УКРАЇНА

(19) UA (11) 145947 (13) U

(51) МПК (2021.01)
H04L 12/28 (2006.01)
H04L 12/701 (2013.01)
H04L 12/741 (2013.01)
G06F 7/00
G06F 17/00
G06F 17/40 (2006.01)

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНЕ ПІДПРИЄМСТВО "УКРАЇНСЬКИЙ ІНСТИТУТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2020 07198**

(22) Дата подання заявки: **11.11.2020**

(24) Дата, з якої є чинними права інтелектуальної власності: **07.01.2021**

(46) Публікація відомостей про державну реєстрацію: **06.01.2021, Бюл.№ 1**

(72) Винахідник(и):
Зубок Віталій Юрійович (UA),
Мохор Володимир Володимирович (UA),
Ланде Дмитро Володимирович (UA)

(73) Володілець (володільці):
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ,
вул. Генерала Наумова, буд. 15, м. Київ, 03164 (UA)

(74) Представник:
Чьочь Вікторія Володимирівна, реєстр. №257

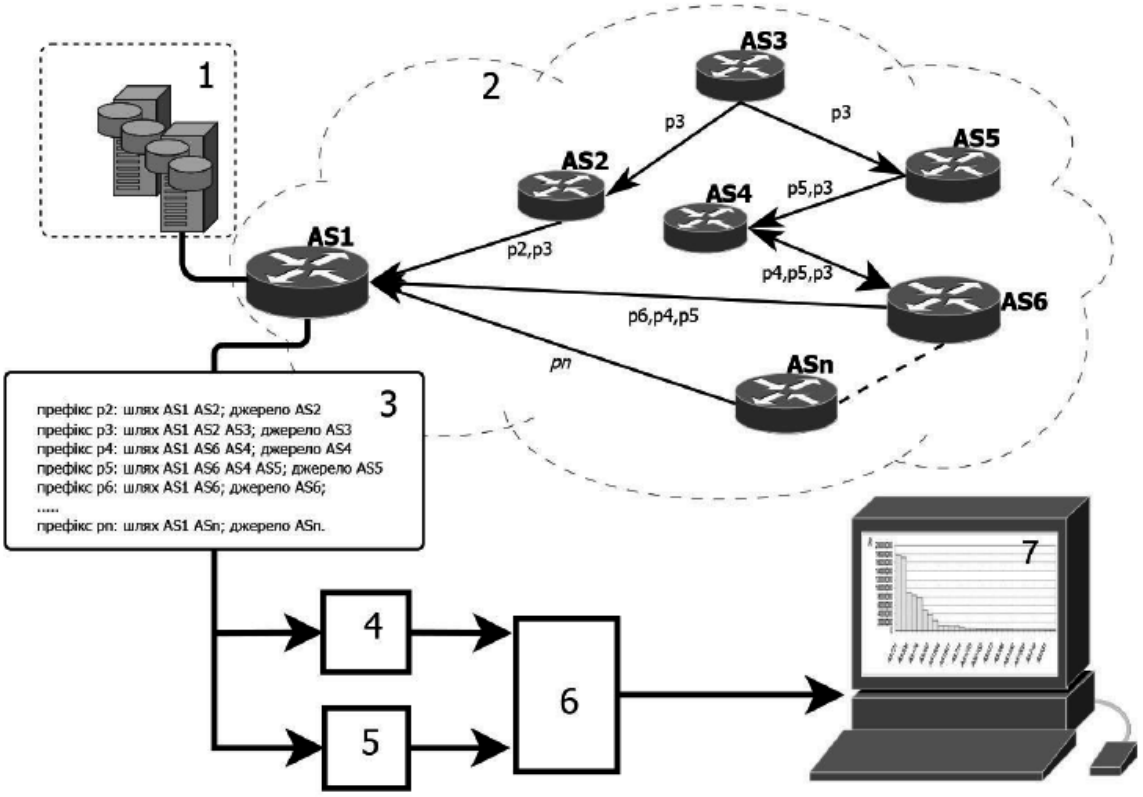
(54) СПОСІБ ВИЗНАЧЕННЯ РИЗИКУ ПЕРЕХОПЛЕННЯ МАРШРУТУ НА ВУЗЛАХ МЕРЕЖІ ІНТЕРНЕТ

(57) Реферат:

Спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет, згідно з яким отримують та зберігають первинні дані про топологію міжмережевих зв'язків та характеристики мережевих префіксів (таблицю глобальної маршрутизації) з власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора), з таблиці глобальної маршрутизації отримують сукупність номерів автономних систем, мережевих IP-префіксів, маршрутів у вигляді послідовності номерів автономних систем. Визначають ризики перехоплення маршруту на вузлах мережі Інтернет, враховуючи ймовірність перехоплення та максимальні втрати інформаційної безпеки, до яких може призвести перехоплення на кожному вузлі, ймовірність перехоплення маршруту на кожному вузлі оцінюють шляхом розрахунку метрики довіри, яка характеризує відносну топологічну близькість даного вузла до інформаційного активу, максимальні втрати інформаційної безпеки на кожному вузлі оцінюють шляхом розрахунку метрики значущості, яка характеризує вплив даного вузла на розповсюдження маршрутів, для обчислення метрики довіри для кожного вузла визначають середню відстань між вузлами мережі та відстань від інформаційного активу до кожного вузла мережі окремо, для обчислення метрики значущості для кожного вузла визначають перелік мережевих префіксів, в чиїх шляхах присутній ідентифікатор даного вузла, для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, визначають відстань від джерела маршруту мережевого префікса до даного вузла та зберігають в тимчасовій таблиці "префікс; відстань", для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, обчислюють вагу кожного IP-префікса у відповідності до довжини його мережевої маски, зберігають отримані дані для подальшої обробки у вигляді бази

UA 145947 U

даних із структурою "префікс; вага; джерело; шлях", за метрикою значущості та метрикою довіри розраховують значення ризику перехоплення маршруту на кожному вузлі мережі Інтернет, результат зберігають в базі даних формату "ідентифікатор вузла; значення ризику", впорядковують перелік вузлів мережі Інтернет за зниженням ризику.



Корисна модель належить до інформаційних технологій, зокрема до інформаційної безпеки, а саме до спеціалізованих способів аналізу характеристик вузлів мережі Інтернет і стосується оцінки ризиків інформаційної безпеки, спричинених атаками на глобальну маршрутизацію в мережі Інтернет, може бути використана для підтримки прийняття рішень з організації та оптимізації міжмережевих зв'язків для інформаційних активів, пов'язаних з глобальною комп'ютерною мережею Інтернет, якими є вебсайти, інформаційні портали, вузли інтернет-доступу, датацентри і т.ін.

Відомі спосіб і пристрій для управління маршрутизацією IP-адрес [1] для налаштування маршрутизатора та одного або декількох серверів для маршрутизації та прив'язки мережевих адрес відповідно, що містить центральний пристрій керування мережею та консоль (діалоговий інтерфейс) керування центральним пристроєм із функціями призначення мережевих адрес, вибору маршруту, опціональної інкапсуляції мережевих пакетів.

Недоліком даного способу є відсутність ризик-аналізу топології мережевих зв'язків, без урахування факторів, що впливають на ймовірність атак перехоплення маршруту та масштаб можливих наслідків.

Відомі спосіб і система моніторингу мережевої маршрутизації [2], що реалізує низку методів для моніторингу маршрутизації в об'єднаних комп'ютерних мережах шляхом збору, аналізу та представлення користувачеві даних з певної множини мережевих маршрутизаторів. Ця система здатна виявляти аномальні стани, пов'язані як з помилками конфігурування маршрутизаторів в глобальній мережі, так і виявляти наслідки атак типу перехоплення маршрутів.

Недоліком відомого рішення є відсутність функцій сприяння прийняттю рішень стосовно зменшення впливу аномалій глобальної маршрутизації, спричинених кібератаками.

Відома система для маршрутизації інтернет-трафіку [3], що реалізує методику вдосконалення алгоритмів маршрутизації, закладених в протоколі глобальної маршрутизації BGP-4, за рахунок врахування параметрів віртуального каналу передачі даних - пропускної спроможності, затримки, надійності. Позитивний ефект полягає в результаті отримання багатофакторної характеристики каналу із застосуванням лінійного програмування.

Недоліком відомої системи є неможливість передбачити зміну характеристик мережі в разі кібератак з перехопленням маршруту.

Відома модель ймовірнісного прогнозування кібернетичних ризиків в комп'ютерній мережі [4], яка кількісно визначає лінійні та нелінійні збитки активам, що пов'язані з комп'ютерною мережею, шляхом розповсюдження імовірнісного розподілу подій у послідовності та в часі для прогнозування збитків протягом певних періодів.

Недоліком відомої моделі є відсутність аналізу топології мережі при складанні чинників кіберзагроз.

Загальним недоліком відомих рішень є брак аналізу вразливості до перехоплення маршрутів як під час аналізу рівня захищеності інформації, так і під час вибору маршруту передачі інформації в комп'ютерній мережі.

Аналіз попереднього рівня техніки дозволяє зробити висновок про неефективність і в деяких випадках про неможливість застосування попередніх технологій для вирішення проблеми ефективної організації міжмережевих зв'язків для певного суб'єкта глобальної маршрутизації мережі Інтернет, яким є власник інформаційного активу, пов'язаного з мережею Інтернет. Таким чином, потрібно створити рішення, яке дозволить на множині інтернет-вузлів визначати шляхи пакетної маршрутизації, найбільш захищені від перехопленням маршруту.

Задачею корисної моделі є підвищення захищеності інформації при міжмережевому обміні шляхом визначення для власника інформаційного активу, пов'язаного з мережею Інтернет, ризиків перехоплення маршруту на кожному з вузлів мережі Інтернет.

Поставлена задача вирішується за рахунок того, що спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет, згідно з яким отримують та зберігають первинні дані про топологію міжмережевих зв'язків та характеристики мережевих префіксів (таблицю глобальної маршрутизації) з власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора), з таблиці глобальної маршрутизації отримують сукупність номерів автономних систем, мережевих IP-префіксів, маршрутів у вигляді послідовності номерів автономних систем, причому визначають ризики перехоплення маршруту на вузлах мережі Інтернет, враховуючи ймовірність перехоплення та максимальні втрати інформаційної безпеки, до яких може призвести перехоплення на кожному вузлі, ймовірність перехоплення маршруту на кожному вузлі оцінюють шляхом розрахунку метрики довіри, яка характеризує відносну топологічну близькість даного вузла до інформаційного активу, максимальні втрати інформаційної безпеки на кожному вузлі оцінюють шляхом розрахунку метрики значущості, яка характеризує вплив даного вузла на розповсюдження маршрутів, для обчислення метрики

довіри для кожного вузла визначають середню відстань між вузлами мережі та відстань від інформаційного активу до кожного вузла мережі окремо, для обчислення метрики значущості для кожного вузла визначають перелік мережевих префіксів, в чиїх шляхах присутній ідентифікатор даного вузла, для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, визначають відстань від джерела маршруту мережевого префікса до даного вузла та зберігають в тимчасовій таблиці "префікс; відстань", для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, обчислюють вагу кожного IP-префікса у відповідності до довжини його мережевої маски, зберігають отримані дані для подальшої обробки у вигляді бази даних із структурою "префікс; вага; джерело; шлях", за метрикою значущості та метрикою довіри розраховують значення ризику перехоплення маршруту на кожному вузлі мережі Інтернет, результат зберігають в базі даних формату "ідентифікатор вузла; значення ризику", впорядковують перелік вузлів мережі Інтернет за зниженням ризику.

Технічний результат, що досягається при здійсненні запропонованого способу, полягає в розширенні переліку відомих характеристик інтернет-вузлів за рахунок отримання користувачем впорядкованої множини ідентифікаторів інтернет-вузлів за зростанням ризику перехоплення маршруту, що дозволить поліпшити якість технічних та управлінських рішень стосовно організації зв'язків з іншими вузлами та в результаті зменшити втрати інформаційної безпеки, спричинені згаданими кібератаками.

Суть способу - визначення ризику перехоплення маршруту на вузлах мережі Інтернет пояснено на кресл., де наведено гібридну схему, яка демонструє реалізацію способу визначення ризику перехоплення маршруту на вузлах мережі Інтернет.

На схемі позначено інформаційний актив 1, підключений до інтернет-вузла AS1 - власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора), який разом з вузлами AS2, AS3, AS4 … ASn входить до мережі Інтернет 2, дані про глобальну маршрутизацію 3, зібрані на вузлі AS1, передають до блоків розрахунку метрики значущості 4 та розрахунку метрики довіри 5, результати розрахунку метрик обробляють в блоці розрахунку ризику перехоплення маршруту 6 та у впорядкованому вигляді виводять на дисплей 7, наприклад, у вигляді графіка або таблиці.

Спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет здійснюють наступним чином.

Відомо, що глобальну маршрутизацію в мережі Інтернет забезпечує взаємодія автономних систем, які є групами з однієї чи більше мереж з спільним адмініструванням та єдиною політикою маршрутизації, по протоколу BGP-4. Кібернетичні атаки на глобальну маршрутизацію використовують вади протоколу та дозволяють зловмиснику надсилати хибні дані до таблиць маршрутизації інших вузлів, спотворюючи легітимні шляхи передачі даних.

Керування ризиками потребує чисельного визначення двох складових ризику - ймовірності настання несприятливої події та втрат внаслідок цієї події: R=LC, де R - ризик, L - ймовірність, C - втрати.

Для оцінки ризику, спричиненого можливістю кібератаки типу "перехоплення маршруту", власник інформаційного активу 1, підключений до інтернет-вузла AS1 - власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора), яке взаємодіє з глобальною комп'ютерною мережею Інтернет 2, проводить аналіз топології міжмережевих зв'язків і отримує чисельну оцінку ризику перехоплення власних маршрутів. Заздалегідь має бути визначена сфера застосування аналізу - попередньо сформований перелік цільових мережевих префіксів (в загальному випадку всі наявні мережеві префікси мережі Інтернет є цільовими).

Для аналізу вузлів на ризик перехоплення отримують та зберігають у базі даних первинні дані про топологію міжмережевих зв'язків та характеристики мережевих префіксів. З власного пристрою - інтернет-вузла AS1, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора) отримують таблицю вхідних маршрутів 3, що містить сукупність наступних даних:

- мережевий префікс, до якого веде маршрут, у форматі "адреса_мережі/довжина_маски";
- ідентифікатор вузла мережі Інтернет, з якого отримано маршрут, у вигляді номеру автономної системи;
- шлях до мережевого префікса у вигляді послідовності номерів автономних систем.

Якщо префікс p входить до переліку цільових префіксів, для кожного мережевого префікса обчислюють його вагу

$$w_p = 2^{24-l(p)},$$

де w_p - вага префікса; $l(p)$ - довжина префікса p.

Для кожного мережевого префікса визначають ідентифікатор вузла - джерело маршруту до префікса (network origin), зберігають отримані дані для подальшої обробки у вигляді бази даних наступної структури: "префікс; вага; джерело; шлях".

Із збережених шляхів складають перелік видимих вузлів, де номер ASi стає унікальним ідентифікатором вузла мережі, цей перелік зберігають в окремому масиві або списку унікальних номерів AS.

Складають перелік унікальних шляхів, в якому будь-яка послідовність ідентифікаторів вузлів зустрічається не більше одного разу, та зберігають в окремій базі даних шляхів у вигляді "AS1 ASi ASj …".

Для кожного вузла оцінюють максимальний збиток шляхом розрахунку метрики значущості, яка характеризує вплив даного вузла на розповсюдження маршрутів. Для цього по кожному вузлу визначають перелік мережевих префіксів p, в чиїх шляхах присутній ідентифікатор даного вузла ASi.

Для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, визначають відстань від джерела маршруту мережевого префікса до даного вузла та зберігають в тимчасовій таблиці "префікс; відстань". Надалі для представлення в формулах вузол AS1 власника інформаційного активу буде іменовано u, а досліджувані вузли мережі ASi - v.

Задавши ваги префікса та відстані обчислюють метрику значущості вузла

$$S_v^u = \sum_p w_p (1 + \delta_p)^{-1},$$

де S_v^u - значущість вузла v за оцінкою u; w_p - вага префікса; $l(p)$ - довжина префікса p, δ_p - відстань між джерелом префікса та вузлом v, та зберігають отримані дані у вигляді бази даних (таблиці) "номер ASi; метрика значущості".

Для кожного номера ASi оцінюють ймовірність перехоплення маршруту шляхом розрахунку метрики довіри, яка характеризує відносну топологічну близькість його до інформаційного активу.

Для цього по базі даних шляхів обчислюють середній шлях $\langle D \rangle$ між всіма вузлами мережі

$$\langle D \rangle = \frac{1}{|V|} \sum_{i=1}^{|V|} \sum_{j=1}^{|V|} d(i,j), \quad i \neq j,$$

де d(i, j) - відстань між вузлами i та j, V - множина всіх цільових вузлів, та зберігають його значення.

Розраховують $T_u = \frac{d(u,v)(|V|-1)}{\sum_{i \neq u}^{|V|} d(u,i)}$ метрику довіри

де T_u^v - метрика довіри вузла v за оцінкою вузла u, V - множина цільових вузлів.

Для кожного номера ASi розраховують ризик перехоплення маршруту як $R_v^u = T_v^u S_v^u$,

де R - ризик, T - довіра і S - значущість, результат зберігають в таблиці бази даних формату "ідентифікатор вузла; значення ризику".

Після здійснення усіх операцій впорядковують ідентифікатори вузлів за зниженням ризику.

Запропонований спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет дає можливість доповнити характеристики інтернет-вузлів завдяки оцінці ризиків інформаційної безпеки, спричинених атаками на глобальну маршрутизацію в мережі Інтернет, і може бути використаний власником певного інформаційного активу, який взаємодіє з глобальною комп'ютерною мережею Інтернет, приймати рішення з удосконалення топології власних мережевих зв'язків з метою забезпечення необхідного рівня інформаційної безпеки.

Використані джерела:

1. Патент US7467229 (B1), Method And Apparatus For Routing Of Network Addresses /Inventors: Brent Biggs; Jason Rudolph; Applicant: Direct Route, LLC, Seattle, WA (US). - Заявл. 05.10.2007.

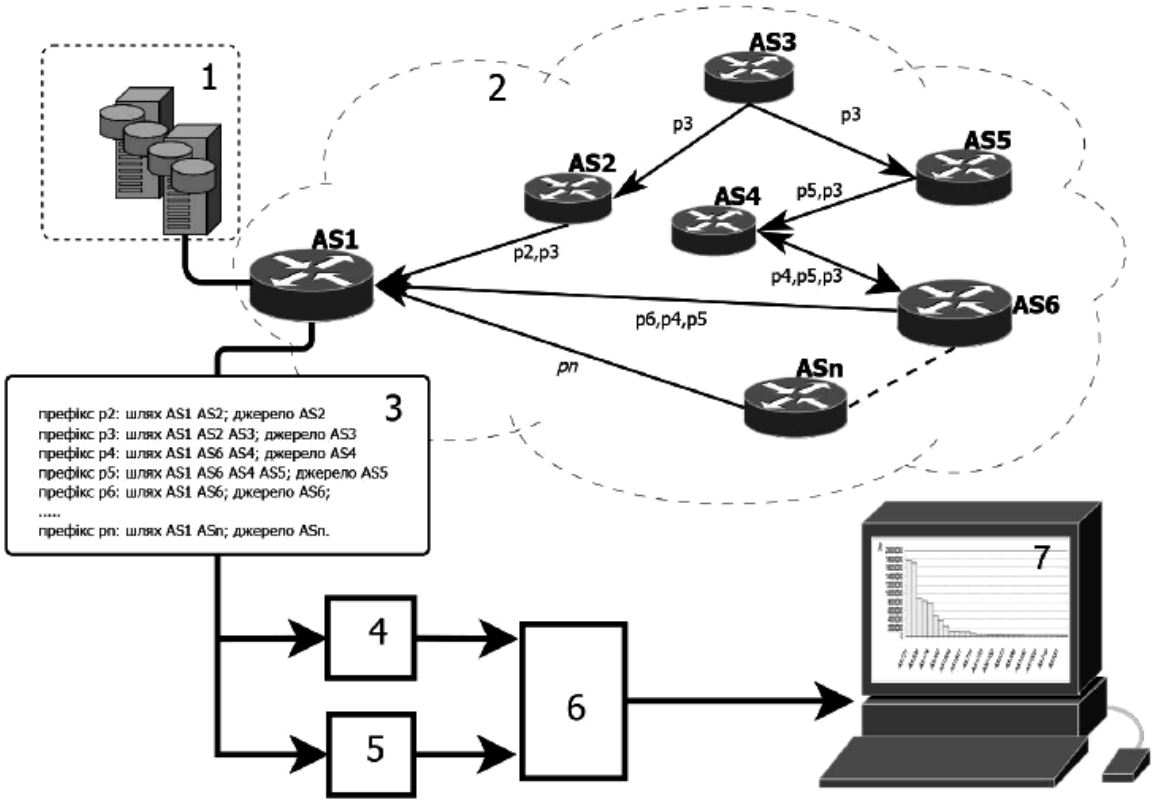
2. Заявка CA2519378, Methods and Systems for Monitoring Network Routing /Inventors: Ogielski, Andrew T.; Cowie, James H.; Applicant: Renesys Corporation, US. - заявл. 18.03.2004.

3. Патент US9525638 (B2), Routing System for Internet Traffic /Inventors: Marco A. Valero; Charles Victor Bancroft, II; William Brian Hammond, et al.; Applicant: Internap Network Services Corporation, Atlanta, GA (US). - заявл. 15.11.2013.

4. Патент US10757127 (B2), Probabilistic Model For Cyber Risk Forecasting /Inventors: Craig A. Schultz; John J. Nitao; Jeffrey M. Starr; John Compton; Applicant: Neo Prime, LLC, Wilmington, DE (US). - заявл. 09.06.2017.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет, згідно з яким отримують та зберігають первинні дані про топологію міжмережевих зв'язків та характеристики мережевих префіксів (таблицю глобальної маршрутизації) з власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора), з таблиці глобальної маршрутизації отримують сукупність номерів автономних систем, мережевих IP-префіксів, маршрутів у вигляді послідовності номерів автономних систем, який **відрізняється** тим, що визначають ризики перехоплення маршруту на вузлах мережі Інтернет, враховуючи ймовірність перехоплення та максимальні втрати інформаційної безпеки, до яких може призвести перехоплення на кожному вузлі, ймовірність перехоплення маршруту на кожному вузлі оцінюють шляхом розрахунку метрики довіри, яка характеризує відносну топологічну близькість даного вузла до інформаційного активу, максимальні втрати інформаційної безпеки на кожному вузлі оцінюють шляхом розрахунку метрики значущості, яка характеризує вплив даного вузла на розповсюдження маршрутів, для обчислення метрики довіри для кожного вузла визначають середню відстань між вузлами мережі та відстань від інформаційного активу до кожного вузла мережі окремо, для обчислення метрики значущості для кожного вузла визначають перелік мережевих префіксів, в чиїх шляхах присутній ідентифікатор даного вузла, для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, визначають відстань від джерела маршруту мережевого префікса до даного вузла та зберігають в тимчасовій таблиці "префікс; відстань", для кожного мережевого префікса, в чиїх шляхах присутній ідентифікатор даного вузла, обчислюють вагу кожного IP-префікса у відповідності до довжини його мережевої маски, зберігають отримані дані для подальшої обробки у вигляді бази даних із структурою "префікс; вага; джерело; шлях", за метрикою значущості та метрикою довіри розраховують значення ризику перехоплення маршруту на кожному вузлі мережі Інтернет, результат зберігають в базі даних формату "ідентифікатор вузла; значення ризику", впорядковують перелік вузлів мережі Інтернет за зниженням ризику.



Комп'ютерна верстка Л. Литвиненко

ДП “Український інститут інтелектуальної власності”, вул. Глазунова, 1, м. Київ – 42, 01601