УДК 004[413.3+738.5.057.4]

Зубок В.Ю.
orcid.org/0000-0002-6315-5259

ПОВОДЖЕННЯ З РИЗИКАМИ ВІД ПЕРЕХОПЛЕННЯ МАРШРУТУ В МЕРЕЖІ ІНТЕРНЕТ З ВИКОРИСТАННЯМ РИЗИК-ОРІЄНТОВАНОЇ МОДЕЛІ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

vitaly.zubok@gmail.com

Вступ

Світові тренди на децентралізацію сховищ даних, міграцію корпоративних та галузевих інформаційно-комунікаційних систем у «хмарні» технології кардинально змінюють роль глобальної комп'ютерної мережі Інтернет в питаннях управління і вимагають сучасних підходів до аналізу чинників, які формують потенційні і реальні загрози у сфері кібербезпеки. Тривалий і незупинний розвиток Інтернету як інформаційно-телекомунікаційної мережі обумовлений фактично безмежною масштабованістю єдиного протокола глобальної маршртутизації BGP-4. Але його відомі недоліки, зокрема, відсутність механізмів верифікації маршрутів, дозволяє суб'єктам глобальної маршрутизації помилково чи зумисно спотворювати шляхи пакетної передачі. Колись ці інциденти носили характер випадкової помилки конфігурації, але протягом 10 років зросла частка зловмисних дій, тобто атак, для реалізації яких використовувалося так зване «перехоплення маршрутів» [1]. Метою атак є перехоплення інформації, дестабілізації роботи мережі або її частини, порушення доступу до певних інформаційних ресурсів тощо. Повне усунення цієї вразливості неможливо без заміни протоколу BGP-4, що може тривати ще десятиліття.

Постановка задачі

Для власників та користувачів інформаційних систем, функціонування яких, чи доступ до яких пов'язані з Інтернет, необхідна нова методологія зменшення можливих наслідків кібератак на глобальну маршрутизацію. В рамках рішення цієї задачі було проведено аналіз топології Інтернет, суб'єктів, об'єктів та процесів глобальної маршрутизації, виявлено і детально досліджено зв'язок між топологією мережевих зв'язків та ризиком перехоплення маршрутів [2].

Метою роботи є розробка методології поводження з ризиками на основі оцінки ефективності міжмережевих зв'язків та удосконалення топології мережі.

Запропоновані рішення

В основі запропонованих рішень лежать нові метрики для оцінки вразливості Інтернет-вузлів. Оцінка ризиків інформаційної безпеки, що базується на цих метриках, послуговує критерієм ефективності топології стосовно захисту від перехоплення маршрутів, та надає можливість приймати рішення з удосконалення міжмережевих зв'язків, використовуючи ризик як міру захищеності інформації.

Запропоновано метрику довіри (trust metrics) вузла u до вузла v – співвідношення середньої відстані між вузлом – суб'єктом довіри u та іншими вузлами, обрахованої по вихідних зв'язках, та відстанню від u до конкретного вузла v, що є об'єктом довіри:

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

Тут $\boldsymbol{T_u^v}$ – 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, при чому

$\boldsymbol{u = v \Leftrightarrow T_u^v = 0}$. Враховуючи, що середня відстань в мережі Інтернет має величину між 4 та 5, а діаметр мережі (тобто максимальна відстань між вузлами) – до 9 [3], метрика довіри коливатиметься від 0,2 до 2. Найвищий рівень довіри з точки власника ризику має його власний вузол, оскільки він є суб'єктом глобальної маршрутизації та анонсує принаймні один префікс.

Для оцінки масштабу збитку в разі сприйняття на вузлі *v* хибного маршруту запропоновано *метрику значущості* (significance metrics), яка пов'язана з кількістю підмереж, які отримують маршрути за посередництва вузла *v*. При цьому мережеві префікси мають різну довжину і вони 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 і так далі [4]. Отже, префікси нерівнозначні і для врахування цього запропоновано поняття ваги префікса:

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

де w_π – вага префіксу; *l(π)* – довжина префіксу π.

Згідно (2) мережевий префікс довжиною 24 біти (256 адрес) враховується із вагою 1, а, наприклад, префікс 19 біт (8192 адреси) – з вагою 32. AS, що анонсує 32 мережеві префікси з 256 адрес, матиме таку саму метрику значущості, що й AS, яка анонсує один префікс з 8192 адрес.

Крім того, слід розуміти, 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 $\boldsymbol{S_v^u}$, відстань між мережевим префіксом та вузлом, через який проходить анонс цього префікса, має бути врахована. Пропонується при розрахунку значущості враховувати кожен префікс $\boldsymbol{\pi_v}$ із зменшувальним коефіцієнтом $\boldsymbol{(1+\delta)^{-1}}$, що залежить від відстані δ між джерелом цього префікса та вузлом *v*, значущість якого розраховується. Тоді мережевий префікс, для якого *v* є джерелом маршруту (δ=0), враховується з коефіцієнтом 1. Якщо джерелом є, наприклад, сусідній до *v* вузол, $(1+\delta)^{-1} = 0.5$. Метрика значущості тоді з урахуванням (2) набуде такого вигляду:

$$S_v^u = \sum_\pi w_\pi (1+\delta_\pi)^{-1} = \sum_\pi 2^{24-l(\pi)}(1+\delta_\pi)^{-1} \qquad (3)$$

де S_v^u – значущість вузла *v* за оцінкою *u*; w_π – вага префіксу; *l(π)* – довжина префіксу π; 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 (1) та (3) утворюють ризик-орієнтовану модель міжмережевих зв'язків, яка основана на розподілі вузлів в просторі (R,T,S):

$$R_v^u = 10^{T_v^u} S_v^u \qquad (4)$$

де *u* – вузол – власник ризику, *v* – вузол – об'єкт оцінки, *R* – ризик, *T* – довіра і *S* – значущість. Для підвищення ваги метрики довіри, вона врахувується в експоненційній формі.

Крім того, можна підрахувати сукупний ризик від перехоплення маршрутів по всіх цільових вузлах:

$$R^u = \sum_{i \neq u}^{|AS|-1} R_i^u \qquad (5).$$

Отже, сформульовано 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 зауважити, що картина розподілу вузлів за ризиком, складена за цією моделлю, є суб'єктивною, бо створена за оцінкою власника ризику – вузла *u*.

Методика розрахунку ризику та поводження з ризиками

Перед розрахунком метрик потрібно отримати дані про топологію Інтернет. 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 так званих upstream-провайдерів

– операторів, які надають власникові ризику послуги доступу до мережі Інтернет.

В [3, гл.1] приведено методики дослідження топології Інтернету 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. Сама по собі інформація про маршрути в глобальній комп‘ютерній мережі є відкритою інформацією, що визначається метою її існування та застосування. Проте, шляхи її оперативного отримання в повному обсязі обмежені. Необхідно мати безпосередній доступ до маршрутизатора, що або виконує роль BGP-шлюзу для певної автономної системи, або є посередником при обміні маршрутами (route reflector). Це завдання може вирішити уповноважений мережевий адміністратор.

Інший шлях отримання інформації – отримання таблиць через так звані сервери-«дзеркала» (looking glass servers). По суті, сервер looking glass діє як обмежений по функціях 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). Найчастіше, looking glass являє собою веб-інтерфейс до команд маршрутизатора. Програмне забезпечення для реалізації цих функцій не є стандартизованим, але є загально прийнятий перелік функцій, які може виконувати такий сервер. Як правило, 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.

Отже, двовимірна модель (4) має бути забезпечена по даних, які має BGP-система, а саме – на множині отриманих маршрутів. Незалежно від формату представлення BGP-таблиці, вона міститиме наступні дані стосовно кожного маршруту:

- мережевий префікс;
- довжина префіксу;
- атрибут as_path.

Крім того, необхідно знати ідентифікатор AS власника ризику.

Атрибут as_path в кожному маршруті має вигляд послідовності ідентифікаторів AS зліва направо від найближчого сусіда власника ризику до кінцевого вузла – джерела префіксу [5]. Відстань d у (1) буде обраховуватись по as_path зліва направо, а відстань δ для (4) – справа наліво.

Підготовчі кроки:

- визначення ідентифікатора AS власника ризику (вузол u);
- отримання повної BGP-таблиці для вузла u;
- формування списку видимих AS з отриманої BGP-таблиці з атрибутів as_path;
- за списком видимих AS кожна з них по черзі призначається вузлом v і далі виконується розрахунок метрики.

Розрахунок метрики значущості вузла v:

- отримується перелік перфіксів π_v, які містять v в as_path;
- для кожного префікса π_v визначається його довжина $l(\pi_v)$;
- для кожного префікса π_v по as_path визначається джерело префікса;
- для кожного префікса π_v по as_path визначається відстань δ між v та джерелом префіксу;
- розраховується метрика значущості S_v^u згідно (3);

Розрахунок метрики довіри вузла v:

- з повного списку атрибутів as_path розраховується середній шлях від u до інших видимих AS за раніше складеним списком;
- для кожного v зі списку AS, шукається найкоротша відстань між u та v з повного списку атрибутів as_path;

- розраховуєтья середня відстань від v серед видимих AS [3, гл.3];
- розраховується метрика довіри *u* до *v* відповідно до (1).

Розрахунок ризику для вузла u:

- по всій множині вузлів для вузла *u* розраховується сумарний ризик перехопелння маршруту за (5).

Практичні результати з розрахунку ризику перехопелення маршруту в українському сегменті мережі Інтернет

За наведеною методикою було обраховано ризик перехоплення маршруту до префіксу 195.64.224.0/22 серед AS що є учасниками Української мережі обміну трафіком (UA-IX). Для цього з прикордонних маршрутизаторів AS8258 було отримано BGP-таблицю маршрутів, отриманих від UA-IX (AS15645), і виконано розрахунки метрики значущості та метрики довіри. З BGP надійшла інформація про 6580 AS та 31420 мережевих префікси.

Після розрахунку метрики значущості *S* перелік AS було впорядковано за спаданням *S*. Було з'ясовано, що таке впорядкування має експоненційний розподіл з «важких хвостом» AS, що мають мінімальну значущість. Так, 1624 з 6580 AS мають метрику значущості 1 та менше, бо або анонсують один мережевий префікс довжини 24 біта, або взагалі лише зустрічаються в шляхах одного чи двох префіксів, що належать іншим AS. Для подальшого аналізу було відібрано 100 AS з максимальною метрикою значущості. Графік розподілу за зменшенням значущості серед цієї групи наведено на рис.1.

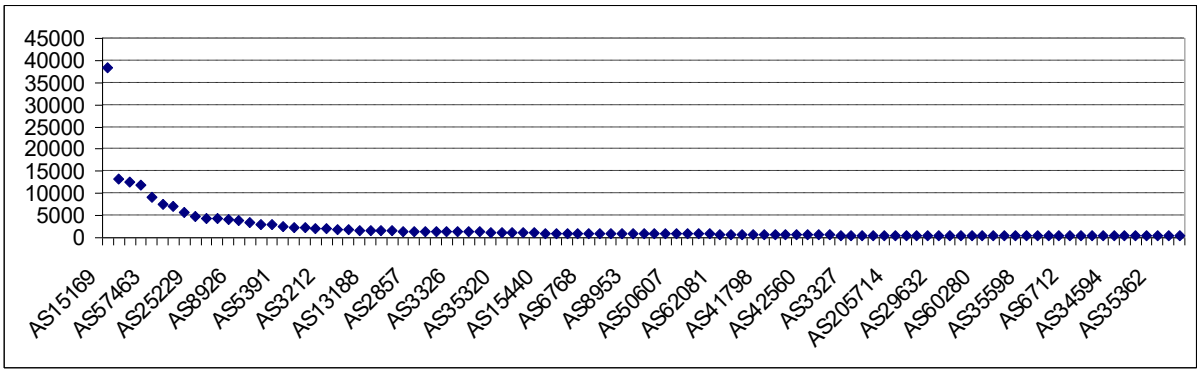

Рис.1. Графік розподілу за зменшенням значущості серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика значущості *S*, вісь абсцис – порядковий номер AS в групі

Для впорядкованої за S_v^u множини AS було розраховано метрику довіри T відповідно до (1), як це показано на рис.2, та ризик відповідно до (4). На рис. 3 продемонстровано вплив метрики довіри на початкове впорядкування вузлів при розрахунку ризику.

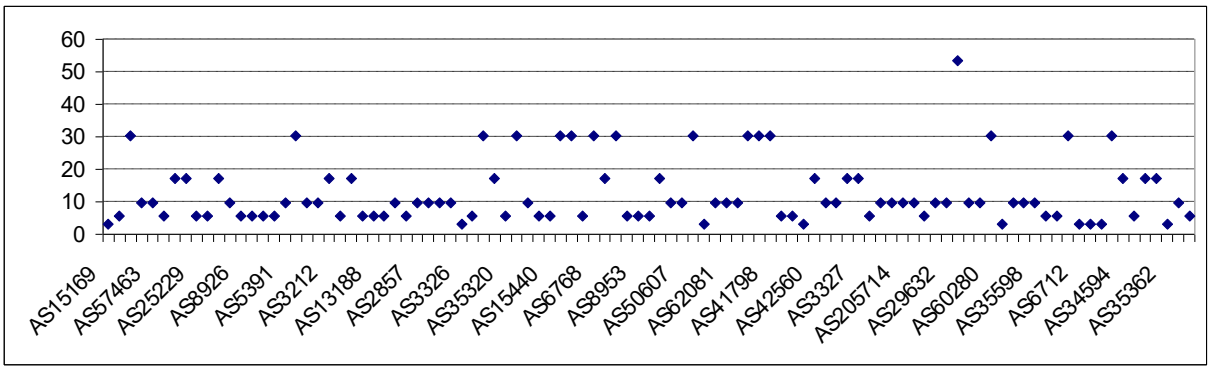

Рис.2. Графік розподілу за метрикою довіри серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика довіри *T* в експоненційній формі, вісь абсцис – ідентифікатор AS.

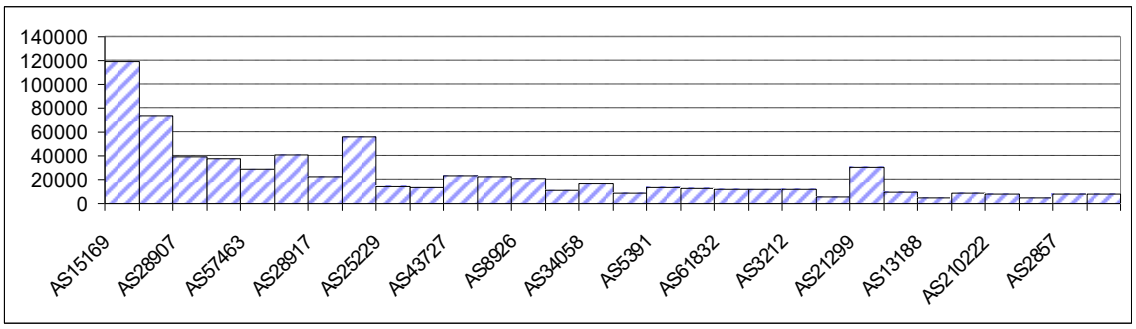

Рис.3. Графік розподілу ризику серед 100 AS з максимальною метрикою значущості. Збережено впорядкування за значенням метрики значущості. Вісь ординат – метрика довіри T в експоненційній формі, вісь абсцис – ідентифікатор AS

Можна пересвідчитись, що метрика довіри змінює порядок вузлів порівняно з впорядкуванням за метрикою значущості. На рис.4. вузли впорядковано за зниженням ризику перехоплення маршруту.

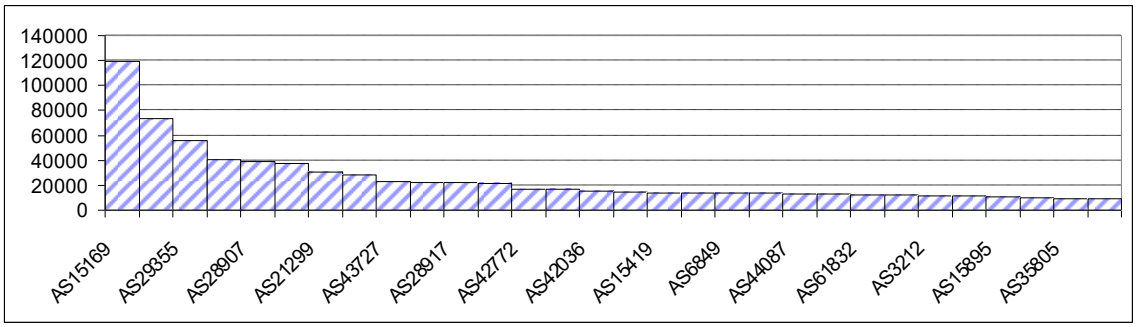

Рис.4. Графік розподілу за зменшенням ризику серед 100 AS з максимальною метрикою значущості. Вісь ординат – ризик R, вісь абсцис – ідентифікатор AS.

Обробляння ризику. Впорядкування вузлів за зменшенням ризику (рис.4) надає зручний спосіб до зниження рівня ризику (risk mitigating). Сумарний ризик можна візуалізувати як площу заштрихованої фігури. Зменшення її площі є зниженням ризику. Є очевидним, що зниження ризику можливе шляхом впливу на метрики довіри певних вузлів, і чим вище значущість вузла, тим вагоміше вплив на ризик. Вплив на довіру можливий за рахунок 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-взаємодію, таким чином зменшивши відстань до 1. Якщо побудова прямого зв'язку ускладнена, можна шукати вузол-посередник, з якими побудова з'єднання здатна забезпечити відстань 2 до одного чи декількох значущих вузлів.

В наведеному прикладі сумарний ризик від перехоплення маршруту серед 100 вузлів з найвищим ризиком становить $R^u = 1098206$. Опишемо першу п’ятірку вузлів в порядку зниження ризику:

AS15169: Google. Видимий в 317 маршрутах UA-IX, в тому числі анонсує 77 мережевих префіксів.

AS9198: казахстанський оператор KazakhTelecom. Видимий в 924 маршрутах UA-IX, в тому числі анонсує 356 мережевих префіксів.

AS29355: казахстанський оператор Kcell. Видимий в 87 маршрутах UA-IX, серед яких 86 власно анонсує.

AS6697: білоруський державний оператор Белтелеком. Видимий в 563 маршрутах UA-IX, серед яких 315 власно анонсує.

AS28907: український Інтернет-провайдер та датацентр «Міроxост». Видимий

в 3351 маршрутах UA-IX, в тому числі анонсує 17 мережевих префіксів.

Зниження ризику перехоплення маршруту можливо за рахунок впливу на метрику довіри. Шляхом моделювання такої таблиці маршрутів, де у власника ризику є безпосередній зв'язок принаймні з трьома вузлами, що є «концентраторами ризику», ми за рахунок зміни метрики довіри можемо отримати таку картину ризику (рис.5).

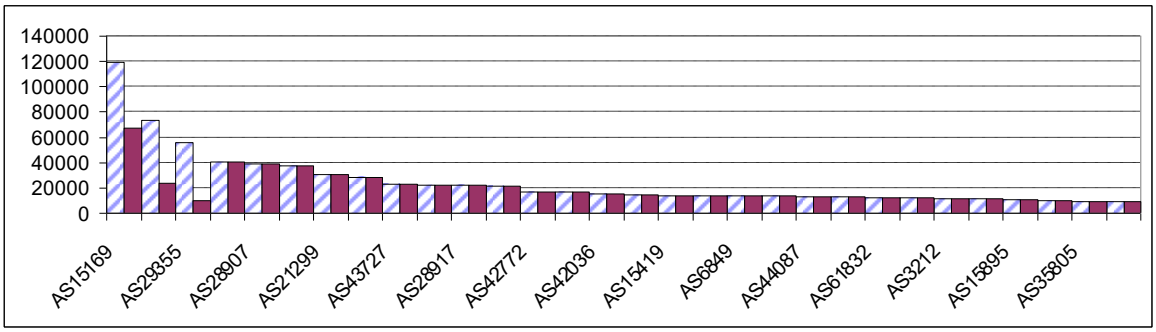

Рис.5. Порівняння зниження ризику за рахунок моделювання прямих з'єднань з трьома «концентраторами ризику». Вісь ординат – ризик R, вісь абсцис – ідентифікатор AS.

Сумарний ризик такої моделі становить від перехоплення маршруту серед 100 вузлів з найвищим ризиком становить $R^u = 950756$. Отже, за допомогою трьох нових міжмережевих зв'язків отримано нову топологію, яка має ризик перехоплення маршруту нижчий на 13,42% від початкового.

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.

Література

1. *Зубок В.Ю.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет. / В.Ю. Зубок. – Електрон. моделювання, 2018. – №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 / В.Ю. Зубок. – Реєстрація, зберігання і обробка даних. – №4. – Том 21. – ІПРІ НАН України, 2019. – С. 67-74.

3. *Мохор, В.* Формування міжвузлових зв'язків в Інтернет з використанням методів теорії складних мереж / В. Мохор, В. Зубок – Київ: Прометей, 2017. – 175 с.

4. *Fuller. V.* Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. / V. Fuller, T. Li. / [Інтернет ресурс]. Веб-сайт: Tools.ietf. Режим доступу: https://tools.ietf.org/html/rfc4632.

5. Dimitropoulos X. Modeling Autonomous–System Relationships / X. Dimitropoulos, G. Riley. / 20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06). – Singapore, 2006.

Зубок В.Ю.

ПОВОДЖЕННЯ З РИЗИКАМИ ВІД ПЕРЕХОПЛЕННЯ МАРШРУТУ В МЕРЕЖІ ІНТЕРНЕТ З ВИКОРИСТАННЯМ РИЗИК-ОРІЄНТОВАНОЇ МОДЕЛІ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ

В останні роки все частіше відбуваються інциденти з глобальною маршрутизацією, що стали новою масштабною кіберзагрозою. 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. Механізми згаданих кібератак спрямовані на нав'язування суб'єктам глобальної маршрутизації помилкового уявлення про топологію мережі при відсутності механізмів валідації цієї інформації в протоколі глобальної маршрутизації BGP-4. Повне усунення цієї вразливості неможливо без заміни протоколу BGP-4 на новий, розробка якого триває. В будь-якому разі повну заміну не слід очікувати в найближче десятиліття. Додаткові засоби, що використовуються для валідації маршрутів, не є надвійними та самі по собі утворюють нову точку відмови.

Таким чином, проблема захищеності інформації при міжмережевому обміні потребує нової методології. Запропонована в статті методологія базується на аналізі топології Інтернет, суб'єктів, об'єктів і процесів глобальної маршрутизації, а також управління ризиками, що є сучасним підходом в інформаційній безпеці. Визначено власника ризику, ідентифіковано самі ризики. Введено нові метрики для оцінки ризику перехоплення маршрутів – метрику довіри і метрику значущості.

В результаті отримана ризик-орієнтована модель глобальної маршрутизації, що описує відносини Інтернет-вузлів з точки зору ризику перехоплення маршруту. Це дозволяє моделювати найбільш ефективні топології, де критерієм ефективності служить оцінка ризику як міра захищеності інформації. У статті продемонстровано практичні результати застосування ризик-орієнтованими моделі глобальної маршрутизації для оцінки та моделювання міжмережевих зв'язків в українському сегменті Інтернет.

Ключові слова: *Інтернет, перехоплення маршруту, поводження з ризиками, глобальна маршрутизація, метрика довіри.*

Zubok V.Yu.

HANDLING RISKS FROM INTERCEPTING A ROUTE ON THE INTERNET USING A RISK-ORIENTED GLOBAL ROUTING MODEL

Global routing incidents have increasingly occurred in recent years, becoming a new large-scale cyber threat. Cyberattacks on global internet routing are used to unauthorizedly change package forwarding paths in order to intercept information, destabilize whole or part of the network, disrupt access to certain information resources, etc. The mechanisms of these cyberattacks are aimed at imposing on the subjects of global routing a misconception about the topology of the network in the absence of mechanisms for validation of this information in the global routing protocol BGP-4. In any case, a complete replacement should not be expected in the coming decade.

Thus, the problem of information security during firewall exchange requires a new methodology. The methodology proposed in the article is based on the analysis of internet topology, subjects, objects and processes of global routing, as well as risk management, which is a modern approach in information security. The owner of the risk has been identified, the risks themselves have been identified. New metrics have been introduced to assess the risk of intercepting routes – trust metrics and metrics of significance.

As a result, a risk-oriented model of global routing is obtained, describing the relationship of Internet nodes in terms of the risk of route interception. This allows you to simulate the most effective topology, where the effectiveness criterion is risk assessment as a measure of information security. The article demonstrates the practical results of the use of risk-oriented models of global routing for the assessment and modeling of inter-network relations in the Ukrainian segment of the Internet.

Keywords: *Internet, route interception, risk management, global routing, trust metrics.*

Зубок В.Ю.

ОБРАБОТКА РИСКОВ ОТ ПЕРЕХВАТА МАРШРУТА В ИНТЕРНЕТЕ С ИСПОЛЬЗОВАНИЕМ РИСК-ОРИЕНТИРОВАННОЙ ГЛОБАЛЬНОЙ МОДЕЛИ МАРШРУТИЗАЦИИ

Глобальные инциденты маршрутизации все чаще происходят в последние годы, становясь новой крупномасштабной киберугрозой. Кибератаки на глобальную интернет-маршрутизацию используются для несанкционированного изменения путей пересылки пакетов с целью перехвата информации, дестабилизации сети или части сети, нарушения доступа к определенным информационным ресурсам и т.д. Механизмы этих кибератак направлены на навязывание субъектам глобальной маршрутизации заблуждения о топологии сети при отсутствии механизмов проверки этой информации в глобальном протоколе маршрутизации BGP-4. В любом случае полной замены не стоит ожидать в ближайшее десятилетие.

Таким образом, проблема информационной безопасности при обмене брандмауэром требует новой методологии. Методология, предложенная в статье, основана на анализе топологии интернета, предметов, объектов и процессов глобальной маршрутизации, а также управления рисками, что является современным подходом в области информационной безопасности. Владелец риска установлен, сами риски выявлены. Были введены новые метрики для оценки риска перехвата маршрутов – метрик доверия и показателей значимости.

В результате получается риск-ориентированная модель глобальной маршрутизации, описывающая взаимосвязь узлов Интернета с точки зрения риска перехвата маршрута. Это позволяет моделировать наиболее эффективную топологию, где критерием эффективности является оценка риска как мера информационной безопасности. В статье демонстрируются практические результаты использования риск-ориентированных моделей глобальной маршрутизации для оценки и моделирования межсетевых отношений в украинском сегменте интернета.

Ключевые слова: *Интернет, перехват маршрутов, управление рисками, глобальная маршрутизация, метрики доверия.*