DOI:**10.33099/2311-7249/2020-39-3-61-66**

УДК 004[413.3+738.5.057.4]

Віталій Юрійович Зубок *(кандидат технічних наук)*

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

ВДОСКОНАЛЕННЯ ТОПОЛОГІЇ МІЖМЕРЕЖЕВИХ ЗВ'ЯЗКІВ ШЛЯХОМ ОЦІНКИ РИЗИКУ

Глобальна комп'ютерна мережа Інтернет функціонує та постійно зростає за рахунок системи глобальної маршрутизації, масштабованість якої беззаперечна. Але ця система має певні вади інформаційної безпеки, через які існують загрози зумисного викривлення шляхів передачі пакетів з метою порушення цілісності, доступності та конфіденційності інформації. Такі дії отримали назву «перехоплення маршруту». 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, що може тривати ще десятиліття.

Зменшення можливих наслідків кібератак на глобальну маршрутизацію потребує нової методології оцінки ефективності міжмережевих зв'язків та удосконалення топології мережі. Для цього в роботі пропонується використати сучасний ризик-орієнтований підхід, коли власник ризику використовує значення ризику в якості міри захищеності інформації. Запропонована методологія базується на аналізі топології Інтернет, суб'єктів, об'єктів та процесів глобальної маршрутизації. Визначено власника ризику, ідентифіковано самі ризики.

Запроваджено нові метрики для оцінки ризику перехоплення маршрутів – метрику довіри та метрику значущості. Метрика довіри характеризує ймовірність перехоплення маршруту на певному вузлі і залежить від метричної відстані між власником ризику та цільовим вузлом. Введено поняття суб'єкта, об'єкта та предмета довіри. Метрика значущості характеризує рівень максимального збитку, що пов'язаний з масштабом очікуваного розповсюдження хибного маршруту. Вона є комплексною і враховує кількість мережевих префіксів, що маршрутизуються через цільовий вузол, вагу префікса відповідно до його довжини, та відстань між джерелом префіксу та цільовим вузлом. 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.

Ключові слова*: глобальна маршрутизація; перехоплення маршруту; метрика довіри; кібербезпека.*

Вступ

Здійснення системних заходів, спрямованих на посилення безпеки у забезпеченні кіберзахисту електронних інформаційних ресурсів, зокрема, державних, критичної інформаційної інфраструктури, та сприяння розвитку інформаційної інфраструктури вимагають сучасних підходів до аналізу чинників, які формують потенційні і реальні загрози у сфері кібербезпеки. В останні роки все частіше відбуваються інциденти з глобальною маршрутизацією, що стали новою масштабною кіберзагрозою [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» та «витік маршруту».

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.

Постановка проблеми. 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. Отже, актуальною є проблема

© В.Ю.Зубок

підвищення захищеності інформації при міжмережевому обміні.

Аналіз останніх досліджень і публікацій. 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.

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 [3, 4], 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 [3].

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 [5].

Виклад основного матеріалу дослідження.

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.

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, метамаршрутізацією, 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 маршрутизатора (border router). Необхідною компонентою прикордонного маршрутизатора є програмний або програмно-апаратний сервер маршрутів. Для того щоб підмережа стала доступною по IP, 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.

Маршрутизація є двоетапним процесом. 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 чи витік маршруту – атаки, спрямовані на другий етап маршрутизації 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 перший етап – вибір префіксу. Відбувається підміна префікса на більш специфічний, через що легітимні маршрути не можуть конкурувати з хибними, тому що маршрутизація вже відбувається 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 ймовірність P (likelihood) того, що в разі перехоплення маршруту переможе хибний маршрут, зростає разом з відстанню між вузлами $d(as_a, as_b)$:

$$P(as_a, as_b) \sim d(as_a, as_b). \quad (1)$$

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

$$L = \sum_i^{\left|\overline{AS}_b\right|} L_i , \quad (2)$$

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

Це дозволяє порівнювати потенційний збиток при моделюванні різних топологій:

$$\Delta L = L_2 - L_1 \Rightarrow$$

$$\Rightarrow \Delta L \sim \sum_i^{|AS|} d_2(as_a, as_i) - \sum_i^{|AS|} d_1(as_a, as_i),$$

де ΔL — різниця збитку вузла as_a за двох різних топологій міжмережевих зв'язків, що порівнюються.

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 (1), в якості метрики довіри (trust metrics) вузла *v*, запишемо співвідношення середньої відстані між 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:

$$T_u^v = \frac{\sum_i^{|AS|} d(u,i)}{d(u,v)\left(|AS|-1\right)}, \quad \{i,u,v\} \in AS,\ u \neq v;\ u \neq i. \tag{3}$$

де: T_u^v – метрика довіри *v* за оцінкою *u*,

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:

$$T_i^u \le T_j^u,$$

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. Відомо, що 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 мають різну вагу. Для визначення метрики значущості пропонується модифікувати формулу (2) для підрахунку не кількості, а сумарної ваги w_π анонсованих префіксів, що розраховується із довжини префікса $l(\pi)$:

$$w_\pi = 2^{24-l(\pi)}, \tag{4}$$

де w_π – вага префіксу;

$l(\pi)$ – довжина префіксу π.

Згідно (3) 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 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 (δ=0), враховується з коефіцієнтом 1. Якщо джерелом є, наприклад, сусідній до *v* вузол, $(1+\delta)^{-1}$=0.5. Метрика значущості з урахуванням (4) набуде такого вигляду:

$$S_v^u = \sum_\pi w_\pi (1+\delta_\pi)^{-1} = \sum_\pi 2^{24-l(\pi)} (1+\delta_\pi)^{-1} \tag{5}$$

де S_v^u – значущість вузла *v* за оцінкою *u*;

w_π – вага префіксу;

$l(\pi)$ – довжина префіксу π;

δ_π – відстань між джерелом префіксу та вузлом *v*.

Введемо відношення порядку за метрикою значущості на множині всіх автономних систем AS:

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

Запровадження відношення порядку за двома метриками (3) та (5) дозволяє власникові ризику чисельно оцінити ризик перехоплення маршруту на кожному цільовому вузлі. Дві метрики утворюють ризик-орієнтовану модель міжмережевих зв'язків, яка основана на розподілі вузлів в просторі (*R,T,S*). Для підвищення ваги метрики довіри її пропонується враховувати в експоненційній формі:

$$R_v^u = 10^{T_v^u} S_v^u,$$

де *u* – вузол - власник ризику;

v – вузол-об'єкт оцінки;

R – ризик;

T – довіра;

S – значущість.

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

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

Адекватність моделі. Розглянемо основні властивості цієї моделі. За даними проекту CAIDA Інтернет наразі налічує понад 80000 автономних систем, понад 820000 префіксів, середня відстань між AS – від 4 до 5, максимальна (діаметр) – до 10. Метрика довіри теоретично може набувати таких значень:

$$0 < T_v^u \le \left(|AS|-1\right),\ \left\langle T_u^v \right\rangle = 1.$$

На практиці з урахуванням середньої відстані та діаметру мережі Інтернет метрика довіри може набувати значень від 0,1 до 5. Значення більше за одиницю означає метрику довіри до вузлів від *u* до *v* більшу, ніж в середньому до інших вузлів, і навпаки.

Метрика значимості 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 значимість 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 більш щільні. Отже, пошук і аналіз зв'язків *AS* з максимальним значенням S_u^v буде важливим етапом поводження з ризиками.

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

Висновки й перспективи подальших досліджень

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. Впорядкування мережевих вузлів за метрикою довіри та метрикою 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 стосовно поводження з ризиками з використанням цієї моделі.

Література

1. Sermpezis P. A survey among network operators on BGP prefx hijacking / Sermpezis P., Kotronis V., Dainotti A., Dimitropoulos X. // ACM SIGCOMM Computer Communication Review, 2018,48(1), pp.64–69. **2. Reuter A**. Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering / Reuter A., Bush R., Cunha I. et al. // Ibid, 2018, 48(1), pp.19–27. **3.** «ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary». ISO/IEC JTC 1/SC 27. Feb. 2018. **4.** «ISO Guide 73:2009. Risk management – Vocabulary». ISO/TMBG, Nov. 2009. **5 Зубок В.Ю.** Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електрон. моделювання, 2018, 40, №5, с.67-76. **6. Mui L**. A computational model of trust and reputation / Mui L., Mohtashemi M., Halberstadt A. // System Sciences, 2002, p. 2431—2439.

СОВЕРШЕНСТВОВАНИЕ ТОПОЛОГИИ МЕЖСЕТЕВЫХ СВЯЗЕЙ МЕТОДОМ ОЦЕНКИ РИСКА

Виталий Юрьевич Зубок *(кандидат технических наук)*

Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, Украина

Глобальная компьютерная сеть Интернет функционирует и постоянно растет за счет системы глобальной маршрутизации, масштабируемость которой бесспорна. Но эта система имеет определенные недостатки информационной безопасности, поскольку существуют угрозы умышленного искажения путей передачи пакетов с целью нарушения целостности, доступности и конфиденциальности информации. Такие действия получили название «перехват маршрута». Механизмы упомянутых кибератак направлены на навязывание субъектам глобальной маршрутизации ложного представления о топологии сети при отсутствии механизмов валидации этой информации в протоколе глобальной маршрутизации BGP-4. Полное устранение этой уязвимости невозможно без замены протокола BGP-4, что может продолжаться еще десятилетия.

Уменьшение возможных последствий кибератак на глобальную маршрутизацию требует новой методологии оценки эффективности межсетевых связей и совершенствования топологии сети. Для этого в работе предлагается использовать современный риск-ориентированный подход, когда владелец риска использует значение риска в качестве меры защищенности информации. Предложенная методология базируется на анализе топологии Интернет, субъектов, объектов и процессов глобальной маршрутизации. Определен владелец риска, идентифицированы сами риски.

Введены новые метрики для оценки риска перехвата маршрутов - метрика доверия и метрика значимости. Метрика доверия характеризует вероятность перехвата маршрута на определенном узле и зависит от метрической расстояния между владельцем риска и целевым узлом. Введено понятие субъекта, объекта и предмета доверия. Метрика значимости характеризует уровень максимального ущерба, связанного с масштабом ожидаемого распространения ложного маршрута. Она является комплексной и учитывает количество сетевых префиксов, маршрутизируются через целевой узел, вес префикса в соответствии с его длиной, и расстояние между источником префикса и целевым узлом. Оценка рисков информационной безопасности, основанная на этих метриках, служит критерием эффективности топологии по защите от перехвата маршрутов, и дает возможность принимать решения по совершенствованию межсетевых связей, используя риск как степень защищенности информации.

Ключевые слова: *глобальная маршрутизация; перехват маршрута; метрика доверия; кибербезопасность*

IMPROVING INTERNET RELATIONSHIP TOPOLOGY BY RISK ASSESSMENT

Vitalii Zubok ***(Candidate of Technical Sciences)***

Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine

The Internet operates and is constantly growing due to global routing system, the scalability of which is indisputable. But this system has certain information security flaws, due to which there are threats of deliberate distortion of packet transmission paths in order to violate the integrity, accessibility and confidentiality of information. Such actions are called "route hijacks". The mechanisms of the mentioned cyberattacks are aimed at imposing on misconception or, in other words spoofing the network topology derived from routing tables, while mechanisms for validation of this information in the global routing protocol BGP-4 are absent. This vulnerability cannot be completely addressed without replacing the BGP-4 protocol, which could take another decade.

Reducing the potential impact of cyber attacks on global routing requires a new methodology for assessing the effectiveness of interconnections and improving the network topology. Thus, the paper studies usage of a modern risk-oriented approach, when the risk owner uses the value of risk as a measure of information security. The proposed methodology is based on the analysis of the topology of the Internet, subjects, objects and processes of global routing. The owner of the risk is determined, the risks themselves are identified.

New metrics have been introduced to assess the risk of route interception - a trust metric and a significance metric. The trust metric characterizes the probability of a route hijack at a certain node and depends on the metric distance between the risk owner and the target node. The concept of subject of trust and object of trust is introduced. Significance metrics characterizes the level of maximum damage associated with the area of the expected spread of the spoofed route. It is complex and takes into account the number of network prefixes routed through the target node, the weight of the prefix according to its length, and the distance between the source of the prefix and the target node. Risk assessment based on these metrics serves as a measure of the effectiveness of the topology in protecting against interception of routes, and provides an opportunity to make decisions on improving interconnections, using risk to measure the information security.

Key words: *global routing; route hijack; trust metrics; cybersecurity.*

References

1. Sermpezis P. A survey among network operators on BGP prefx hijacking / Sermpezis P., Kotronis V., Dainotti A., Dimitropoulos X. // ACM SIGCOMM Computer Communication Review, 2018,48(1), pp.64–69. **2. Reuter A**. Towards a rigorous methodology for measuring adoption of RPKI route validation and fltering / Reuter A., Bush R., Cunha I. et al. // Ibid, 2018, 48(1), pp.19–27. **3.** «ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary». ISO/IEC JTC 1/SC 27. Feb. 2018. **4.** «ISO Guide 73:2009. Risk management — Vocabulary». ISO/TMBG, Nov. 2009. **5 Зубок В.Ю.** Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електрон. моделювання, 2018, 40, №5, с.67-76. **6. Mui L**. A computational model of trust and reputation / Mui L., Mohtashemi M., Halberstadt A. // System Sciences, 2002, p. 2431—2439.