DOI: 10.35681/1560-9189.2020.22.3.218882

УДК 004.7

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

Аналіз захищеності інтернет-вузлів від кібератак типу «перехоплення маршруту»

Кібератаки на глобальну маршрутизацію в глобальній комп'ютерній мережі Інтернет (перехоплення маршруту, витік маршруту) призводять до масштабних наслідків з порушенням цілісності, доступності та конфіденційності інформації підчас міжмережевого обміну. Запропоновано новий, ризик-орієнтований підхід до підвищення захищеності інформації підчас міжмережевого обміну, націлений на вдосконалення топології міжмережевих зв'язків. При такому підході критерієм ефективності топології проти атак на глобальну маршрутизацію послуговує оцінка ризику як міра захищеності інформації. Для оцінки ризику атак з перехоплення маршрутів запропоновано дві нові метрики інтернет-вузлів, які пов'язують топологію з двома складовими ризику — ймовірністю настання та максимальним збитком. Наведено дослідження вузлів українського сегменту мережі Інтернет за метрикою значущості, яка пов'язана з одним із компонентів ризику — оцінкою максимального збитку, і підтверджено можливість використання цієї метрики для оцінки ризику атак на глобальну маршрутизацію.

Ключові слова: *Інтернет, перехоплення маршрутів, оцінка ризику, метрика довіри, кібербезпека.*

Вступ

На сьогодні Інтернет об'єднує понад 950 тис мереж, побудованих на загальних принципах адресації і маршрутизації [1]. Кожного року трапляється декілька глобальних інцидентів через викрадення та витік маршрутів (route hijack та route leak), які є однією із масштабних проблем кібербезпеки. Викрадення маршруту, чи викрадення префіксу — це явище, при якому одна з понад 70000 автономних систем (AS), які є суб'єктами глобальної маршрутизації, нелегітимно оголошує себе як джерело маршруту (route origin) замість справжнього джерела. Витік маршруту означає, що AS пропонує маршрути до чужих префіксів нелегітимно, з пору-

шенням політики маршрутизації. Ці нелегітимні маршрути забруднюють таблиці маршрутизації BGP, спотворюють шляхи проходження мережевого трафіка та впливають на конфіденційність, цілісність і доступність IP-комунікацій. Інколи вони пояснюються помилками конфігурації маршрутизаторів, але значна міра таких інцидентів визнається цілеспрямованою атакою. Такі атаки використовуються для маніпуляцій із трафіком з метою дестабілізації телекомунікаційної мережі Інтернет, перехоплення трафіка, шпигунства, крадіжок даних, нанесення матеріальної шкоди, дезінформації тощо. Остаточне усунення вразливостей, що уможливлюють такі кібератаки, на цей час є задачею далекої перспективи [2]. Отже існує проблема зменшення наслідків цих вразливостей і вона потребує принципово нової методології.

Маршрутизація безпосередньо пов'язана з топологією мережі. Наявність або відсутність BGP-взаємодії між парою вузлів є критерієм наявності або відсутності між ними безпосереднього зв'язку, тобто на рівні глобальної маршрутизації саме зв'язки BGP-4 формують топологію Інтернет. Механізми атак перехоплення та витоку маршруту впливають на топологію, спотворюючи реальне уявлення про неї шляхом застосування додаткових хибних маршрутів. Таким чином, логічно шукати рішення поставленої проблеми захисту інформації у глобальній комп'ютерній мережі Інтернет шляхом врахування топологічних особливостей мережі та пошуку таких змін топології, які здатні знизити ризик настання шкоди, а отже, і підвищити рівень захищеності інформації.

Сучасна методологія управління інформаційною безпекою базується на управлінні ризиками. Ризик кількісно прийнято виражати як добуток суми збитку від реалізації певної загрози на ймовірність реалізації цієї загрози [3–5]. Найважливішою стадією управління ризиками є ідентифікація ризику та кількісна оцінка збитку від реалізації кожної загрози.

Існує зв'язок між топологією міжмережевих зв'язків і ризиком від кіберінцидентів, пов'язаних з перехопленням маршрутів. Проведені автором дослідження показали, що ризик перехоплення маршрутів може бути оцінений шляхом аналізу міжмережевих зв'язків. Тоді керування ризиком (зменшення ймовірності настання тригера ризику, зниження максимального збитку) можливо шляхом вдосконалення топології зв'язків. При цьому критерієм ефективності топології проти атак на глобальну маршрутизацію послуговує оцінка ризику як міра захищеності інформації. Для кількісної оцінки ризику потрібні методи оцінювання ймовірності настання збитку та масштабу цього збитку. При наявності таких методів, завдання підвищення захищеності інформації від загроз, пов'язаних з глобальною маршрутизацією, можна буде вирішувати шляхом поводження з ризиками.

Нові метрики вузлів для оцінки ризику атак на глобальну маршрутизацію

Маршрутизація в IP-мережах є процесом, який складається з двох етапів. На першому етапі відбувається вибір у базі маршрутів префіксу 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 префіксу. Перехоплення, витік маршруту, в будь-якому випадку означають, що механізм атаки спрямований саме на дру-

гий етап, і в результаті 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.

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 $d\left(as_a, as_b\right)$:

$$P\left(as_a, as_b\right) \sim d\left(as_a, as_b\right). \tag{1}$$

Розглянемо другий аспект ризику, а саме розмір збитку (losses), який є багатофакторною компонентою, як і ймовірність збитку. В разі перехоплення маршруту, кожен довільно обраний вузол as_b буде належати або підмножині AS_b, де переміг істинний маршрут, або підмножині $\overline{AS}_b$, де переміг хибний:

$$as_b \in \overline{AS}_b \Leftrightarrow \ as_b \notin AS_b ; \ AS_b \cup \overline{AS}_b \in AS .$$

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.

У загальному випадку сума збитків по конкретних вузлах $as_b \in \overline{AS}_b$, в яких переміг хибний маршрут, має вигляд

$$L = \sum_{i}^{\left|\overline{AS}_b\right|} L_i , \tag{2}$$

а кардинальне число множини $\overline{AS}_b$ залежить від того, наскільки джерело істинного маршруту as_a віддалене від інших вузлів мережі:

$$|\overline{AS}_b| \sim D : D = \sum_{i}^{|AS|} d\left(as_a, as_i\right),$$

де D — сумарна відстань від as_a до інших вузлів множини AS.

Це дозволяє порівнювати потенційний збиток при моделюванні різних топологій:

$$\Delta L = L_2 - L_1 \;\Rightarrow\; \Delta L \sim \sum_i^{|AS|} d_2\left(as_a, as_i\right) - \sum_i^{|AS|} d_1\left(as_a, as_i\right),$$

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 і 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 із 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), як метрику довіри вузла v запишемо співвідношення середньої відстані між суб'єктом довіри u та іншими вузлами, обрахованої за вихідними зв'язками, і відстанню від u до конкретного вузла v, що є об'єктом довіри:

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

Тут T_u^v — метрика довіри вузла v з точки зору u; u та v — суб'єкт і об'єкт довіри; i, u, v — автономні системи мережі з множини AS; 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. Отже, на множині вузлів AS запропоновано ввести відношення порядку за сумою кількості вихідних зв'язків та анонсованих префіксів, яка отримала назву «значущість» (significance):

$$S_v^u = \left|\pi_v\right|, \tag{4}$$

де S_v^u — значущість вузла v за оцінкою u; $\left|\pi_v\right|$ — кількість отриманих від BGP-системи вузла u маршрутів, що пролягають через v. Необхідно введення відношення порядку за метрикою значущості на множині всіх автономних систем AS:

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

Запровадження відношення порядку за двома метриками дозволить власникові ризику сформувати двовимірну модель безпеки глобальної маршрутизації в Інтернеті, в основі якої лежить розподіл вузлів мережі Інтернет за зростанням ризику. Вона дозволяє виразити ризик R через довіру як оцінку ймовірності, та значущість як оцінку потенційних збитків. Дві метрики утворюють ризик-орієнтовану модель міжмережевих зв'язків, яка основана на розподілі вузлів у просторі (R,T,S), де R — ризик, T — довіра та S — значущість:

$$R^u = \frac{\sum\limits_{i\neq u}^{|AS|-1} S_i^u T_i^{u-1}}{\left|AS\right|-1}\,. \tag{5}$$

Метрика довіри, що має знаходитись у знаменнику, має вигляд T_i^{u-1}, і тому її можна назвати «антидовірою», що підвищує ймовірність настання збитку.

Методика отримання даних для розрахунку метрик довіри та значущості

У [7] 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. 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 за функціями портал доступу до функцій маршрутизатора в режимі «тільки читання» (тобто, дозволяє лише отримувати інформацію і не дозволяє вносити зміни, наприклад, у 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 інтернет-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 (рис. 1). Такий запис містить наступні дані:

— версія BGP-таблиці — її унікальний «серійний номер», зміна якого однозначно дозволяє відстежувати наявність змін у BGP-таблиці. BGP Version постій-

но інкрементується, коли в таблицю вносяться зміни — додаються чи вилучаються маршрути;

— усі наявні шляхи до префіксу, чи їхню відсутність;

— атрибути кожного шляху;

— ідентифікатор BGP-партнера, від якого отримано префікс,

та інші дані.

```
> show ip bgp routes detail 195.64.225.0/24
  Number of BGP Routes matching display condition : 2
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
1       Prefix: 195.64.224.0/22, Rx path-id:0x00000000, Tx path-id:0x00600001, rank:0x00000001, Status: BMI,  Age: 7d9h22m36s
         NEXT_HOP: 80.81.193.180, Metric: 1405, Learned from Peer: 216.218.252.169 (6939)
          LOCAL_PREF: 140,  MED: 0,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 1
         AS_PATH: 3326 8258 8258 8258 8258 8258
2       Prefix: 195.64.224.0/22, Rx path-id:0x00000000, Tx path-id:0x00000000, rank:0x00000002, Status: MI,  Age: 7d9h24m51s
         NEXT_HOP: 80.81.193.180, Metric: 1405, Learned from Peer: 216.218.252.171 (6939)
          LOCAL_PREF: 140,  MED: 0,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 0
         AS_PATH: 3326 8258 8258 8258 8258 8258
       Last update to IP routing table: 7d9h22m36s, 1 path(s) installed
```

Рис. 1. Приклад даних BGP, отриманих стосовно префікса 195.64.225.0/24

Іншою типовою функцією looking glass server є надання загальної статистики BGP (BGP Summary).

Ця інформація містить такі дані (рис. 2):

— ідентифікатор маршрутизатора (його IP-адресу);

— номер автономної системи, до якої він належить;

— дані стосовно версії таблиць маршрутизації

— дані стосовно ресурсів операційної системи маршрутизатора (вільна та зайнята оперативна пам'ять);

— загальна кількість префіксів;

— загальна кількість унікальних шляхів (за атрибутом AS PATH);

— ідентифікатори BGP-партнерів, з якими обмінюється анонсами даний сервер.

Наступною типовою функцією є видача детальної статистики по певному BGP-партнеру, ідентифікатор якого треба дати в запиті. Серед інших даних, зокрема, можна отримати перелік префіксів, які прийняті від цього BGP-партнера. Саме ця функція дає можливим вивчення топології взаємодії автономних систем, особливо в мережах обміну трафіком. На рис. 3 наведено фрагмент таблиці префіксів, які отримані та прийняті сервером маршрутів мережі обміну трафіком DE-CIX від одного з учасників — AS12883 (це український телеком-оператор, відомий за торгівельною маркою «Вега»).

Таким чином, спостереження таблиць маршрутизацій за допомогою публічно доступних серверів маршрутів і сервісів looking glass дозволяє отримати інформацію, необхідну для розрахунку метрики довіри та метрики значущості.

Метрика значущості теоретично лежить у межах $1 \le S_u^v < \left|AS\right|$. Зважаючи на результати багатьох досліджень Інтернету, переважна більшість автономних систем анонсують лише один мережевий префікс і не є транзитними, мають $S_u^v = 1$. А загалом розподіл вихідного ступеню має степеневий (power-law) характер і в окремих AS він сягає декількох тисяч.

BGP router identifier 195.35.65.1, local AS number 15645
BGP table version is 189521579, main routing table version 189521579
29448 network entries using 7303104 bytes of memory
55890 path entries using 6706800 bytes of memory
26648/9292 BGP path/bestpath attribute entries using 6395520 bytes of memory
10827 BGP AS-PATH entries using 558700 bytes of memory
1749 BGP community entries using 94358 bytes of memory
41 BGP extended community entries using 1240 bytes of memory
442 BGP route-map cache entries using 28288 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 21088010 total bytes of memory
8856 received paths for inbound soft reconfiguration
BGP activity 19566602/19536700 prefixes, 114662008/114605505 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
185.1.50.4	4	12294	170683	1822548	189521579	0	0	13w3d	164
185.1.50.5	4	24700	147700	652145	189521579	0	0	6w4d	26
185.1.50.6	4	44827	51705	245910	189521579	0	0	2w2d	23
185.1.50.7	4	12788	138273	1053266	189521579	0	0	13w3d	5
185.1.50.8	4	8856	299213	1300671	189521579	0	0	13w3d	19

Рис. 2. Приклад даних BGP Summary

ROUTES ACCEPTED

Showing **1 - 250** of **754** total routes

	Network	Next-Hop	AS Path	Local Pref.	MED	Origin
	109.72.152.0/24	80.81.194.177	12883 12593 199098	100	0	IGP
	109.72.153.0/24	80.81.194.177	12883 12593 199098	100	0	IGP
	109.72.154.0/24	80.81.194.177	12883 12593 199098	100	0	IGP
	109.72.155.0/24	80.81.194.177	12883 12593 199098	100	0	IGP
	129.35.189.0/24	80.81.194.177	12883 6703 1786 1786 1786 1786	100	0	IGP
	130.0.32.0/19	80.81.194.177	12883 6876 6876 6876	100	0	IGP
	141.98.148.0/22	80.81.194.177	12883 12883 6886	100	0	IGP

Рис. 3. Дані про маршрути, отримані від певного учасника мережі обміну трафіком

Якщо AS анонсує певний мережевий префікс, це означає, що або цей префікс є частиною даної AS, і вона є джерелом маршруту (route origin), або вона отримала анонс цього префікса від іншої AS і пропонує транзитний шлях до цього префіксу через себе. Кількість префіксів, до яких AS пропонує маршрут, характеризує її значущість. Оцінка цієї кількості має відбуватися з позиції власника ризику. Це означає, що для отримання даних він має користуватися 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.

Розрахунок метрики значущості для ранжування інтернет-вузлів

Продемонструємо на практиці ранжування AS за метрикою значущості. Для прикладу уявімо, що власник ризику зацікавлений у поліпшенні топології з метою зниження ризику від перехоплення маршрутів саме в українському сегменті мережі Інтернет. За джерела даних візьмемо інформацію з сервера маршрутів оператора Hurricane Electrics, що підключений до багатьох мереж обміну трафіком. У результаті отримано інформацію про 89 автономних систем, з якими оператор взаємодіє в м. Києві, та мережеві префікси, анонси яких він отримує від кожної AS. Результати ранжування наведені на рис. 4. Метрика значущості *S* представлена по логаріфмічній осі ординат. Окремо в таблиці надано дані про 40 AS з найвищою кількістю анонсів.

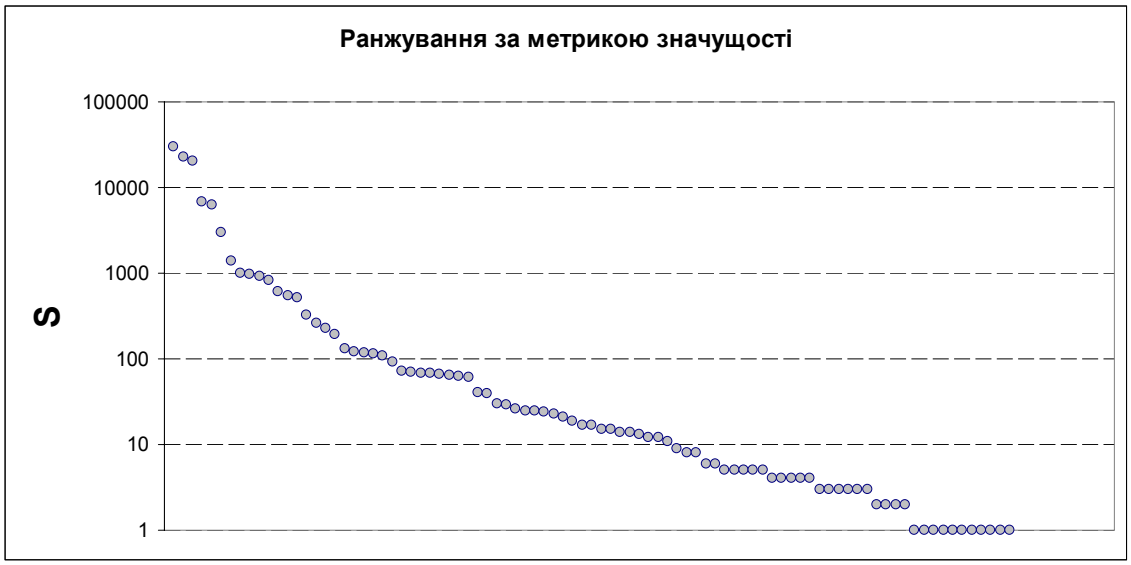

Рис. 4. Результат ранжування 89 AS українського сегменту Інтернет

Проаналізуємо декілька верхніх позицій рейтингу з метою оцінки адекватності результату. На першому місці знаходиться AS31210. Це мережа обміну трафіком DTEL-IX, що на даний час налічує понад 211 учасників, а середньодобовий трафік складає 1,2 Тбіт/с. На другому місці — AS15645, мережа обміну трафіком UA-IX, що налічує 201 учасника та декларує середньодобовий трафік 700 Гбіт/с. На третьому місці — AS59613, мережа обміну трафіком Giganet, яка налічує 115 учасників і середньодобовий трафік якої складає 1,12 Тбіт/с. Зауважимо, що призначення мереж обміну трафіком і їхнє місце у функціонуванні та формуванні топології Інтернет були досліджені у [8] та [9].

З четвертого місця списку починаються AS великих українських телекомоператорів, які за вказаними характеристиками поступаються мережам обміну трафіком. Такі результати свідчать про те, що дані, отримані з серверу маршрутів, а також результат ранжування AS за метрикою значущості є адекватними.

Ранжування «Top-40» автономних систем за кількістю анонсів

Ідентифікатор AS	***S***	**Ідентифікатор AS**	***S***
AS31210	29995	AS29632	117
AS15645	22966	AS25133	114
AS59613	20313	AS48648	108
AS29076	6892	AS29107	92
AS41095	6320	AS60159	71
AS43727	2956	AS21500	70
AS3255	1384	AS34867	69
AS1820	1000	AS35362	69
AS13249	978	AS48422	66
AS35297	929	AS30886	64
AS15169	825	AS12687	62
AS31148	616	AS6886	61
AS3303	545	AS12593	41
AS13335	518	AS41820	39
AS50581	322	AS6876	30
AS199995	260	AS35213	29
AS49544	229	AS24700	26
AS13188	192	AS48438	25
AS15895	133	AS48919	25
AS16276	122	AS51500	24

Висновки

У рамках застосування нового ризик-орієнтованого підходу до підвищення захищеності інформації підчас міжмережевого обміну запропоновано нові метрики для інтернет-вузлів У даній статті проведено дослідження вузлів українського сегменту мережі Інтернет за метрикою значущості, яка пов’язана з одним із компонентів ризику — оцінкою максимального збитку, показано методику отримання та аналізу даних. Результати демонструють придатність метрики значущості для використання як однієї із компонент при оцінці ризику атак на глобальну маршрутизацію.

1. Stroves S. Visibility of IPv4 and IPv6 Prefix Lengths in 2019. URL: https://labs.ripe.net/Members/stephen_strowes/visibility-of-prefix-lengths-in-ipv4-and-ipv6 (Дата звернення: 20.04.2020).

2. Зубок В. Ретроспективний аналіз інцидентів кібербезпеки, пов’язаних з атаками на глобальну маршрутизацію. *Моделювання та інформаційні технології*. 2019. Вип. 86. С. 42–49.

3. Boehm B. Software Risk Management. Washington, DC, USA: IEEE Computer Society (CS) Press, 1989.

4. ISO/IEC 27000:2018 Information technology. Security techniques. Information security management systems. Overview and vocabulary. ISO/IEC JTC 1/SC 27. Feb. 2018.

5. ISO Guide 73:2009. Risk management — Vocabulary. ISO/TMBG, Nov. 2009.

6. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation. *System Science.* 2002. P. 2431–2439.

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

8. Зубок В.Ю. Аналіз характеристик нових мереж обміну інтернет-трафіком. *Реєстрація, зберігання і оброб. даних*. 2013. Т. 15. № 2. С. 48–54.

9. Зубок В.Ю. Європейські мережі обміну Інтернет-трафіком та їхній вплив на зв'язність між автономними системами: зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України, 2011. № 58. С. 34–43.

Надійшла до редакції 28.09.2020