливостей	Ніяких дій відносно обладнання чи програмного забезпечення власної ІТС

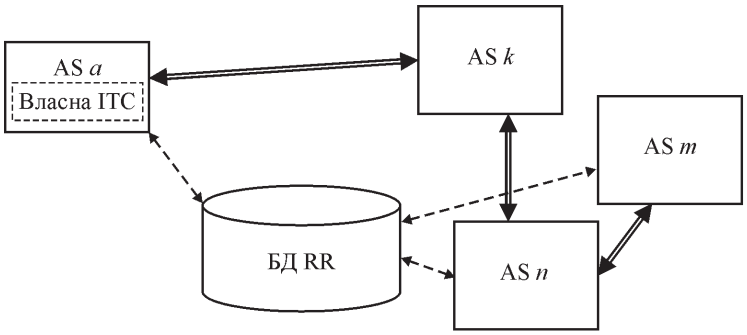

Схема інформаційних потоків у глобальній маршрутизації: подвійна лінія — обмін маршрутами між AS; штрихова лінія — збереження даних в БД RR та запити до неї

перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем;

захоплення маршруту, в якому вузол ретранслює легально отриманий анонс чужого адресного простору, пропонуючи транзит через себе: в результаті перенаправлення трафік, можливо, доставляється коректному одержувачу, але передається шляхом, відмінним від істинного;

захоплення підмереж через анонсування більш специфічних префіксів: при виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість;

захоплення нерозподіленого або невикористаного адресного простору: анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.

Припустимо, що власній ІТС належить AS *a*. Перелічені способи проведення атак виконуються поза межами власної ІТС і навіть поза межами AS *a* в цілому. Адміністратор AS *a* здатен:

контролювати інформацію, яка виходить з AS *a* у напрямку БД RR та інших AS;

перевіряти інформацію, яка надходить від інших AS, за допомогою запитів до БД RR.

Незважаючи на те, що існують інструменти перевірки інформації від інших AS в автоматизованому та навіть автоматичному режимі, через загальні розміри таблиць маршрутизації та поліноміальну обчислювальну складність ці перевірки не мають всеосяжного характеру. Вони загалом відбуваються на початкових ланцюгах при передаванні маршрутів від кінцевих AS до їхніх провайдерів, та дуже рідко — між великими інтернет-

провайдерами [6]. Отже, адміністратор AS *a*, і тим більше адміністратори власної ІТС, в загальному випадку не мають змоги забезпечити доступність та цілісність інформації про маршрути до власної ІТС, а також не здатні контролювати цілісність інформації про маршрути, яка надходить до власної ІТС.

Таблиця 4. **Категорії та специфікації порушника з урахуванням специфіки атак на глобальну маршрутизацію**

Позначення	Категорія та специфікація	Потенційний рівень загрози
П1	Відвідувач	1
П2	Технічний персонал	2
П3	Представник обслуговуючої організації	2
П4	Авторизований користувач	3
П5	Адміністратор AS	5
	За мотивом порушення	
М1	Безвідповідальність (недбалість)	3
М2	Корисна цілеспрямованість	5
	За рівнем кваліфікації та обізнаності	
К1	Володіє базовими знаннями щодо функціонування глобальної маршрутизації	3
К2	Володіє глибокими знаннями з глобальної маршрутизації, засобів та механізмів використання БД RR	4
К3	Володіє глибокими знаннями з глобальної маршрутизації, вади протоколу BGP-4, вади захисту даних в БД RR	5
	За повноваженнями, набутими в AS	
А1	Має можливість вносити зміни в налаштування BGP-4 на маршрутизаторах AS	3
А2	Додатково до А1 має авторизований доступ до публікації даних в БД RR та обміну інформацією з адміністраторами сусідніх AS	5
	За часом дії	
Ч1	Не може планувати дії на конкретний час	2
Ч2	Може планувати дії на конкретний час в залежності від мети	4
	За місцем дії	
Д1	Порушник має доступ до AS кінцевого типу (корпоративна мережа, установа)	1
Д2	Порушник має доступ до AS Інтернет сервіс-провайдера локального характеру (населений пункт, географічний регіон)	3
Д3	Порушник має доступ до AS Інтернет сервіс-провайдера великого масштабу (міжнародні оператори, мережі обміну трафіком)	5

Відтак, основні загрози атак на глобальну маршрутизацію полягають у впливі на інформаційні потоки поза межами власної ІТС. Це означає, що загрози надходять від порушників, які є сторонніми особами і перебувають за межами контрольованої території вузлів власної ІТС. Це певним чином змінює традиційну оцінку небезпеки порушників і виводить на значуще місце саме зовнішнього порушника.

У запропонованій моделі небезпечним зовнішнім порушником є особа з повноваженнями адміністратора будь-якої AS. Адміністратор будь-якої AS — це принаймні спеціаліст із знаннями, який керує спеціальними засобами і в разі помилки чи навмисно може створити атаку на глобальну маршрутизацію.

У табл. 4 наведено категорії та специфікації порушника відносно традиційних, поданих у табл. 2. Профіль такого порушника, потенційного джерела атаки на глобальну маршрутизацію, має наступний вигляд:

категорія порушника — П1—П5;
мотиви — М1, М2;
кваліфікація — К1—К3;
можливості — А1, А2;
час дії — Ч1,Ч2;
місце дії — Д1—Д3;
сумарний рівень загроз — 13 — 30.

Висновки

Відсутність надійних засобів забезпечення цілісності та доступності інформації про маршрути саме за межами власної ІТС є причиною атак на глобальну маршрутизацію. Вся сукупність AS на рівні глобальної маршрутизації є однією IP-мережею, що певною мірою розмиває межу між внутрішнім та зовнішнім порушниками. Через те що впливати на інформаційний обмін в глобальній маршрутизації може будь-який її суб'єкт, більший рівень мають зовнішні загрози. Потенційним порушником безпеки — джерелом загрози глобальній маршрутизації — є адміністратор будь-якої AS в Інтернеті або інша особа, яка набула рівня доступу такого адміністратора та володіє відповідними знаннями. Це має бути враховано при створенні моделі порушника інформаційної безпеки.

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. *Levy M.J.* The deep-dive into how Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Monday. [Електронний ресурс] Режим доступу: https://blog.cloudflare.com/the-deep-dive-into-how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-monday/ . Дата звернення: 27 липня, 2019.
3. *Зубок В.Ю.* Оцінювання ризику кібератак на глобальну маршрутизацію // Електрон. моделювання, 2019, **41**, № 2, с. 97—110.
4. *Bates T., Gerich E.* Representation of IP Routing Policies in a Routing Registry (ripe-181). 1994. [Електронний ресурс] Режим доступу: ftp://ftp.ripe.net/ripe/docs/ripe-181.txt. Дата звернення: 20 червня, 2019.
5. *Грайворонський М.В.* Безпека інформаційно-комунікаційних систем : підручник / М.В. Грайворонський, О.М. Новіков. Київ : Вид. група BHV, 2009, 608 с.
6. *Shapelez A.* Eliminating opportunities for traffic hijacking. [Електронний ресурс] Режим доступу: https://habr.com/en/company/qrator/blog/442264/. Дата звернення: 27 Липня, 2019.

Отримано 23.08.19

REFERENCES

1. Bates, T. and Gerich, E. (1994), “Representation of IP Routing Policies in a Routing Registry (ripe181)”, available at: ftp://ftp.ripe.net/ripe/docs/ripe-181.txt (accessed Jun 20, 2019).
2. Zubok, V. (2018), “Determining the ways of counteraction To cyberattacks on the Internet global routing”, Elektron. modelyuvannya, Vol. 40, no. 5, pp. 67-76.
3. Levy, M.J. (2019), “The deep-dive into how Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Monday”, available at: https://blog.cloudflare.com/the-deep-dive-into-how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-monday/ (accessed Jul 27, 2019).
4. Zubok, V. (2019), “Global Internet Routing Cyber attacks Risk Assessment”, *Elektronne modelyuvannya*, Vol. 41, no. 2, pp. 97-110.
5. Graivoronskyi, M. and Novikov, O. (2009), Bezpeka informatsiyno-kommunikaciynykh system [Security of Information Communication Systems], Vyd. hrupa BHV, Kiev, Ukraine.
6. Shapelez, A. (2019), “Eliminating opportunities for traffic hijacking”, available at: https://habr.com/en/company/qrator/blog/442264/ (accessed Jul 27, 2019).

Received 23.08.19

В.Ю. Зубок

ОСОБЕННОСТИ МОДЕЛИ НАРУШИТЕЛЯ ПРИ АНАЛИЗЕ АТАК НА ГЛОБАЛЬНУЮ МАРШРУТИЗАЦИЮ В ИНТЕРНЕТЕ

Предложена модель нарушителя безопасности информации. Посредством анализа угроз и методов проведения атак на глобальную маршрутизацию установлено, что источником таких угроз являются внешние нарушители. Представлена классификация таких нарушителей и разработана неформальная модель нарушителя безопасности, учитывающая специфику указанных атак.

К л ю ч е в ы е с л о в а: глобальная маршрутизация, перехват маршрутов, модель угроз, модель нарушителя безопасности информации, кибербезопасность.

V.Yu. Zubok

FEATURES OF THE MODEL
OF THE OFFENDER AT THE ANALYSIS
OF ATTACKS ON GLOBAL INTERNET ROUTING

A model of information security breach is proposed. Through analysis of threats and methods of conducting attacks on global routing it is established that the source of such threats are external violators. The classification of such violators is given and an informal model of the security violator is developed.

K e y w o r d s: global routing, route hijack, threats model, information security intruder model, cybersecurity

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