НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ІМ. Г. Є. ПУХОВА

В.Ю. ЗУБОК, В.В. МОХОР

КІБЕРБЕЗПЕКА ТОПОЛОГІЇ INTERNET

КИЇВ
2022

УДК 004 [413.3+738.5.057.4] : 519.173

Наукове видання.

Рекомендовано до видання Вченою радою Інституту проблем моделювання в енергетиці імені Г.Є. Пухова НАН України (протокол № 4 від 26 травня 2022 р.)

Автори:

Зубок Віталій Юрійович, докт. техн. наук, ст. досл., ст. наук. співр. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова.

Мохор Володимир Володимирович, чл.-кор. НАН України, докт. техн. наук, професор, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова.

Рецензенти:

Литвиненко Олександр Євгенович, докт. техн. наук, професор, завідувач кафедри комп'ютеризованих систем управління Національного авіаційного університету, лауреат Державної премії України в галузі науки і техніки.

Ланде Дмитро Володимирович, доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУУ «Київський політехнічний інститут імені Ігоря Сікорського».

Зубок, В.Ю. Кібербезпека топології INTERNET : монографія / В. Ю. Зубок, В. В. Мохор. — К. : ІПМЕ ім. Г.Є.Пухова, 2022. — 191 с. – ISBN 978-966-02-9929-0.

Монографію присвячено розвитку теоретичних засад та методик підвищення захищеності топології глобальної комп'ютерної мережі Інтернет від атак на систему глобальної маршрутизації. Проведено аналіз методів протидії кібернетичним атакам на систему глобальної маршрутизації та реагування на інциденти з перехопленням маршрутів. Запропоновано варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет, що утворений системою глобальної маршрутизації на множині з'єднань між вузлами, та обґрунтовано, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію комп'ютерної мережі. Запропоновано нові метричні характеристикі мережі, що походять з топологічних характеристик її вузлів та характеризують безпосередні складові ризику перехоплення маршруту – ймовірність перехоплення маршруту та коло його розповсюдження.

В монографії представлено методику зниження ризику перехоплення маршруту шляхом формування ефективних міжвузлових зв'язків. Методика включає опис способу отримання необхідних даних для розрахунку ефективності зв'язків, а також приклади програмної реалізації таких розрахунків.

Видання орієнтоване на спеціалістів з комп'ютерних систем та мереж, а також з інформаційної безпеки.

The monograph is devoted to the development of theoretical principles and methodology for increasing the security of the Internet topology from attacks on the global routing system. An analysis of methods of counteracting cyber attacks on a global routing system and responding to incidents with interception of routes has been carried out. An innovative representing of the Internet's topological space is proposed, which is formed by global routing system on a set of connections between nodes, and substantiated that cyber attacks against global routing system infract the Internet topology. New metric characteristic networks originating from the topological characteristics of its nodes are to characterize specifically the risk of route hijack - the likelihood of hijack and potential distribution area of the forged route.

The monograph provides a method for mitigating route hijack risk by forming effective node interlinks. The methodology includes a description of the ways for obtaining the necessary data to calculate the effectiveness of links, as well as examples of software implementation of such calculations.

The publication is oriented on computer systems and networks professionals, as well as information security specialists.

УДК УДК 004[413.3+738.5.057.4] : 519.173

ISBN 978-966-02-9929-0

ЗМІСТ

ПЕРЕДМОВА

Як відомо, існує умовний поділ комп’ютерних мереж на локальні та глобальні. Для глобальних мереж є типовим широкий територіальний розподіл вузлів, розташування в різних країнах та різне підпорядкування.

Маршрутизацією в комп'ютерних мережах називається процес пересилання логічно адресованого пакета від джерела в сторону пункту призначення через проміжні вузли. Принципи маршрутизації дозволяють досить чітко відокремити процеси локальної та глобальної маршрутизації, зокрема, в таких мережах, як глобальна мережа телефонного зв'язку, мережі, побудовані на архітектурі Frame Relay та ATM, а також мережа INTERNET (надалі – Інтернет), що була створена і досі розвивається як об'єднання комп'ютерних мереж. В Інтернеті розрізняють дві системи маршрутизації: внутрішня (внутрішньомережева, внутрішньодоменна) і зовнішня, (глобальна, міжмережева, міждоменна). Завдяки системі глобальної маршрутизації Інтернет став де факто найбільшою комп'ютерною системою, яка протягом 30 років довела свою масштабованість.

Сьогодні домінує тенденція децентралізації трудомістких обчислень та сховищ даних, а також перенесення поширених прикладних задач, властивих колись локальним мережам (в тому числі звичайного офісного програмного забезпечення) в так звані «хмари» – розподілені гнучко конфігуровані обчислювальні ресурси, часто разом з програмним забезпеченням, які беруться в оренду у Інтернет сервіс провайдерів нового типу. Продовжується тенденція геометричного зростання обсягів інформаційних ресурсів, понад усе – мультимедіа, до швидкості і якості передачі яких пред'являються високі вимоги з боку споживачів.

Протягом останніх років напрями «цифровізації» держави і суспільства, державних послуг, відносин між громадянином і державою, законодавчо визначено державними пріоритетами. Забезпечення безперешкодного доступу до суспільно значущих Інтернет-ресурсів, насамперед державних, є невід‘ємною частиною інформаційної безпеки та конкурентоздатності держави на світовому рівні. Тому на сьогоднішній день недостатньо надійна або недостатньо швидка взаємодія з мережею Інтернет негативно відбивається на взаємодії підприємства або організації з зовнішнім світом, на внутрішніх процесах, та, як наслідок, на конкурентоздатності.

Разом із визначенням пріоритетів розвитку технологій цифрової ери, також визначено і пріоритети безпеки цієї ери, а саме – кібернетичної безпеки, що визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Система глобальної маршрутизації в Інтернеті складається з *мережевих префіксів* – ідентифікаторів окремих комп’ютерних мереж, *автономних систем*

(*AS*) – груп з одного чи більше мережевих префіксів під загальним керуванням, та *протоколу маршрутизації,* який забезпечує обмін між AS інформацією про досяжність мережевих префіксів відповідно до закладеного алгоритму та додаткових адміністративно встановлених правил, що також мають назву «політика маршрутизації».

Протокол маршрутизації, який використовується для взаємодії між AS, має назву «протокол прикордонної взаємодії» (Border Gateway Protocol) версії 4, і широко відомий за скороченням BGP-4, або просто BGP (оскільки інших версій наразі не застосовується). В даній роботі буде показано, що саме за допомогою інформації, яку передає BGP-4, утворюється топологічний простір Інтернету $T := (V, M)$, де V – множина автономних систем, а M – сукупність маршрутів до мережевих префіксів, утворених протоколом BGP-4, де кожен з маршрутів є топологією на множині V.

Незважаючи на свою фундаментальну значущість, протокол BGP-4 має вади інформаційної безпеки, оскільки від початку базується на довірі між сусідніми BGP-системами. В протокол не закладено механізмів перевірки цілісності та автентичності даних про зв'язок між парою AS, про належність мережевого префікса до певної AS, що призводить до можливості несанкціонованої зміни шляхів пересилання пакетів з метою перехоплення інформації, дестабілізації роботи мережі або її частини, порушення доступу до певних інформаційних ресурсів і т.д. Такі кібернетичні атаки мають назву «перехоплення маршруту» і «витік маршруту».

Механізми атак спрямовані на утворення хибних маршрутів, що спричиняє втрату даних та несанкціоноване перехоплення інформації. Ці уразливості добре відомі і використовуються із зловмисними цілями. Так, с початком активної фази російської агресії проти України, ворожі кібервійська почали інтенсивно перемаршрутизовувати Інтернет-трафік українських користувачів за допомогою перехоплення маршрутів з метою прослуховування[1].

Вирішенням проблеми уразливості BGP-4 опікуються понад 25 років. Найбільші надії в запобіганні перехопленню маршрутів пов'язані із розробкою нового протоколу глобальної маршрутизації, здатного вирішити в повній мірі задачу валідації маршруту. Та процес розробки триває десятиліттями, а по завершенні розробки очікується не менш тривалий процес його стандартизації та глобальної імплементації.

Основною причиною неможливості розробки та впровадження уніфікованих систем захисту інформації, що реалізували б єдину політику безпеки для цілої мережі, є те, що Інтернет є основним і найхарактернішим прикладом глобальних комп'ютерних мереж, яким властивий широкий територіальний розподіл вузлів, розташування в різних країнах та різне підпорядкування.

[1] Першим про це повідомив Афтаб Сіддік (Aftab Siddiqui) в статті «Did Ukraine suffer a BGP hijack and how can networks protect themselves?», опублікованій на вебсайті MANRS: https://www.manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/

Існує два типи методів боротьби з атаками на систему глобальної маршрутизації. Перший напрям – реагування на інциденти, тобто, виявлення та інформування про несанкціоновані зміни в глобальній маршрутизації. Для цього суб'єкти глобальної маршрутизації використовують власні чи сторонні служби моніторингу глобальної маршрутизації, такі як BGPmon, QRATOR.Radar, ARTEMIS, для виявлення несанкціонованих змін атрибутів маршрутів. Розробці методів та засобів швидкого виявлення та реагування на перехоплення маршрутів присвячені дослідження К.Шрірама та Д.Монтгомері, П.Семпретіса та колег, Т.Макданіела, Дж.М.Сміта, М.Шухарда та інших. Цей напрям здатен дієво знизити збитки в разі перехоплення маршруту, зменшивши час від початку інциденту до його виявлення, та ніяк не впливає на саму можливість виникнення інциденту.

Другий напрям – запобігання інцидентам. Напрям запобігання атакам на систему глобальної маршрутизації здебільшого представлений методами криптографічного захисту цілісності маршрутів. В цьому напрямку відомі публікації Р. Буша, Р.Ауштейна, А.Азимова, Е.Богомазова та інших. Розробці нового протоколу присвячені наукові роботи С. Кента, Ч.Лінн, К. Сео, Ю. Хагі та інших. Дієвим на сьогодні напрямом протидії перехопленню маршрутів є методи криптографічного захисту. Вони потребують публікування політики взаємодії між AS про наявність зв'язку та ступінь («провайдер-клієнт») для можливості валідації маршрутів за допомогою цієї інформації, та подальшої верифікації цієї інформації суб'єктами глобальної маршрутизації шляхом використання інфраструктури публічних ключів (Resource Public Key Infrastructure, RPKI).

Впровадження RPKI дозволяє захищати електронним підписом, та, відповідно, виконувати валідацію атрибутів маршруту. Цей метод має наступні недоліки: наразі дозволяє валідацію лише одного атрибуту маршруту – його джерело (route origin), а отже не охоплює всі сценарії атак з перехопленням маршруту. Технологічна складність використання RPKI для валідації зупиняє широке впровадження. Крім того, централізоване зберігання сертифікатів несе нові ризики інформаційної безпеки, і як мінімум є новою єдиною точкою відмови (single point of failure) для глобальної маршрутизаціїі. Ці недоліки мають бути вирішені в новому протоколі глобальної маршрутизації (робоча назва – «BGPSec»), та, поряд з невизначеністю критеріїв достатності засобів для надійного захисту маршрутів, дослідники зауважують майбутні проблеми його глобального впровадження.

Питанням розвитку, тестування та глобального впровадження нового захищеного протоколу глобальної маршрутизації присвячені секції на міжнародних конференціях DefCon, Internet Measurment Conference (IMC), Інституту інженерів електротехніки та електроніки (IEEE) та багатьох інших. Цьому питанню приділено увагу в заключному звіті дослідницької комісії Міжнародного союзу електрозв'язку (ITU) за період 2014-2017 років.

Визначити «правильну» систему маршрутизації надзвичайно складно, і набагато легше зрозуміти, коли і де виникає аномалія, і реагувати відповідно. Отже, підвищення захищеності топологічного простору глобальної

комп'ютерної мережі Інтернет від кібернетичних атак на систему глобальної маршрутизації *залишається актуальною науково-прикладною проблемою*.

Сучасна інформаційна безпека базується на управлінні ризиками. Для ризику, пов'язаного з уразливими глобальної маршрутизації в комп'ютерній мережі Інтернет, важливим фактором є топологія, і це показано в роботі. Аналізуючи топологію, можна оцінити ризик, пов'язаний з уразливими глобальної маршрутизації. Синтезуючи нову топологію, можна управляти цим ризиком. Кількісна оцінки ризику, пов'язаного з глобальною маршрутизацією, може бути важливими критерієм оцінки ефективності топології міжмережевих зв'язків Інтернет.

Дослідженням топологічних властивостей складних мереж та, зокрема, Інтернета, приділено увагу в працях Р. Альберта та А.-Л. Барабаші, С. Строгаца та Д. Уоттса, М. Фалутсоса та П. Фалутсоса, М. Ньюмана, П. Болді, І. Євіна, О. Олємського, Д. Ланде, А. Снарського, Ш. Джина, Д. Алдерсона та інших вчених. Напрям розвитку теорії і практики оцінювання ризику в кібербезпеці, забезпечення живучості та підвищення захищеності розподілених комп’ютерних систем і мереж розвинуто, зокрема, в працях В. Мохора, О.Додонова, О.Корченка, О.Новікова, К. Юдіна, С.Гончара, F.D. Kramer, O. Borchert, K. Sriram, D. Montgomery та багатьох інших.

Необхідність розвитку методології як сукупності методів, моделей, практик з застосування ризик-орієнтованого підходу до підвищення захищеності інформації підчас міжмережевого обміну визначила тему даної дисертаційної роботи.

В цій книзі запропоновані методи аналізу та удосконалення топології міжмережевих зв'язків глобальної комп'ютерної мережі Інтернет, що знижують можливості нав'язування хибного уявлення про топологію. При цьому критерієм ефективності топології проти атак на глобальну маршрутизацію послуговує оцінка ризику як міра захищеності інформації.

ГЛАВА 1.
ГЛОБАЛЬНА МАРШРУТИЗАЦІЯ В INTERNET

1.1. Становлення сучасної системи глобальної маршрутизації мережі Інтернет

Глобальну комп'ютерну мережу Інтернет можна уявити, як сукупність мережевих вузлів (хостів), з'єднаних за допомогою засобів передачі даних та комутації. Керування цією сукупністю хостів, а також засобами телекомунікацій, що разом складають мережеві ресурси глобального Інтернету, є неоднорідними та розподіленими між багатьма адміністраторами [1].

Багато років поспіль в Інтернеті спостерігається геометричне зростання обсягів інформаційних ресурсів, понад усе мультимедіа, до швидкості і якості передачі яких пред'являються високі вимоги з боку користувачів. Ще на початку 1980 років розробники Інтернет-технологій бачили тенденцію щодо швидкого зросту мережі, неструктурованого збільшення кількості шлюзів, які були під керуванням зовсім різного програмного забезпечення та не підлягали типовому обслуговуванню. Передбачуваними наслідками такого зросту стали:

– багаторазове збільшення потоків інформації, пов'язаної з передачею та обробкою таблиць маршрутизації;

– неможливість обслуговування Інтернету як єдиної системи через неможливість ізоляції помилок, збоїв маршрутизації;

– через різноманітність мережевого обладнання, алгоритмів маршрутизації та програмного забезпечення в мережах, які взаємодіють через Інтернет, неможливо забезпечити пропоновані зміни у всій мережі одночасно, бо це потребує адаптації до кожної окремої системи.

Тоді й виникла ідея увести поняття домену, або автономної системи, єдиної частки мережі, із будь-яким внутрішнім устроєм, але стандартними зовнішніми маршрутизаторами, які реалізують стандартні протоколи взаємодії з іншими автономними системами. Автономні системи повинні мати можливість не тільки взаємодіяти одна з одною, але й забезпечувати транзитні функції для автономних систем, які не мають безпосереднього зв'язку, аби забезпечити для кінцевого користувача „прозорість" Інтернету як єдиної мережі.

Було запропоновано, що мережеві ресурси, підконтрольні одній адміністрації, утворюють домен [1]. Для підтримки автономії кожного домену маршрутизація має складатись з двох різних компонентів: внутрішньодоменної (внутрішньої) маршрутизації та міждоменної (зовнішньої) маршрутизації. Внутрішньодоменна маршрутизація забезпечує підтримку для передачі даних між хостами, де дані циркулюють в межах засобів передачі та комутації одного домену. Міждоменна маршрутизація забезпечує підтримку передачі даних між хостами, де дані проходять засоби передачі та комутації, що охоплюють декілька доменів. Пристрої, які пересилають пакети через кордони доменів,

називаються прикордонними маршрутизаторами (border routers). Пристрої, відповідальні за обмін інформацією про маршрути між доменами, називаються серверами маршрутів (route servers). Частіше функції маршрутизатора і сервера маршрутів об'єднуються в одному пристрої.

На теперішній час термін «домен» стосовно маршрутизації замінено на термін «автономна система» [2].

У 1983 році протоколи TCP/IP було стандартизовано як військові стандарти. В університеті Берклі, Каліфорнія, ці протоколи було інтегровано в операційну систем BSD UNIX. У 1985 році до існуючої мережі приєдналась наукова мережа Національної наукової фундації (NSF) – NSFnet. З того часу термін Інтернет став загальновживаним.

Велика кількість вузлів Інтернет стала проблемою для керування мережею. Тому з 1986 р. в NSFNet застосовувалась трирівнева мережна архітектура: місцеві локальні мережі, мережі кампусів, підключались до регіональних мереж; регіональні в свою чергу підключались до опорної мережі (backbone), що підтримувалась 6 загальнонаціональними суперкомп'ютерними центрами NSF, як наведено на рис. 1.1.1.

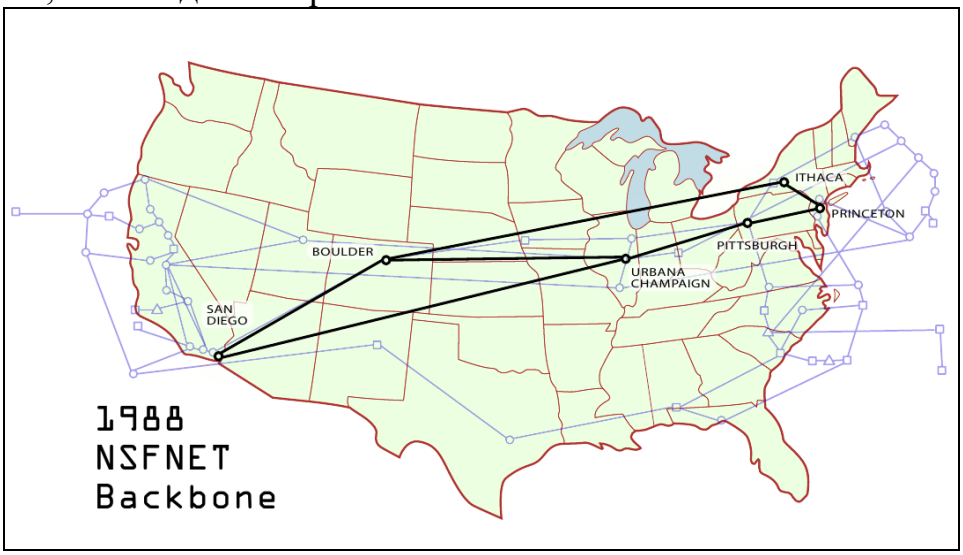


Рисунок 1.1.1 – Мережа NSFNet в 1986 – 1988 роках[1]

До backbone входили так звані місця доступу до мережі (Network access points, NAP). За термінологією NSFNET, NAP – це комплекс з одного чи більше швидкісних комутаторів, до яких під'єднується певна кількість маршрутизаторів для обміну трафіком. Всі мережі при підключенні до NAP автоматично отримують дозвіл обміну трафіком з іншими мережами. Пропускна спроможність мережі, що підключається, має бути відповідною до обсягів трафіку, який очікується із вже підключеними мережами.

В 1987 році консорціум за участі Merit (міжуніверситетської комп'ютерної дослідницької мережі), IBM та MCI виграв грант NSF на реінжиніринг та обслуговування NSFNet. В ході робіт ядро мережі, що складалось з каналів зі швидкістю передачі T0 (56 кбіт/с) було перебудовано на

[1] Джерелом ілюстрацій рис. 1.1.1 – 1.1.3 є вебсайт Каліфорнійського університету Сан Дієго (www.ucsd.edu)

канали T1 (1,5 Мбіт/с). Канали T1 об‘єднали 6 суперкомп‘ютерних центрів та ще 13 вузлів мереж по всій території США (рис. 1.1.2).

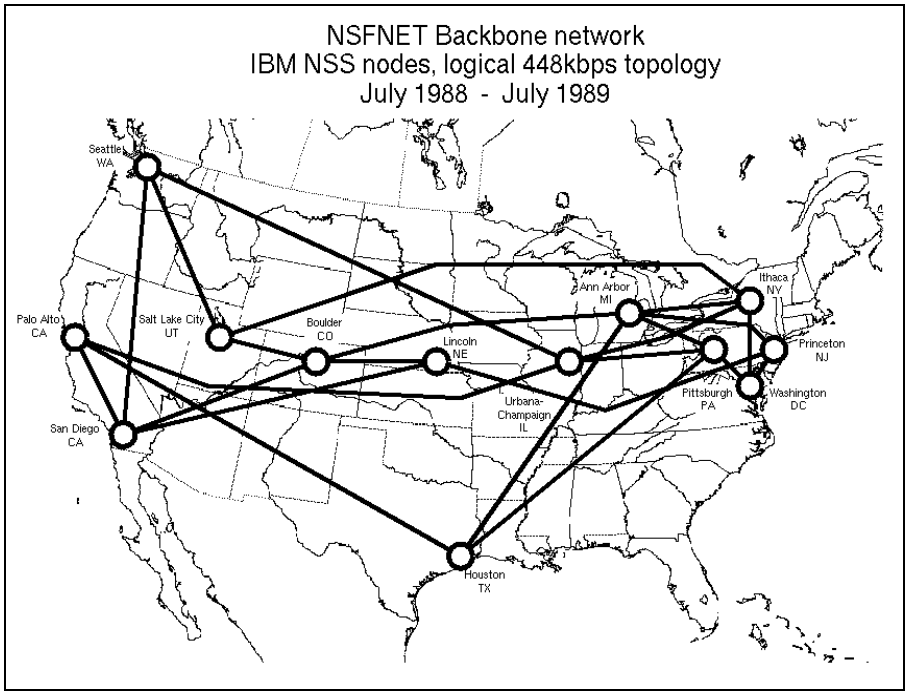


Рисунок 1.1.2 – T1-мережа NSFNet в 1988 – 1989 роках

За словами Елізи Геріх, віце-президента ICANN (нинішнього керівного органу Інтернету), яка особисто приймала участь в цих роботах, така інфраструктура мала б слугувати становим хребтом мережі протягом 5 років. Але вже за 18 місяців, у 1991 році, обсяги трафіку змусили переводити канали T1 на T3 – 45 мбіт/с (з виступу на форумі RIPE NCC Regional Meeting, Москва, 29.09–01.10.2010). Схему нової мережі наведено на рис.1.1.3.

Точки доступу (network access point – NAP) спочатку були розділені на державні (федеральні – FIX) та комерційні (CIX). Приблизно з 1994 року такий розподіл зник. Разом з цим, зник розподіл користувачів на державні, академічні та комерційні організації. Поняття NAP та вимоги до них були формалізовані, і це відкрило шлях до побудови нових точок.

Але завжди існувала можливість взаємного підключення вузлів поза межами NAP, тому топологія Інтернет в результаті розвитку отримала так звану безмасштабну структуру.

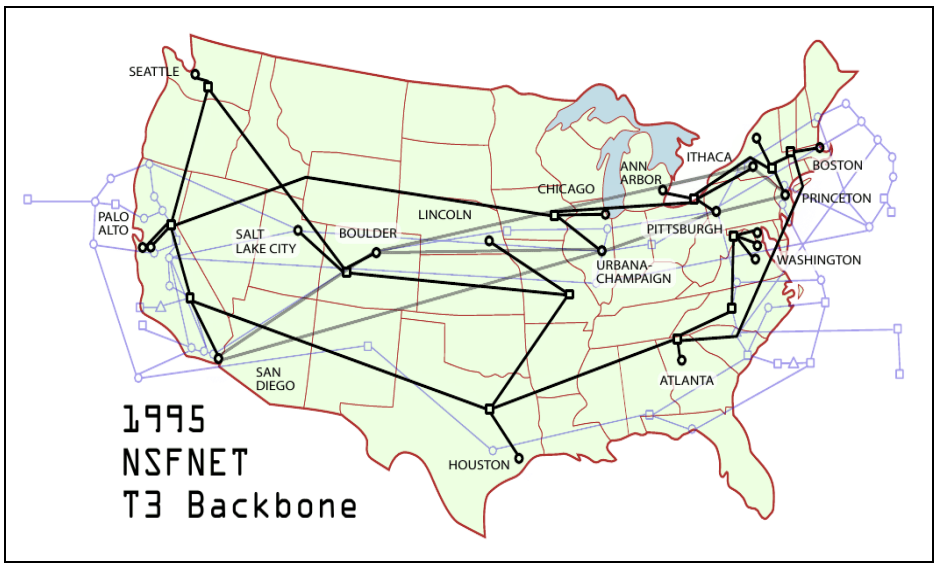


Рисунок 1.1.3 – Т3-мережа NSFNet в 1992 – 1995 роках

В результаті розробки та публікації «NSFNet Acceptable Use Policy» та відкритості точок доступу Інтернет набула стрімкого розвитку. Тому вже у 1995 році близько 44% префіксів в таблиці маршрутизації були з поза меж США і глобальна комп'ютерна мережа набула всіх ознак всесвітньої.

1.2. Переваги та недоліки сучасної системи глобальної маршрутизації

Як відомо, 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 якому розрізняють дві системи маршрутизації: внутрішня (внутрішньомережева, intra-domain) і зовнішня, (глобальна, міжмережева, inter-domain). Для глобальної маршрутизації діють по всій мережі єдині правила і протоколи обміну інформацією.

В Інтернеті існує система глобальної маршрутизації, яка складається з *мережевих префіксів* – ідентифікаторів окремих комп'ютерних мереж, *автономних систем* (*AS*) – груп з одного чи більше мережевих префіксів під загальним керуванням, та *протоколу маршрутизації* BGP-4 [3], який забезпечує обмін між AS інформацією про досяжність мережевих префіксів відповідно до закладеного алгоритму та додаткових адміністративно встановлених правил, що також мають назву «політика маршрутизації». Автономна система (AS) – це комп'ютерна мережа або сукупність мереж під загальним управлінням. Суб'єктами глобальної маршрутизації є AS.

Як відомо, маршрутизація в складових мережах – процес мережевого рівня. Особливістю і важливою перевагою маршрутизації в Інтернеті і взагалі мережах, що функціонують на базі протоколів 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 виключно виходячи з власних даних, наявних на момент прийняття рішення; до таких даних відноситься список активних мережевих інтерфейсів, локальні метрики (правила, переваги, звані політикою маршрутизації), і таблиця маршрутизації, створена з адміністративно заданих правил, інформації від сусідніх пристроїв, статусу мережевих інтерфейсів і т.д.;
2) зменшення розмірності адресного простору з допомогою його агрегування в підмережі (subnets) за допомогою 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 досить знати мережеву адресу шлюзу (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 по протоколу BGP-4. Дві головних властивості – визначення маршруту тільки на один крок вперед і агрегація адрес в префікси – притаманні і глобальної маршрутизації. Останні три десятиліття безперервного зростання Інтернет і розвитку технологій, що базуються на використанні Інтернет, безумовно показали масштабованість системи глобальної маршрутизації.

У той же час, разом з масштабами мережі зростають загрози інформаційній безпеці, пов'язані з глобальною маршрутизацією. Дані загрози відносяться до всіх суб'єктів, чиї інформаційні активи взаємодіють з глобальною комп'ютерною мережею Інтернет. Обидві властивості глобальної маршрутизації – визначення маршруту тільки на один крок вперед і агрегація адрес в префікси – експлуатуються при атаках на маршрутизацію. Це відбувається тому, що, незважаючи на свою фундаментальну значимість, протокол BGP-4 заснований на довірі між з'єднаними мережами, приймаючи отриману від них інформацію за істину. Більш того, довіра ця має транзитивну властивість – сусідні BGP-системи довіряють одна одній, ті, в свою чергу, довіряють своїм сусідам і в підсумку всі довіряють всім. Функціональну схему протоколу BGP-4 наведено на рис. 1.2.1. На ній виокремелено проблемну зону – відсутність механізмів валідації вхідної інформації.

На рівні протоколу BGP-4 немає перевірок достовірності даних, перевірок авторства анонсів, або повноважень робити певний анонс. Також немає механізмів перевірки автентичності атрибутів шляху, які можуть вплинути на перевагу маршруту. Тобто, вузол мережі (на рівні глобальної маршрутизації він називається автономною системою – AS) може оголосити

про те, що знає маршрут до префікса, до якого не має відношення; що маршрут через нього – коротше, а отже – краще; що певна підмережа підключена безпосередньо до нього.

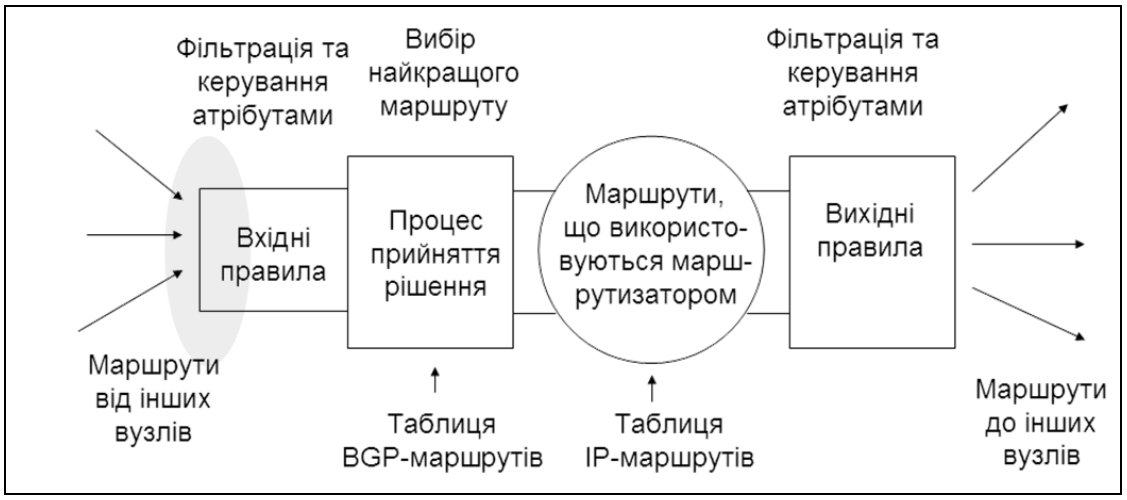


Рисунок 1.2.1 – Функціональна схема протоколу маршрутизації BGP-4

Це вже неодноразово приводило і продовжує призводити до випадків так званого перехоплення маршрутів (route hijacking, prefix hijacking, BGP hijacking). Колись ці перехоплення носили характер випадкової помилки конфігурації, але можна впевнено сказати, що протягом 5 років зросла частка ворожих дій, тобто – атак, для реалізації яких використовувався перехоплення маршрутів.

Визначити «правильну» систему маршрутизації надзвичайно складно, і набагато легше зрозуміти, коли і де виникає аномалія, і реагувати відповідно. «Завдання спроби побудувати безпечну систему BGP нагадує спробу зупинити спалення будинків. Ми могли б спробувати домогтися поведінки як будівельної галузі, наших меблів та фурнітури, так і нашої поведінки, яка унеможливлює загоряння будинку. Або ми могли б мати пожежну команду, щоб ліквідувати пожежу якомога швидше. Протягом багатьох років ми обирали останній варіант як прийнятний компроміс між вартістю та безпекою» [4].

Паралель із безпекою BGP полягає в наступному. Була б ідеальна ситуація, коли не можна було б продукувати хибну інформацію в BGP. Де будь-яка спроба «синтезувати» інформацію BGP може бути легко визначена та відкинута як неправдива. Але це дуже висока планка для зустрічі. І приблизно тридцять років зусиль показують, наскільки важким є насправді це завдання.

Це важко, бо ніхто конкретний за це не відповідає. Це важко, тому що неможливо перевірити BGP, оскільки немає стандартних довідкових даних для порівняння. Неможливо арбітрувати суперечливу інформацію BGP, оскільки немає стандартної контрольної точки. Не існує облікових даних, які дозволяють порівнювати оновлення BGP-маршрутів із початковим введенням маршруту, оскільки BGP – це покроковий протокол.

При цьому існує також проблема, що в BGP дуже легко нашкодити. Випадкова неправильна конфігурація в BGP, як видається, є постійною

проблемою, і неможливо визначити різницю між нещасним випадком та навмисною спробою ввести в систему маршрутизації неправдиву інформацію.

Таким чином, на сьогодні та в осяжній перспективі існуючі методи та засоби не здатні в повній мірі забезпечити захист від перехоплення маршрутів і загрози інформаційній безпеці в наслідок атак на глобальну маршрутизацію є невідворотними.

Попри різноманіття сучасних кібератак, найбільш небезпечними поки що вважаються найбільш поширені – це атаки, спрямовані на відмову (Denial Of Service) і атаки, спрямовані на здирництво (Ransomware) [5]. Ці атаки є комплексними, бо мають принаймні дві фази: фазу інфікування та активну фазу. Фаза інфікування є відносно довгою, в деяких випадках вона триває декілька діб, а в деяких – місяці, в залежності від вибірковості зараження. У випадку атак класу DDoS інфіковані елементи однієї підмережі (так звані боти) часто використовуються для атак на іншу мережу. У випадку атак класу Ransomware активна фаза атаки спрямована безпосередньо на користувачів тієї мережі, де ці боти «оселилися». За даними Cybersecurity Ventures, втрати від ransomware в 2017 році сягнули 5 мільярдів доларів США [6]. Але в останні роки все частіше інциденти з глобальною маршрутизацією в Інтернеті перетворюються на ще більшу кіберзагрозу. Поки що жодного разу офіційно не заявлено, що ці інциденти були атаками. Втім, масштаб цих інцидентів на кілька порядків перевершує широко відомі атаки класу DDoS і Ransomware. Таким може стати і масштаб збитку, оскільки атака на глобальну маршрутизацію здатна забезпечити шкідливий вплив на мільйони мережевих пристроїв (і користувачів) значно меншими зусиллями, ніж згадані вище популярні атаки.

1.3. Кібератаки на систему глобальної маршрутизації

Перші спроби дати загальне визначення для інцидентів з глобальною маршрутизацією відбулись пічдчас розробки методів протидії в міжнародній групі з розробки Інтернет-стандартів Internet Engineering Task Force (IETF).

«Витік маршруту – це поширення анонсів маршрутизації за межами їх передбачуваного обсягу. Тобто оголошення отриманого з AS маршруту BGP до іншої AS, яке є порушенням передбачуваної політики приймача, відправника та (або) однієї з AS уздовж попереднього шляху. Передбачувана політика зазвичай визначається набором місцевих політик перерозподілу та фільтрації, розподілених між залученими AS. Найчастіше ці передбачувані політики визначаються в термінах попарних відносин між AS (наприклад клієнт, провайдер IP-транзиту, або партнер – peer).

«Результатом витоку маршруту може бути перенаправлення трафіку через неочікуваний шлях, який може призвести до підслуховування або аналізу трафіку, а також може призвести до перевантаження або чорній дірі. Витоки маршруту можуть бути випадковими або зловмисними, але частіше за все виникають від випадкових помилок» [7].

Загальна форма витоку маршруту виникає, коли AS – клієнт, що користується транзитами від декількох AS – провайдерів дізнається про оновлення префікса від одного транзитного провайдера та пересилає ці маршрути до іншого транзитного провайдера у порушення очікуваної політики маршрутизації, а далі, другий транзитний провайдер не виявляє витоку маршруту та розповсюджує ці оновлення до своїх клієнтів, пірів та транзитних провайдерів.

Але аналіз задокументованих інцидентів, наведений в розділі 3, свідчить, що кібернетичні атаки з перехопленням чи витоком маршрутів мають більше варіантів реалізації.

1) Захоплення префіксу, коли автономна система анонсує у якості джерела адресний простір що не належить їй. При виборі маршруту BGP віддасть перевагу більш короткий, вимірюваний числом мереж між джерелом і одержувачем, маршрут. Таким чином цей маршрут буде конкурувати з істинним (рис.1.3.1). Така атака може бути швидко виявлена, бо з точки зору «полісі» глобальної маршрутизації, наявність двох джерел в одного префікса є помилкою.
2) Захоплення маршруту, коли вузол ретранслює легально отриманий анонс «чужого» адресного простору, пропонуючи транзит через себе. Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, «джерело» не підмінюється і виявити такий інцидент складніше. Зазвичай він виявляється у випадку неспіввідносності пропускної здатності мережі «загарбника» і обсягу трафіку, який він перемикає на себе в результаті ретрансляції чужих маршрутів. Прикладом такого порушення є ситуація, коли мережа-клієнт підключена до двох Інтернет-провайдерів та починає реанонсіровать маршрути, отримані від одного провайдера, іншому провайдеру. Таким чином мережа-клієнт сама стає провайдером послуги транзиту, часто з сумними для себе наслідками – обсяг перенаправленого трафіку набагато перевищує ресурси мережі.
3) Захоплення підмереж, коли анонсуються більш специфічні префікси. При виборі маршруту BGP воліє той, який вказується більш специфічним префіксом, і таким чином атакуючий виграє незважаючи на топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру, захоплення має глобальний ефект (рис. 1.3.2).
4) Захоплення нерозподіленого або невикористаного адресного простору. В цьому випадку анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.
5) Перенаправлення трафіку. В цьому випадку трафік спочатку перехоплюється за допомогою анонсування хибного маршруту, і потім повертається його легітимному отримувачу.

Наслідки цих атак можуть бути різними. Захоплення маршруту призводить до перетягування трафіку, призначеного «захопленої» мережі, який, як правило, потім відкидається. Така стратегія має назву створення «чорної

діри» (blackholing). Тобто відбувається DoS-атака на всі сервіси мережі. У цю категорію потрапляє більшість помилок конфігурації.

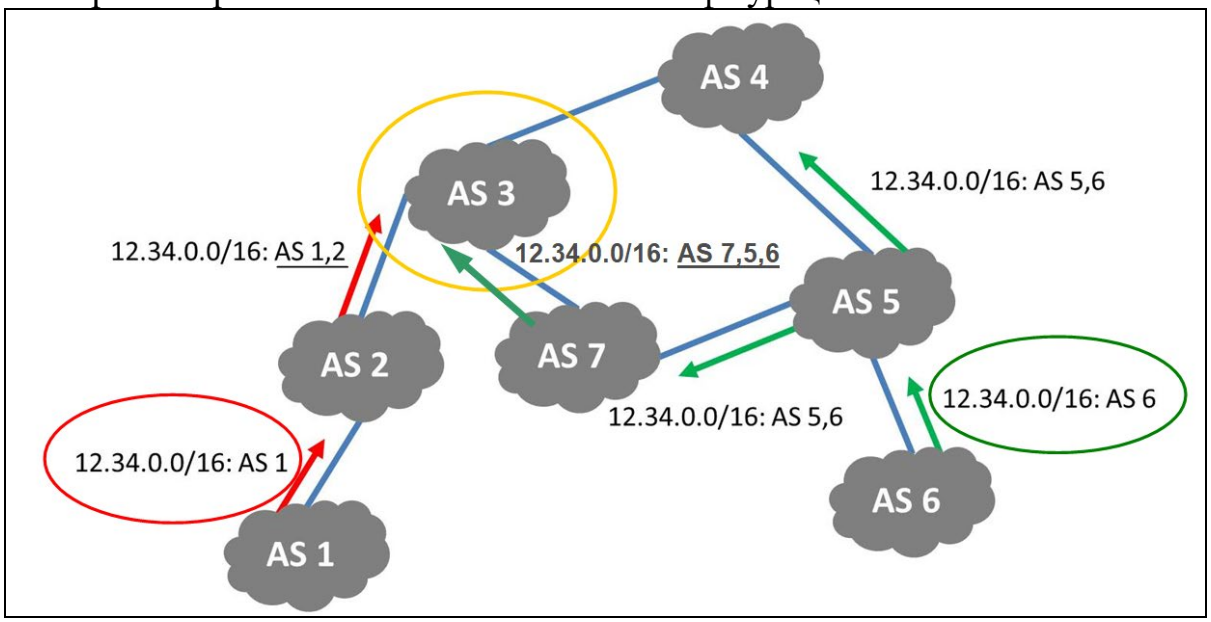


Рисунок 1.3.1 – Перехоплення маршруту шляхом пропонування коротшого шляху. AS6 надсилає істинний анонс, AS1 – хибний, який конкурує з істинним за критерієм коротшого шляху. Для AS3 хибний маршрут матиме перевагу через меншу довжину

Якщо атака анонсує фрагмент нерозподіленого адресного простору («нічиї» мережі), вона може бути використана для короткострокової генерації не просто трафіку, а доставки шкідливого контенту, в елементарному випадку – для розсилки спаму. Хоча в цьому випадку система маршрутизації як така не піддається атаці, даний метод широко використовується в так званих атаках на відображення. У цьому випадку зворотний трафік, наприклад, відповіді на споконвічні запити, спрямовується не до істинного джерела, а до одержувача, чию адресу був сфабрикований. Як правило, такі атаки використовують протокол без встановлення з'єднання UDP (User Datagram Protocol) і засновані на ефекті посилення, коли невеликі запити від багатьох джерел породжують відповіді значно більшого розміру. Одна з критичних систем, в основному використовує UDP і підвладна атакам такого роду, є DNS.

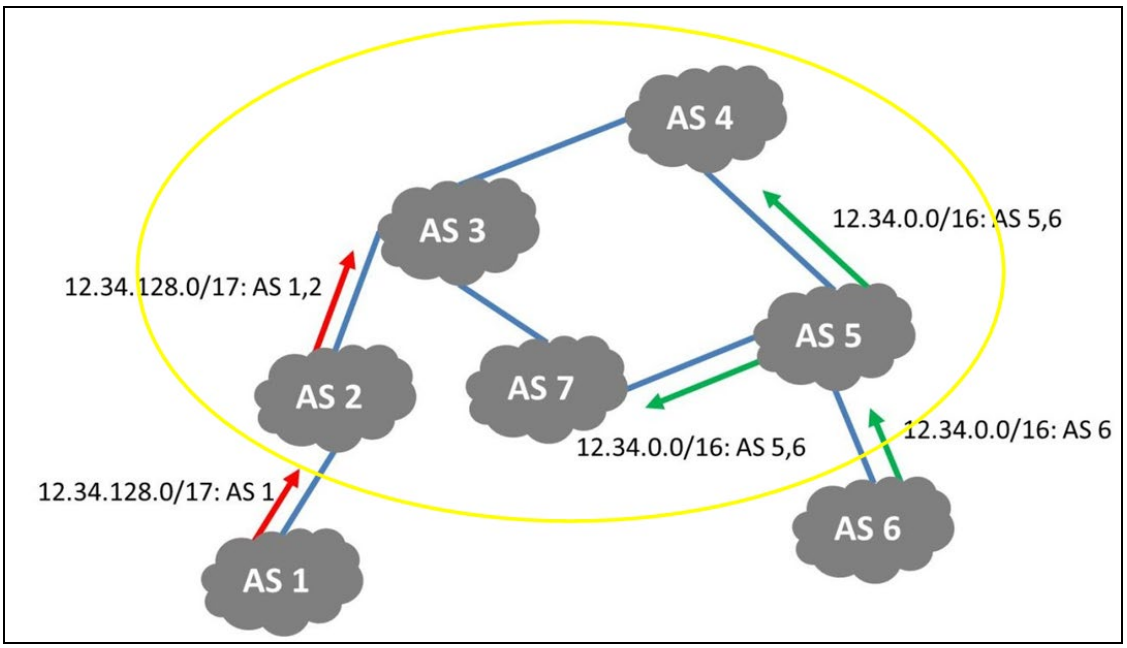


Рисунок 1.3.2 – Захоплення маршруту через анонсування більш специфічного префіксу. AS6 надсилає істинний анонс, AS1 – більш специфічний та перехоплює трафік в глобальному масштабі

Інший варіант стратегії – перенаправлення трафіку. Трафік йде не в «чорну діру», а перехоплюється і аналізується. Іноді атака ще глибже, і перехоплений трафік не тільки не йде в «чорну діру» і не тільки аналізується, але після перехоплення повертається знову в Інтернет, щоб бути доставленим істинному одержувачу. Через це таку атаку важче виявити. Метою може бути не тільки "підслуховування", але і модифікація переданих даних. У більш витонченому вигляді захоплення маршруту може бути спрямований на захоплення деякого інформаційного ресурсу, наприклад веб-сайту, з наданням користувачам підробленого сайту. Зловмисники часто використовують такий вид атаки для пасивної розвідки ресурсів і потенційно слабких місць мережі організації. Прикладом такої атаки є атака Пілосова-Капели [8].

1.4. Відомі методи протидії кібератакам на систему глобальної маршрутизації

1.4.1. Загальні умови безпеки глобальної маршрутизації

Безпека, тобто процес захисту, системи маршрутизації потребує постійного визначення відповідей на такі питання:

- чи є мережевий префікс, отриманий в повідомленні BGP, чинним, тобто чи представляє легітимно розподілений адресний простір і право на його використання);
- чи є автономна система-джерело маршруту правомочним власником префікса;

- чи відповідає атрибут AS_PATH, отриманий в повідомленні BGP, дійсному шляху, який пройшов анонс цього мережевого префіксу в системі глобальної маршрутизації Інтернет.

Проаналізуємо, якими засобами володіє суб'єкт глобальної маршрутизації для вирішення цього завдання. Як вже було зазначено, сам протокол BGP не дозволяє здійснити перевірку справжності маршрутів, отриманих від іншої мережі. Основу рішення становлять бази достовірної інформації про розподіл адресного простору, про маршрути і їх легітимні джерела.

Таких баз існує три типи:

- бази даних розподілених номерних ресурсів регіональних Інтернет-реєстрів (Regional Internet Registry, RIR), часто згадувані як «сервіс whois»;
- реєстри маршрутизації IRR (Internet Routing Registry);
- репозиторії інфраструктури зберігання публічних ключів від ресурсів (Resource Public Key Infrastructure, RPKI).

1.4.2. Засоби веріфікації даних про маршрутизацію

Для протоколу IP, який забезпечує зв'язність мережевого рівеня в Інтернеті, важливо аби кожнен підключений пристрій мав мати унікальну адресу, тому важливо, щоб розподіл IP-адрес був ретельно зареєстрований аби уникнути конфліктів.

Спочатку глобальний реєстр IP-адрес був просто переліком діапазонів IP-адрес, а також деталей організацій, для яких вони були виділені. Довгий час ця важлива роль була формалізована у вигляді організації IANA – Internet Assigned Numbers Authority. Все одно, із зростанням Інтернету по всьому світу, стало зрозуміло, що навіть IANA недостатньо масштабована, щоб задовольнити попит на адреси або вміти обслуговувати широкий спектр різних регіональних потреб. У 1992 році Internet Engineering Task Forces (IETF) рекомендувала, щоб ресурси інтернет-ресурсу управлялись допоміжними організаціями на регіональному рівні. Як наслідок, були створені регіональні інтернет-реєстри (RIR) для прийняття цієї ролі регіонального розподілу та управління у співпраці з IANA. Сьогодні існує п'ять RIR:

- APNIC в регіоні Східної Азії та Тихого Океану;
- ARIN в Північній Америці;
- RIPE NCC в регіонах Європи, Азії та Ближнього Сходу;
- LACNIC в Латинській Америці;
- AfriNIC в Африці.

Протягом двох десятиліть ця структура забезпечила систему управління номерних ресурсів, яка є масштабованою, ефективною, стабільною, відкритою та справедливою. Це є важливим фактором забезпечення сталості функціонування та масштабування Інтернету.

Кожен з RIR надає публічний доступ до своїх реєстрів, які дозволяють встановити легітимність використання того чи іншого блоку мережевих адрес, його поточного власника (не мається на увазі право власності) та прив'язку до певної AS.

Отже, дані RIR теоретично дозволяють компенсувати брак таких функцій протоколу BGP-4: виявити маршрути до неіснуючих мережевих префіксів (які належать до нерозподіленого адресного простору), а також легітимність анонсування маршуту до певного мережевого префіксу певною AS.

Політика маршрутизації – це набір правил, за якими автономна система приймає рішення стосовно маршрутизації. Обмін цими правилами з іншими автономними системами (за допомогою протоколів зовнішньої маршрутизації) також є частиною політики маршрутизації. Протокол маршрутизації BGP-4 не містить істотної функції, а саме – не має засобів повідомлення "сусідів" щодо власнолї політики імпорту, експорту та реекспорту анонсів. Для вирішення цієї проблеми у 1995 році був заснований Реєстр маршрутизації в Інтернеті (Internet Routing Registry, IRR).

Мета IRR – забезпечити обмін між операторами мережі актуальною інформацією з маршрутизації та, таким чином, сприяти стабільності та цілісності маршрутизації Інтернет в цілому. IRR складається з декількох баз даних, в яких оператори публікують власні політики маршрутизації та анонси таким чином, що інші оператори можуть будувати свої вхідні та вихідні фільтри на основі даних IRR. За допомогою IRR топологія Інтернет стала більш наглядною. Суть IRR полягає в наступному: мережеві оператори реєструють в базі даних свою політику маршрутизації, а саме з ким і як мережа взаємодіє, і мережеві префікси, які мережа використовує і анонсує в Інтернет. Для опису політик використовується формальна мова RPSL. Також існує інструментарій для програмування, найбільш відомий з яких IRRToolset, який дозволяє автоматизувати конфігурацію маршрутизації провайдера за даними IRR.

Інформація з маршрутизації в IRR публікується на сервері маршрутів (routing information server, RIS) та зберігається в об‘єктах за номером AS (aut-num object). Інформація в об‘єкті показує як певна мережа маршрутизується в Інтернеті. Будується інформація на основі угод про взаємодію між AS з використанням понять import та export, які відображають зв’язки.

Слід зазначити, що записи в полі members на сторінці в БД можуть бути двох типів:

- безпосередньо номери автономних систем;
- as-set – об’єднання автономних систем (зазвичай as-set це провайдер, який обслуговує клієнтів).

Дані про взаємодію автономних систем, представлені в RIS, є найбільш загальними. Їхні особливість в тому, що вони відображають саме політику маршрутизації, але не містять даних про стан взаємодії між вузлами в певний момент часу. Можна сказати, що вони відображають можливість транзиту трафіку однієї автономної системи через іншу, але не відображають факту – чи

є такий транзит в даний момент. Загалом, в даних IRR міститься інформація про кількість зв‘язків, що на 20-50% перевищує справжню, яку можна дослідити аналізом таблиць BGP-маршрутизаторів [9]. Реєстрація інформації про взаємодію учасниківв глобальної маршрутизації в IRR є добровільною.

IRR відображають вельми неповну картину, так як реєстрація даних в цих базах даних суто добровільна. Багато операторів з різних причин не приділяють уваги роботі з IRR, частина операторів не реєструє через небажання розголошувати свою політику. Ті ж, хто все ж зареєстрував свою політику, не завжди підтримують актуальність даних. Проблема в тому, що хоча ця діяльність служить на благо спільної справи – безпечної системи маршрутизації, користь для самого провайдера не завжди відчутна. Необхідність будувати та підтримувати в актуальному стані правила маршрутизації на основі політик, опублікованих в мільйонах записів в різних базах даних викликає складнощі в суттєвої частини учасників глобальної маршрутизації. Для так званих провайджерів вищего рівня (Tier I) це питання масштабу даних. Для протилежної ланки – кінцевих провайдерів – часто бракує досвіду та розуміння. Неповнота і ненадійнісь даних, а також погана масштабованість підходу робить IRR малопридатними для перевірки достовірності всіх маршрутів в глобальному масштабі. IRR є досить зручним інструментом лише на кінцевому ланцюжку – для автоматизації побудови фільтрів у Інтернет-провайдера стосовно підключених кінцевих мереж.

1.4.3. Використання інфраструктури публічних ключів системи маршрутизації (RPKI)

З огляду на недоліки IRR, вже в кінці 90-х технічне співтовариство почало працювати над створенням більш надійної інформаційної системи, заснованої на цифровий сертифікації номерних ресурсів. Система отримала назву RPKI (Public Key Infrastructure, PKI). Її елементами є сертифікати інтернет-ресурсів. Як і будь-яка система PKI, RPKI має ієрархічну структуру з кореневим сертифікатом. Кореневий сертифікат в якості списку номерних ресурсів охоплює весь адресний простір IPv4, IPv6 і автономних систем. За допомогою цього сертифіката можуть бути згенеровані сертифікати RIR відповідно до фактично розподіленим адресним простором. В даний час RIR забезпечують власні кореневі сертифікати, таким чином адресний простір Інтернету розподілений на п'ять ієрархічних структур RPKI [12, 13].

Система RPKI має суттєві переваги над IRR:

- дані про розподілених номерних ресурсах надаються в стандартній формі цифрових сертифікатів зі стандартними розширеннями стандарту X.509
- достовірність і актуальність даних може бути перевірена з використанням криптографічних засобів третіми особами: для перевірки необхідна конфігурація довіри тільки до одного сертифікату – так званої точки довіри (Trust Anchor, TA);

– сертифікати ресурсів можуть використовуватися їх власниками (власниками адресного простору) для, наприклад, електронної авторизації певних автономних систем для анонсування цього адресного простору, виконуючи, таким чином, функцію об'єктів route традиційних IRR.

RIR здійснюють сертифікацію ресурсів, які вони розподіляють локальним реєстрам (Local Internet Registry, LIR) [15]. Локальні реєстратури можуть здійснювати подальший розподіл і відповідну сертифікацію. Мережеві оператори, багато з яких є локальними реєстрами, фактично використовують адресний простір, також мають можливість генерування тимчасових сертифікатів для «підписання» (криптографічного завірення) вторинних об'єктів RPKI, наприклад, джерела маршруту (Route Origin Authorization, ROA), що вказують на автономні системи, які можуть бути джерелом певного маршруту.

Route Origin Authorization.

Структуру авторизації джерела маршруту, або RPKI ROA, наведено на рис.1.4.1 [14].

Функціонування та реалізацію ROA детально описано в [16, 17]. ROA на даний момент є ключовим елементом RPKI і є дозволом, виданим мережею-власником прав на використання адресного простору на анонсування даних ресурсів конкретною автономною системою, зазначеною в ROA. Відповідно до специфікації, ROA містить IP-префікс, номер авторизованої АС, яка має дозвіл анонсувати цей префікс, а також дозвіл чи заборону анонсувати окремі частини префіксу. До цих «заяв» додається сертифікат, і весь об'єкт підписано з використанням ключа, зазначеного в сертифікаті.

Для отримання переваг ROA, автономні системи в RPKI використовують так зване програмне забезпечення довіреної сторони (relying party, RP) щоб завантажувати та валідувати об'єкти RPKI. Так, з усіх об’єктів ROA, програмне забезпечення RP складає кортежі, що називаються Validated ROA Payloads (VRP), куди входять:

- номер AS;
- префікс ;
- довжина мережевого префіксу;
- максимальна допустима довжина суб-префіксу.

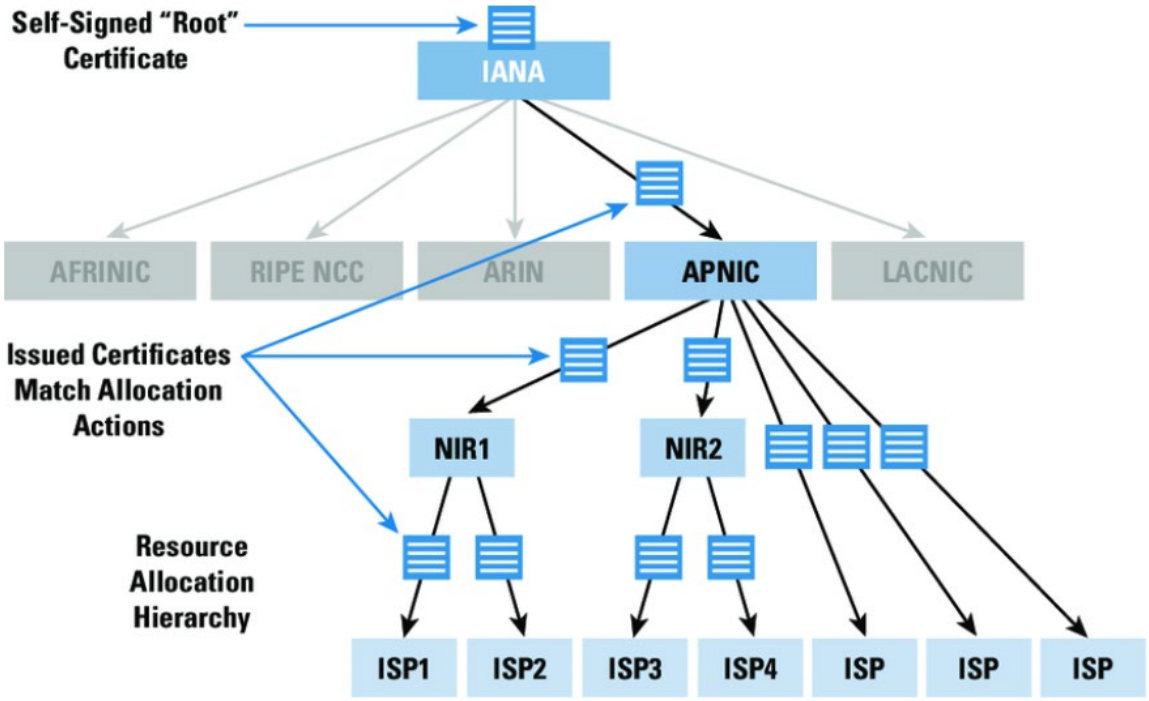


Рисунок 1.4.1 – Інфраструктура сертифікації ресурсів RPKI[1]

Використання ROA можливо як для побудови фільтрів, так і в якості додаткового правила в процесі вибору шляху BGP. Логічно припустити, що інтеграція інформації, отриманої від системи RPKI, безпосередньо в функціональну схему BGP-4, є більш масштабованим рішенням.

RPKI AS Path Authorization

Авторизація шляху (AS path authorization, ASPA) – запропонований метод для верифікації атрибуту BGP AS_PATH, в якому міститься послідовність AS в шляху. Його мета – автоматизація виявлення та запобігання зловмисним викраденням та витокам маршрутів додатково до механізму ROA. Скоріше за все, ASPA є продовженням ідеї BGP Peer Lock.

ASPA – процедура перевірки AS_PATH, яка допомагає автоматично виявляти неправильно сформовані AS_PATH в оголошеннях за допомогою класифікації взаємозв'язків між AS [19]. Для цього власник мережевого префікса визначає та декларує свої відносини з сусідніми AS в спільній базі даних взаємозв’язків і відносини мають три типи: клієнт-провайдер (customer-to-provider, C2P), провайдер-клієнт (P2C), «рівний з рівним» (peer to peer, P2P), яка будується за допомогою нового об’єкта RPKI – ASPA: об’єкта з цифровим підписом, який засвідчує, що власник AS клієнта (customer AS, CAS) уповноважив конкретну AS (provider AS, PAS) або множину провайдерських AS (set of PAS, SPAS) розповсюджувати повідомлення про маршрути BGP клієнта далі. Якщо дійсний маршрут отримано від клієнта або «рівного» – вузла-сусіда, він повинен мати лише пари C2P у своєму AS_PATH. За наявності

[1] Діаграма розподілу ресурсів RPKI на прикладі APNIC - за матеріалами сервісу QRator.Radar

верифікованої бази даних, є можливість перевірити шлях в будь-якому маршруті та виявити перехоплення.

На даний час ASPA, на відміну від ROA, не підтримується регіональними реєстрами та проходить випробування в окремих операторів.

1.4.4. RPKI як нова єдина точка відмови

Як вже згадувалось, AS використовують програмне забезпечення довіреної сторони щоб завантажувати та валідувати об'єкти RPKI. Крім того, репозиторій цих даних є такою ж самою «довіреною стороною», що на даний момент керується, безумовно, авторитетною та досвіченою організацією. У випадку регіону Європи, Близького Сходу та Північної Азії – це RIPE Network Coordination Centre.

31 березня 2020 року в ході роботи з програмним забезпеченням реєстру з бази даних випадково видалили 4100 записів ROA. Адміністратор європейського реєстру повідомив у середині дня 1 квітня 2020, що «це сталося під час технічного обслуговування нашого внутрішнього програмного забезпечення». Більш детальну інформацію було опубліковано у пост-фактумному звіті, з якого стала зрозумілою тривалість та масштабність збоїв, що виникли в результаті проблем підчас оновлення програмного забезпечення [20].

Оновлення програмного забезпечення та видалення записів ROA трапилось у неробочий час, що призвело до невчасного детектування проблеми. Повідомлення постраждалих клієнтів були оброблені вже наступного ранку, 1 квітня 2020 року. Відновлення видалених записів не вдалося без втручання наших інженерів і загалом тривало до середини дня 2 квітня. Після того проводилося розслідування, чи страждали якісь IP-префікси підчас збою від витоку чи перехоплення маршруту.

Помилкове видалення записів, випадково чи ні, співпало з іншою проблемою, масштаб якої описаний спеціалістами компанії QRATOR [21]. Можливо через інший збій програмного забезпечення, але в той самий час, коли відновлювали БД з ROA, 8877 маршрутів від 200 автономних систем були неправомірно анонсовані державним російським провайдером Ростелеком. Масштаб був би менший, проте неправомірність анонсів неможливо було встановити через відсутність сертифікатів походження маршруту, що були видалені. Понад годину були недосяжні великі сегменти сервісів Hetzner, Amazon AWS, Akamai, Cloudflare, Digital Ocean, і це набуло розголосу [22].

Викладені матеріли інциденту дають привід вважати, що з точки зору безпеки глобальної маршрутизації в Інтернеті, локальне програмне забезпечення інтернет-реєстру на сьогодні є новою єдиною точкою відмови (single point of failure – SPoF), саме завдяки розвитку механізму RPKI, що призваний захистити глобальну маршрутизацію.

1.4.5. Очікування від нового захищеного протоколу BGPSec

Слід зазначити, що RPKI сама по собі не є вирішенням проблем безпеки, оскільки рішення про вжиття додаткових заходів (наприклад, додаткових перевірок при надання транзиту мережі або фільтрація маршрутів) залишається за мережевим оператором. Розглянутий інструментарій може реально вирішити проблему безпеки системи маршрутизації тільки при достатньому рівні впровадження. Але зусилля окремого провайдера вносять несуттєвий внесок у поліпшення глобальної системи і, як не парадоксально, ще менш суттєвий – у поліпшення власної безпеки. Наприклад, валідація анонсів маршрутів, отриманих від клієнтів, безумовно запобігає атаки захоплення префіксів цими клієнтами, але не є захистом від захоплення їх адресного простору в іншій частині Інтернету. При розгляді проблематики безпеки глобальної системи маршрутизації ми стикаємося зі свого роду феноменом трагедії громад. Спільні зусилля можуть значно зменшити проблему, але тенденція перекладання цього тягаря на інших не дозволяє домогтися істотних результатів. Здійснюючи фільтрацію анонсів або обмежуючи поширення помилок і навмисних захоплень, оператор фактично захищає чужі мережі, на безпеку же власної його дії не впливають. Лише підтримання всіма учасниками глобальної маршрутизації єдиного протоколу здатне надати гарантії захисту маршрутів.

Такі гарантії може надати, в разі 100% впровадження, новий протокол. Робоча група з безпечної міждоменної маршрутизації (secure interdomain routing, SIDR) почала роботу над новим стандартом для BGP у 2005 році з огляду та систематизації вже існувавших на той момент пропозицій змін джо протоколу (з робочими назвами sBGP, soBGP, psBGP) [23]. І, нарешті, восени 2017 року результат під назвою BGPSec (Border Gateway Protocol Security) був опублікований в якості єдиної офіційної пропозиції стандарту. Він викладений в [24].

Основною ідеєю BGPsec є розширення функціональних можливостей протоколу BGP-4 за рахунок запровадження нового атрибуту та механізму його передачі в протокольному повідомленні «UPDATE», яке в BGP-4 використовується для оновлення інформації про доступність мережевих префіксів. Атрибут BGPsec_Path несе захищену інформацію щодо шляху крізь AS, через які проходить повідомлення про оновлення. Сюди входять цифрові підписи, що використовуються для захисту інформації про шлях. Повідомлення про оновлення, що містять атрибут BGPsec_Path, називаються "Повідомлення про оновлення BGPsec". Атрибут BGPsec_Path замінює атрибут AS_PATH у повідомленні про оновлення BGPsec. Тобто повідомлення про оновлення, що містять атрибут BGPsec_Path, не повинні містити атрибут AS_PATH, і навпаки.

Атрибут BGPsec_Path складається з декількох частин:

- Secure_Path: атрибут, що містить перелік AS, якими пройшло оголошення маршруту, функціонально ідентичний атрибуту AS_PATH в BGP-4;
- Signature_Block: блок цифрових підписів, в якому представлені:
- ідентифікатор набору криптоалгоритмів;

- ідентифікатор ключа (secure key identifier) кожної AS, присутної в Secure_Path. представлено структуру атрибута AS_PATH та BGPsec_Path;
- цифровий підпис кожної AS, присутної в Secure_Path. представлено структуру атрибута AS_PATH та BGPsec_Path.

BGPsec_Path повинен містити ідентифікатор та підпис принаймні однієї AS – джерела маршруту. Отримавши повідомлення оновлення BGPsec від зовнішнього BGP-вузла, спікер BGPsec повинен перевірити це повідомлення, щоб визначити достовірність інформації про шлях, що міститься в атрибуті BGPsec_Path.

В разі 100% впровадження BGPSec вирішує проблему викрадень маршрутів з дуже високою точністю, але витрати на обчислення суворої криптографічної перевірки AS_Path є на цей час неприйнятними для більшості гравців, за винятком, можливо, найбагатших операторів AS у світі. І знову ж таки – для належної роботи BGPSec повинен бути впроваджений у кожній мережі, яка керує власним оголошеним маршрутом.

На даний час навколо дизайну BGPsec все ще продовжується дискусія [25], в тому числі, з питань взаємодії процесу BGP з RPKI, реакції на помилки та нештатні ситуації.

1.4.6. Інші системи та сервіси виявлення інцидентів з глобальною маршрутизацією

Технологія BGP Peer Lock

Технологія під назвою «фіксація партнера» (Peer Lock) пропонувала побудову BGP-пірінгу з фіксацією відносин між усіма сусідніми AS у вигляді відносин «клієнт-провайдер» чи «сусід-сусід». Ці відносини мали реалізуватись у вигляді адміністративно заданих фільтрів для повідомлень протоколу BGP, аби убезпечити певну BGP-систему від ситуації, коли «клієнт» чи «сусід» анонсують маршрути до великих адресних посторів, до яких, насправді, не мають відношення.

Peer Lock був представлений в 2016 році як результат пошуку реального для імплементації рішення. Кожне розгортання Peerlock відбувається між двома AS, одна з яких зветься захищеною, а інша – захисником. Захисник погоджується на фільтрування (тобто, відсікання) маршрутів, що транзитують префікси захищеної AS, якщо вони не надходять безпосередньо від захищеної, як або одного з його визначених нею провайдерів. Фільтрація запобігає поширенню нелегітимних маршрутів захисником та скеровуванню по них трафіку від захисника до префіксів, адресованих захищеній AS, незалежно від префіксу чи його джерела.

Захисниками стають найбільші оператори, в першу чергу так звані Tier 1 – оператори, вище яких вже нема нікого, хто міг би назватись їхнім провайдером (рис. 1.4.2).

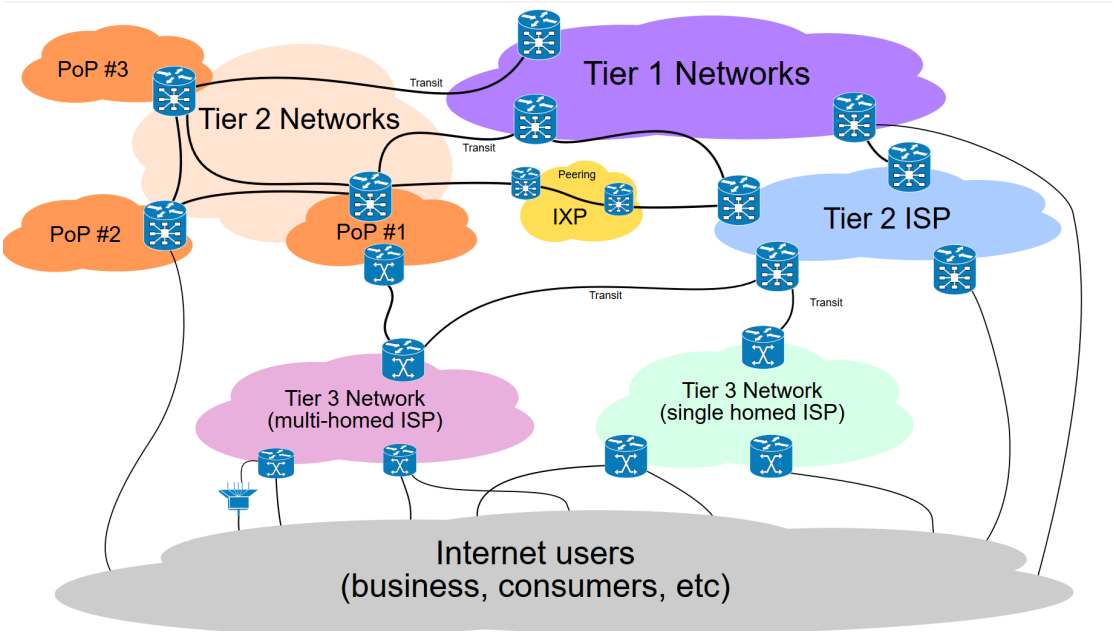
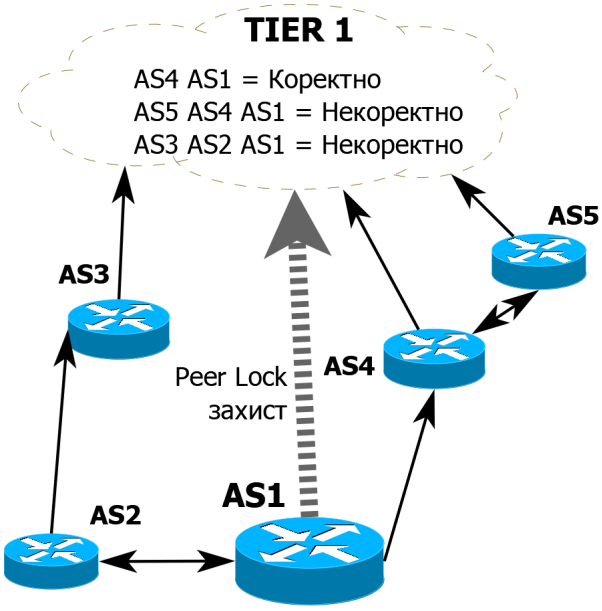


Рисунок 1.4.2 – Умовний розподіл операторів за рівнями в мережі Інтернет[1]

Відповідно до ідеї Peer Lock, оператори Tier 3 зазначають для операторів вищих рівнів, перш за все Tier 1, які ідентифікатори AS можуть знаходитись в атрибутах їхніх маршрутів. Наприклад, для AS1 транзитними провайдерами є AS2 та AS3, а AS4 є «сусідом», з яким AS1 та AS4 обмінюються виключно трафіком своїх клієнтів. Ідея PeerLock полягає. в тому, щоб великий оператор ігнорував (не використовував, не розповсюджував) маршрути, в яких фігурує AS1, та які не відповідають описаній політиці.

На рис. 1.4.3 продемонстровано умовну ситуацію з легітимним та нелегітимним маршрутом від AS1.



[1] За матеріалами сторінки «Tier 1 Network» ресурсу Wikipedia.

Рисунок 1.4.3 – Схема взаємодії операторів із застосуванням механізму Peer Lock

На рисунку AS1 є захищеною AS, двонаправленими стрілками показані відношення «сусідів», а однонаправленими – «клієнт-провайдер». Пропозиція та практична реалізація Peer Lock описані в [18]. Офіційного статусу ця методика не набула.

Peer Lock має очевидні недоліки – це негнучкий адміністративний механізм взаємодії, неможливість верифікації заявлених даних, відсутність впливу на маршрути, що не проходять через «захисника», неможливість протидії захопленню префіксу через нелегітимну підміну джерела.

Система моніторингу та виявлення перехоплень маршруту ARTEMIS

ARTEMIS (від «Automatic and Real-Time dEtection and MItigation System» – автоматична та система виявлення та пом'якшення наслідків у режимі реального часу) – це програмне забезпечення з відкритим кодом, яке надає наступні послуги до операційної мережі, яка розгортає її:

– моніторинг оновлень маршрутів BGP в реальному часі з використанням потокових даних спеціальних служб, що збирають дані про маршрути з розподіленої мережі «датчиків»;

– точне та комплексне виявлення атак з перехопленням префікса BGP протягом декількох секунд від їх ініціації.

Системі ARTEMIS присвячено декілька наукових робіт, а також система була представлена на заходах IEEE [10, 11].

Автори претендують і на можливість швидкого реагування на перехоплення маршрутів, але механізм протидії базується на превентивній деагрегації перехопленого префікса, він може бути ефективний лише в окремих випадках.

Найбільшу цінність ARTEMIS має завдяки вбудованій взаємодії з низкою публічно доступниїх сервісів – збірників маршрутів (серед яких RIPE RIS Live, RouteViews, CAIDA BMP), можливість взаємодії з обладнанням BGP-системи, гнучкість та платформонезалежність програмного забезпечення.

В ARTEMIS запропонована таксономія атак на систему глобальної маршрутизації. Вона буде детально розібрана в гл.3 підчас розробки моделі порушника та моделі загроз.

Використання універсальних засобів моніторингу

У складі комп’ютерної мережі зазвичай присутні системи моніторингу (контролю працездатності). Програмне забезпечення моніторингу численних параметрів мережі а також стану і працездатності серверів використовує гнучкий механізм повідомлень, що дозволяє користувачам налаштовувати оповіщення по e-mail, sms, онлайн-месенджерам практично для будь-якої події. Накопичення та аналіз даних від таких підсистем дозволяє вести спостереження за груповими відхиленнями від звичайного стану в компонентів ІТС. Такі

відхилення, в свою чергу, можуть бути наслідками прихованого шкідливого зовнішнього впливу чи використання ІТС для реалізації кібератак. Знання принципів і механізмів реалізаіції кібератак на глобальну маршрутизацію дає можливість сформулювати критерії зміни виявлення змін в маршрутизації, що виникли під впливом кібератаки. Багатовекторний аналіз даних, отриманих від систем моніторингу працездатності, дає можливість виявлення штучних втручань в маршрутизацію при відсутності чітких характеристик таких втручань та без попереднього опису притаманних такому впливові подій. Тому необхідно зробити огляд деяких методів аналізу, прийнятних для поставленої задачі, та певний функціональний підхід до розпізнавання аномалій в глобальній маршрутизації за допомогою популярних систем моніторингу працездатності.

Системи моніторингу ІТС відстежують критичні характеристики мережі в режимі реального часу або з певною періодичністю, та сигналізують про перехід числових характеристик через певні встановлені рівні. В глобальній маршрутизації задіяні понад 70 тисяч вузлів, що обмінюються понад 700 тисячами маршрутів. Багатовекторний аналіз накопичених даних змін в глобальній маршрутизації може слугувати альтернативним джерелом інформації для виявлення шкідливого зовнішнього впливу при відсутності чітких характеристик такого впливу та без попереднього опису притаманних такому впливові подій. Для цієї мети необхідно:

розробити моделі збору та накопичення даних про зміни в глобальній маршрутизації за допомогою існуючих та широко вживаних систем моніторингу;

- обрати методи та моделі дослідження даних, зібраних та накопичених системами моніторингу для автоматичного виявлення аномалій, спричинених шкідливим зовнішнім впливом на маршрутизацію.

Як відомо з принципів організації глобальної маршрутизації та протоколу BGP-4, основним транзитивним параметром, що характеризує привабливість маршруту, є довжина шляху. Довжина шляху – це фактор, який дозволяє маршрутам до однакових префіксів конкурувати.

Якщо зловмисник вдало провів перехоплення маршруту чи захоплення префіксу, це означає, що для певної цільової групи вузлів маршрут до префікса жертви через вузол зловмисника став коротшим, ніж інші, природні маршрути, а отже – буде перехоплено трафік до цього префіксу від згаданої групи вузлів.

Загалом, аномалії глобальної маршрутизації можуть досліджуватись:

- по змінах в глобальній таблиці маршрутизації у певного Інтернет-вузла;
- по змінах інформації в офіційних реєстрах маршрутів, що мають вільно доступні бази даних;
- за допомогою зовнішніх мережевих сервісів, прикладом яких є BGPmon (див. в наступному підрозділі).

В залежності від місця дослідження мають бути обрані засоби збору та накопичення даних, а також та методи їхнього дослідження.

Для визначення атаки за характером змін в маршрутизації, система повинна навчатись визнавати нормальний стан вузла та відхилення. Для цього потрібні дві фази: тренування, де будується профіль звичайної поведінки, та тестування, де поточний трафік чи картина подій порівнюється з профілем, створеним на етапі навчання. Аномалії виявляються кількома способами, найчастіше з використанням методів штучного інтелекту. Вже понад 10 років досліджується можливість повністю автоматичного поведінкового аналізу трафіку з метою виявлення атак.

В роботі [26] використовується навчання детектора «типовому» профілю трафіку та виявлення аномалій на осонові відстані Магаланобіса. Детектор аномалії фіксує вхідні "корисні навантаження" (payload) та перевіряє корисне навантаження на його узгодженість (або відстань) від моделі центроїда. Це досягається шляхом порівняння двох статистичних розподілів.

Використовувана метрика відстані являє собою метрику відстані Магаланобіса, яка застосовується до кінцевої дискретної гістограми частоти символів, що обчислюються на етапі навчання. Будь-яке нове тестове корисне навантаження, яке виявилося занадто далеким від нормального очікуваного корисного навантаження, вважається аномальним та генерує попередження.

Попередження може бути співвіднесено з іншими даними датчиків, і процес прийняття рішення може відповісти кількома можливими діями. Залежно від політики безпеки захищеного сайту, можна фільтрувати, переадресовувати або навпаки, перехоплювати мережеве з'єднання та доправляти "отруйний" трафік на дослідження [69].

В роботі [27] пропонуються методи виявлення вторгнень шляхом складання профілю легітимних користувачів. Запропоновано трактування аномалії як події, які впливають на "спектр" трафіку, де обсязг трафіку є одним з показників. Такий трафік-аналіз має дві основні переваги.

По-перше, це дозволяє виявити аномалії, які важко ізолювати дослідженням обсягу трафіку. Деякі аномалії такі як сканування (probing) або специфічні атаки DOS прикладного рівня можуть мати незначний вплив на обсяг трафіку магістральної лінії, і, мабуть, краще можуть бути виявлені шляхом систематичного аналізу змін в розподілі замість зміни обсягу.

По-друге, незвичайні розподіли виявляють цінні відомості про структуру інформаційних аномалій, які відсутні при вимірюванні обсягів трафіку. Досліджується структура впливу аномалії на характер трафіку і за допомогою цього проводиться автоматична класифікація аномалій по значимих категоріях. Автори вважають це прогресом порівняно з евристичним дослідженням аномалій, заснованим на правилах, бо саме такий метод може виявити нові, невідомі аномалії.

Важливим напрямком захисту є виявлення аномалій в поведінці користувачів шляхом аналізу протоколів рівня застосунків. Запропоновано розширену напівмарківську модель для опису поведінки веб-користувачів. Щоб зменшити обсяг обчислень, пов’язану з просторовою складністю моделі, запропоновано модифікований алгоритм.

У якості критерію вимірювання нормальності користувача використовується ентропія його HTTP-запитів. Поведінка користувача описується як періодична зміна станів між «кліком» на гіперпосилання та читанням отриманого матеріалу і описується за допомогою прихованої напівмарківської моделі (HsMM). Веб-сайт, яки є потенційно атакованим, описується за допомогою марківського простору станів. Кожен основний напівмарковський стан використовується для представлення унікальної веб-сторінки, натиснутою веб-користувачем. Таким чином, матриця ймовірності стану переходу представляє відношення гіперпосилання між різними веб-сторінками. Тривалість стану представляє кількість HTTP-запитів, отриманих веб-сервером, коли користувач переходить за «кліком» на відповідну сторінку. Вихідна символьна послідовність кожного стану представляє ті запити на натиснутій сторінці, які проходять через всі проксі або кеш браузера і, нарешті, надходять на веб-сервер.

Метод містить декілька послідовностей спостереження за поведінкою декількох користувачів, отримується алгоритм переоцінки HsMM для декількох послідовностей спостережень за частотою в цій статті. Автори розробили алгоритм переоцінки, встановлюється новий HsMM для опису звичайної поведінки веб-користувачів, просуваючи модель із набору послідовностей запитів, зроблених багатьма звичайними користувачами. Визначається відхилення від середньої ентропії даних тренувань і це й є аномалія спостережуваної послідовності запиту, яку виконує користувач. Чим менше відхилення, тим вище нормальність спостережуваної послідовності.

Існує багато вдалих та широко вживаних рішень з автоматизації такого моніторингу, зокрема, для серверів на базі UNIX-подібних операційних систем. Збір, накопичення та збереження даних для такого аналізу можуть виконувати системи моніторингу працездатності. Найбільш широко вживаними системами, за власними спостереженнями автора, є Nagios, Cacti та Zabbix.

Nagios (офіційний сайт – www.nagios.org) складається з двох складових. Перша – це серверна частина (Nagios Core), основне завдання якої – обробка даних (отриманих від агентів і зовнішніх програм) і оповіщення при досягненні критичних станів. Сервер Nagios встановлюється тільки на Unix-подібні ОС. Для включення в моніторинг будь-якого сервісу чи системи необхідно в конфігураційних файлах прописати їх параметри, а також підключити графіки і плагіни. Статистика може виводитися по хостах, по процесах і службах, по помилках, як окремо, так і у вигляді груп. В результаті виходить сформований звіт зі зведеними таблицями і діаграмами в процентному і числовому співвідношенні за потрібний період, який є помічником при аналізі інцидентів. Можливість розширення штатного функціоналу Nagios досягається за рахунок підключення великої кількості плагінів (ручна установка), які дозволяють створювати свої способи перевірки служб і обробників подій.

Cacti (офіційний сайт – www.cacti.net) є веб-застосунком, збирає статистичні дані за певні часові інтервали і дозволяє відобразити їх у графічному вигляді. Переважно використовуються стандартні шаблони для відображення статистики по завантаженню процесора, виділенню оперативної

пам'яті, кількістю запущених процесів, використання вхідного та вихідного трафіку. Для візуалізації використовується стандартний інструмент реєстрації даних RRDtool. Так Cacti дозволяє користувачеві опитати послуги за заданими інтервалами та графік отриманих даних. Він зазвичай використовується для графіка даних про часові ряди таких показників, як завантаження процесора та використання пропускної здатності мережі. Також звичайно використовується для моніторингу мережевого трафіку шляхом опитування мережевого комутатора або інтерфейсу маршрутизатора через простий протокол керування мережею (SNMP).

Основними особливостями Cacti є:

- гнучкість конфігурування джерел даних за допомогою шаблонів;
- гнучкість механізму та періодичності отримання даних;
- необмежена кількість графічних елементів;
- автоматична побудова мережі у вигляді графа;

Окремої згадки потребує *RRDTool* (офіційний сайт – http://oss.oetiker.ch/rrdtool/). «Round Robin Database Tool» – це програмний засіб для зберігання, впорядкування та аналізу великої кількості даних від моніторингу. Частина аналізу даних RRDtool базується на здатності швидко генерувати графічні уявлення значень даних, зібраних протягом певного періоду часу. RRDtool приймає дані про часові змінні в інтервалах певної довжини. Цей інтервал, який зазвичай називається «крок», вказується при створенні файлу RRD і не може бути змінений пізніше. Оскільки дані не завжди доступні в потрібний час, RRDtool буде автоматично інтерполювати будь-які надані дані, щоб відповідати його внутрішнім крокам часу.

Значення для певного кроку, який був інтерпольований, називається первинною точкою даних (PDP). Кілька PDP можуть бути об'єднані відповідно до функції консолідації (CF) для формування консолідованої точки даних (CDP). Типова функція консолідації – середня, мінімальна, максимальна.

Після того, як дані були об'єднані, результуючий CDP зберігається в циклічному архіві (RRA). Циклічний архів зберігає фіксовану кількість CDP і вказує, скільки PDP потрібно об'єднати в один CDP і який CF використовувати. Коли архів добіг останнього «кроку», він буде «обертатися»: наступна вставка перезапише найстаріший запис. Завдяки цій властивості бази даних RRDTool завжди мають однаковий фіксований об’єм. Аналіз та візуалізація даних моніторингу є типовими сферами застосування RRDTool.

Zabbix (офіційний сайт – www.zabbix.com) також є системою моніторингу, яка складається з декількох компонентів. Zabbix-сервер – ядро системи, яке може віддалено перевіряти мережеві сервіси і є сховищем, в якому зберігаються всі конфігураційні, статистичні та оперативні дані. До функцій сервера також належить оповіщення. Zabbix-проксі збирає дані про продуктивність і доступність від імені Zabbix-сервера.

Всі зібрані дані заносяться в буфер на локальному рівні та передаються Zabbix-сервера, до якого належить проксі-сервер. Він може бути також використаний для розподілу навантаження одного Zabbix-сервера. В цьому випадку, проксі тільки збирає дані, тим самим на сервер лягає менше

навантаження на процесор і системи введення-виведення. Zabbix-агент – програма контролю локальних ресурсів і додатків (таких як накопичувачі, оперативна пам'ять, статистика процесора і так далі) на мережевих системах, ці системи повинні працювати з запущеним Zabbix-агентом.

Отже, обидві системи надають широкі можливості для моніторингу, звітування, візуалізації зібраних даних. Інструменти моніторингу обох систем допрацьовуються до потреб певної ІТС завдяки широким можливостям конфігураційних параметрів та наявності власних мов скриптового програмування для побудови власних процедур. Також, ці системи чудово піддаються горизонтальному і вертикальному масштабуванню.

Вочевидь, є шляхи практичного використання обох систем з метою виявлення аномальних змін в глобальній маршрутизації. Завдяки засобам зберігання та накопичення результатів моніторингу та наявності засобів розширення функціоналу, перелічені системи можуть використовуватись для сигналізування про зміну поведінки елементів системи в разі розробки і підключення модуля для аналізу, який можна назвати аналізом поведінки.

- Наступний набір функцій для системи виявлення аномалій дозволить їй функціонувати та розвиватись:
- 1) збір даних;
- 2) навчання: визначення характеристик нормального стану;
- 3) моніторинг;
- 4) виявлення відхилень;
- 5) отримання негативного зворотного зв’язку;
- 6) коригування порогових значень для характеристик нормального стану.

Негативний зворотний зв’язок необхідний для навчання системи. Із плином часу топологія зв’язків між вузлами в Інтернеті змінюється, отже необхідно передбачити можливість автокорекції – переходу аномалії в стан норми.

Розглянемо приклади деяких даних, збір та накопичення яких необхідно забезпечити системами моніторингу для подальшого профілювання системи та виявлення аномалій в глобальній маршрутизації, викликаних кібератаками:

- зміна атрибуту origin у мережевого префіксу;
- поява маршруту до префіксу з іншим origin;
- поява маршруту до «деагрегованого» префіксу, тобто підмережі з довшою маскою;
- зміна довжини кращого маршруту до префіксу;
- поява нового маршруту до префіксу.

Кожна окрема ознака не є чіткою ознакою кібератаки, втім, різні комбінації таких аномалій мають бути досліджені.

Таким чином, знання принципів і механізмів реалізаіцї кібератак на глобальну маршрутизацію дає можливість сформулювати критерії виявлення аномалій в маршрутизації під впливом кібератаки. Для виявлення таких змін можуть бути використані звичайні системи контролю працездатності

(моніторингу) що широко застосовуються в сучасних ІТС. Таке програмне забезпечення пропонує широкі можливості звітності і візуалізації, чудово піддаються горизонтальному і вертикальному масштабуванню.

Багатовекторний аналіз даних, зібраних цими системами, може бути застосований для виявлення аномальних змін під впливом кібератаки, в тому числі дозволить виявляти аномалії маршрутизації від подій, чіткого опису яких ще не існує. Це відкриває перспективу підвищення ефективності виявлення прихованих атак на глобальну маршрутизацію Інтернеті.

Сервіс BGPmon

Сервіс BGPmon забезпечує моніторинг стану маршрутів до вказаного префікса на постійній основі. Сервіс має офіційний веб-сайт за адресою www.bgpmon.com і наразі належить компанії Cisco. Ще до зміни власника сервіс використовував сотні точок спостереження за маршрутами по всьому світу.

Принцип функціонування BGPmon наступний. Після того, як мережевий префікс реєструється в системі BGPmon, він буде контролюватися з більш ніж ста точок по всьому світу, що дозволяє виявити регіональні події, які можуть не бути виявлені системою моніторингу з однією точкою спостереження.

Моніторинг стосується перехоплення маршрутів, перехоплення префіксів, деагрегації префіксів (рис.1.4.4), зміни джерела маршруту чи будь-якого іншого порушення політики маршрутизації.

BGPmon забезпечує набір функцій для моніторингу для таких подій. Наприклад, це дозволяє користувачеві визначити список дозволених «сусідів» та провайдерів, а також шаблони шляхів, які повинні відповідати тим, що будуть у анонсах маршрутів.

```
==========================================================================
Possible Prefix Hijack (Code: 11)
==========================================================================
Your prefix:         195.64.228.0/22:
Prefix Description:   2nd route for ORG-EVLL1-RIPE
Update time:          2019-06-19 16:07 (UTC)
Detected by #peers:   1
Detected prefix:      195.64.230.0/24
Announced by:          AS205459 (UCCI, UA)
Upstream AS:           AS61297 (DATACENTER-, UA)
ASpath:               199181 174 21488 61297 205459
Alert details:        https://portal.bgpmon.net/alerts.php?details&alert_id=88854054
Mark as false alert:  https://portal.bgpmon.net/fp.php?aid=88854054
```

Рисунок 1.4.4 – Звіть-попередження, згенероване сервісом BGPmon при виявленні деагрегації мережевого префікса

BGPmon також забезпечує моніторинг доступності мережі та виявляє нестабільність мережевих префіксів, так званий route flapping. Це виконується

шляхом моніторингу BGP-повідомлень зі скасуванням маршрутів. Це важливо, бо в BGP-системі закладено «пониження в правах» та навіть ігнорування маршрутів, які найчастіше анонсовуються та скасовуються (flapping), зазвичай перевіряєтья чи певний часовий поріг. Програмне забезпечення BGPmon буде сповіщати, коли мережа не є недосяжною, або в усьому світі, або в певному географічному регіоні. Порогові параметри дозволяють добре налаштувати частоту оповіщення. Ця функція дозволяє мережевим операторам швидко ідентифікувати регіональну нестабільність, яка в іншому випадку може не бути виявлена традиційною системою моніторингу.

Відносно нещодавно в BGPmon було додано моніторинг помилок перевірки ROA (авторизація походження маршруту, що описана в цьому підрозділі раніше, і є частиною RPKI). Якщо включено опцію моніторингу RPKI, програмне забезпечення BGPmon попередить користувача, якщо в мережі буде виявлено помилку валідації електронного підпису ROA, з будь якої причини. Основні причини – це наявність хибних маршрутів, або недозволена в ROA-записі деагрегація префіксу, або тому, що ключ для підпису ROA закінчується.

Стверджується, що BGPmon є на сьогодні єдиною системою виявлення аномалій маршрутизації, якак має підтримку RPKI.

Веб-інтерфейс BGPmon дозволяє користувачеві пріоритезувати кожний тип попереджень і повідомлень. Інформація про сповіщення демонструється в графічному внтерфейсі на мапя задля регіональної прив'язки виявленого інциденту.

Qrator.Radar

Qrator.Radar від Qrator Labs – платформа для аналізу маршрутної інформації та змін мережевої зв'язності в реальному часі. Система моніторингу Інтернету Qrator.Radar дозволяє виявляти мережеві аномалії, які можуть зробити істотний вплив на доступність і якість роботи сервісів на глобальному рівні маршрутизації. Офіційний вебсайт сервісу – http://radar.qrator.net.

Qrator Labs повідомляють, що Qrator.Radar щодня фіксує в світі кілька тисяч інцидентів маршрутизації. За допомогою Qrator.Radar можна робити моніторинг змін в зв'язності і інцидентів безпеки як для вхідного, так і для вихідного трафіку наступних видів:

Витік маршрутів – перенаправлення або концентрація трафіку на проміжній мережі, якої в шляху бути не повинно, коли, наприклад, невеликі оператори в результаті тривіальної помилки можуть перенаправити на себе трафік магістральних мереж і цілих континентів.Перехоплення – нелегітимне анонсування чужих префіксів за усіма сценаріями.

Bogons – анонсування префіксів і номерів автономних систем, які не повинні зустрічатися в таблицях маршрутизації. В результаті подібних анонсів може відкритися доступ до локальної мережі всім зовнішнім користувачам, а в гіршому випадку – вся мережа може стати недоступна.

Оскільки відомо, що виявити мережеві інциденти практично неможливо, перебуваючи всередині мережі жертви, Qrator.Radar декларує, що це один з

найбільших в світі колекторів по збору BGP даних (за кількістю сесій і таблиць маршрутизації). Сотні операторів зв'язку по всьому світу надають маршрутну інформацію Qrator Labs у вигляді таблиць маршрутів всіх доступних операторам підмереж Інтернету.

Для обробки отриманих даних і виявлення інцидентів застосовуються спеціально розроблені алгоритми Qrator Labs. Велику роль у виявленні інцидентів грає унікальна математична модель визначає відносини між АС.

Інформація про події, пов'язані з аномальним зміною маршрутної інформації, розсилається клієнтам в режимі реального часу. Можливість отримання інформації про BGP аномаліях, дозволяє негайно реагувати на інциденти.

1.5. Вимоги до засад захисту системи глобальної маршрутизації

1.5.1. Узагальнення факторів, які перешкоджають впровадженню захисту системи глобальної маршрутизації

Підсумуємо, які фактори на цей час не дозволяють запровадити безпечний протокол глобальної маршрутизації та убезпечити систему глобальної маршрутизації від кібернетичних атак.

Таким чином, уразливості глобальної маршрутизації є загрозами інформації, для захисту від яких потрібні нові підходи, ефективні для конкретних учасників глобальної маршрутизації.

Таблиця 1.5.1 – Порівняння методів та засобів протидії атакам на систему глобальної маршрутизації

Напрям	**Склад заходів**	**Приклади**	**Переваги та недоліки**
Реагування	моніторинг, виявлення та інформування про несанкціоновані зміни в глобальній маршрутизації	BGPmon ARTEMIS QRator	(+) зменшує час від початку інциденту до його виявлення; (-) не впливає на саму можливість виникнення інциденту.
Запобігання	публікування політики взаємодії між AS про наявність та ступінь зв'язку	IRR RIS	(+) Задатний запобігти більшості інцидентів (-) Проблеми якості інформації в реєстрах (-) Нема 100% впровадження
	валідація атрибутів шляху екстрапротокольними засобами	ROA ASPA PeerLock	(+) Забезпечує цілісність окремих атрибутів (-) Частковий захист атрибутів,

			(-) проблеми 100% впровадження, (-) утворення нових точок відмови
	криптографічний захист атрибутів шляху в протоколі маршрутизації	BGPSec	(-) дискусії про обчислювальну складність (-) проблеми стандартизації, (-) неможливість 100% впровадження

Існують обгрунтовані сумніви стосовно практичної досяжності такої мети як централізоване та загальноохоплююче впровадження змін в базові технології комп'ютерної мережі Інтернет [4]. З одного боку, існує достатній досвід з вдалого впровадження в Інтернеті сутностей, які не потребували тотальної участі всіх учасників мережі. З іншого боку, є кілька глобальних прикладів з невдалого (повільного, відкладеного на роки, такого, що і досі не завершилось) впровадження сутностей, які за своєю архітектурою потребують 100% охоплення для досягнення успіху. Вдало і швидко розвиваються технології потокової передачі за допомогою мереж доставки контенту, нові протоколи мереж пірінгових мереж (p2p), розширення протоколів для веб-технологій, і кожне нове впровадження приносить користь.

Натомість, на десятиліття розтягнулись і досі не завершені впровадження мережевого протоколу IPv6 та захищеної системи ломенних імен (DNSSec). Причина вбачається в тому, що застосування нової технології певним учасником має принести практичну (насамперед – економічну) користь саме йому. На жаль, перелічені фундаментальні зміни, до яких належить і проект нового протоколу BGPSec, не мають такої властивості.

1.5.2. Формулювання вимог до нових методів як робота над помилками

З урахуванням відсутності швидких перспектив впровадження в світовому масштабі нового, більш захищеного протоколу глобальної маршрутизації, необхідно, маючи знання про будову і динаміку топології Інтернет, поєднати теорію і практику і запропонувати підходи, які б можна було застосовувати на рівні великого оператора, галузі, регіону, і досягти зменшення можливих збитків від атак на глобальну маршрутизацію. Враховуючи викладені проблеми існуючих підходів, необхідно визначити пріоритетні вимоги до розроблюваних методів, моделей, методик.

Вимога універсальності.

З попереднього аналізу встановлено, що задача застосування існуючих методів захисту системи глобальної маршрутизації та маршрутів до власних мережевих префіксів має різну складність та різну ефективність для різних

учасників глобальної маршрутизації. Це є стримуючим фактором в запровадженні цих методів.

Тому теоретичні засади та методи, що розробляються, мають бути дієвимі в разі застосування для будь-якого суб'єкта глобальної маршрутизації.

Вимога безмасштабності.

Розвиток інструментів на базі RPKI може реально вирішити проблему безпеки системи маршрутизації тільки при достатньому рівні впровадження. Адже зусилля окремого провайдера мають несуттєвий вплив у поліпшення системи глобальної маршрутизації. Відсутність відчутного ефекту для окремого учасника глобальної маршрутизації також є стримуючим фактором при впровадженні існуючих методів та засобів.

Тому розроблювані методи мають демонструвати ефективність незалежно від того, скільки учасників глобальної маршрутизації їх використовують.

Вимога автономності.

Підвищення захисту маршрутів до власних мережевих префіксів існуючими методами потребує імплементації цих методів перш за все не у захищуваного суб'єкта, а в інших суб'єктів глобальної маршрутизації. Так, зусилля окремого провайдера в розвитку RPKI не мають впливу на поліпшення безпеки власних мережевих префіксів.

Тому необхідно, щоб розроблювані методи підвищення захищеності топології для одного суб'єкта глобальної маршрутизації відбувались без втручання в діяльність інших суб'єктів.

Вимога непротирічності.

Наведений вище аналіз поточного стану і перспектив підвищення захищеності системи глобальної маршрутизації показав, що багаторічні зусилля з удосконалення системи глобальної маршрутизації, розробки та поширення механізмів ROA та RPKI мають певні результати. Діяльність з доведення BGPsec до статуса прийнятого стандарту вочевидь буде продовжена ы колись почнеться його впровадження.

Отже необхідно, щоб розроблювані методи підвищення захищеності топології не вступали у протиріччя з існуючими, згаданими вище, та могли доповнювати їх, не знижуючи їхню ефективність.

Вимога сучасності.

Сучасне управління інформаційною безпекою базується на управлінні ризиками [28, 29, 30, 31]. Тому теоретичні засади та практичні методики підвищення захищеності системи глобальної маршрутизації варто роздивлятись в аспекті менеджменту ризиків інформаційної безпеки. Ризик кількісно прийнято виражати як добуток суми збитку від реалізації певної загрози на ймовірність реалізації цієї. Для кількісної оцінки ризику потрібно метод оцінювання збитку та ймовірності настання збитку. При наявності таких

методів, підвищення захищеності інформації від загроз, пов'язаних з глобальною маршрутизацією, можна буде вирішувати шляхом поводження з ризиками.

ГЛАВА 2.
ТОПОЛОГІЧНИЙ ПРОСТІР ІНТЕРНЕТУ

2.1. Від локальної до глобальної мережі

Як вже зазначалось раніше, Інтернет є мережею, що постійно зростає за рахунок приєднання нових окремих комп'ютерних мереж та організації нових зв'язків. Цими приєднуваними комп'ютерними мережами є будь-які комп'ютерні системи, а також телекомунікаційні системи. Базовим типом з'єднання пристроїв у глобальній мережі є канал «точка-точка». Топології, які використовуються у мережах дрібнішого обсягу, на зразок шинної або кільцевої, у глобальних мережах не придатні.

В найпростішому випадку глобальна мережа (wide-area network, WAN) являє собою фізичне з'єднання типу «точка-точка» між регіонами розташування локальних мереж, що взаємодіють між собою (рис. 2.1.1.). Для організації фізичного рівня такого з'єднання типово використовуються спеціальне каналостворююче обладнання. Призначенням каналостворюючого обладнання є, по-перше, формування у фізичному середовищі, що використовується, передачі даних електромагнітних сигналів з належними параметрами, та, по-друге, модуляція цих сигналів згідно даних, що мають бути передані [58]. Пристрої, що виконують першу задачу – це пристрої формування каналу (загальновживаний англійський термін – Channel Service Unit, або CSU), а пристрої, що виконують другу задачу – wt пристрої підготовки даних (Data Service Unit, DSU). В типовому випадку сучасні каналостворюючі пристрої поєднують в собі функції як CSU, так і DSU, в наслідок чого найчастіше зустрічається позначення не CSU/DSU, а DCE – Data Communication Equipment. Функції інтерфейсу з комп'ютерною мережею виконує обладнання, яке має загальну назву DTE – Data Terminal Equipment, або термінали даних.

Рис. 2.1.1 – Схема взаємодії LAN-WAN-LAN

Варто погодитись, що будь-яка сучасна телекомунікаційна система також є комп'ютерною, а комп'ютерна – телекомунікаційною, оскільки обом видам сьогодні властиві як наявність системи передачі інформації, так і засоби її обробки та збереження в цифровому вигляді. Цей процес об'єднання функцій та послуг систем часто називають конвергенцією – поєднанням інформаційних та телекомунікаційних функцій, що раніше були властиві різним телекомунікаційним системам, завдяки новому типу обладнання, що поєднує

різні функції і розробці уніфікованих структур систем обміну та обробки інформації.

Таким чином утворюються так звані «мережі наступного покоління» (next generation networks, NGN). Вони вже не є мережами зв'язку чи мережами суто телекомунікаційними, оскільки підтримують інтеграцію послуг передавання мови, даних та мультимедіа [59]. Основна відмінність мереж наступного покоління від традиційних мереж в тому, що вся інформація, яка циркулює в мережі, розбита на дві складові. Це сигнальна інформація, що забезпечує комутацію абонентів та надання послуг (і це не є IP-рівень, а глибші, фізичні та канальні рівні), і безпосередньо дані користувача, що містять корисну інформацію, призначену абоненту (голос, відео, дані). Шляхи проходження сигнальних повідомлень і даних користувача можуть не збігатися.

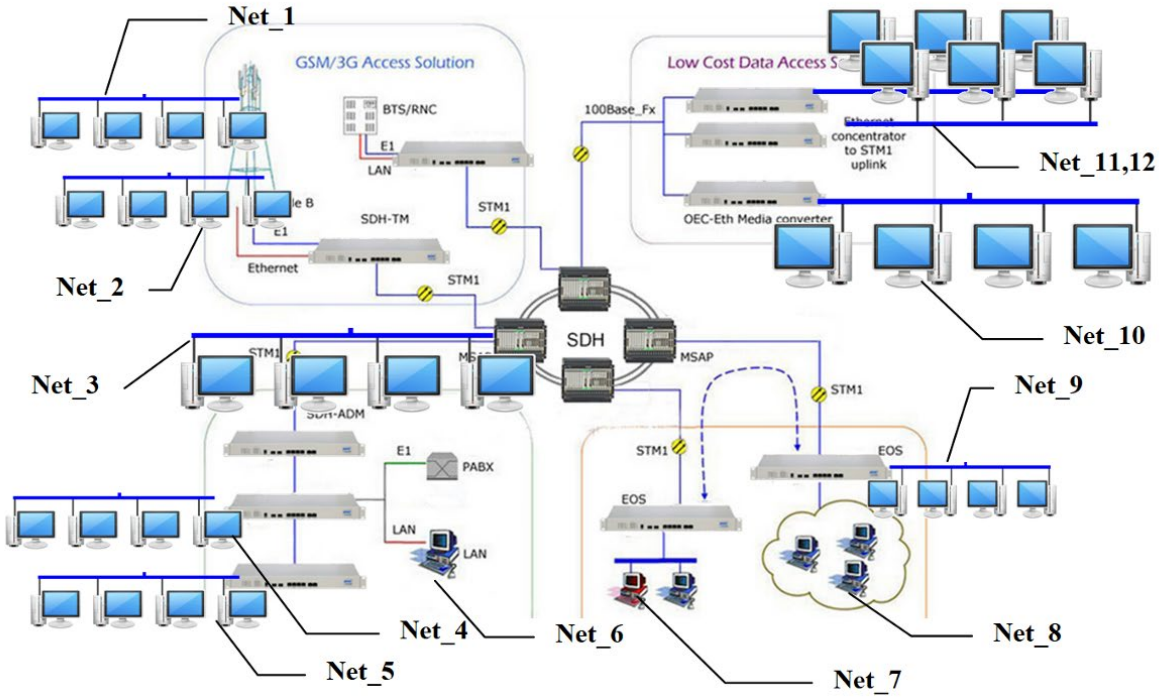


Рисунок 2.1.1 – Конвергенція різноманітних комп'ютерних та телекомунікаційних систем за допомогою Інтернет

Окремі комп'ютерні мережі мають зазвичай різноманітну архітектуру, в тому числі різні і несумісні між собою принципи адресації та маршрутизації. Функції адаптації та конверсії між окремими комп'ютерними мережами виконують так звані шлюзи. Заради забезпечення можливості передачі даних між всіма об'єднаними мережами, всі пристрої, що входять в об'єднану мережу (це можуть бути і кінцеві пристрої, але шлюзи – обов'язково) підтримують єдину спільну систему адресації.

В світовій практиці найбільш розповсюджені мультисервісні мережі на базі IP-мережі. Але не тільки протокол IP використовувався та використовується в глобальних комп'ютерних мережах. На початку 2000 років це були мережі, що базуються на технології ISDN, Frame Relay, ATM. Розглянемо архітектуру деяких таких мереж, які функціонують на цей час, та

визначимо особливості їхньої топологічної організації та методів забезпечення глобальної маршрутизації.

2.1.1. Топологія, адресація та засоби маршрутизації мереж Frame Relay, ATM, SDH/SONET

Frame Relay

Протокол ретрансляції кадрів («Frame Relay», FR) – один з широко відомих протокол канального рівня, який базується на сеансовій моделі з'єднань між абонентськими пристроями [58, 59].

Ефективність Frame Relay великою мірою завдячує наявним двом механізмам повідомлень про затори:

Пряме повідомлення про затори (forward-explicit congestion notification, FECN);

Зворотне повідомлення про затори (backward-explicit congestion notification, BECN).

FECN та BECN керуються єдиним бітом у заголовку кадру Frame Relay. У заголовку кадру є також біт збросу (Discard Eligibility, DE), який ідентифікує пакети, що можуть бути відкинуті у випадку затору.

Механізм FECN полягає у тому, що пристрої DCE у випадку заторів встановлюють біт FECN у кадрах, що мандрують між парою DTE. DTE-отримувач передає інформацію про затор до процесу вищого рівня, який відповідно корегує темп взаємодії.

У механізмі BECN біти BECN встановлюються DCE у кадрах, що мандрують назустріч кадрам з встановленим FECN. Таким чином повідомлення про затор одержує DTE-відправник та передає її до процесу вищого рівня. Для перевірки наявності помилок у Frame Relay використовується підрахунок контрольної суми даних (CRC).

Якщо, скажімо, IP – це передача даних пакетами, або дейтаграмами, то Frame Relay – це передача кадрів по віртуальних каналах. Для передачі даних від відправника до отримувача в мережі Frame Relay будуються віртуальні канали (virtul circuits) двох видів:

PVC (Permanent Virtual Circuit) – створюється адміністратором мережі між двома DTE та існує навіть при відсутності даних для передачі.

SVC (Switched Virtual Circuit) – створюється між двома DTE безпосередньо перед передачею та руйнується після закінчення передачі. Такий віртуальний канал створюється по наявних в FR-маршрутизаторах таблицях маршрутизації, по яких однозначно ідентифікуються пристрої DTE та порти, до яких вони підключені.

Кожний віртуальний канал однозначно визначається ідентифікатором канального з'єднання – Data-Link Connection Identifier (DLCI). Ці ідентифікатори є унікальними у межах конкретного оператора мережі Frame Relay.

Досить традиційними для FR є 3-байтові ідентифікатори DLCI та 2-байтові адреси кінцевих пристроїв.

До заготовка кадра Frame Relay (рис.2.1.2) входить наступна інформація:

DLCI (Data Link Connection Identifier) – ідентифікатор віртуального каналу (PVC), який мультиплексується у фізичний канал.

Address Field Extension Bit (EA) – біт розширення адреси. DLCI міститься в 10 бітах, що входять в два байти заголовка, проте можливе розширення заголовка на ціле число додаткових октетів з метою вказівки адреси. EA встановлюється в кінці кожного октету заголовка; якщо він має значення «1», то це означає, що даний октет в заголовку останній.

Forward Explicit Congestion Notification (FECN) – повідомлення про перевантаження каналу в прямому напрямі.

Backward Explicit Congestion Notification (BECN) – повідомлення про перевантаження каналу у зворотному напрямі.

Discard Eligibility Indicator (DE) – індикатор дозволу скидання кадру при перевантаженні каналу. Виставляється в «1» для даних, що підлягають передачі в негарантованій смузі (EIR) і указує на те, що даний кадр може бути знищений в першу чергу.

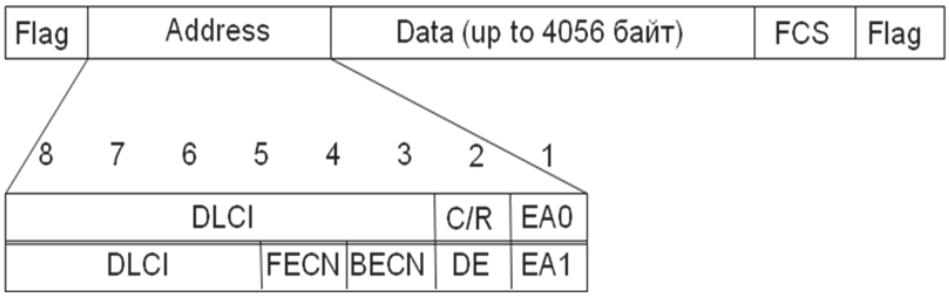


Рисунок 2.1.2 – Формат кадра Frame Relay

Одним з прогресивних рішень протоколу Frame Relay є специфікація Logical Management Interface (LMI). Головними рисами LMI є глобальна адресація, повідомлення про стан віртуального каналу та багатоадресна розсилка. Глобальна адресація перетворює ідентифікатори DLCI на унікальні адреси DTE в межах глобальної мережі Frame Relay. DLCI мають унікальне значення в глобальній мережі, але не забезпечують внутрішньорегіональної адресації, оскільки є однаковими у всії фреймів, що адресовані певному регіону (чи, краще сказали, локальній мережі). Тобто кадри, передавані через конкретний PVC в будь-якому напрямі (від абонента або до абонента), містять однаковий DLCI.

Повідомлення про стан віртуального каналу забезпечують обмін даними та синхронізацію між DTE та DCE. Ці повідомлення використовуються для періодичного аналізу стану PVC та уникання відправлення даних до «чорних дір» (по неіснуючим PVC).

В мережах Frame Relay Протокол Q.933 використовує адреси кінцевих вузлів, між якими встановлюється віртуальний канал. Адреса складається з 15

десяткових цифр, які діляться, як і звичайні телефонні номери, на поля коду країни (від 1до 3 цифр), коду міста і номера абонента. До адреси додається до 40 цифр під адреси, які потрібні для нумерації термінальних пристроїв, якщо у одного абонента їх кілька.

Таблиці маршрутизації для технології Frame Relay створюються вручну. Протокол автоматичного складання не визначений стандартом, можуть використовуватись пропрієтарні протоколи.

У мережах Frame Relay після встановлення віртуального з'єднання дані передаються тільки за допомогою протоколу канального рівня, що значно знижує накладні витрати. За віртуальним каналам Frame Relay можуть передаватися дані різних протоколів. Специфікація RFC 1490 визначає методи інкапсуляції в кадри Frame Relay пакетів мережевих протоколів, таких як IP і IPX, протоколів локальних мереж, наприклад Ethernet, а також протоколу SNA.

Таким чином, про топологію мережі Frame Relay можна сказати, що вона побудована на системі адресації і технології віртуальних каналів PVC та SVC, та слугує базою для інших, більше розвинутих та росповсюджених протоколів комп'ютерних мереж.

Мережа ATM

Асинхронний режим передачі даних (Asynchronous Transfer Mode, ATM) – універсальна транспортна мережа, яка проєктувалась для передачі неоднорідного трафіка: даних, голосу і відео [59].

Протокол ATM розбиває весь трафік на пакети строго фіксованої довжини (їх називають комірками – cell), що асинхронно мультиплексуються в єдиний цифровий тракт відповідно до привласненого пріоритету. Слово асинхронний у назві означає, що тактові генератори передавача і приймача не синхронізовані, а самі комірки передаються і мультиплексуються по запитах. Завдяки малій довжині комірок (53 байта, з них 48 байт несуть корисну інформацію, а комірка ATM у випадку транспортування голосових даних відповідає 6 мс звучання), можна організувати одночасну передачу потоку даних відразу декількох служб, критичних вчасно доставки – комірки з даними різних додатків будуть вставлятися в потік поперемінно, забезпечуючи кожному додатку необхідну швидкість обміну даними. У залежності від обсягу трафіка можуть бути організовані ATM-канали зі швидкістю передачі від 1,5 Мб/с до 40 Гб/с, при цьому дана технологія дозволяє уникати простою каналів.

Протокол ATM виконує комутацію за номером віртуального з'єднання (аналог DLCI в Frame Relay, див.2.2.1), який у технології ATM розбитий на дві частини – ідентифікатор віртуального шляху (VPI) і ідентифікатор віртуального каналу (VCI). Крім цієї основної задачі протокол ATM виконує ряд функцій по контролю за дотриманням трафік-контракту з боку користувача мережі, маркуванню осередків-порушників, відкиданню осередків-порушників при перевантаженні мережі, а також керуванню потоком осередків для підвищення продуктивності мережі (природно, при дотриманні умов трафік-контракта для усіх віртуальних з'єднань). Формат комірок протоколу ATM наведено на рис. 17. Вертикально розташовані байти, горизонтально – біти.

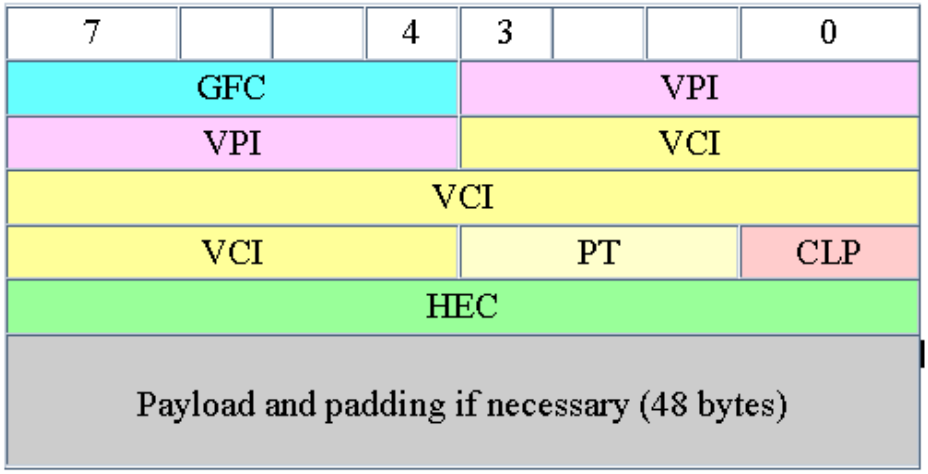


Рисунок 2.1.2 – Формат UNI (user-to-network interface) ATM cell

Поле *Керування потоком* (Generic Flow Control) використовується тільки при взаємодії кінцевого вузла і першого комутатора мережі. В даний час його точні функції не визначені.

Поля *Ідентифікатор віртуального шляху* (Virtual Path Identifier, VPI) і *Ідентифікатор віртуального каналу* (Vitual Channel Identifier, VCI) займають відповідно 1 і 2 байти. Ці поля задають номер віртуального з'єднання, розділений на старшу (VPI) і молодшу (VCI) частини.

Поле *Ідентифікатор типу даних* (Payload Type Identifier, PTI) складається з 3-х біт і задає тип даних, що переносяться коміркою, користувацькі або керуючі (наприклад, керуючі встановленням віртуального з'єднання). Крім того, один біт цього поля використовується для вказівки перевантаження в мережі – він називається Explicit Congestion Forward Identifier (ECFI) – і передає інформацію про перевантаження але напрямок потоку даних.

У полі *Пріоритет втрати кадру* (Cell Loss Priority, CLP) комутатори ATM відзначають комірки, що порушують угоди про параметри якості обслуговування, щоб видалити їх при перевантаженнях мережі. Таким чином, осередку з CLP-0 є для мережі високо пріоритетними, а з комірки CLP-1 – низько пріоритетними.

Поле *Керування помилками* в заголовку (Header Error Control, HEC) містить контрольну суму, обчислену для заголовка комірки. Контрольна сума обчислюється за допомогою техніки коригувальних кодів Хеммінга. Комутатор ATM обчислює контрольну суму для послідовності з 5 байт, що знаходяться в поле даних кадру CTM-N, і, якщо обчислена контрольна сума говорить про коректність заголовка комірки ATM, перший байт стає границею комірки. Якщо ж це не так, то відбувається зрушення на один байт і операція продовжується. Таким чином, технологія ATM виділяє асинхронний потік комірок ATM у потоці біт фізичного рівня, заснованого на комірках.

Адаптаційні рівні ATM (ATM Adaptation Levels):

AAL1 – AAL5, призначені для передачі трафіку з різними характеристиками. Наприклад AAL1 – для потоку з постійною швидкістю та

контролем послідовності комірок; AAL2 – для потоку зі змінною швидкістю. AAL реалізується кінцевими пристроями.

ATM гарантує якість задану обслуговування (Quality of Service, QoS) для з'єднань. Засобами забезпечення QoS є:

Контракт трафіка – параметри передбачуваного потоку даних, такі як максимальна смуга пропускання, постійна середня полоса пропускання, розмір пакету. Коли кінцева ATM-система підключається до мережі ATM, вона заключає з мережею контракт, базований на параметрах QoS.

Формування трафіку – засіб використання черг для обмеження виплесків потоків даних, максимальної швидкості передачі та забезпечення рівномірного „дріб'язгу" (jitter) відповідно до контракту.

Керування трафіком – комутатори ATM забезпечують примусове виконання контракту за допомогою керування трафіком. Комутатор визначає поточний трафік та порівнює його з параметрами контракту. Якщо трафік перевищує контрактний рівень, дял пакетів може бути встановлено біт пріоритету відкидання CLP (Cell Loss Priority).

Взаємодія через мережу ATM. Розглянемо методи комутації комірок ATM на основі пари чисел VPI/VCI. Комутатори ATM можуть працювати в двох режимах – комутації віртуального шляху і комутації віртуального каналу. У першому режимі комутатор виконує просування комірки тільки на підставі значення поля VPI, а значення поля VCI він ігнорує. Вони доставляють комірки з однієї мережі користувача в іншу на підставі тільки старшої частини номера віртуального каналу. У результаті один віртуальний шлях відповідає цілому набору віртуальних каналів, що комутуються як єдине ціле.

Після доставки комірки в локальну мережу ATM її комутатори починають комутувати всередині із врахуванням як VPI, так і VCI, але при цьому їм вистачає для комутації тільки молодшої частини номера віртуального з'єднання, так що фактично вони працюють з VCI, залишаючи VPI без зміни. Останній режим називається режимом комутації віртуального каналу.

При необхідності передачі даних кінцевий пристрій, який є джерелом цих даних, надсилає до пункту призначення запит на створення з'єднання. Цей запит несе в своєму складі параметри QoS. Запит поширюється мережею через комутатори та досягає пристроя призначення, який може або задовольнити запит, або відмовити, про що він повідомляє відправника запиту.

Для визначення маршрутів передачі даних через мережу ATM комутатори мають знати топологію мережі та характеристики каналів зв'язку. Для поширення цієї інформації використовується протокол Public-Network Node Interface, PNNI, який є подібним до протоколу OSPF та додатково враховує пропускну спроможність каналів.

Емуляція LAN. LAN Emulation (LANE) – стандарт для надання кінцевим пристроям мережі ATM послуг, еквівалентним тим, що надаються мережами Ethernet або Token Ring. LANE полягає в тому, що в мережі ATM емулюється мережне середовище (фізичний та канальний рівні) мереж Ethernet IEEE 802.3 або Token Ring IEEE 802.5. Головна суть технології LANE – встановлення відповідності між ATM-адресами та MAC-адресами. Протокол

LANE регламентує функціонування однієї емульованої LAN в ATM-мережі, але реально в одній й тій самій мережі ATM одночасно можуть бути емульовані декілька LAN, що робить можливим утворення за допомогою ATM розгалужених локальних мереж, віртуальних робочих місць та інших досі актуальних мережевих послуг.

Мережі SDH/SONET

Мережі SONET (Synchrous Optical Network) та SDH (Syncrous Digital Hierarchy) [63, 64] є результатом об'єднання та гармонізації умовно американського та умовно евпропейського стандарту передачі трафіку цифрових каналів PDH (Plesiosynchrous Digital Hierarchy), ієрархія яких наведена в табл. 2.1.1.

Кадри STM-N мають досить складну структуру, що дозволяє агрегувати в загальні й магістральний потік потоки SDH і PDH різних швидкостей, а також виконувати операції введення-виведення без повного демультиплексування магістрального потоку. Операції мультиплексування і введення-виведення виконуються за допомогою віртуальних контейнерів (Virtual Container, VC), в яких блоки даних PDH можна транспортувати через мережу SDH. Крім блоків даних PDH в віртуальний контейнер поміщається ще деяка службова інформація.

Таблиця 2.1.1 – Рівні ієрархії SDH та SONET

SDH	SONET	Швидкість
	STS-1.OC-1	51,84 Мбіт/с
STM-1	STS-3, OC- 3	155,520 Мбіт/с
STM-3	OC-9	466,560 Мбіт/с
STM-4	OC-12	622,080 Мбіт/с
STM-6	OC-18	933,120 Мбіт/с
STM-8	OC-24	1,244 Гбіт/с
STM-12	OC-36	1,866 Гбіт/с
STM-16	OC-48	2,488 Гбіт/с
STM-64	OC-192	9,953 Гбіт/с
STM-256	OC-768	39,81 Гбіт/с

Віртуальні контейнери є одиницею комутації мультиплексорів SDH. У кожному мультиплексоре існує таблиця з'єднань (звана також таблицею кросс з'єднань).

Таблицю з'єднань формує адміністратор мережі за допомогою системи управління або керуючого терміналу на кожному мультиплексоре так, щоб забезпечити наскрізний шлях між кінцевими точками мережі, до яких підключено призначене для користувача устаткування.

Щоб поєднати в рамках однієї мережі механізми синхронної передачі кадрів (STM-N) і асинхронний характер призначених для користувача даних PDH, в технології SDH повинні застосовуватися вказівні знаки (покажчики). Концепція покажчиків – ключова в технології SDH. Покажчик визначає поточний стан віртуального контейнера в агрегированной структурі вищого рівня, якою є трибутарний блок (Tributary Unit, TU) або адміністративний блок (Administrative Unit, AU). Основна відмінність цих блоків від віртуального контейнера полягає в наявності додаткового поля покажчика. За допомогою цього покажчика віртуальний контейнер може «зміщуватися» в певних межах всередині свого трибутарного або адміністративного блоку, якщо швидкість призначеного для користувача потоку дещо відрізняється від швидкості кадру SDH, куди цей потік мультиплексуюча.

Саме завдяки системі покажчиків мультиплексор знаходить положення призначених для користувача даних в синхронному потоці байтів кадрів STM-N і «на льоту» витягує їх звідти, чого механізм мультиплексування, застосовуваний в PDH, робити не дозволяє.

Трибутарні блоки об'єднуються в групи, а ті, в свою чергу, входять в адміністративні блоки. Група адміністративних блоків (Administrative Unit Group, AUG) в кількості N і утворює корисне навантаження кадру STM-N. Крім цього в кадрі є заголовок із загальною для всіх блоків AU службовою інформацією. На кожному кроці перетворення до попередніми даними додається кілька службових байтів: вони допомагають розпізнати структуру блоку або групи блоків і потім визначити за допомогою покажчиків початок призначених для користувача даних.

Основним елементом мережі SDH є мультиплексор. Зазвичай він оснащений деякою кількістю портів PDH і SDH. Порти мультиплексора SDH діляться на агрегатні і трибутарні. Є термінальні мультиплексори, з одним агрегатним та декількома (чи, скоріше, багатьма) трибутарними каналами, є так звані add-drop мультиплексори, на яких в головний транспорт додаються чи «виймаються» з нього окремі канали.

В SDH існує власний стек протоколів, але з точки зору моделі OSI вони всі утворюють та обслуговують фізичний рівень цієї мережі.

Однією з сильних сторін первинних мереж SDH є різноманітний набір засобів відмовостійкості, який дозволяє мережі швидко (за десятки мілісекунд) відновити працездатність в разі відмови будь-якого елементу мережі – лінії зв'язку, порту або карти мультиплексора, мультиплексора в цілому.

Живучісті складних комп’ютерних систем присвячено багато уваги в [65, 66]. Загальна назва механізмів відмовостійкості в SDH має назву «автоматичне захисне перемикання» (Automatic Protection Switching, APS), що відображає факт переходу на резервний шлях або резервний елемент мультиплексора при відмові основного. Мережі, які підтримують такий механізм, в стандартах SDH названі такими, що самовідновлюються.

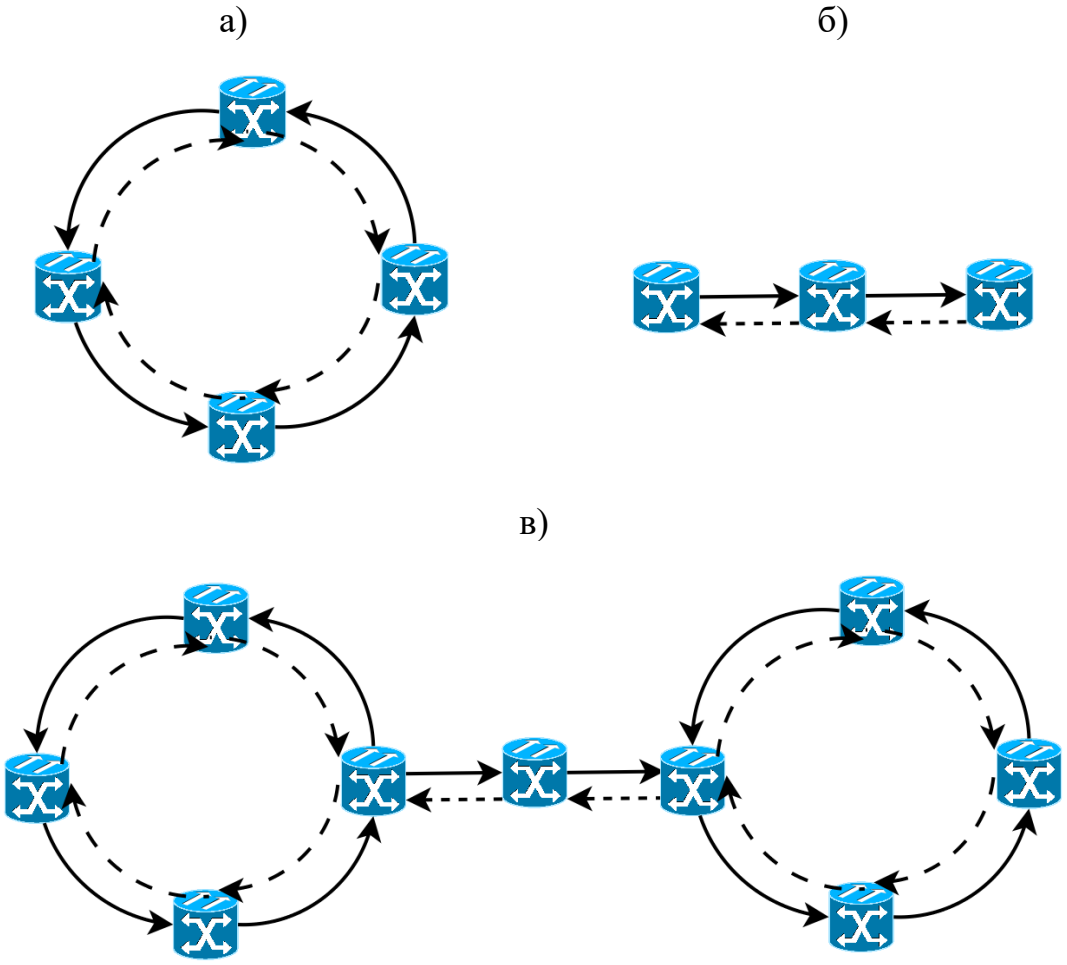


Рисунок 2.1.7 – Топології SDH

Залежно від обраної топології, в мережах SDH застосовуються три схеми захисту. Захист «1+1» означає, що резервний елемент виконує ту ж роботу, що і основний. Наприклад, при захисті трибутарних карти по схемі «1+1» трафік проходить як через робочу карту (резервовану), так і через захисну (резервну). Захист «1:1» передбачає, що захисний елемент в нормальному режимі не виконує функції захищається елемента, а переключається на них тільки в разі відмови. Захист «1:N» передбачає виділення одного захисного елемента для захисту N інших елементів. При відмові одного з елементів, що захищаються його функції починає виконувати захисний, при цьому інші елементи залишаються без захисту – до тих пір, поки що відмовив елемент не буде замінений.

Залежно від топології і типу об'єкта, що захищається шляхом резервування елемента, мережі в обладнанні та мережах SDH застосовуються такі основні види автоматичного захисту: захисне перемикання обладнання, захист карт, захист мультиплексной секції, захист мережевого з'єднання, колективна захист мультиплексной секції в кільцевої топології.

Захист SNC-P працює в будь-яких топологиях мереж SDH, в яких є альтернативні шляхи прямування трафіку, тобто кільцевих і пористих. Колективний захист мультиплексной секції в кільцевої топології (Multiplex

Section Shared Protection Ring, MS-SPRing) показаний на рисунку вище у вигляді пунктирної риски. Він забезпечує в деяких випадках більш економічну захист трафіку в кільці. Хоча захист SNC-P цілком підходить для кільцевої топології мережі SDH, в деяких випадках її застосування знижує корисну пропускну здатність кільця, так як кожне з'єднання споживає подвоєну смугу пропускання вздовж усього кільця.

Захист MS-SPRing дозволяє використовувати пропускну здатність кільця більш ефективно, так як смуга пропускання не резервується заздалегідь для кожного з'єднання. Замість цього резервується половина пропускної здатності кільця, але ця резервна смуга виділяється для з'єднань динамічно, в міру необхідності, тобто після виявлення факту відмови лінії або мультиплексора. Ступінь економії смуги при застосуванні захисту MS-SPRing залежить від розподілу трафіку. Якщо весь трафік сходиться в один мультиплексор, тобто є звездообразное розподіл, захист fvlS-SPRing економії в порівнянні з SNC-P взагалі не дає. Приклад такої ситуації представлений на рис. 5, а, де центром «тяжіння» трафіку є мультиплексор Л, а в кільці встановлені ті ж 16 захищених з'єднань, що і в прикладі захисту SNC-P на рис. 4 Для захисту з'єднань резервується 8 з 16 віртуальних контейнерів агрегатного потоку STM-16.

2.1.2. Топології в MetroEthernet та MPLS

Мережі MetroEthernet

Під терміном MetroEthernet розуміють багатофункціональну мережу масштабу міста. Це рішення будується на базі швидкісних комутаторів Ethernet і засноване на мережевій архітектурі, що припускає швидке зростання сервісів, що вимагають великої смуги пропускання, таких як відео по IP і мультимедійними додатками [60]. Особливостями архітектури MetroEthernet є:

- модульність – рівні будуються на основі модулів, кожен модуль являє собою функціонально закінчену одиницю, що виконує функції відповідно рівня.
- ієрархічність – мережа поділяється на декілька рівнів, кожен рівень виконує певні функції;

Рівні архітектури мережі Metro Ethernet:

- ядро мережі – високошвидкісна комутація трафіку;
- рівень агрегації – виконує сполучну функцію і функцію агрегації трафіку абонентів;
- рівень доступу – для підключення абонентів до мережі оператора

В топології Metro Ethernet присутні два типи з’єднань [61] (рис.2.1.5):

1) UNI (User-to-Network Interface) являє собою фізичний інтерфейс – точку розмежування між сервіс-провайдером і користувачем, яку ще називають точкою надання послуг.
2) NNI (Network-to-Network Interface) – точка розмежування між сервіс-провайдерами (E-NNI), або між внутрішніми мережами сервіс-провайдера (I-NNI).

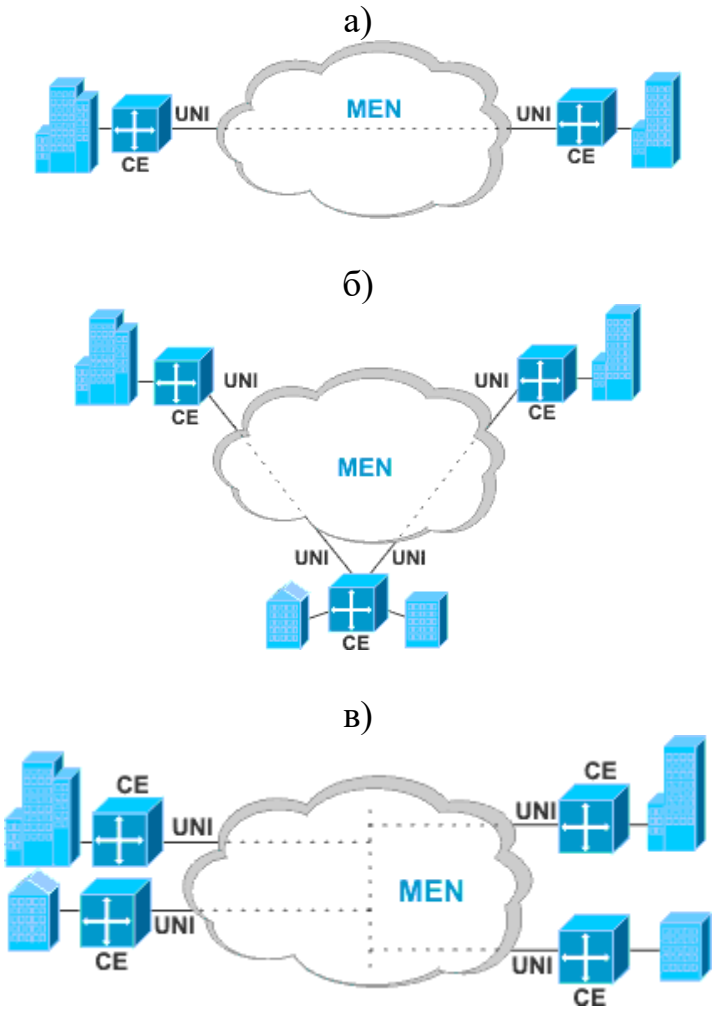


Рисунок 2.1.5 – схема архітектури MetroEthernet: E-Line (а), E-Tree (б), E-LAN (в)

Головною послугоє мережі є Ethernet Virtual Connection (EVC) – з'єднання двох або більше UNI. Саме EVC дозволяє створювати різноманітні топології в мережі Metro Ethernet, типу розгалужених дерев. Розрізняють три типи EVC:

- точка-точка (E-Line);
- багатоточка-багатоточка (E-LAN);
- точка-багатоточка, або дерево (E-Tree).

У мережі, що створюється за допомогою сервісів Metro Ethernet, користувачі використовують звичайне обладнання Ethernet. Дані транспортуються по з'єднаннях точка-точка, точка-багатоточка і багатоточка-багатоточка EVCs відповідно до атрибутами і визначеннями, зробленими в E-Line і E-LAN службах.

Мережі MPLS

Мультипротокольна комутація за допомогою міток (Multiprotocol Label Switching, MPLS) є стандартизованим [62] методом швидкої маршрутизації для застосування, перш за все, в швидкісних (0,1 – 40 Гбіт/с) IP-мережах. Створення технології дозволило об'єднати переваги методу віртуальних каналів

з дейтаграмним. У цій технології протоколи маршрутизації стека TCP/IP використовуються для дослідження топології мережі і знаходженні раціональних маршрутів, а просуваються пакети на основі техніки віртуальних каналів.

В традиційних IP-мережах кожен маршрутизатор визначає маршрут для кожного пакета на основі даних його заголовка (destination-адреса та маска підмережі), аналізу власної таблиці маршрутизації (порівняння адреси/маски, обрання найкращого співпадіння), та інколи за допомогою інших параметрів. В будь-якому разі необхідно розібрати заголовок пакета, який містить значно більше інформації, ніж потрібно для обрання маршруту на один наступний крок. В MPLS, визначення маршруту відбувається зовсім іншим шляхом – за допомогою мітки (label), яку встановлює попередній маршрутизатор (див. далі).

Головна перевага технології MPLS – це створення основи для розгортання нових типів послуг, що не підтримуються традиційною маршрутизацією або підтримуються занадто складно. MPLS дозволяє зменшити собівартість та покращити якість базових послуг, розширює існуючі можливості маршрутизації. Можливість класифікації пакетів за багатьма параметрами дозволяє адміністратору скеровувати потоки трафіку за обраним і оптимальним шляхом.

Технологія MPLS розширює можливості з контролю трафіку. Це означає більш ефективну роботу мережі, передбачувану якість послуг і гнучкість, що дозволяє задовольняти потреби користувачів.

MPLS дозволяє підтримувати наступні послуги:

- трафік інжиніринг (TE);
- якість послуг (QoS);
- intranet VPN;
- extranet VPN;
- VPN другого рівня (MPLS L2 VPN);
- VPN третього рівня (MPLS L3 VPN);
- доступ до зовнішніх послуг;
- доступ в Інтернет тощо.

У IP-мережах будь-який маршрутизатор аналізує заголовок кожного пакету, щоб визначити адресу призначення пакету та обрати напрямок до наступного маршрутизатора.

В технології MPLS до IP-пакетів додаються мітки-ідентифікатори невеликої та фіксованої довжини. Мітка має локальне значення – вона дійсна на ділянці між двома сусідніми маршрутизаторами. Кожен маршрутизатор, пересилаючи пакет, позначає його іншою міткою. На вході до MPLS-мережі маршрутизатор встановлює відповідність між пакетом і так званим „класом еквівалентності пересилки” (англ. Forwarding Equivalence Class, FEC). До одного FEC відносяться пакети, що мають схожі характеристики, і можуть бути направлені тим самим шляхом. Параметри, що визначають FEC, залежать від конфігурації маршрутизатора. Типовим є використання IP-адреси призначення для визначення FEC. Кожен FEC має свій набір міток, що визначає шлях

доставки пакетів. Застосування міток значно прискорює доставку пакетів, тому що маршрутизатор не аналізує заголовок IP-пакету, а виконує комутацію за допомогою міток, що займає значно менше часу.

На схемі (рис. 2.2.5) зображена MPLS-мережа, яка містить маршрутизатори двох типів:

- прикордонні маршрутизатори MPLS (англ. Label Edge Router, LER);
- транзитні маршрутизатори MPLS (англ. Label Switched Router, LSR).

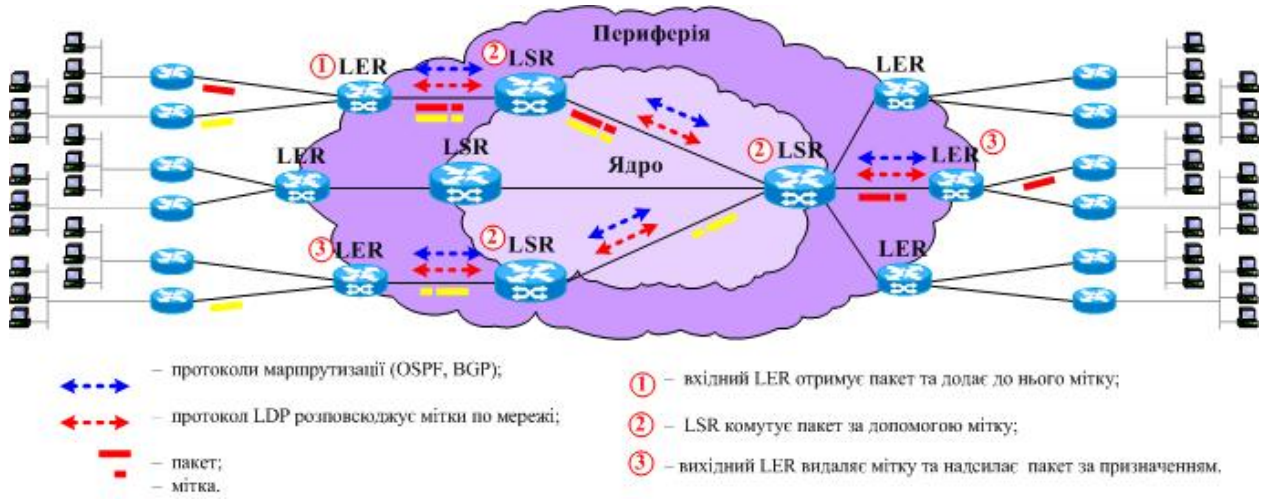


Рис. 2.1.6 – Схема функціонування MPLS-мережі

По відношенню до будь-якого пакету, що проходить по MPLS-мережі, один LER є вхідним, а інший LER – вихідним. Вхідний LER аналізує заголовки пакету, що надійшов зовні, встановлює до якого FEC він належить та надсилає пакет до відповідного LSR. Долаючи кілька LSR, пакет потрапляє до вихідного LER, що видаляє з пакету мітку, аналізує заголовок та надсилає його адресату, що знаходиться зовні MPLS-мережі.

Послідовність ($LER_{вх}$, LSR, ..., LSR_n, $LER_{вих}$) маршрутизаторів, через які проходять пакети, що належать одному FEC, утворює шлях з комутацією за допомогою міток (англ. Label Switched Path, LSP). Той самий LER може бути для одних потоків вхідним, для інших – вихідним.

На сьогодні MPLS є основною технологією надання корпоративним клієнтам послуг об'єднання різних підрозділів в межах опорної мережі одного сервіс провайдера. Після чого по ємульованій локальній мережі, зазвичай, замовник будує корпоративну мережу на принципах тієї ж IP-маршрутизації, яка лежить і в основі мережі, по якій побудована мережа MPLS. Міжоператорська взаємодія з побудови спільних чи об'єднаних MPLS мереж не є загальною практикою, на відміну від мереж TCP/IP.

2.2. Архітектура глобальної мережі Інтернет

2.2.1. Мережеві префікси та автономні системи

Спільна адресація в мережі Інтернет називається IP-адресацією і полягає в присвоєнні кожному мережевому пристрою унікального цифрового ідентифікатора. IP адреса протоколу мережевого рівня IPv4 складається з 32 біт, а протоколу IPv6 – з 128 біт, але не всі біти в адресі мають однакове значення. Біти діляться на дві частини: зліва кілька біт позначають мережу, до якої належить цей адреса, що залишилися біти справа ідентифікують пристрій всередині мережі. Кордон між цими двома групами бітів може проходити в різних місцях, наприклад, для 32-бітного адреси, перші 16 біт можуть позначати мережу, другі – хост всередині мережі, можливі будь-які інші поєднання (10 і 22, 8 і 24, 30 і 2) – в принципі, будь-які два числа, що дають в сумі 32. Для опису того, де проходить ця межа, використовується мережевий префікс. Він записується зазвичай після адреси у вигляді десяткового числа через слеш, наприклад 10.0.0.0/8 або 192.168.10.123/19 (8 і 19 – префікси).

Префікс позначає, скільки біт в наведеному адресу зберігають інформацію про мережі. Наприклад, якщо префікс /24, це означає, що в адресі з 32-х біт 24 біта зберігають інформацію про мережі, а решта 8 – інформацію про вузол. Межа між адресою хоста та підмережі проходить по будь-якому біту в адресі, тому в підмережі може бути лише кількість адрес кратна ступеню двійки. Параметрично ця межа задається при налаштуванні пристрою у вигляді так званої мережевої маски. Мережевий префікс і мережева маска означають одне і те саме, тільки різними способами, які відрізняються нотацією.

Ще на початку 1980 років розробники Інтернет-технологій бачили тенденцію щодо швидкого зросту мережі, неструктурованого збільшення кількості шлюзів, які були під керуванням зовсім різного програмного забезпечення та не підлягали типовому обслуговуванню. Передбачуваними наслідками такого зросту стали:

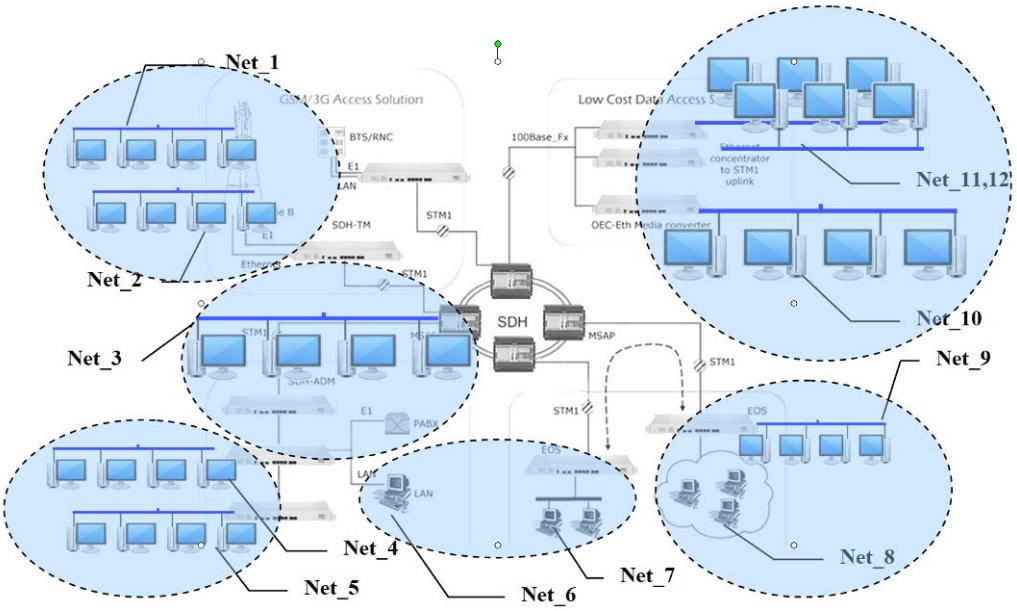
- багаторазове збільшення потоків інформації, пов‘язаної з передачею та обробкою таблиць маршрутизації;
- неможливість обслуговування Інтернету як єдиної системи через неможливість ізоляції помилок, збоїв маршрутизації;
- сталі алгоритми маршрутизації та ПО зовсім негнучкі через те, що неможливо забезпечити пропоновані зміни у всій мережі одночасно, бо це потребує адаптації до кожної окремої системи.

Тоді й виникла ідея увести поняття домену, або *автономної системи*, єдиної частки мережі, із будь-яким внутрішнім устроєм, але стандартними зовнішніми маршрутизаторами, які реалізують стандартні протоколи взаємодії з іншими автономними системами.

На сьогодні термін «автономна система» використовується не стосовно обладнання, а стосовно певної групи IP-адрес – мережевих префіксів. На рис.

2.2.1 схематично зображений процес переходу, чи конверсії *окремих мереж в автономні системи*.

а)



б)

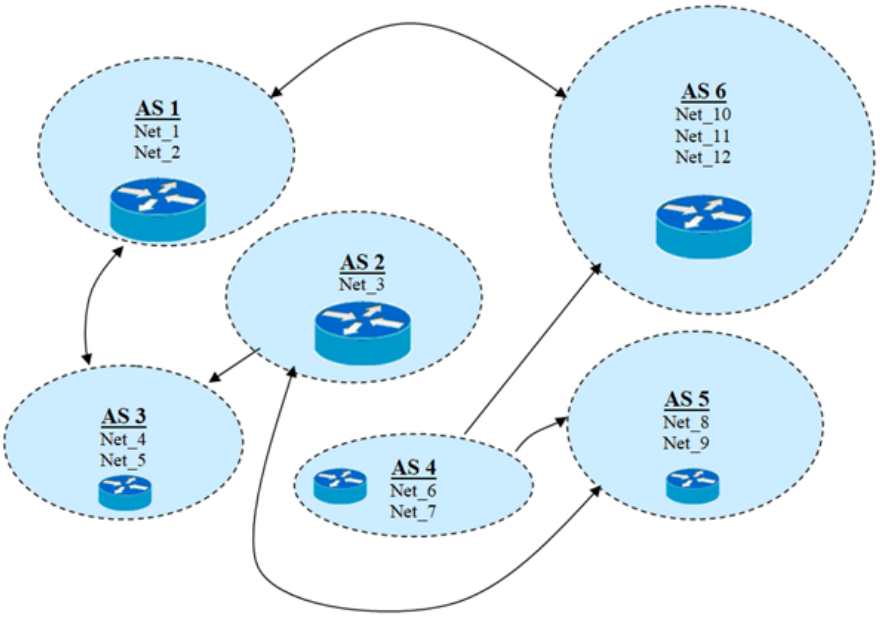


Рисунок 2.2.1 – Конверсія окремих мереж в автономні системи: об'єднання мереж спільним управлінням (а) та перехід до системи глобальної маршрутизації (б)

Автономна система (AS) – це поєднана група з одного або більше IP-префіксів, які керуються одним чи більше операторами, які мають єдину та чітко визначену політику маршрутизації. Кожна AS має 16- або 32-бітний номер для ідентифікації в процесі обміну інформацією с іншими AS [2].

Обмін інформацією між AS здійснюють сусідні шлюзи (neighbors, peers).

Автономні системи повинні мати можливість не тільки взаємодіяти одна з одною, але й забезпечувати транзитні функції для автономних систем, які не

мають безпосереднього зв‘язку, аби забезпечити для кінцевого користувача „прозорість” Інтернету як єдиної мережі. Ця ідея знайшла відображення в документі RFC 827 «Зовнішній шлюзовий протокол» (Exterior Gateway Protocol – EGP), або протокол зовнішньої маршрутизації [70].

2.2.2. Маршрути та маршрутизація

Як було сказано, обмін даними між окремими мережами виконують маршрутизатори. Для цього на маршрутизаторах виконуються спеціальні програми, які називають протоколами маршрутизації.

Множина оптимальних маршрутів

Формальним результатом рішення завдання вибору оптимальних потоків в мережі [70] є множина змінних $x_{kl}^{(i,j)};\ \ i,j,k,l=1,2,...,N.$ Якщо ці змінні відомі, легко визначити величини потоків в лініях зв’язку f_{kl}, множину оптимальних маршрутів для всіх пар «джерело-адресат» і частки від вхідних потоків γ_{ij}, які треба передавати за оптимальними маршрутами. Самі по собі змінні $x_{kl}^{(i,j)}$ не мають суттєвого смислу, тому багато з алгоритмів рішення завдання вибору оптимальних потоків, визначають лише потоки в лініях зв’язку f_{kl}, за допомогою яких визначається час мінімальної затримки T.

У деяких випадках необхідно знати, які саме маршрути приводять до оптимального розподілу потоків. Тобто ставиться завдання: для кожної пари вузлів «ДА (i,j)» необхідно визначити множину оптимальних маршрутів $\Pi_{ij}=\left\{\pi_{ij}^{(r)}\right\},\ \ r=1,2,...,R_{ij}$ ($R_{ij}-$ кількість оптимальних маршрутів від вузла i до вузла j) та долі потоків $\alpha_{ij}^{(r)}$ від вхідного потоку γ_{ij}, у відповідності до яких використовуються маршрути $\pi_{ij}^{(r)}$ $\left(\sum_{r=1}^{N}\alpha_{ij}^{(r)}=1\right)$. Очевидно, для фіксованої маршрутизації $R_{ij}=1$ та $\alpha_{ij}^{(1)}=1.$

Рішення цього завдання здійснюється за допомогою відповідних алгоритмів.

Динамічна маршрутизація

Динамічною маршрутизацією (або дейтаграмною маршрутизацією, динамічною адаптивною маршрутизацією) зветься такий варіант маршрутизації, при якому для кожного пакета даних вибирається визначений шлях в мережі на базі поточної інформації, що одержується від вузлів, через які проходить цей пакет. На практиці динамічна маршрутизація – це процес використання певних протоколів взаємодії між мережними маршрутизаторами для поновлення їхніх таблиць маршрутизації. Динамічна маршрутизація має певні недоліки:

- навантаження CPU маршрутизаторів;
- службовий трафік, який навантажує канали з'єднання між маршрутизаторами.

При динамічній маршрутизації маршрутизатори, які встановлені на вузлах мережі, надають одне одному інформацію про відомі маршрути. Спочатку кожен маршрутизатор має інформацію лише про безпосередньо приєднані до нього вузли (підмережі) та ті, що явно було вписано до його таблиці маршрутизації адміністратором. В процесі роботи інформацію про всі маршрути передається кожному з маршрутизаторів.

Дистанційно-векторний протокол маршрутизації (протокол Беллмана-Форда) побудований на обчисленні дистанційного вектору (distance vector), який водночас вказує напрямок маршруту (IP-префікс) та відстань до нього. Відстань в комп'ютерних мережах зазвичай визначалась не в одиницях довжини, а або в часі, або в кількості ретрансляцій між маршрутизаторами. Зрозуміло, що один і той самий маршрут може мати відмінні дистанційні характеристики на кожному з маршрутизаторів. До таких протоколів відносяться RIP, RIP-2, BGP. Отримуючи дистанційні вектори від сусідів, маршрутизатор обчислює найкоротший, вносить його до своєї таблиці адресації (forwarding table) та передає вже власний обчислений вектор сусідам.

Протоколи на основі аналізу стану каналу (link-state routing protocols) побудовані на основі обміну так званими звітами про стан з'єднання (link states). Кожний маршрутизатор передає дані про найближчих сусідів, під'єднані мережі та стан каналів, у якому (вручну чи динамічно) враховується пропускна спроможність та затримки передачі в каналі. Кожний маршрутизтор зберігає отриману інформацію у власну базу даних (link state database), з якої обирає найкращий маршрут за допомогою алгоритму Дейкстри.

Роботу такого протоколу порівнюють із збиранням пазлу, де кожний маршрутизатор мережі є елементом пазлу. До переваг таких протоколів відноситься велика швидкість обрання оптимального маршруту, до недоліків – погана масштабованість (важко уявити собі динамічно поновлювану базу на мільйони та мільйони з'єднань). Найуживанішим прикладом link-state протоколу є OSPF (open shortest path first), який успішно працює в межах окремих автономних систем, про які буде надано інформацію далі.

Концепція міждоменної маршрутизації

У випадку збільшення обсягу мережі виникають такі проблеми:

- зростання кількості маршрутів – збільшення навантаження на CPU маршрутизаторів та на мережу;
- зростання часу на поширення інформації між маршрутизаторами;
- важкість узгодження налаштувань маршрутизації між адміністраторами, які супроводжують різні підмережі;
- необхідність реалізації політик маршрутизації.

Для подолання цих проблем і застосовується концепція AS, якими найчастіше виступають підмережі провайдерів та корпоративні мережі [1, 2, 70].

В процесі розвитку системи глобальної маршрутизації в Інтернеті з'явились два типи протоколів динамічної маршрутизації:

– Interior Gateway Protocol (IGP);
– Exterior Gateway Protocol (EGP).

IGP використовується для обміну інформацією про маршрути між окремими маршрутизаторами, які належать до АС.

EGP використовується для обміну інформацією про маршрути між автономними системами.

Для кожної автономної системи вибирається власний протокол маршрутизації, за допомогою якого здійснюється взаємодія між маршрутизаторами в цій автономній системі. Такий протокол називається протоколом внутрішніх маршрутизаторів (IGP – interior gateway protocol) або протоколом внутрішньої доменної маршрутизації (intradomain routing protocol). Найбільш популярні IGP – це протокол обміну інформацією про маршрутизації RIP-2 (Routing Information Protocol), Open Shortest Path First (OSPF) та Intermediate System to Intermediate System (IS-IS).

В якості EGP використовується вже згаданий Border Gateway Protocol (BGP). Маршрутна інформація має вигляд послідовності AS на шляху до призначення, що може використовуватись як критерій для обрання оптимального (найкоротшого) маршруту. На відміну від IGP, BGP-взаємодія відбувається між парами безпосередньо поєднаних маршрутизаторів. Більш детальна інформація щодо протоколу BGP буде розглянута нижче.

Шлюз – це маршрутизатор, який забезпечує взаємодію з зовнішніми мережами. Мета існування шлюзу – застосування політики маршрутизації та обмін маршрутами із сусідніми шлюзами.

Сусідніми є шлюзи, якщо вони або безпосередньо підключені один до одного (принаймні на мережевому рівні), або взаємодіють крізь мережу, структура якої їм відома та використовується для адресації пакетів один одному. Остання обмовка важлива для розуміння: шлюзи не можуть бути peers, якщо вони не знають маршруту один до одного ще до обміну маршрутами. Тобто, якщо адреси шлюзів належать до різних префіксів, в кожного з них має бути закладена адреса наступного маршрутизатора на шляху до шлюзу, який має стати сусідом. В протоколі BGP 4 (далі) цей механізм реалізовано за допомогою атрибута next hop.

Сусідні шлюзи звуться *внутрішніми* (interior peers), якщо вони частиною тієї самої AS.

Сусідні шлюзи звуться *зовнішніми* (exterior peers), якщо вони належать до різних AS.

Аби AS1 мала змогу використовувати AS2 для передачі даних, шлюз AS1 повинен мати змогу визначити за допомогою сусіднього, який належить AS2, які мережі (префікси) є досяжними через нього (рис. 2.1.3). Неважливо, чи NET1 належить до ASx, чи просто ASx якимось чином знає маршрут до

NET1, якщо ASx передасть ASy інформацію, що NET1 є досяжною через ASx, ця дія є елементом політики маршрутизації, а передана інформація – анонсом. ASy може скористатись цим анонсом, шляхом внесення відповідні зміни в маршрутизацію, або проігнорувати (не прийняти) його.

NET1 ..... ASx <---> ASy NET2

Рисунок 2.1.3 – Приклад взаємодії автономних систем з RFC1930

Отже, префікси анонсуються автономними системами (в іноземній літературі використовується термін «originating», отже в кожного префіксу є свій «origin» – автономна система, до якої він належить. Така AS анонсує префікс і є джерелом маршруту до цього префікса. Приклад такої взаємодії AS було наведено на рис. 2.1.2 (б).

2.2.3. Система глобальної маршрутизації Інтернету

Узагальнимо, що входить до системи глобальної маршрутизації Інтернет на основі рис.2.1.2 (б). До неї належать такі об'єкти:

1) p ={Net_1, Net_2,..Net_10} – множина **мережевих префіксів**, кожен префікс прив'язаний до певного та єдиного вузла v, званого "*джерелом*":

$$\forall p : p \in v_{\text{i}} \Leftrightarrow p \notin v_j,\ v_i, v_j \in V\ ;$$

2) V = {AS1,AS2,..AS5} – множина **вузлів** V, кожен вузол є джерелом для певних префіксів:

$$\forall v \in V : \exists \{p_1, p_2, ..., p_n\} \in v\ ;$$

3) направлені **з'єднання суміжних AS,** по яких *анонсуються* префікси p:

$$l_p = \{AS_i, AS_j\} \neq \{AS_j, AS_i\}$$

З'єднання можуть розглядатись виключно в контексті передачі по них інформації про доступність мережевих префіксів.

Крім того, до системи глобальної маршрутизації належать і процеси, які виконуються алгоритмами протоколу BGP-4, основною функцією якого є обмін інформацією про доступність окремих мереж.

2.3. Визначення топологічного простору Інтернету

2.3.1. Проблеми визначення терміну «топологія Інтернет»

Топологією комп'ютерної мережі називають визначений її архітектурою спосіб організації чи взаємного розташування її елементів, до яких входять всі види пристроїв мережі (кінцеві пристрої, комутатори, маршрутизатори, подовжувачі, таке інше, та власне з'єднання) [32].

Також топологією комп'ютерної мережі називають структуру у вигляді графа, яка може представити взаємодію елементів мережі як на так званому фізичному рівні (де демонструються розташування пристроїв та маршрути прокладання кабелів), так і на логічному, де описуються потоки даних. Оскільки відомо, що Інтернет є об'єднанням комп'ютерних мереж, і сутність його саме в цьому об'єднанні за принципами загальної логічної адресації та маршрутизації, варто розглядати «топологію Інтернет» саме на логічному рівні, де описуються потоки даних.

В [33] топологією Інтернету називають неформалізовану конструкцію, в якій кінцеві пристрої, маршрутизатори, автономні системи з'єднані одне з одним. Таке визначення містить очевидні протиріччя. Перше протиріччя полягає в тому, що з'єднання кінцевих пристроїв та маршрутизаторів властиве будь-якій составній комп'ютерній мережі і, таким чином, таке визначення не є специфічним для Інтернету. Друге протиріччя полягає в тому, що автономна система за визначенням є результатом адміністративного об'єднання маршрутизаторів, а тому припущення про кінцевий пристрій, з'єднаний з автономною системою, є некоректним.

Робота [34], на яку посилаються автори [33], пропонує інше визначення топології Інтернет, а саме – сукупність взаємопоєднаних доменів маршрутизації (routing domains). Ці домени являють собою «групу вузлів (маршрутизатори, комутатори та хости) під єдиним технічним адмініструванням, в яких спільна маршрутизаційна інформація та правила».

Отже, тут топологія являє собою з'єднання груп неоднорідних вузлів, при чомі визначення цих груп співпадає з наведеними раніше у р.2.1 визначенням автономної системи. Тобто, синтезуючи це визначення, з більш загальними поняттями топології комп'ютерних мереж, можна запропонувати два формулювання:

1) Топологією комп'ютерної мережі Інтернет є визначений системою глобальної маршрутизації спосіб з'єднання її автономних систем, до яких входять окремі мережеві префікси зі спільною політикою маршрутизації.
2) Топологією комп'ютерної мережі Інтернет є структура у вигляді графа, яка може представити взаємодію її автономних систем, до яких входять окремі мережеві префікси зі спільною політикою маршрутизації.

Таке визначення не містить заздалегідь відомих протиріч, і, відповідно до них, топологія Інтернет базується на з'єднаних одна з одною автономних системах. Вона є найбільш часто досліджуваною [34, 35] [36], [37], [38].

При цьому дослідники акцентують увагу на наступному:

- топологія Інтернету на рівні AS є найкрупнішою деталізацією Інтернету, інші рівні топології Інтернету частково залежать від топології рівня AS;
- отримати топологію рівня AS відносно просто, а інші рівні топології іноді розглядаються як приватна інформація, і їх важче отримати;
- топологія рівня AS не розробляється безпосередньо людьми; натомість це сукупний результат технологічних та економічних сил, а отже, його походження та еволюція викликають значний інтерес з боку дослідників.

Необхідно зауважити, що уявлення про «відносну простоту» отримання інформації про зв'язки між AS, яке було наведене в [33] та інших роботах, дуже спрощене. Функціонування системи глобальної маршрутизації не дає можливості в окремій AS отримати інформацію про усі зв'язки в мережі безпосередньо за допомогою протоколу BGP. А інші джерела містять неточну та неповну інформацію, як це пояснено в розділі 1.2. Відсутність єдиної точки огляду для всіх зв'язків та маршрутів підтверджує також Джеф Х'юстон в [4] і акцентує увагу на тому, що «не існує абсолютної правди про топологію; є лише набір відносних маршрутних карт, зібраних окремими BGP-системами».

Отже, основні проаналізовані дослідження не дають визначення топології Інтернет, натомість вважають топологією Інтернету щось само собою зрозуміле – з'єднання на рівні AS. Відсутність конкреного визначення топології Інтернет як поняття, та, водночас, проведення дослідження топології Інтернет, є протиріччам, що є перепоною на шляху пошуку нових методів захисту від кібернетичних атак на систему глобальної маршрутизації.

В п.2.1 дане визначення всіх елементів глобальної комп'ютерної мережі Інтернет, які складають її архітектуру, і яка відрізняє її від будь-якої іншої комп'ютерної мережі. Необхідно визначити, що є топологією Інтернету, який складається з цих елементів. Це дасть змогу усунути наведене протиріччя.

2.3.2. Математична топологія і топологічний простір Інтернету

Існує чітке математичне визначення поняття топології. Воно походить з визначення поняття топологічного простору, яке використовується у загальній топології. Визначення топологічного простору спирається лише на теорію множин, і є найбільш загальним поняттям математичного простору, що дозволяє визначити концепції, такі як безперервність, зв'язність та конвергентність [67, 68].

Нехай існує множина елементів X. Система T відкритих підмножин його елементів є топологією на X, якщо що відповідає вимогам, які звуться аксиомами топології:

об'єднання довільного сімейства підмножин L з елементів X належить T:
$\forall L', L'' \in T : \left(L' \cap L'' \in T\right)$;

перетин довільного скінченного сімейства L з підмножин елементів X належить T:

$\forall L', L'' \in T : \left(L' \cup L'' \in T\right)$;

сама множина X та порожня множина належать T:

$\varnothing \in T,\ X \in T$.

Окремим випадком топологічного простору є простір з дискретною топологією. В дискретному топологічному просторі множина точок не є безперервною, всі точки простору в якомусь сенсі ізольовані одна від іншої. Топологією дискретного топологічного простору (дискретною топоплогією) є сімейство всіх його підмножин, що відповідають аксиомам топології. Особливістю дискретної топології є те, що її базою послуговують всі підмножини множини X, що складаються з одного елемента.

Мережеві структури утворюють топологічний простір. Метричні структури часто моделюють у вигляді графа. В роботі [39] продемонстровано представлення топологічного простору логістичного графа на множині його ребер, з якого витікає, що граф є прикладом моделі.

Ми також роздивляємось топологію Інтернет як «структуру у вигляді графа, яка може представити взаємодію її автономних систем, до яких входять окремі мережеві префікси зі спільною політикою маршрутизації», оскільки представлення мережі у вигляді графа є типовим і загально прийнятим. Якщо граф Інтернет теж є прикладом дискретного топологічного простору, необхідно визначити на множині яких елементів задано цю топологію.

2.3.3. Топологічний простір Інтернету на основі глобальної маршрутизації

Оскільки топологія – це система підмножин з елементів множини, на якій вона задається, необхідно визначити, на якій саме множині задається топологія.

Основною функцією системи глобальної маршрутизації є обмін інформацією про доступність мережі. Ця інформація про доступність мережі включає список автономних систем (AS), крізь які проходить інформація про доступність мережі. Цієї інформації достатньо для побудови графа зв'язків AS.

Маршрут – це одиниця інформації, яка поєднує набір пунктів призначення з атрибутами шляху до цих пунктів призначення. Набір пунктів призначення – це системи, чиї IP-адреси містяться в одному IP-префіксі, розташованому в повідомленні про доступність мережі (network layer reachability information, NLRI). Шлях – це дані у вигляді списку AS, крізь які проходить інформація про доступність мережі. Дані містяться в полі атрибутів шляху того самого повідомлення [3].

Початкові дані, доступні нам з системи глобальної маршрутизації, виглядають так.

1) множина вузлів (AS);

2) множина мережевих префіксів (ідентифікатори IP-мереж, до яких прокладаються маршрути), причому кожен префікс прив'язаний до певного вузла, званого "джерела";
3) з'єднання – спрямований зв'язок двох суміжних AS, по якому передається анонс конкретного префікса; з'єднання можуть розглядатись виключно в контексті передачі по них інформації про доступність мережевих префіксів;
4) маршрут до певного префікса – безперервна послідовність унікальних зв'язків, що закінчується джерелом префікса;
5) множина маршрутів до певного префікса, яка охоплює всі можливі комбінації зв'язків, за якими анонсується певний префікс, з кінцевою точкою в вузлі-джерелі;
6) множина всіх маршрутів до всіх префіксів.

Необхідно встановити зв'язок, чи, скоріше, відповідність між структурами, що утворюються в результаті процесів глобальної маршрутизації, та математичним визначенням топології.

Твердження 1. Окремий маршрут до префікса є топологією на множині з'єднань.

Твердження 2. Сукупність усіх маршрутів до префікса є топологією на множині з'єднань.

Твердження 3. Сукупність усіх маршрутів до всіх префіксів є топологією на множині з'єднань.

Наведемо обгрунтування тверджень 1,2,3. Попередньо сформулюємо засади та наведемо визначення, на яких базується обгрунтування.

За визначенням [3] маршрут містить мережевий префікс та шлях до нього. Оскільки нами прийнято, що з'єднання між суміжними AS ми розглядаємо виключно в контексті передачі по ньому NLRI певного префікса, то маршрути відрізняються виключно шляхами, тому далі замість «шлях» ми використовуватимемо термін «маршрут».

Мережа Інтернет є системою сполучених комп'ютерних мереж, об'єднаних принципами маршрутизації [40]. Отже, мережевий префікс є ідентифікатором окремої комп'ютерної мережі, яку можна вважати сполученою з Інтернет тоді і лише тоді, коли до неї існує маршрут з кожної іншої сполученої мережі. Тому вважатимемо, що в кожній AS наявний принаймні один маршрут до кожного мережевого префіксу.

AS за визначенням обмінюється інформацією про маршрути до префіксів з іншими AS [2]. Тому вважаємо, що будь-яка AS має з'єднання з принаймні однією іншою AS, і кожне з'єднання задіяне принаймні в одному маршруті, тобто через нього може бути прокладено шлях від хоча б однієї AS до джерела хоча б одного префіксу.

Обгрунтування Твердження 1.

Маршрут $m(p)$ до префікса p за визначенням є впорядкованою безперервною послідовністю з'єднань . Дискретна топологія сключає в себе всі можливі комбінації елементів множини, на якій вона визначається. Дискретна топологія на множині з'єднань, які належать префіксу, включає в себе всі комбінації з'єднань. Впорядкована безперервна послідовність з'єднань є однією з можливих комбінацій з'єднань. Отже, *окремий маршрут до префікса є топологією на множині з'єднань.*

Обгрунтування Твердження 2.

Нехай M є сімейством всіх можливих безперервних послідовностей з'єднань $m(p) = \{l_1, l_2, l_3, ..., l_i, ...l(p)\}$, що належать префіксу p. Очевидно, що тоді кожне окреме з'єднання l належить якомусь елементові m сімейства M, і не існує жодного з'єднання, яке не належало би до жодного елемента сімейства M.

Отже, сукупність усіх маршрутів до префікса є топологією на множині з'єднань.

Обгрунтування Твердження 3.

Нехай в кортежі (V,E) до V належать всі AS, а до E належать всі з'єднання між AS. Нехай T є топологією, заданою на множині всіх з'єднань. З визначення AS витікає, кожен зв'язок використовується при побудові принаймні одного маршруту до якогось префікса. Тоді всі маршрути до всіх префіксів «задіюють» всі зв'язки в такій чи іншій комбінації, а отже – сукупність всіх маршрутів довсіх префіксів є топологією, заданою на множині всіх зв'язків між AS в мережі Інтернет.

Крім того, до топології має належати порожня множина елементів, на яких вона задана. Для топології Інтернет порожньою множиною може послуговувати комбінація зв'язків, по якій AS анонсує мережевий префікс, який належить їй самій. Розглянемо приклад на рис. 2.2.1. Нехай 10,11,12,13,77 – ідентифікатори автономних систем (AS), при чому AS 13 є джерелом префіксу 192.168.0.0/20. Нехай L={$a,b,c,d,,f$} – направлені зв'язки суміжних AS, якими передається інформація про доступність мережевого префіксу p.

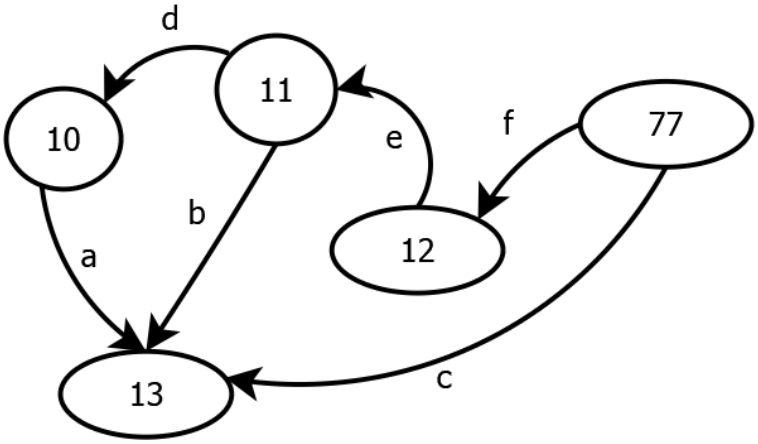


Рисунок 2.2.1 – Наочний приклад утворення маршрутів з елементів топології

Розглянемо сімейство підмножин з елементів *L*, які є маршрутами до префіксу p, які мають завершуватись його джерелом – AS 13, тобто утворення яких обумовлено правилами формування шляхів в протоколі BGP-4:

(13,13)= {∅};
(10,13)={a};
(11,13)={a,b,{a,b}};
(12,13)={{e,b},{e,d,a}};
(77,13)={c,{f,e,b},{f,e,d,a}}.

Резюмуємо міркування. Нехай існує множина всіх з'єднань l між вузлами $\exists L: l \in L$. Нехай існує система елементів множини цих з'єднань *T*, до якої належать порожня множина, сама множина всіх з'єднань, та будь-які комбінації (об'єднання та перетини) з цієї множини:

$$\exists T \ : \varnothing, L \in T; \ \forall L', L'' \in T : \left(L' \cap L'' \in T; \ L' \cup L'' \in T\right).$$

В такому разі система *T* відповідає визначенню топології на множині з'єднань *L*, а пара $G(L,T)$ відповідає визначенню топологічного простору, де множина з'єднань є «носієм» топології. Формалізуємо визначення маршруту до певного префікса як безперервної послідовності унікальних з'єднань, що закінчується джерелом префікса. Відповідно до цього визначення всі маршрути належать топології, бо безперервна послідовність елементів може бути утворена об'єднанням елементів і за визначенням є елементом топології:

$$m(p) = \{l_1, l_2, l_3, ..., l_i, ...l(p)\}; \quad l_i = \{v_i, v_j\}; \quad v_i, v_j \in V$$
$$\Rightarrow \forall p, m(p) \in T.$$

$$\forall m(p'), m(p'') \in T : \begin{pmatrix} m(p') \cup m(p'') \in L \subset T; \\ m(p') \cap m(p'') \in (\varnothing, L) \subset T \end{pmatrix}$$

Сутність «порожня множина» в даній топології символізує з'єднання, по якому вузол-джерело передає анонс власного префікса сам собі.

Таким чином, алгоритм протоколу BGP обирає кращі шляхи для кожного префікса з елементів топології, що належать топологічному простору цього префікса $G_p(L_p, T_p)$ та складаються виключно із з'єднань, по яких передається анонс цього префікса. А сукупність топологічних просторів всіх мережевих префіксів охоплює всі існуючі з'єднання між вузлами Інтернету і таким чином є топологічним простором Інтернету, який утворено системою глобальної маршрутизації:

$$G = \bigcup_p G_p, \ G_p := \left(L_p, T_p\right).$$

2.4. Кібератаки на топологічний простір Інтернету

Формування топологічного простору Інтернет системою глобальної маршрутизації

З матеріалів, викладених в попередньому підрозділі, зрозуміло, що BGP-зв'язки між вузлами є елементною базою топологічного простору Інтернету. Маршрут в BGP-4 – це одиниця інформації, яка поєднує адресу призначення (destination) з атрибутами шляху (path) до адреси призначення.

Кожна BGP-система зберігає маршрути в базах (Routing Information Base, RIB) трьох типів:

- *Adj-RIBs-In* – маршрути, які отримані від інших BGP-спікерів в результаті повідомлень UPDATE (див. далі). Ці маршрути є вхідними даними для процесу застосування локальної політики маршрутизації.
- *Loc-RIB* – маршрути, які застосовуються локально після їхнього відбору BGP-спікером із застосуванням локальної політики маршрутизації.
- *Adj-RIBs-Out* – маршрути, які будуть запропоновані іншим BGP-спікерам в повідомленнях UPDATE.
- BGP-4 є дистанційно-векторним протоколом. Взаємодія двох BGP-партнерів відбувається наступним чином.

BGP-4 використовує протокол TCP як транспортний протокол з гарантованою доставкою пакетів. Спочатку BGP-спікери встановлюють TCP-з'єднання та обмінюються його параметрами. Після встановлення з'єднання вони обмінюються таблицями маршрутизації в тому обсязі, в якому передбачено конфігурацією BGP-системи. При кожній передачі повної таблиці їй присвоюється унікальний серійний номер. Потім BGP-спікери обмінюються лише змінами до таблиць маршрутизації. Зміни надсилаються накопичувально, або інкрементально, відносно початкового стану таблиці. Це означає, що в разі зміни маршрутів BGP-4 не потребує повного оновлення всієї таблиці. В разі, якщо шлюз спілкується одночасно з декількома іншими шлюзами, він отримує і має зберігати повну таблицю від кожного BGP-спікера один раз за сеанс, а згодом вносить туди із зміни, отримані від кожного BGP-спікера. Для підтвердження наявності BGP-з'єднання в протоколі передбачений періодичний обмін так званими keep-alive пакетами. Зазвичай, при відсутності таких пакетів протягом встановленого BGP-сесією часу, BGP-спікер вважає з'єднання втраченим та буде намагатись встановити його знову.

BGP не використовує складних схем взаємодії типу широкомовних повідомлень. Він працює по схемі «клієнт-сервер». BGP-системи, що сконфігуровані бути сусідами, встановлюють одна до другої з'єднання «клієнт-сервер» у вигляді вдох зустрічних TCP-сесій і обмінюються в кожній сесії командами, які в BGP мають назву «повідомлення». Типи повідомлень, якими обмінюються BGP-партнери:

1) «OPEN». Початок сесії. Містить версію протоколу (версія 4), номер AS, запропонований інтервал інактивності (hold time – див. keepalive), ідентифікатор BGP-партнера (дорівнює його IP-адресі, також називається Router ID).
2) «UPDATE». Найважливіше повідомлення. Анонсування та скасування маршрутів. Має складний формат, в якому передається 1 чи більше destination у вигляді префіксу, та відповідно до кожного destination йього path attributes (див. далі).
3) «NOTIFICATION». Повідомлення про помилку, через яку подальша взаємодія двох BGP-спікерів є неможливою. Після отримання NOTIFICATION, спікер, який надіслав повідомлення, розриває bgp-з‘єднання. Цей тип повідомлення містить код помилки та додатковий код помилки.
4) «KEEPALIVE». Повідомлення містить тільки заголовок (19 байт), надсилається кожної хвилини, якщо протягом неї не передавались інші повідомлення. Призначене для впевненості BGP-партнерів, що їхнє з‘єднання досі існує. KEEPALIVE також надсилається у відповідь на повідомлення OPEN, якщо BGP-спікер, який отримав це повідомлення, приймає умови BGP-з‘єднання.

Загалом атрибути шляху класифікуються по типах: обов’язковість чи опціональність, транзитивність чи локальність. Це необхідно в подальшому для розуміння методики використання даних BGP-таблиць в аналізі та моделюванні топологічного простору мережі. Роздивимось деякі атрибути маршруту.

1) ORIGIN – звідки отримано маршрут (номер AS, з якої від походить), він зовнішній чи внутрішній (internal, external)
2) AS_PATH – шлях, який пройшов цей анонс до даного BGP-спікера. Це зворотна послідовність від AS, де був згенерований маршрут, по всіх транзитних AS. Використовується для обрання найкоротшого шляху за критерієм довжини шляху, а також для запобігання утворення кілець маршрутизації при подальшому експорті маршрутів.
3) NEXT_HOP – IP-адреса прикордонного маршрутизатора.
4) LOCAL_PREF – „вага” (чи перевага) даного маршруту на локальній системі, також один з критеріїв обирання шляху. Як видно з назви, цей атрибут є локальним та не передається при експорті анонсів. Це необов‘язковий атрибут.
5) COMMUNITY – групування префіксів для спрощеного застосування правил анонсування та зміни атрибутів. Якщо атрибути анонса містять COMMUNITY NO_EXPORT, цей анонс має не виходити за межі AS; NO_ADVERTISE – не повинен анонсуватись іншим BGP-вузлам. Інші значення формуються у вигляді номер_AS:номер_community (наприклад 12293:5), за номером community BGP-спікер застосовує визначені на ньому для такого community правила.

Атрибути 1,2,3 є обов'язковими і мають бути присутніми в повідомленні UPDATE.

BGP-система має такі джерела інформації для роботи:

- набір маршрутів отриманих ззовні;
- вхідні правила маршрутизації (input policy engine)
- процедура прийняття рішення щодо власної routing table;
- власна таблиця маршрутизації;
- вихідні правила маршрутизації (output policy engine);
- набір вихідних маршрутів (які мають бути передані).

На рис. 2.3.1 наведено схему роботи BGP, складену у відповідності до його документації. Процес отримання та обробки вхідної інформації від інших BGP-систем, виокремлений пунктиром, має назву «вивчення маршрутів» (learning routes). На цьому етапі на вхід процесу обробки вхідних маршрутів (input policy engine) від різних сусідніх BGP-систем потрапляє по одному чи більше маршруту до кожного мережевого префікса. Маршрути містять шлях, який складається із зворотної послідовності ідентифікаторів AS. Кожна пара сусідніх AS в шляху представляє «з'єднання» – *елемент топологічного простору* цього мережевого префікса.

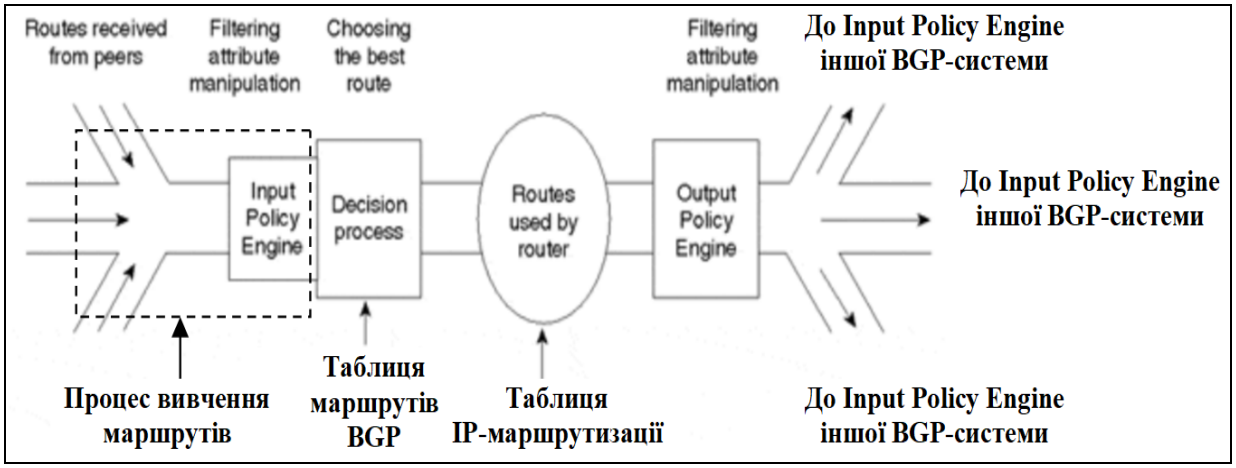


Рисунок 2.3.1 – Функціональна схема BGP-4 з поясненням функціональних блоків

Важливо звернути увагу на порядок проходження інформації крізь три види RIB: в Adj-RIB-Out потрапляють виключно маршрути з Adj-RIB-Loc. Це демонструє виконання наступного правила: BGP-система може анонсувати лише маршрути, які використовує сама.

Процес прийняття рішення про використання маршруту до певного destination (яке задано завжди у вигляді мережевого префікса) відбувається на основі обробки атрибутів маршруту.

Перший вибір маршруту здійснюється за найнижчою метрикою маршруту, локальним необов'язковим атрибутом. За замовчанням для всіх вхідних маршрутів BGP цей атрибут є однаковим, але адміністратор може конфігурувати преференції для певних сусідів чи окремих префіксів.

Другий крок у виборі маршруту зазвичай розглядається як перший крок. Обирається маршрут з найвищим значенням атрибуту LOCAL_PREF. Значення за замовчуванням для всіх вивчених маршрутів BGP є однаковим, тому, як правило, це не призводить до вибору маршруту.

Третій крок у виборі маршруту – це вибір маршруту з коротшим AS_PATH. Це є основним етапом і основним критерієм обрання маршруту.

Четвертий крок – з маршрутів з однаковою довжиною шляху обрати той, в якого значення ORIGIN нижче. Значення нижчого ORIGIN є таким, що IGP (I) є переважним над EGP (E), а EGP є переважним над неповним.

П'ятий крок – пошук найнижчого значення атрибуту MED. Якщо він не встановлений, вважається рівним 0.

Шостий крок порівнює тип маршруту (внутрішній iBGP чи зовнішній eBGP). Маршрути, отримані ззовні (eBGP) є переважними над внутрішніми маршрутами (iBGP) на цьому етапі. Це принцип «гарячої картоплини», що шукає шлях найшвидшого виходу мережевих пакетів з AS. Якщо після цього етапу до певного префікса залишилось ще більше одного маршрута, вони всі мають однакове походження – є або внутрішніми, або зовнішніми.

Сьомий крок вибирає маршрут з найнижчою вагою в атрибуті Next-Hop.

Восьмий крок відрізняється для внутрішніх маршрутів та зовнішніх маршрутів. Для внутрішніх маршрутів він віддає перевагу маршруту з найнижчим значенням ROUTER_ID в параметрах налаштування bgp-сесії. Тобто буквально перевагу буде віддано маршрутизатору з арифметично меншою IP-адресою. Для зовнішніх маршрутів на цьому етапі обирається найстаріший активний маршрут.

В стандарті визначено понад 30 критеріїв, за якими BGP-система може обирати маршрут. Не всі вони реалізовані в будь-якій системі, але з рештою в таблиці маршрутизації має залишитись один маршрут до кожного мережевого префікса.

Отже, в результаті обробки маршрутів до кожного префікса, має лишитись виключно один маршрут, який дана BGP-система вважає кращим. Він, і тільки він може бути переданий до інших BGP-систем, якщо це буде дозволено заданою адміністративно політикою маршрутизації. При подальшій передачі маршрут буде подовжено шляхом додавання до нього ідентифікатора тієї AS, якій належить дана BGP-система. Таким чином, на виході BGP-системи буде утворено принаймні *один новий елемент топологічного простору* мережевого префікса у вигляді послідовності з попередньої та цієї AS.

Таким чином в процесі функціонування системи глобальної маршрутизації утворюється топологічний простір Інтернету, що складається з топологічних просторів окремих мережевих префіксів. З кожного вузла можна «побачити» лише окремі структури цього топологічного простору, які з математичної точки зору є елементами його топології. Ці елементи топології є маршрутами між цим вузлом та вузлом, якому належить мережевий префікс.

Важко уявити собі реальну автономну систему в Інтернеті, в якій можна було б спостерігати всі маршрути до певного префікса, а отже – всі елементи множини його топологічного простору (з'єднання). Проте, якщо б знайшлась

технічна можливість отримати таблиці Adj-RIP-in з усіх BGP-систем, за ними було б складено повний топологічний простір Інтернету.

Проєкція проблем захищеності протоколу BGP-4 на захищеність системи глобальної маршрутизації

Багато викладеного раніше матеріалу було присвячено опису функціонування протоколу BGP-4. Необхідно зробити акцент на наступному: BGP – це «самонавчальний» протокол маршрутизації, який, функціонуючи на кожному вузлі мережі, виявляє всі елементи топології мережі (або, точніше, частину ту частину елементів топології, які можна спостерігати на конкретному вузлі). Виявлення відбувається за інформацією, отриманою від сусідів, про ті топології, що відомі їм. Так само, BGP-система кожного вузла повідомляє сусідам відомі їй топології (нагадаємо, що було доведено, що кожен маршрут є елементом топології).

В цій формі розповсюдження інформації є очевидна вразливість: розробники протоколу робили припущення, що кожен вузол забезпечує коректне функціонування BGP. Але через відсутність засобів верифікації цей механізм поширює викривлену інформацію так само успішно. В [4] Джеф Х'юстон (Geoff Huston), видатний австралійський діяч науки та техніки, порівнює обмін маршрутами з розповсюдженням чуток, оскільки протоколом не передається оригінальна інфромація про доступність мережевого префіксу, а лише її інтерпретація, яка пройшла крізь інтерпретацію на декількох вузлах.

Будь-який елемент мережі Інтернет має унікальну мережеву адресу. Маршрут до будь-якої адреси утворюється шляхом анонсу мережевого префіксу, до якого належить адреса. Кожен мережевий префікс має власний топологічний простір. Кібернетичні атаки, вектором яких є система глобальної маршрутизації, спотворюють топологічний простір певного мережевого префіксу шляхом пропонування BGP-системам неіснуючих з'єднань, або приховуючи існуючі. Зміна множини з'єднань лише на одиницю призводить до утворення чи знищення величезної кількості елементів топології, частина з яких задовольняє визначенню поняття «маршрут»:

$$\left|T\right| = \left|L\right|^{\left|L\right|};\ \exists L_f : L, l_f \in L_f \quad => \quad \left|T_f\right| = \left(\left|L\right|+1\right)^{\left(\left|L\right|+1\right)}.$$

В результаті алгоритм маршрутизації BGP-4, використовуючи хибну топологію на вході модуля обробки вхідних маршрутів, може дати хибний результат вибору маршруту, а також сприяти утворенню нових хибних елементів топології на виході і передачі їх до наступних вузлів.

Таким чином, задача підвищення захищеності від перехоплення маршрутів стає відтепер більш конкретною і її можна сформулювати як зменшення можливостей з викривлення топологічного простору, через зловмисне утворення чи знищення елементів топології.

ГЛАВА 3.
ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМІ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ ІНТЕРНЕТУ

3.1. Ризик перехоплення маршруту в термінах та визначеннях міжнародних стандартів

В сучасній світовій практиці поводження з ризиками існує основа єдиного методичного підходу до сприйняття документів, які регламентують різні аспекти діяльності. Такою основою є настанови ISO Guide 73:2009 "Risk Management – Vocabulary", які тлумачать зміст відповідних термінів [41] а також [42]. Головним є поняття ризику, яке надано як вплив невизначеності на досягення цілі або мети. Проте, оскільки таке поняття ризику неможливе у знеособленому сенсі, важливо насамперед визначити, хто є зацікавленою стороною (stakeholder) в оцінюванні ризику. В представленій роботі такою стороною є суб'єкт глобальної маршрутизації, оскільки в наслідок можливого перехоплення маршруту саме він отримає збитки.

Ризик може матеріалізуватись як настання потенційно можливих подій та (або) наслідків цих подій. Значення ризику можна виразити як поєднання подій (і їхніх наслідків) із вірогідністю їх настання. Такою подією вважатимемо свідомі чи несвідомі дії третіх сторін, які призвели до такого наслідку, як несанкціонована поява в мережі альтернативних, більш пріоритетних маршрутів.

Ризик має аналізуватись у контексті оточення, яке поділяється на зовнішнє та внутрішнє. До внутрішнього оточення спробуємо віднести внутрішню політику маршрутизації, а о зовнішнього оточення – весь процес глобальної маршрутизації в цілому, який полягає у відносинах зацікавленої сторони з усіма іншими суб'єктами глобальної маршрутизації. Ці відносини матеріалізуються, зокрема, в обміні маршрутами по протоколу BGP-4 та в інтерпретації (сприйнятті) глобальної таблиці маршрутизації.

Оцінювання ризику потребує, серед іншого, його ідентифікації. Оскільки ризик обумовлений особливостями зовнішнього і внутрішнього середовища, розглядаються всі можливі джерела ризику, а також наявна інформація про сприйняття ризику (усвідомлення ризику) причетними сторонами, як внутрішніми по відношенню до компанії, так і зовнішніми. Особливі вимоги висуваються до якості інформації (максимально можливий рівень повноти, точності і тимчасової відповідності при наявних ресурсах на її отримання) та її джерел. Результат ідентифікації повинен бути структурованим та охоплювати чотири елементи – джерела виникнення; події, що виникнуть; причини цих подій; наслідки подій.

Рішенню цих задач сприятиме ретроспективний аналіз кіберінцидентів. Термін «ретроспективний» вжито саме тому, що інформація щодо наслідків, масштабу, засобів, а інколи і справжніх цілей атак стає відомою згодом.

Систематизовані ретроспективні дані стосовно кіберінцидентів з глобальною маршрутизацією в Інтернеті свідчать, що дедалі зростає доля очевидних зумисних дій, спрямованих на скоєння атак на глобальну маршрутизацію, а наслідки атак стають більш глобальними.

В міжнародному стандарті «Інформаційні технології. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій» [43], остання ревізія якого відбулась в 2015 році, визначено основні принципи оцінки безпеки інформаційних технодогій, які полягають у тому, що слід чітко сформулювати загрози безпеки і положення політики безпеки організації, а достатність запропонованих заходів безпеки повинна бути продемонстрована.

Крім того, слід вжити заходів щодо зменшення ймовірності наявності вразливостей, можливості їх прояву (тобто навмисного використання або ненавмисної активізації), а також ступеня шкоди, який може бути наслідком прояву уразливості. Додатково слід вжити заходів для полегшення подальшої ідентифікації вразливостей, а також щодо їх усунення, ослаблення, та (або) оприлюднення про їх використання або активізації. Саме цим напрямам присвячені наступні підрозділи цього розділу дисертації.

3.2. Ретроспективний аналіз інцидентів з глобальною маршрутизацією

3.2.1. Інцидент з AS3252

Перші випадки подій, пов’язаних з певною недосконалістю протокола BGP-4 і, як наслідок, захопленням маршрутів, особисто відомі автору з середини 1990 років. Так, український Інтернет сервіс провайдер «Релком-Україна» з автономною системою AS3252 одним з перших побудував два міжнародні канали (став «multihomed»): перший – наземний канал до провайдера в Російській Федерації, яка була попереду в питаннях розвитку Інтернету; другий – супутниковий, пропускною здатністю 64 кбіт/с, до одного з європейських операторів (EUnet). Через помилку в налаштуванні BGP-4 у українського та російського провайдерів, відбувся витік (route leak) європейських маршрутів через канал до російського провайдера. Ці маршрути, потрапивши в російську мережу, виявились кращими з точки зору BGP-4 (best route) для майже всіх російських мереж, підключених до Інтернет. Трафік російського походження, замість звичайних напрямків по магістральних міжнародних каналах з Москви та Санкт-Петербургу, намагався надходити до європейських мереж через AS3252. Схему інциденту наведено на рис.3.2.1 (мапу регіону запозичено з ресурсу mapswire.com). В результаті вкрай недостатньої для такого обсягу трафіку пропускної здатності каналів, AS3252 утворила «чорну діру» для російського трафіку. Через недостатній досвід інцидент було припинено російським провайдером шляхом відключення каналоутворюючого обладнання (модему) на каналі з AS3252.

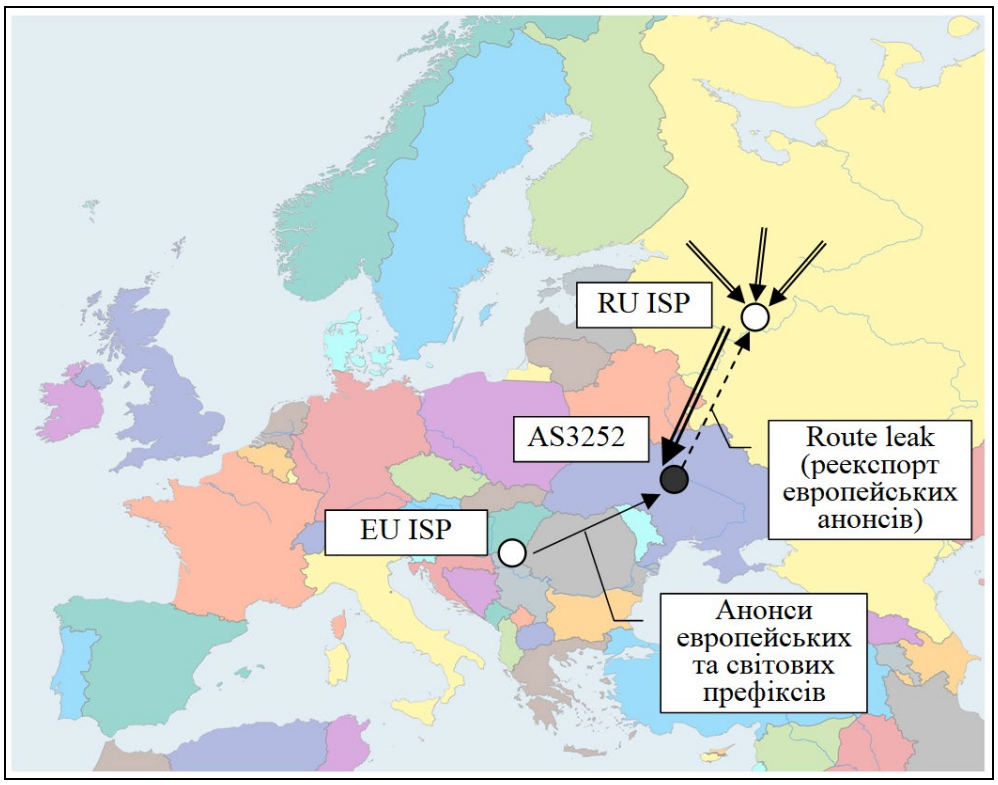


Рисунок 3.2.1 – Схема інциденту з AS3252. Подвійні стрілки – трафік, що потрапив в «чорну діру»

На деякий час певна частка мереж РФ лишалась без доступу до закордонних Інтернет-ресурсів. Через вичерпання пропускної здатності каналів припинився доступ до мережі у AS3252 та її клієнтів (джерело інформації не наводиться, оскільки автор був свідком цих подій підчас виконання службових обов'язків).

Але в ті роки основними Інтернет-послугами були електронна пошта та офлайн-форуми USENET (обидві послуги зазвичай передбачали сеансовий зв'язок з мережею з пакетною обробкою даних, а не постійний, як зараз), тому звичайні кініеві користувачі навряд чи помітили такий збій.

3.2.2. Інцидент з AS7007

Маловідомий інцидент 1997 року, який стався у провайдера MAI (AS7007) в штаті Вірджинія, США, був відзначений в тогочасній пресі. Ця автономна система отримала від одного з своїх клієнтів не тільки префікси його мереж, а й всю глобальну таблицю маршрутизації (full view). Через нестачу досвіду адміністратори AS7007 досі не використовували фільтрацію маршрутів на клієнтських підключеннях, та взагалі припутились багатьох помилок. Так, через помилку в маршрутизаторі, отримані префікси було ще й деагреговано до найдрібніших префіксів з довжиною мережевої маски 24 біти. Загалом так було перекручено близько 23 000 префіксів різної довжини, з яких утворилось близько 73000 префіксів довжиною 24 біти. В результаті 73000 хибних маршрутів було анонсовано в Флорідську мережу обміном трафіком MAE-East

(AS1790). Ці маршрути отримали всі учасники мережі обміну трафіком і стали в них кращими (best route). AS7007 отримала від інших учасників трафік, що був адресований всьому світові. Через нестачу пропускної здатності її каналів учасники інциденту лишались без Інтернет-доступу. Ефект «чорної діри» відчувався по всій мережі до 4 годин. Сьогодні такі атаки мають назву «route deaggregation» [44]. Схему інциденту наведено на рис.3.1.2.

В день Різдва, 24 грудня 2004 року ініціатором масштабного перехоплення маршрутів став національний телеком-оператор Туреччини TTNet. Цей випадок був першим, добре задокументованим в цифрах і графіках завдяки дослідженню MERIT [45].

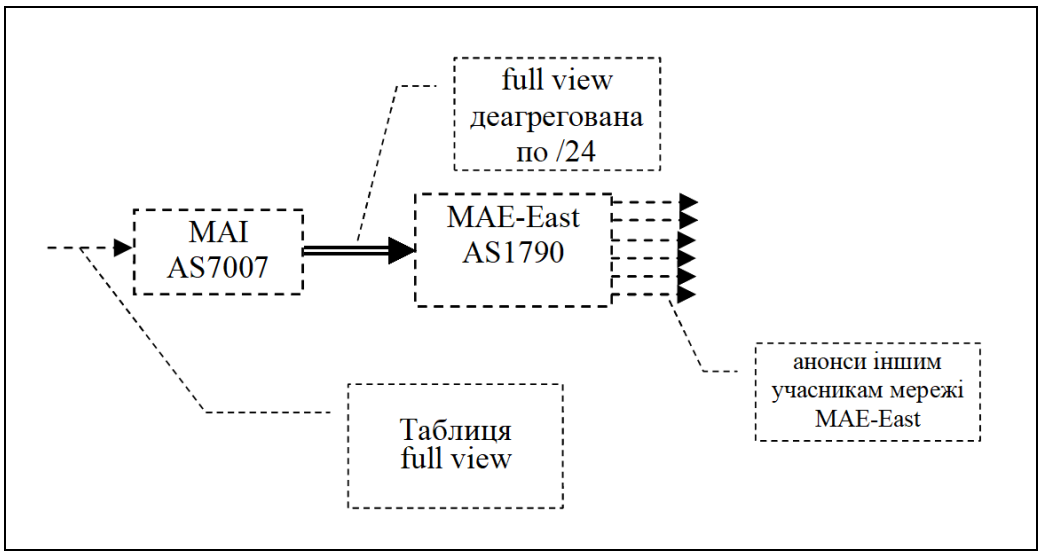


Рисунок 3.2.2 – Схема інциденту з AS7007

3.2.3. Інцидент з AS9121 «Christmas Eve»

Станом на час інциденту TTNet (AS9121) був транзитним провайдером для 60 інших операторів та анонсував приблизно 200 IP-префіксів. Вже на той час мав оформлену політику маршрутизації в реєстрі маршрутів RIPE NCC. На жаль, політика була сформована некоректно, а саме – не було обмежень на вхідні префікси від клієнтських AS.

На ранок 24/12/2004 AS9121 почала раптово анонсувати від власного імені (тобто анонсувати зі зміною атрибуту origin) до 105000 префіксів. Протягом понад годину ці префікси приймали та ретранслювали всі вищі провайдери та партнери (peers) TTNet, серед яких були великі трансрегіональні оператори: Telecom Italia (AS6762), Sprint (AS1239), Telia (1299), Cable & Wireless (1273). Кожен з них ретранслював по своїх інших каналах принаймні частку хибних маршрутів (рис.3.1.3). Збій повторювався ще двічі з меншою кількістю префіксів, як показано на рис.3.1.4 (можливо, то були невдалі спроби імплементувати коректну routing policy в TTNet).

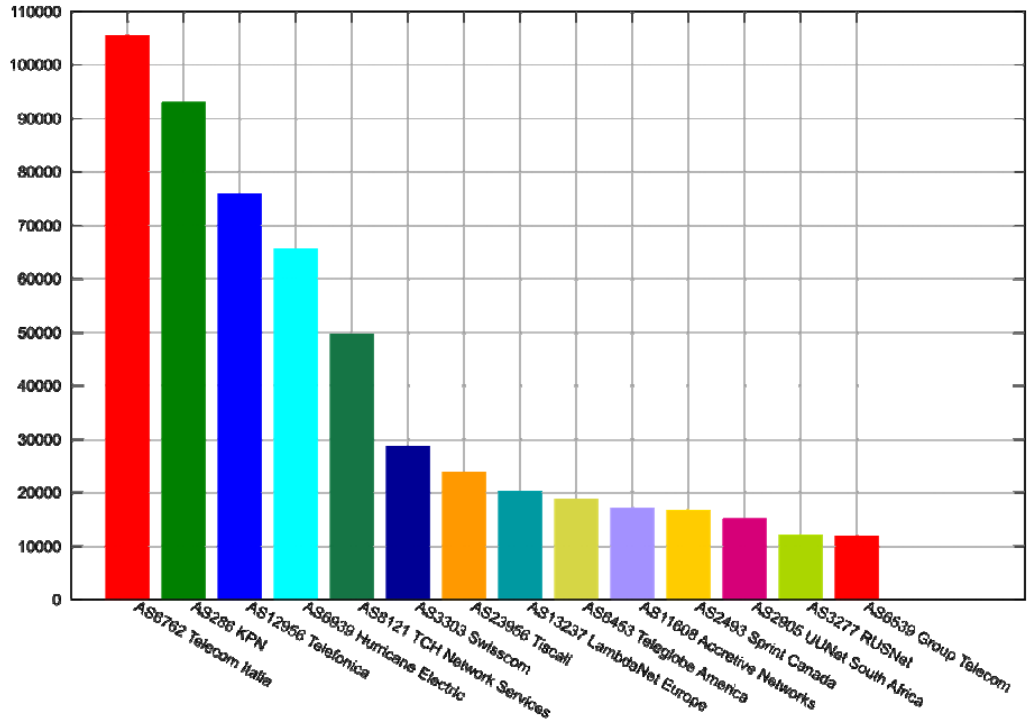


Рисунок 3.2.3 – Кількість ретрансльованих хибних префіксів (вісь ординат) через інші AS (вісь абсцис). Джерело даних – MERIT

Як видно з рис. 3.2.4, інцидент з різною інтенсивністю тривав майже 9 годин. Завдяки тому, що TTNet та його апстрім провайдери мал чималі потужності, лише деякі частини Інтернету були тотально недоступними протягом того часу. Проте погіршення сервісу відчули більшість користувачів завдяки зміні маршрутів до Youtube, Amazon і т.і.

Згадані раніше інциденти за загальною думкою відбувались через помилку чи бездіяльність мережевих адміністраторів. Аж в лютому 2008 року відбулась перша широко відома умисна дія з блокування первних інтернет-ресурсів шляхом атаки на глобальну маршрутизацію.

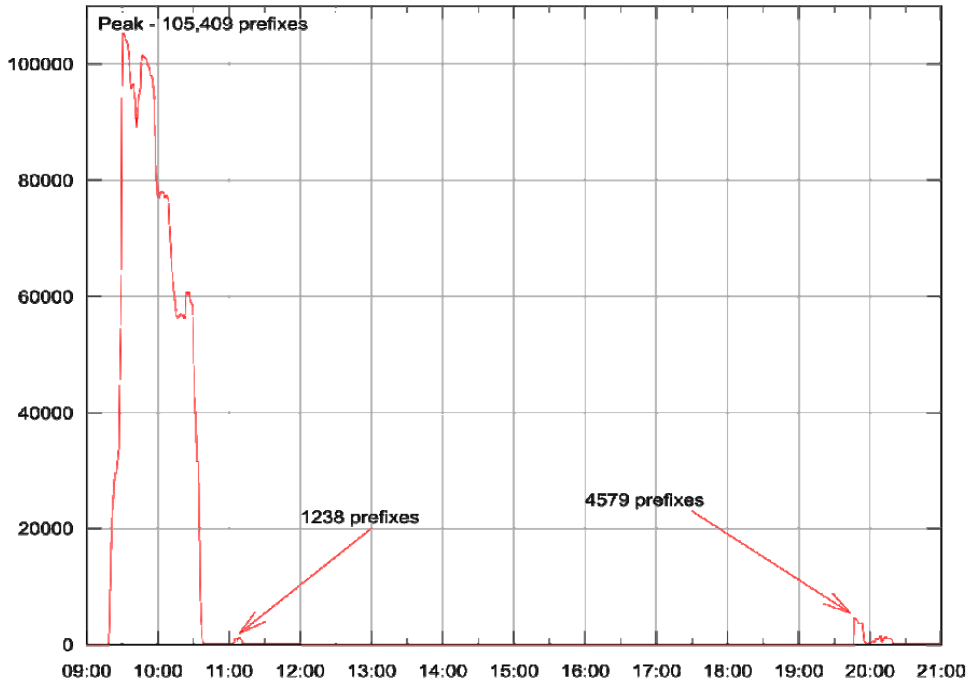


Рисунок 3.2.4 – Кількість хибних префіксів (вісь ординат), анонсованих AS9121 в ході інциденту 24.12.2004. Джерело даних – MERIT

3.2.4. Інцидент з Youtube 2008 року

24 лютого 2008 року пакістанський державний національний оператор Pakistan Telecom (AS17557) намагався виконати завдання свого уряду по блокуванню якогось медіаконтенту, який було розміщено на сервісі YouTube (AS36561). Для цього було обрано такий шлях: часку IP-префіксу, який використовував YouTube, а саме – підмережу 208.65.153.0/24 з більшої мережі 208.65.152.0/22, AS17557 анонсувала від свого імені (тобто із зміною origin). Анонсував не тільки своїм пакістанським клієнтам, а й свому апстрім-провайдеру PCCW (AS3491) з базою в Гонконзі. Нажаль, на той час не імплементувала фільтрацію BGP-анонсів.

Хибний префікс розповсюдився досить широко. Та, оскільки префікс з довжиною мережевої маски 24 є «more specific», маршрут до нього через PCCW (AS3491) та Pakistan Telecom став єдиним і, відповідно, кращим. Сервіс YouTube в результаті інциденту був недоступний протягом 2 годин (рис.3.1.5). Всі оператори, починаючи з AS3491, отримавши повідомлення від YouTube про проблеми з маршрутизацією, зафільтрували хибний анонс. Проте сам Pakistan Telecom не припинив виконувати наказ свого державного регулятора у цей спосіб.

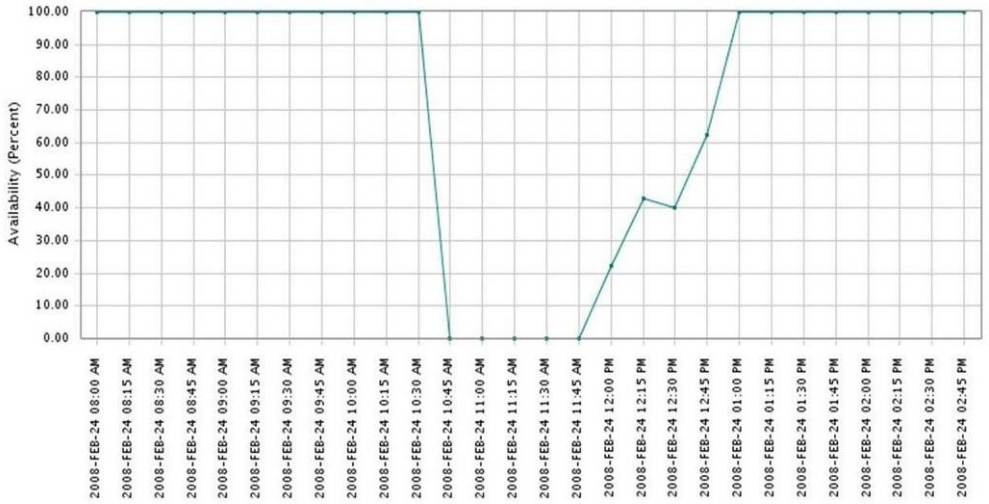


Рисунок 3.2.5 – Падіння доступності сервісу YouTube в результаті інциденту з AS17557. Джерело – Keynote Systems

Хоча минуло понад 10 років, цей інцидент став хрестоматійним прикладом атаки на інформаційні ресурси в ході інформаційної спецоперації, яка мала значно ширші і несподівані для атакуючої сторони наслідки [46]. Фрагменти опису цього інциденту досі використовуються в демонстрації необхідності застосування існуючих технологій захисту маршрутів.

3.2.5. Інцидент з масовим видаленням записів ROA

31 березня 2020 року в ході роботи з програмним забезпеченням реєстру з бази даних випадково видалили 4100 записів ROA. Адміністратор регіонального європейського Інтернет-реєстру повідомив у середині дня 1 квітня 2020, що «це сталося під час технічного обслуговування нашого внутрішнього програмного забезпечення». Більш детальну інформацію було опубліковано у пост-фактумному звіті, з якого стали зрозумілі тривалість і глобальність збоїв, що виникли в результаті проблем підчас оновлення програмного забезпечення [20]. Модернізація програмного забезпечення має критичний вплив на безпеку [72], але це не було прийнято до уваги. Оновлення програмного забезпечення та видалення записів ROA проводилось у неробочий час, що призвело до невчасного детектування проблеми. Повідомлення постраждалих клієнтів були оброблені вже наступного ранку, 1 квітня 2020 року. Відновлення видалених записів не вдалося без втручання інженерів і загалом тривало до середини дня 2 квітня. Після того проводилося розслідування, чи страждали якісь IP-префікси підчас збою від витоку чи перехоплення маршруту.

Помилкове видалення записів, випадково чи ні, співпало з іншою проблемою, масштаб якої описаний спеціалістами компанії QRATOR.Radar [47]. Можливо через інший збій програмного забезпечення, але в той самий час,

коли відновлювали БД з ROA, 8877 маршрутів від 200 автономних систем були неправомірно анонсовані державним російським провайдером Ростелеком. Масштаб був би менший, проте неправомірність анонсів неможливо було встановити через відсутність сертифікатів походження маршруту, що були видалені. Понад годину були недосяжні великі сегменти сервісів Hetzner, Amazon AWS, Akamai, Cloudflare, Digital Ocean, і це набуло розголосу [48]. Викладені матеріли інциденту дають привід вважати, що з точки зору безпеки глобальної маршрутизації в Інтернеті, локальне програмне забезпечення інтернет-реєстру, попри те, що воно регулярно проходить аудит безпеки [73] на сьогодні є новою єдиною точкою відмови (single point of failure – SPoF, [74]), саме завдяки розвитку механізму RPKI, що призваний захистити глобальну маршрутизацію.

3.2.6. Інші широко відомі інциденти

Ось дані про резонансні інциденти в мережі Інтернет, які трапились протягом 2014-2019 і були пов’язані з глобальною маршрутизацією.

Canadian Bitcoin Hijack. Лютий-березень 2014 року: перехоплення трафіку до майнінгових пулів криптовалют Bitcoin, Dogecoin, HoboNickels та Worldcoin [49].

За інформацією від команди Dell SecureWorks Counter Threat Unit, невідомі особи анонсували IP-адреси великих mining pool'ов криптовалюта Bitcoin, Dogecoin, HoboNickels і Worldcoin протягом 4 місяців: з 3 лютого по 12 травня 2014 року. Провернути таке було можливо через відсутність як перевірки автентичності сервера, так і шифрування в протоколі Stratum, який використовується більшістю пулів.

Перші ознаки підозрілої активності зауважив користувач з форуму bitcointalk 22 березня. Його майнер підключилися до невідомої IP-адреси і, з якоїсь причини і процес майнінгу зупинився.

Зловмисники анонсували IP-адреси пулів тільки на короткий час, ймовірно, всього протягом декількох хвилин або секунд, завершували TCP-з'єднання, всім майнерам відправляли команду reconnect із зазначенням адреси свого майнінгового пулу, потім прибирали хибний анонс. Працюючи короткими інтервалами, їм вдалось уникати викриття протягом 4 місяців. Всього їм вдалося роздобути близько $ 83000 за все 4 місяці.

BGP-анонси проводилися з одного ISP в Канаді. Через 3 дні після оприлюднення даних ISP, підміни припинилися.

Rostelecom-Mastercard (квітень 2017 року). Державний російський оператор «Ростелекомом» перехопив трафік платіжних систем шляхом анонсування протягом деякого часу значної кількості префіксів, які належали міжнародним платіжним системам та фінансовим сервісам [50, 51].

Зазвичай, мережевий трафік, пов'язаний з MasterCard, Visa, а інші постраждалі компанії проходять через постачальників послуг, які наймають та дозволяють компанії. Використовуючи таблиці маршрутизації BGP,

уповноважені постачальники "оголошують" свою власність на великі блоки IP-адрес, що належать до клієнтських компаній. Однак, Ростелеком раптом анонсував відповідні префікси від імені власної AS12389. Як результат, трафік, що протікає у постраждалі мережі, розпочато через маршрутизатори Ростелеком. Викрадення трафіку тривало всього сім хвилин. Коли Викрадення могли дозволити в РФ перехопити або маніпулювати трафіком, що протікає у постраждалий адресний простір. Максимально легко маніпулювати таким чином з даними, які не були зашифровані, але навіть у випадках, коли вони була зашифровані, трафік все ще може бути розшифрований за допомогою кількох відомих атак із словарем та іншими. Навіть якщо дані не можуть бути розшифровані, зловмисники можуть потенційно використовувати зворотний трафік, щоб ідентифікувати клієнтів сервісів за зв'язками з MasterCard та інших постраждалих компаній, і далі проводити проти них цілеспрямовані кібератаки.

Повний опис інциденту зроблений сервісом BGPmon та візуалізовано за допомогою BGPlay [51].

Google Japan (серпень 2017). Google перехопив трафік багатьох операторів в Японії в наслідок технічної помилки конфігурування маршрутизаторів [52].

Найбільше постраждали мережеві префікси AS4713 NTT OCN, найбільшого інтернет-провайдера у Японії. Дані BGPmon показують більше 24000 нових більш специфічних префіксів для OCN, які раптово стали видимими через Google та Verizon протягом часу інциденту, отже інцидент трапився з деагрегацією трафіку.

Також відбулась деагрегація понад 7000 префіксів для AS7029 (Windstream). Загальний список нових (переважно більш специфічних) становить близько 50000.

Всі ці витоки були видимими між 03:22 UTC та 03:33 UTC, але в деяких BGP-системах «витоки» префіксів продовжувались до 04:00 UTC, тобто між 0:22 та 01:00 місцевого часу.

В Google пояснили проблему помилкою конфігурації маршрутизаторів мережі Google Global Cache, яка є, мабуть, найбільшою мережею доставки контенту (CDN) в Інтернеті.

Деякі інші інциденти, які окремо описані інших публікаціях:

- грудень 2017: перехоплення трафіку Google, Facebook, VK.com та інших відомих контент-провайдерів телеком-оператором з Хабаровська (умовна назва інциденту – «Khabarovsk-SM»);
- квітень 2018 року: атака route hijack застосована до інфраструктурного IP-префіксу широко відомого хмарного сервісу Amazon AWS, метою якого була фішингова атака на криптовалютний сервіс «MyEtherWallet» шляхом перенаправлення трафіку (умовна назва інциденту – «Amazon EtherWallet») [53];
- листопад 2018 року: збій глобальної маршрутизації, що торкнувся сервісів G Suite, Google Пошук і Google Аналітика, стався завдяки невеликому нігерійському провайдеру за участю China Telecom та Ростелекому, визнаний фахівцями як умисні дії (умовна назва

інциденту – «China-Rostelecom») [54, 55];

– червень 2019 року: атака на відомий сервіс мережевого захисту CloudFlare (умовна назва інциденту – «CloudFlare») [56].

Це дає достатньо даних для аналізу з метою ідентифікації ризику, а саме – визначення джерела виникнення; події, що виникнуть; причини цих подій; наслідки подій. Структуровані за цими чотирма елементами дані про інциденти кібербезпеки, пов'язані з глобальною маршрутизацією, зведено в табл. 3.1.1.

Таблиця 3.1.1. – Характеристики атак на глобальну маршрутизацію

Назва інциденту	Джерело	Подія	Причина	Наслідки
Інцидент з AS3252, 1994	приватний оператор	витік маршрутів	технічна помилка	Мінімальні (затримка передачі e-mail)
Інцидент з AS7007, 1997	приватний оператор	перехоплення маршрутів з деагрегацією	технічна помилка	Постраждалі – активні Інтенет-користувачі
Інцидент з AS9121, 2004	приватний оператор	витік маршрутів	технічна помилка	Постраждалі – 1/4 IP-мереж та їхні користувачі
Інцидент з Youtube, 2008	державний оператор	перехопдення маршруту з деагрегаією	зумисні дії	Постраждав сервіс YouTube та користувачі
Canadian Bitcoin Hijack, 2014	приватні особи	перехоплення маршруту	зумисні дії	Постраждалі – користуачі криптомайнерів та власники криптовалют
Rostelecom-Mastercard, 2017	державний оператор	перехоплення маршрутів	невідомо	Постраждалі – користувачі платіжних систем, здебільшого з РФ
Khabarovsk-SM, 2017	приватний оператор	витік маршрутів	невідомо	Постраждалі – соцмережі, контент-провайдери та їхні користувачі з РФ
Amazon EtherWallet, 2018	приватні особи	перехоплення маршрутів з деагрегацією	зумисні дії	Постраждалі – всі клієнти сервісу Amazon AWS, а також їхні користувачі з усього світу
China-Rostelecom, 2018	державний оператор	витік маршрутів	підозра на зумисні дії	Постраждалі – платіжні системи та клієнти
CloudFlare, 2019	приватний оператор	витік маршрутів	технічна помилка	Постраждалі – клієнти Cloudflare та їхні користувачі
RPKI Deletion, 2020	державний оператор	перехоплення маршрутів	підозра на зумисні дії	Постраждалі – провайдери перш за все європейського регіону.

3.2.7. Перехоплення маршрутів підчас російської агресії

15 лютого 2022 року кілька українських міністерств, зокрема Міністерство оборони, та два великі національні банки, зокрема Приватбанк,

були атаковані DDoS (Distributed Denial of Service). Фінансове обслуговування було перервано на кілька годин. Атаки не вплинули на цілі критично, але ці інциденти стривожили українську владу та громадян і послужили міжнародним тривожним сигналом про важливість системи маршрутизації Інтернету та необхідність її захисту.

28 лютого 2022 року були атаковані мережеві префікси компанії «Український центр інтернет імен», якому належить AS197726. Перехоплення вчинила AS210512[1]. Видатні члени міжнародного співтовариства, зокрема Барт Грутуїс, член Європейського парламенту, згадували про випадки викрадення українських мережевих префіксів за участю російських операторів. Його пост в соціальній мережі Twitter 28 лютого 2022 року: «Росія навмисно змінює маршрути та перехоплює величезні обсяги інтернет-трафіку з України. Дзвінки, смс, можливі геолокації: ймовірно, використовується для військових цілей»[2]. Йому відповідає інший користувач: «AS210512 – Internet Technologies LLC виглядає як російська установа, зареєстрована в юрисдикції Сполучених Штатів».

З систематизованих даних можна пересвідчитись, що дедалі росте доля очевидних зумисних дій, спрямованих на скоєння атак на глобальну маршрутизацію, а наслідки атак стають більш глобальними.

Для ідентицікації ризику перехоплення маршруту зробимо опис цього ризику на основі дослідження відомих тактик та стратегій таких атак перехоплення маршрутів та узагальнимо цю інформацію.

Отже:

- джерелами виникнення ризику обов'язково є інші суб'єкти глобальної маршрутизації;
- подіями, виникнення яких спричинює ризик, це несанкціоновані зміни в глобальній таблиці маршрутизації чи її інтерпретації на інших суб'єктах глобальної маршрутизації;
- наслідками цих подій є несанкціонована зміна напрямку проходження мережевого трафіку.

3.3. Модель порушника в системі глобальної маршрутизації

Модель порушника – традиційний підхід

В цьому розділі використовуються терміни та визначення, що надані в документі «ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення» [75], а також поняття «Власна ІТС» – інформаційно-телекомунікаційна система, для захисту якої розробляється модель порушника.

Модель порушника – це всебічна структурна характеристика порушника, яка є частиною моделі загроз та використовується під час розроблення політики безпеки інформації [75 – 77]. Сукупність типових

[1] https://grip.inetintel.cc.gatech.edu/events/moas/moas-1646067600-197726_210512
[2] https://twitter.com/bgroothuis/status/1498377147450331141

критеріїв для класифікації порушника та розробки неформального опису (неформальної моделі) [78] порушника наведено в табл. 3.3.1.

Таблиця 3.3.1 – Основні характеристики порушника

Порушник безпеки інформації			
Компетенція	**Оснащеність**	**Мотивація (мета)**	**Повноваження в системі**
– початківець з частковими знаннями – спеціаліст із знаннями – професіонал із знаннями та досвідом	– має звичайні користувацькі засоби – має спеціальні програмні та апаратні засоби – має змогу виготовляти/розробляти власні інструменти	– навмисні дії – ненавмисні дії	– віддалене виконання фіксованого набору дій – віддалене керування функціями, зміна конфігурації – віддалене створення та запуск власних функцій – фізичний доступ до обладнання

Порушник є джерелом загрози. Відповідно до локалізації джерела, загрози поділяються на внутрішні та зовнішні. До зовнішніх відносяться загрози, джерело яких знаходиться поза межами власної мережі. Внутрішні загрози реалізуються в межах контрольованої зони, шляхом керування мережевими пристроями, які є частиною власної ІТС. Відповідно до цього розрізняються два види порушників: зовнішній та внутрішній.

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

Категорії осіб, які можуть бути зовнішніми порушниками:

- сторонні особи, що знаходяться за межами контрольованої території вузлів власної ІТС;
- відвідувачі;
- представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності.

Внутрішній порушник – це порушник, що діє з середини власної ІТС. У цій моделі розглядається як особа, що має доступ до приміщень, у яких розташовані засоби обчислювальної техніки власної ІТС. Внутрішній порушник має можливість реалізувати загрозу інформації, й може бути як авторизованим користувачем, так і не авторизованим.

Внутрішнім порушником може бути особа з наступних категорій персоналу організації:

- технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС;
- персонал, який обслуговує технічні засоби (інженери, техніки);
- системний адміністратор;
- адміністратор безпеки;
- користувачі.

Потенційним порушником безпеки інформації є особа, яка помилково, внаслідок необізнаності, або цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснила спробу виконати операції, які призвели або можуть призвести до порушення конфіденційності, цілісності та доступності інформації.

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

- адміністратори власної ІТС (системний адміністратор, адміністратор мережі, адміністратор безпеки);
- користувачі власної ІТС;
- технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС;
- представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності;
- сторонні особи, що знаходяться за межами контрольованої території вузлів власної ІТС.

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

У табл. 3.3.2 наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо власної ІТС, за показником можливостей використання засобів власної ІТС для реалізації загроз, за часом дії, за містом дії. У графі «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника (можливих збитків). Рівень загрози характеризується наступними категоріями:

1 – незначний (низький),
2 – нижче середнього,
3 – середній,
4 – вище середнього,
5 – значний (високий).

Таблиця 3.3.2 – Категорії та специфікації порушників

Позначення	**Визначення категорії та специфікації**	**Потенційний рівень загрози**
П1	Системний адміністратор власної ІТС	5

Позначення	Визначення категорії та специфікації	Потенційний рівень загрози
П2	Відвідувачі	2
П3	Технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС	3
П4	Персонал, який обслуговує технічні засоби (інженери, техніки)	3
П5	Представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності	3
П6	Сторонні особи, що знаходяться за межами контрольованої території вузлів власної ІТС	2
За мотивом порушення		
М1	Безвідповідальність (недбалість)	3
М2	Корисна цілеспрямованість	5
За рівнем кваліфікації та обізнаності		
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами системи.	1
К2	Має навики щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення та операційних систем, та практичними навичками роботи з засобами що реалізовані в власної ІТС.	4
К4	Володіє знаннями щодо функціонування засобів та механізмів захисту, що використовуються в ІТС та їх недоліки	5
За можливостями використання засобів ІТС		
З1	Має фізичний доступ до програмно-апаратних засобів, але не є авторизованим користувачем ІТС	1
З2	Має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;	3
З3	Має можливість керування функціонуванням елементів ІТС, тобто конфігурує програмне забезпечення	5
З4	Не має фізичного доступу	1
За часом дії		
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час).	4
Ч2	Під час функціонування ІТС	5

Позначення	Визначення категорії та специфікації	Потенційний рівень загрози
Ч3	Під час перерв у роботі для обслуговування та ремонту	3
За місцем дії		
Д1	Усередині будівлі та приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів	5
Д3	З інших об'єктів ІТС, в тому числі каналів зв'язку	2

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

Модель порушника з урахуванням особливостей атак на глобальну маршрутизацію

Як було описано в гл.1, розробниками системи ARTEMIS [11] було запропоновано та класифікації атак за різними критеріями.

1. Класифікація по анонсованому шляху.

Атаки відрізняються способом маніпуляції з довжиною шляху та його вмістом, який містить перелік транзитних AS від джерела префіксу.

Перехоплення Origin-AS (або Type-0): зловмисник анонсує чужий мережевий префікс наче свій, не маючи на це права. Тобто, підмінює джерело маршруту (це буде детальніше пояснено в гл.2 та гл.3). На думку авторів ARTEMIS, це найбільш популярний тип атаки.

Перехоплення Type-N (N більше 1): зловмисник передає маршрут до префіксу, який йому не належить, несанкціоновано додаючи свою AS останньою в маршруті. N залежить від довжини шляху.

Перехоплення Type-U: зловмисник не змінює шлях (підробка маршруту полягає в іншому).

2. Класифікація по враженому мережевому префіксу.

Перехоплення цілого префікса: зловмисник анонсує маршрут до префікса, який повністю співпадає з префіксом жертви. Анонсується підробний маршрут коротший за справжній, тому це призводить до перетікання трафіку.

Перехоплення частини префікса: зловмисник анонсує маршрут до більш специфічного мережевого префікса, що покриває частину адресного простору жертви. Такий маршрут не конкурує зі справжнім а повністю його перехоплює.

Сквоттінг: зловмисник анонсує адресний простір жертви, який вона сама (за будь-яких причин) сама в даний момент не анонсує.

3. По типу маніпуляції з мережевим трафіком (data-plane).

ВН: black-holing, або dropping – те ж саме, що і blackholing. Перехоплення трафіку робиться з метою запобігти доступності даних. Перехоплений трафік не обробляється, потрапляючи на хибний маршрут, виявляється втраченим через невідповідність правилам фільтрації чи невідповідність пропускній здатності каналів.

ММ: man-in-a-middle, або manipulating. Перехоплений трафік прослуховується з метою отримання інформації з обмеженим доступом, чи задля збору статистичних даних (розвідка) [71]. Загальною рисою атаки є те, що перехоплений трафік після маніпуляцій повертається в мережу на легітимний маршрут.

ІМ: imposture. Мета перехоплення трафіку – перехоплення сервісів жертви – підробка відповідей, використиання фішингових сайтів тощо. Загальною рисою атаки є те, що перехоплений трафік після маніпуляцій повертається в мережу на легітимний маршрут.

3. Класифікація за сценарієм та мотивацією атаки.

Людська помилка: некоректна конфікурація обладнання в результаті незловмисних дій чи бездіяльності персоналу. Часто «зловмисник» (саме в лапках) стає і жертвою атаки. Так, в разі витікання суттєвой частино префіксів, отриманих в провайдера, «зловмисник» отримає неочікуваний більший трафік, що може призвести до перевантаження його мережі.

Атака з метою нанести максимальний збиток: цілеспрямована атака з широким поширенням перехоплення, типу інциденту Pakistan-Youtube.

Прихована цільова атака: це комбінація Type-N чи Type-U атаки з тактикою ММ, коли жертва не підозрює якийсь час, що отримує не весь трафік, або трафік зманіпульовано. Інцидент Bitcoin 2014 та AWS-Ether були саме такі.

Проаналізуємо всі з категорій порушників, які можуть створити обставини (чи сприяти таким обставинам), що призведуть до перехоплення маршрутів, шляхом моделювання їхніх повноважень та можливих дій (табл.3.3.3).

Таблиця 3.3.3 – Моделювання дій порушника по відношенню до атак на глобальну маршрутизацію

Тип порушника	**Особливі можливості цього типу порушника**	**Можливі дії**
адміністратори ІТС	– мережевий доступ до обладнання власної ІТС; – знання з налаштувань СЗІ; – керування	припинення глобальной маршрутизації адресного простору власної ІТС чи його частки; внесення некоректних даних стосовно

Тип порушника	Особливі можливості цього типу порушника	Можливі дії
	функціями, зміна конфігурації обладнання, зокрема маршрутизаторів; – розуміння системи аудиту (реєстрації дій в системі);	маршрутизації в RR; втрата (розголошення) атрибутів доступу до RR;
користувачі власної ІТС;	– мережевий доступ до обладнання власної ІТС	злам слабкої автентифікації обладнання власної ІТС та отримання повноважень адміністратора
технічний персонал, який обслуговує будівлю та приміщення, в яких розташовані компоненти власної ІТС	– фізичний доступ до приміщень та обладнання власної ІТС	несанкціонована комутація, вмикання, вимикання пристроїв, підключення до них носіїв інформації
представники організацій, що взаємодіють з питань обслуговування власної ІТС, технічного забезпечення та підтримки її функціональності;	– доступ до апаратного та програмного забезпечення обладнання власної ІТС	отримання даних про налаштування апаратного та програмного забезпечення обладнання власної ІТС; внесення несанкціонованих змін програмне забезпечення власної ІТС
сторонні особи, що знаходяться за межами контрольованої території вузлів власної ІТС.	– ніяких особливих можливостей	ніяких дій по відношенню до обладнання чи програмного забезпечення власної ІТС

Без урахування особливостей атак на глобальну маршрутизацію найвищий рівень небезпеки отримав би внутрішній порушник. Проте, Інтернет є IP-мережею, що складається з понад 70000 AS. Кожна AS обмінюється маршрутами принаймні з однією іншою AS (це є запорукою зв'язності мережі). Відсутність надійних засобів забезпечення цілісності та доступності інформації

про маршрути саме за межами власної ІТС є причиною атак на глобальну маршрутизацію.

Роздивимось узагальнену схему інформаційних потоків, які виникають між суб'єктами глобальної маршрутизації на рис.3.3.1. Крім того, адміністратори кожної AS зобов'язані розміщувати інформацію про взаємодію з іншими автономними системами в БД RR. Хоч ця вимога є суто адміністративною, інші адміністратори часто спираються на неї при конфігуруванні BGP-фільтрів.

Вище описано у який спосіб проводяться атаки на глобальну маршрутизацію:

- захоплення префіксу, коли вузол анонсує у якості джерела адресний простір, який йому не належить; при виборі маршруту BGP віддасть перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем;
- захоплення маршруту, в якому вузол ретранслює легально отриманий анонс чужого адресного простору, пропонуючи транзит через себе; в результаті перенаправлення трафік, можливо, доставляється коректному одержувачу, але передається шляхом, відмінним від істинного;
- захоплення підмереж через анонсування більш специфічних префіксів; при виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість;
- захоплення нерозподіленого або невикористаного адресного простору: анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.
-

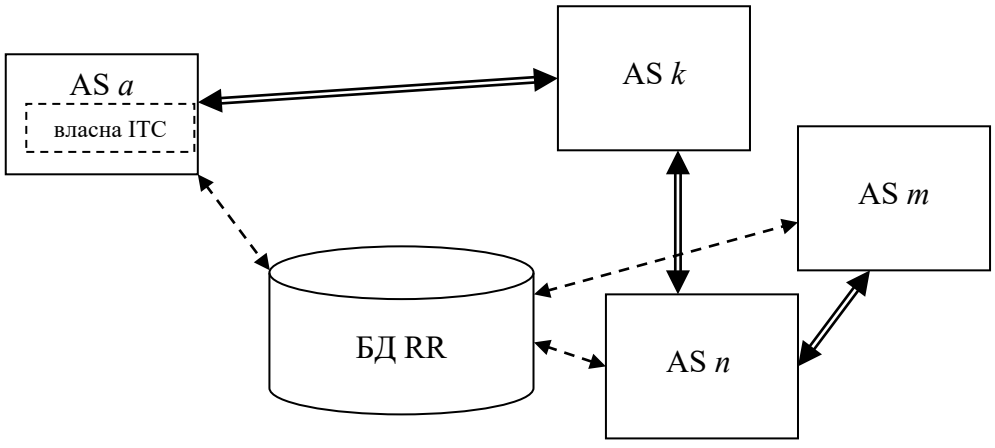


Рисунок 3.3.1 – Схема інформаційних потоків в глобальній маршрутизації: обмін маршрутами між AS (товсті лінії); збереження даних в БД RR та запити до неї (пунктирні лінії)

Припустимо, що власної ІТС належить до AS *a*. Перелічені вище способи проведення атак насправді виконуються по за межами власної ІТС і навіть по за межами AS *a* в цілому. Адміністратор AS *a* здатен:

- контролювати інформацію, що виходить з AS *a* в напрямку БД RR та інших AS;
- перевіряти інформацію, що надходить від інших AS, за допомогою запитів до БД RR.

Хоча існують інструменти перевірки інформації від інших AS в автоматизованому та навіть автоматичному режимі, через загальні розміри таблиць маршрутизації та поліноміальну обчислювальну складність ці перевірки не мають всеосяжного характеру і перевірки мають місце загалом на початкових ланцюгах при передаванні маршрутів від кінцевих AS до їхніх провайдерів, та дуже рідко – між великими інтернет-провайдерами [6]. Отже, адміністратор AS *a,* і тим більше адміністратори власної ІТС, в загальному випадку не мають змоги забезпечити доступність та цілісність інформації про маршрути до власної ІТС, а також не здатні контролювати цілісність інформації про маршрути, яка надходить до власної ІТС.

Таким чином ми бачимо, що основні загрози від атак на глобальну маршрутизацію полягають у впливі на інформаційні потоки по за межами власної ІТС. Це означає – загрози надходять від порушників, які є сторонніми особами, що знаходяться за межами контрольованої території вузлів власної ІТС. Це певним чином перевертає традиційну оцінку небезпеки порушників і виводить на значуще місце саме зовнішнього порушника.

В запропонованій моделі небезпечним зовнішнім порушником є особа з повноваженнями адміністратора будь-якої AS. Адміністратор будь-якої AS – це принаймні спеціаліст із знаннями, який керує спеціальними засобами і в разі помилки чи навмисно може створити атаку на глобальну маршрутизацію. Отже, в табл. 3.3.4 пропонується коригування категорій та специфікацій порушника відносно традиційних, наведених в табл. 3.3.2.

Таблиця 3.3.4 – Специфікації порушників глобальної маршрутизації

Позначення	**Визначення категорії порушника та специфікації**	**Потенційний рівень загрози**
П1	Відвідувач	1
П2	Технічний персонал	2
П3	Представник обслуговуючої організації	2
П4	Авторизований користувач	3
П5	Адміністратор AS	5
За мотивом порушення		
М1	Безвідповідальність (недбалість)	3
М2	Корисна цілеспрямованість	5
За рівнем кваліфікації та обізнаності		
К1	Володіє базовими знаннями щодо функціонування глобальної маршрутизації	3
К2	Володіє глибокими знаннями з глобальної маршрутизації, засобів та механізмів використання	4

Позначення	Визначення категорії порушника та специфікації	Потенційний рівень загрози
	БД RR	
К3	Володіє глибокими знаннями з глобальної маршрутизації, вади протоколу BGP-4, вади захисту даних в БД RR	5
За повноваженнями, набутими в AS		
А1	Має можливість вносити зміни в налаштування BGP-4 на маршрутизаторах AS	3
А2	Додатково до А1 має авторизований доступ до публікації даних в БД RR та обміну інформацією з адміністраторами сусідніх AS	5
За часом дії		
Ч1	Не може планувати дії на конкретний час	2
Ч2	Може планувати дії на конкретний час в залежності від мети	4
За місцем дії		
Д1	Порушник має доступ до AS кінцевого типу (корпоративна мережа, установа)	1
Д2	Порушник має доступ до AS Інтернет сервіс-провайдера локального характеру (населений пункт, географічний регіон)	3
Д3	Порушник має доступ до AS Інтернет сервіс-провайдера великого масштабу (міжнародні оператори, мережі обміну трафіком)	5

Профіль такого порушника представлено в табл.3.3.5.

Таблиця 3.3.5. – Профіль порушника – потенційного джерела атаки на глобальну маршрутизацію

Категорія порушника	Мотиви	Кваліфікація	Можливості	Час дії	Місце дії	Сумарний рівень загроз
П1-П5	М1, М2	К1-К3	А1,А2	Ч1,Ч2	Д1-Д3	13 – 30

3.4. Загрози інформаційної безпеки на рівні системи глобальної маршрутизації

Деякі методи аналізу загроз і оцінки ризиків

В даному розділі на основі єдиного методичного підходу, що викладено в настановах ISO Guide 73:2009 «Risk Management – Vocabulary» [41] проводиться систематизація та класифікація загроз, що з’являються від атак на

глобальну маршрутизацію, а також пропонується підхід до оцінювання ризиків, що виникають внаслідок цих загроз.

При забезпеченні інформаційної безпеки необхідно дослідити ланцюжок від потенційного зловмисника, наявної вразливості, загрози її використання, безпосередньої дії (атаки) та її наслідків.

Класифікація загроз охоплює сукупність можливих варіантів дій джерел загроз, які призводять до реалізації цілей атаки. Мета атаки може не співпадати з метою реалізації загроз і може бути направлена на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози. У разі такого незбігу атака розглядається як етап підготовки до здійснення дій, направлених на реалізацію загрози, тобто як «підготовка до здійснення» протиправної дії. Завдяки такому підходу можливо:

- встановити пріоритети цілей безпеки;
- визначити перелік актуальних джерел загроз;
- визначити перелік актуальних вразливостей;
- оцінити взаємозв'язок загроз, джерел загроз і вразливостей;
- визначити перелік можливих атак на об'єкт;
- описати можливі наслідки реалізації загроз.

Результати проведення оцінки і аналізу можуть бути використані при виборі адекватних оптимальних методів протидії загрозам, а також при аудиті реального стану інформаційної безпеки об'єкту для цілей його страхування.

При визначенні актуальних загроз, експертно-аналітичним методом визначаються об'єкти захисту, схильні до дії тієї або іншої загрози, характерні джерела цих загроз і уразливості, які сприяють реалізації загроз. На підставі аналізу складається матриця взаємозв'язку джерел загроз і вразливостей з якої визначаються можливі наслідки реалізації загроз (атаки) і обчислюється коефіцієнт небезпеки цих атак як добуток коефіцієнтів небезпеки відповідних загроз і джерел загроз, визначених раніше.

Аналіз потенційно можливих загроз інформації є одним з перших і обов'язковим етапом розробки будь-якої захищеної інформаційної системи. При цьому складається якомога повніша сукупність загроз, аналізується ступінь ризики при реалізації тієї або іншої загрози, після чого визначаються напрями захисту інформації в конкретній системі.

Краще всього аналізувати наслідки реалізації загроз ще на стадії проектування локальної мережі, робочого місця або інформаційної системи, щоб заздалегідь визначити потенційні втрати і встановити вимоги до заходів забезпечення безпеки. Вибір захисних і контрольних заходів на ранній стадії проектування ІС вимагає набагато менших витрат, чим виконання подібної роботи на експлуатованій ІС [79, 80, 81].

Модель STRIDE (за першими буквами назв категорій) була розроблена фірмою Microsoft і майже 20 років успішно застосовується для визначення та «зважування» загроз [82]. STRIDE базується на класифікації загроз безпеці по наступних шести категоріях:

- *Підміна мережевих об'єктів (Spoofing identity)*. Атаки подібного типу дозволяють зловмисникові видавати себе за іншого користувача або підміняти справжній сервер підробленим. Приклад підміни особи користувача – використання чужих автентифікаційних даних (імені користувача, пароля) для атаки на систему.
- *Модифікація даних (Tampering with data)*. Атаки цього типу порушують цілісність даних, що зберігаються, обробляються чи передаються. Приклади: несанкціоновані зміни даних (наприклад, що зберігаються в базі даних).
- *Відмова від авторства (Repudiation)*. Легальний користувач може виконати певну операцію і відмовитися від її «авторства», а адміністраторові не вдасться нічого довести в разі відсутності чи несправності механізмів аудиту та протоколювання дій користувачів.
- *Розголошування інформації (Information disclosure)*. Мається на увазі розкриття інформації особам, доступ до якої їм заборонений, тобто, порушення конфіденційності.
- *Відмова в обслуговуванні (Denial of service)*. В атаках такого типу зловмисник намагається позбавити доступу до сервісу правомочних користувачів, наприклад, зробивши веб-сервер тимчасово недоступним або непридатним для роботи.
- *Підвищення привілеїв (Elevation of privilege)*. В даному випадку непривілейований користувач дістає привілейований доступ, що дозволяє йому «проникнути» в систему – отримати конфіденційну інформацію, підмінити чи впровадити власний програмний код, чи знищити систему.

У табл. 3.4.1 перераховані методи, які застосовуються для боротьби з небезпеками, описаними в моделі STRIDE. Запропоновані засоби боротьби з загрозами можна звести до наступних:

- автентифікація користувачів;
- розподіл повноважень (авторизація);
- захист від несанкціонованого доступу;
- аудит;
- фільтрація.

Таблиця 3.4.1 – Основні методи боротьби з загрозами

Тип небезпеки	**Засоби боротьби**
Підміна мережевих об'єктів (S)	– Надійний механізм автентифікації – Захист секретних даних – Відмова від зберігання секретів
Модифікація даних (T)	– Надійний механізм авторизації – Використання хеш-кодувань – MAC-коди

Тип небезпеки	**Засоби боротьби**
	– Цифрові підписи – Протоколи, що запобігають прослуховуванню трафіку
Відмова від авторства (R)	– Цифрові підписи – Мітки дати і часу – Контрольні сліди
Розголошування інформації (I)	– Авторизація – Протоколи з посиленим захистом від несанкціонованого доступу – Шифрування – Захист секретів – Відмова від зберігання секретів
Відмова в обслуговуванні (D)	– Надійний механізм автентифікації – Надійний механізм авторизації – Фільтрація – Управління числом вхідних запитів – Якість обслуговування
Підвищення рівня привілеїв (E)	– Виконання з мінімальними привілеями

М. Ховардом і Д. Лебланком був запропонований один з способів оцінки ризиків – DREAD [83], який також названий за першими буквами п’яти категорій:

1) *Потенційний збиток (Damage potential)* – міра реального збитку від успішної атаки. Найвищий ступінь небезпеки означає практично безперешкодний злом засобів захисту і виконання практично будь-яких операцій. Підвищенню привілеїв зазвичай привласнюють оцінку 10. У інших ситуаціях оцінка залежить від цінності даних, що захищаються.
2) *Відтворюваність (Reproducibility)* – міра можливості реалізації загрози. Деякі вразливості доступні постійно, інші – тільки залежно від ситуації, і їх доступність непередбачувана, тобто не можна напевно знати, наскільки успішною виявиться атака. Наприклад, вразливості, знайдені у типовому програмному забезпеченні, характеризуються високою відтворюваністю.
3) *Легкість організації атаки (Exploitability)* – міра зусиль і кваліфікації, необхідних для проведення атаки. Так, якщо її може реалізувати недосвідчений програміст на домашньому комп'ютері – 10. Якщо ж для її проведення треба витратити 100 млн. доларів, оцінка небезпеки – 1. Атака, для якої можна написати алгоритм (а значить, розповсюдити у вигляді сценарію серед любителів), також оцінюється в 10 балів. Слід також враховувати необхідний для атаки рівень автентифікації і авторизації в системі. Наприклад,

якщо це доступно будь-якому видаленому анонімному користувачеві, подібна небезпека оцінюється 10 балами;

4) *Коло користувачів, що потрапляють під удар (Affected users)* – частка користувачів, робота яких порушується із-за успішної атаки. Оцінка виконується на основі процентної частки: 100% всіх користувачів відповідає оцінка 10, а 10% – 1 бал. Іноді небезпека стає реальною тільки в системі, яка конфігурована особливим чином;
5) *Важкість виявлення (Discoverability)* – наскільки швидко і чи взагалі можна виявити факт реалізації загрози. Вважається найскладнішою для визначення оцінкою.

Інтегральний ризик в методиці DREAD оцінюється за формулою

$$R_{DREADx} = \frac{R_D + R_R + R_E + R_A + R_{Dx}}{5} = \sum_{i=\{D,R,E,A,Dx\}} R_i \ / 5 \ , \qquad (3.1)$$

де R з індексом – чисельні оцінки відповідних типів ризику.

Подекуди в методику DREAD включають ще один показник – *витрати* на усунення наслідків успішної атаки, умовно названий X (*eXpense*). Таким чином, для кількісної оцінки ризику використовується модель DREADX і сумарна DREADX-оцінка дорівнює сумі всіх оцінок, поділеній на шість).

Ідентифікація ризику перехоплення маршруту в термінах ISO/IEC 73:2009

В розділі 3.1 сформулюовано поняття ризику, описано причетні сторони, ознаки, за якими можна ідентифікувати ризики, а саме:

- джерелами виникнення ризику обов'язково є інші суб'єкти глобальної маршрутизації;
- події, виникнення яких спричинює ризик, це несанкціоновані зміни в глобальній таблиці маршрутизації чи її інтерпретації на інших суб'єктах глобальної маршрутизації;
- наслідками цих подій є несанкціонована зміна напрямку проходження мережевого трафіку.

Спробуємо описати ризики, які виникають внаслідок загроз глобальній маршрутизації, по методу DREAD.

По-перше, міра, чи межа потенціального збитку (damage potential) може бути дуже високою в наслідок того, що така впливає на всі аспекти інформаційної безпеки, як це буде показано далі.

Відтворюваність (reproducibility), тобто можливість використати вразливість «типовими» засобами, які не потрібно розробляти під конкретну атаку, є також високою. Для проведення атаки з перехопленням маршруту використовуються стандартні засоби керування глобальною маршрутизацією.

Легкість організації атаки на практиці умовно ділиться на три рівні: атаку може організувати будь-який користувач, чи тільки з професійними

навичками і інструментами, чи тільки освічений спеціаліст рівня розробника. Попри те, що багато атак типу перехоплення маршруту відбуваються саме помилково, через низьку кваліфікацію чи брак досвіду, все ж атаку може виконати лише професіонал з навичками та інструментами.

«Область ураження», коло користувачів, які опиняться під впливом перехоплення маршруту, є потенційно надзвичайно великим і зазвичай перевищує кількість уражених від більш типових DDoS з використанням виснаження ресурсів.

За показником складності виявлення (discoverability) атаки перехоплення маршруту є такими, виявити які найпростіше. З перелічених інцидентів всі атаки і їхні джерела були виявлені протягом декількох годин. Проте лишається відомий інцидент з крадіжкою криптовалют у 2014, коли підміною маршрутів зловмисники досягали своїх цілей протягом чотирьох місяців.

Атака класу BGP hijacking має кілька варіантів реалізації:

1) Захоплення префіксу, коли вузол анонсує у якості джерела адресний простір що йому не належить. При виборі маршруту BGP віддасть перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем. Цей маршрут конкуруватиме з істинним (рис.1.3.1). Така атака може бути швидко виявлена, бо з точки зору глобальної маршрутизації, наявність двох джерел в одного префікса є помилкою.
2) Захоплення маршруту, в якому вузол ретранслює легально отриманий анонс чужого адресного простору, пропонуючи транзит через себе. Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, джерело не підмінюється і виявити такий інцидент значно складніше.
3) Захоплення під мереж через анонсування більш специфічних префіксів. При виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру захоплення має глобальний ефект.
4) Захоплення нерозподіленого або невикористаного адресного простору. Анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.
5) Перенаправлення трафіку. Трафік доставляється коректному одержувачу, але передається шляхом, відмінним від істинного.

Наслідки атак на глобальну маршрутизацію можуть бути різними. Захоплення маршруту призводить до перетягування трафіку, призначеного для захопленої мережі, який зазвичай потім відкидається. Така стратегія має назву створення «чорної діри» (blackholing) – мережеві пакети проходять хибним маршрутом та «зникають». Таким чином відбувається DoS-атака на всі сервіси мережі. У цю категорію атак потрапляє більшість помилок конфігурації маршрутизаторів.

Якщо при атаці анонсується фрагмент адресного простору, який досі не використовувався (так звані «нічиї мережі», можливо нерозподілений адресний простір), вона може бути використана для короткострокової генерації не просто трафіку, а для доставки шкідливого контенту, тобто елементарно – для розсилки спаму.

Інший варіант стратегії – перенаправлення трафіку. Трафік йде не в «чорну діру», а перехоплюється і аналізується. Іноді атака ще більш глибока, і перехоплений трафік не тільки не йде в «чорну діру» і аналізується, але після перехоплення повертається знову в Інтернет, щоб бути доставленим істинному одержувачу. Таку атаку важче виявити. Метою може бути не тільки підслуховування, але і модифікація переданих даних. У більш витонченому вигляді захоплення маршруту може бути спрямоване на захоплення деякого інформаційного ресурсу, наприклад веб-сайту, з наданням користувачам підробленого сайту.

Проведемо класифікацію цих загроз відповідно до моделі STRIDE.

Загроза *підміни мережевих об'єктів* притаманна атакам на глобальну маршрутизацію. Механізм реалізації загрози наступний:

- IP-адреси мережі жертви присвоюються іншим мережевим пристроям, розташованим під керуванням зловмисника;
- зловмисник анонсує IP-адреси жертви так, щоб новий хибний маршрут мав вищий пріоритет за істинний маршрут;
- зловмисник набуває можливості створювати мережеву активність (навіть ініціювати та приймати повноцінні сеанси клієнт-сервер) з власних мережевих пристроїв, видаючи їх за пристрої жертви.

Реалізація атаки за таким сценарієм лежить в основі інших загроз, наведених далі.

Загроза *модифікації даних,* або порушення цілісності даних, є реальною в разі, коли перехоплений зловмисником завдяки хибному анонсу трафік повертається зловмисником знову в Інтернет, щоб бути доставленим істинному одержувачу. Така атака може відбуватись з *підміною мережевих об'єктів* або без неї.

Загроза *відмови від авторства* також є можливою в ході атаки, разом із з підміною мережевих об'єктів.

Однією з найсуттєвіших загроз є *розголошування інформації* в наслідок перехоплення трафіку. Порушення конфіденційності є можливим в разі виконання атаки методом перехоплення трафіку та повернення його в мережу, бо це часто є необхідною умовою з урахуванням особливостей побудови мережевих протоколів рівня застосувань.

Відмова в обслуговуванні є найчастішим наслідком перехоплення маршрутів. Створення «чорної діри», в яку потрапляє частина трафіку, який адресовано мережі жертви, не потребує отримання та аналізу трафіку.

Загроза *підвищення рівня привілеїв,* на наш погляд, не властива атакам з захопленням префіксу, оскільки керування глобальною маршрутизацією не має ієрархії повноважень.

3.5. Ідентифікування загроз та оцінювання ризиків за допомогою моделі STRIDE×DREAD

Інтегральний ризик в методиці DREAD оцінюється за формулою (3.1). В той же час, кожен *R* з індексом є функцією, яка пов'язує вірогідність настання певного наслідку в разі реалізації певної загрози. З урахуванням пояснень до оцінки ризиків DREAD та запропонованої класифікації конкретних загроз глобальній маршрутизації, спробуємо скласти матрицю ризиків шляхом поєднання класифікації загроз STRIDE та оцінки ризиків DREAD. Як запропоновано в моделі DREAD, оцінки для кожної з загроз будуть виставлені, як і запропоновано в моделі DREAD, від 0 до 10, таким чином, що 10 означатиме високу вірогідність настання певного наслідку від реалізації даної загрози, а 0 – або відсутність наслідку або невластивість подібної загрози при атаках типу перехоплення маршруту.

Якщо поєднати методи STRIDE та DREAD для отримання двовимірної моделі безпеки для оцінки ризиків кібератак на глобальну маршрутизацію, запропонований підхід дозволяє не тільки розрахувати інтегральний ризик за факторами методом DREAD, а й оцінити вагу кожної загрози з моделі STRIDE в формуванні ризику. Тобто, на прикладі оцінки ризику потенціального збитку (damage potential):

$$R_{Dam} = R_{Dam}^{S} + R_{Dam}^{T} + R_{Dam}^{R} + R_{Dam}^{I} + R_{Dam}^{D} + R_{Dam}^{E} \qquad (3.2)$$

Тепер запишемо формальне представлення інтегрального ризику запропонованого методу:

$$R = \frac{\sum^{STRIDE} R_{Dam} + \sum^{STRIDE} R_{R} + \sum^{STRIDE} R_{E} + \sum^{STRIDE} R_{A} + \sum^{STRIDE} R_{Dis}}{5} \qquad (3.3)$$

де *R* з індексом – чисельні оцінки відповідних типів ризику.

Приклад такої оцінки наведено в табл. 3.4.1, а також на рис.3.4.1 та рис.3.4.2. Для демонстрації застосовано оцінки автора, що базуються на його особистому досвіді та аналізі відомих інцидентів безпеки в глобальній маршрутизації. Ці результати можна візуалізувати у вигляді двох діаграм: на які ризики впливає певний тип загрози (рис.3.4.1) і які загрози є складовими в оцінці певного фактор у ризику (рис.3.4.2).

В поєднаній моделі для кожного фактору ризику за DREAD складається своя модель загроз за STRIDE, що дозволяє визначити:

- долю кожної загрози в кожному окремому факторі ризику;
- на які фактори ризику і як впливає окрема загроза.

Таблиця 3.4.1 – Оцінка загроз за факторами ризику

	R_{Dam}	R_R	R_E	R_A	R_{Dis}	**Інтегральний ризик**
S	10	5	5	10	9	7,8
T	10	4	1	8	5	5,8
R	10	4	1	8	5	5,8
I	5	5	5	10	5	6
D	8	8	8	10	0	6,8
E	0	0	0	0	0	0
Сума по категоріях	43	26	20	46	24	32.2

Комбіновану модель можна умовно назвати «STRIDExDREAD» і представити у вигляді декартового добутку наборів:

$$\{D,R,E,A,D\} \to \{D,R,E,A,D\} \times \{S,T,R,I,D,E\};$$

$$R_D = \frac{R_{DS} + R_{DT} + R_{DR} + R_{DI} + R_{DD} + R_{DE}}{6}.$$

Так само для R_R, R_E, R_A, R_{Dx}:

$$R_R = \frac{R_{RS} + R_{RT} + R_{RR} + R_{RI} + R_{RD} + R_{RE}}{6};$$

$$R_E = \frac{R_{ES} + R_{ET} + R_{ER} + R_{EI} + R_{ED} + R_{EE}}{6};$$

$$R_A = \frac{R_{AS} + R_{AT} + R_{AR} + R_{AI} + R_{AD} + R_{AE}}{6};$$

$$R_{Dx} = \frac{R_{DxS} + R_{DxT} + R_{DxR} + R_{DxI} + R_{DxD} + R_{DxE}}{6};$$

$$R_{DREADx} = \sum_{i=\{D,R,E,A,Dx\}} \left(\sum_{j=\{S,T,R,I,D,E\}} R_{ij} \right) /30.$$

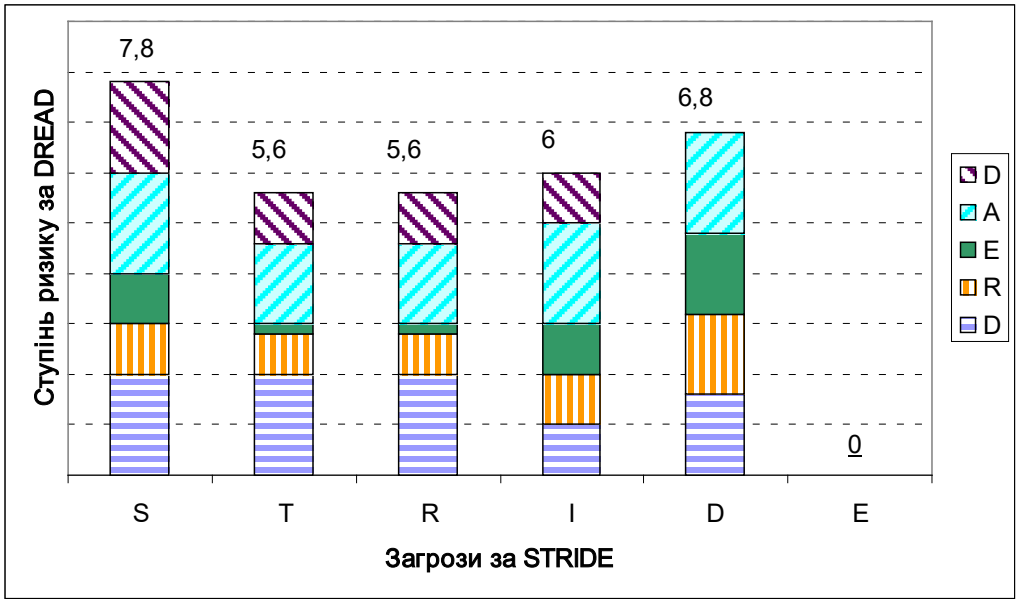


Рисунок 3.4.1 – Оцінка загроз від атак на глобальну маршрутизацію по методу STRIDE за факторами ризику DREAD

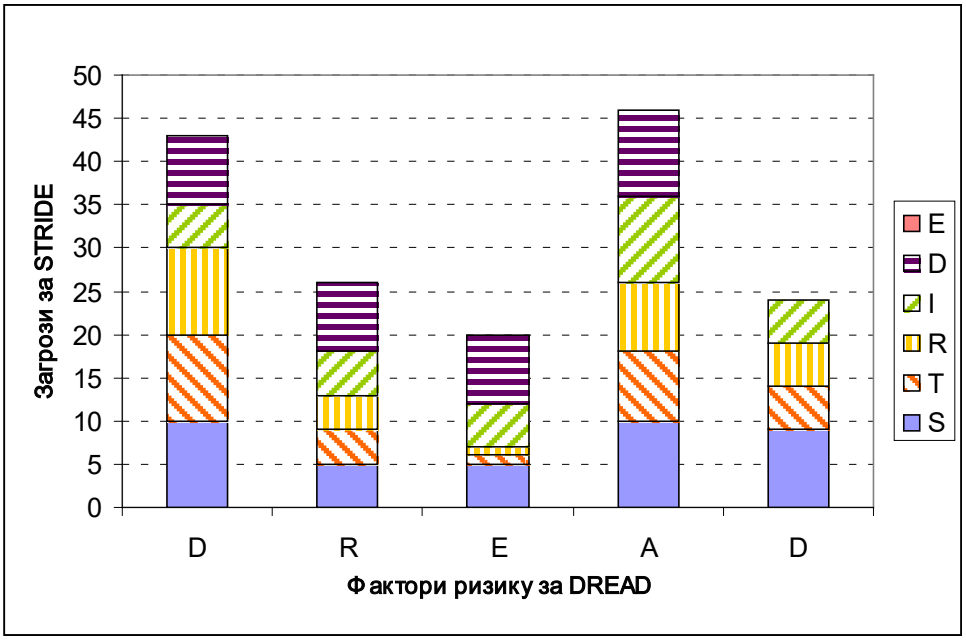


Рисунок 3.4. – Вага загроз STRIDE в оцінці різних типів ризику від атак на глобальну маршрутизацію

Завдяки визначенню кожного фактора DREAD за шістьма показниками, сукупна оцінка ризику стає фактично на 80% точнішою за оцінку по традиційній моделі DREAD.

3.6. Стратегії поводження з ризиком кібератак на систему глобальної маршрутизації

Факторний аналіз та декомпозиція ризику

Забезпечення захищеності таких складних систем, як система глобальної маршрутизації Інтернету, є комплексною задачею та потребує уваги в процесі розробки, впровадження та експлуатації (включаючи оновлення програмного чи програмно-апаратного забезпечення). Розглянемо проблеми поводження з ризиками системи глобальної маршрутизації на прикладі інциденту з видаленням записів ROA з БД регіонального реєстру, наведеного в підрозділі 3.1. Розробка, впровадження та експлуатація програмних та комп'ютерних компонентів – це діяльність, яка використовує різноманітні технологічні досягнення і вимагає високого рівня знань. Через ці та інші фактори кожен проєкт з розробки, впровадження та експлуатації програмно-апаратного забезпечення складної системи містить елементи невизначеності. Це відомо як проєктний ризик. Управління ризиками включає такі завдання [21]:

1) визначення ризиків і їхніх тригерів, або факторів, що призводять до настання ризику;
2) класифікування та визначення пріоритетів ризиків;
3) розробка плану з усунення чи мінімізації наслідків кожного ризику;
4) моніторинг стану тригерів ризику в ході проєкта;
5) у разі матеріалізації ризику – виконання плану з усунення чи мінімізації наслідків.

Один лише факт того, що інцидент тривав майже 2 доби і набув планетарного масштабу, свідчить про те, що при плануванні та (або) виконанні перелічених вище заходів було допущено суттєвих помилок. Розберемо їх.

Проблема з базою даних стала зрозумілою на ранок 1 квітня, проте інцидент не було усунено, і масштабне перехоплення маршрутів завдяки цій проблемі відбулося ввечері 1 квітня. Вочевидь, *при аналізі факторів ризику* та *визначенні пріоритетів були допущені помилки*.

Більшість проектів програмної інженерії за своєю суттю ризиковані через різноманітність потенційних джерел. Досвід інших проектів програмного забезпечення може допомогти менеджерам класифікувати ризик шляхом якомога точнішого визначення та опису всіх реальних загроз. Є велика кількість класифікації, ранжування та оцінки ризиків. Для аналізу ризиків даного проєкта застосуємо метод декомпозиції, де кожен фактор ризику розкладається на фактори більш низького рівня. Розкладання (drill-down) факторів на більш дрібні проводиться, допоки не з'являється можливість надати факторам кількісну оцінку [85]. Формальний підхід до декомпозиції ризику наведений на рис. 3.6.1.

Кожен із факторів нижнього рядка таблиці або може бути охарактеризований кількісно, або має бути декомпонований на ще дрібніші фактори. Наприклад, фактори (властивості) загрози, що обумовлюють збиток, декомпонуються наступним чином (рис. 3.6.2).

Очевидним є те, що сукупність факторів «випадковий користувач, який виконує штатні дії ззовні» має найменший вплив на ризик, порівняно із сукупністю «професіонал, який виконує цілеспрямовані зловмисні дії зсередини».

Проведемо декомпозиційний аналіз факторів ризику інциденту з реєстром маршрутів відповідно до формальної моделі. Наголошуємо, що ризик-аналіз мав робитися до настання інциденту на етапі планування дій з реєстром, які стали тригером (подією), що призводить до настання ризику. В даному випадку тригером було оновлення програмного забезпечення.

Спочатку роздивимося ланцюг факторів, починаючи з тригеру.

1. Тригер: оновлення ПЗ.
2. Фактор ризику: втрата даних.
3. Максимальний збиток: високий; аргументи надані в ході опису інциденту в п.3.1.
4. Частота настання загрози: низька, оскільки оновлення ПЗ є рутинною процедурою, але рідкісною, порівняно з іншими операціями, що супроводжують процес експлуатації ПЗ.
5. Складність реалізації загрози: середня; помилки в програмному коді чи процесі оновлення з’являються з вини персоналу. Не слід переоцінювати рівень розробників, тестувальників та інженерів розробки та операційної підтримки, які задіяні в життєвому циклі ПЗ.
6. Заходи захисту (захищеність): пропонується додаткова декомпозиція захищеності і оцінка дрібніших факторів ризику відповідно до табл. 3.6.1. Стовпчики захисту конфіденційності не заповнені через те, що в даному інциденті мала місце проблема з публічними даними.

Декомпозиція факторів втрат, особливо аналіз втрат внутрішніх і втрат за межами організації, мав би дати важливі результати, але в цій статті акцентуємо увагу на факторах, що мають впливати на настання ризику. Отже, на етапі декомпозиції захищеності власнику системи має бути зрозуміло, які фактори впливають на ймовірність настання ризику для активу.

Моніторинг ризику має включати:

— публікацію звітів про стан проєкту, включно з питаннями управління ризиками;
— перегляд планів ризику відповідно до будь-яких основних змін у графіку проєкту;
— перегляд і репріоритізація ризиків;
— мозковий штурм щодо потенційно нових ризиків підчас непланованих змін у проєкті.

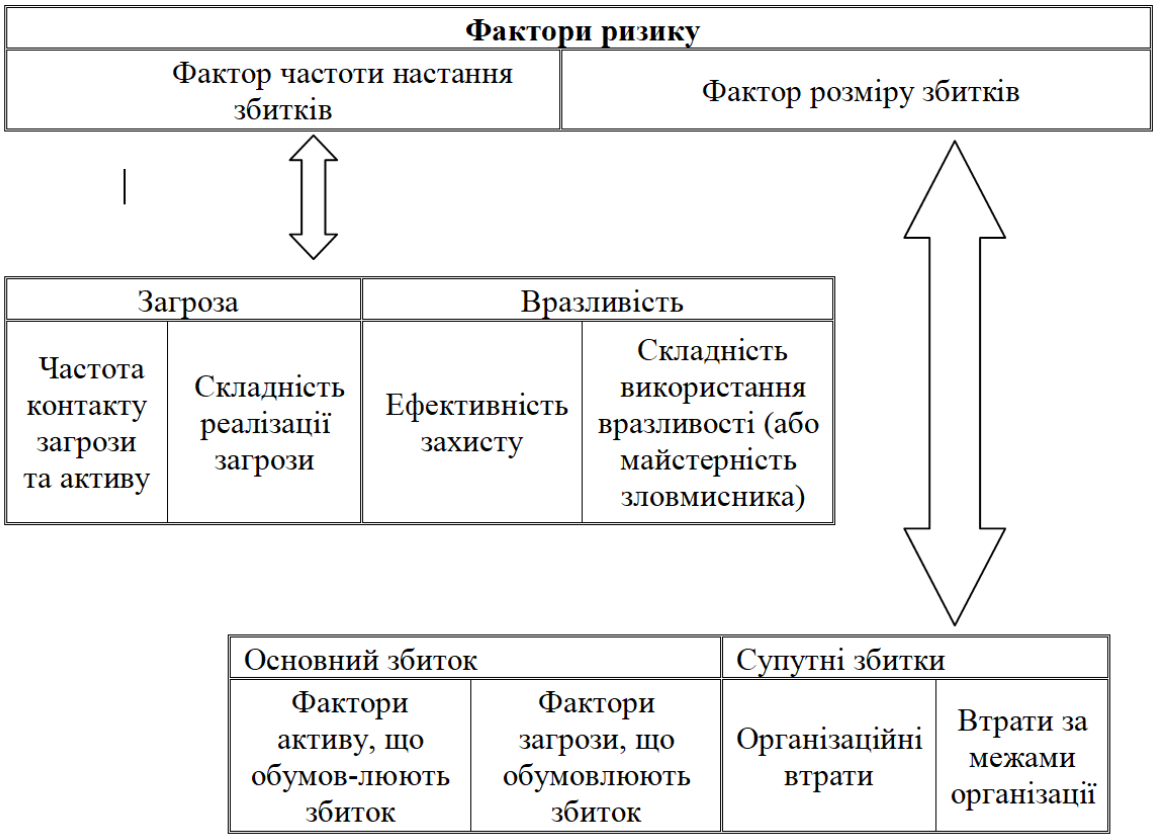


Рисунок 3.6.1 – Загальний підхід до декомпозиції ризику

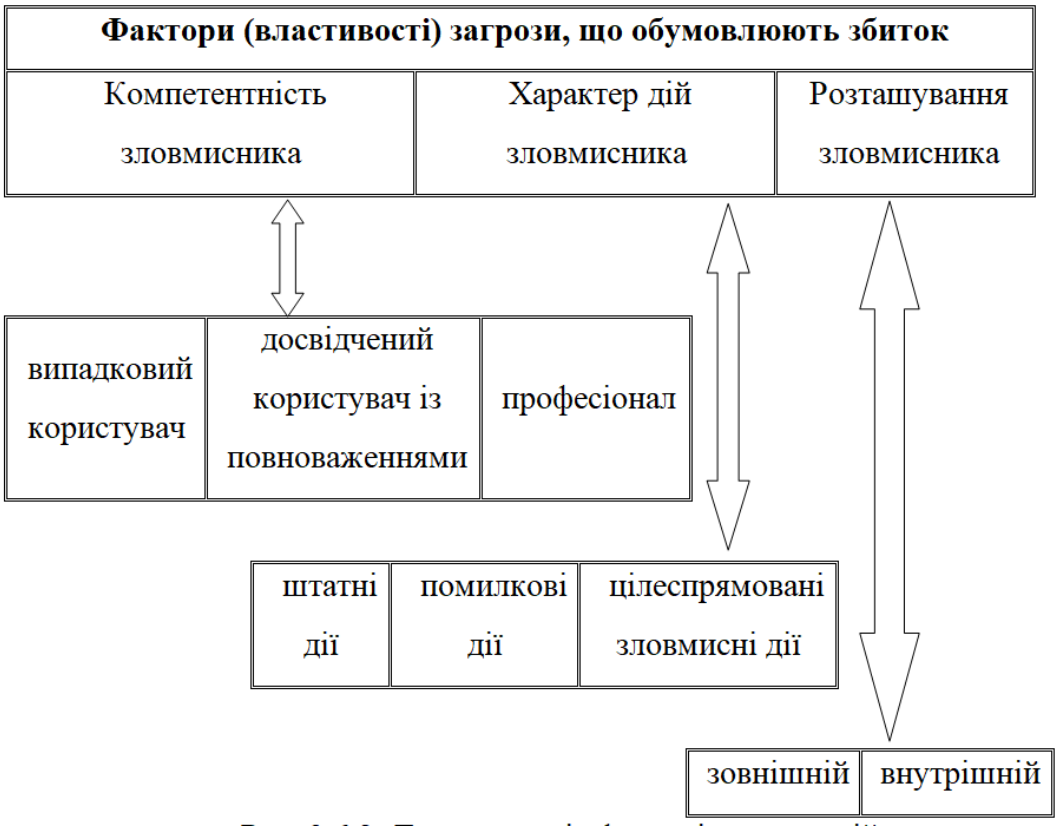


Рисунок 3.6.2 – Декомпозиція факторів ризику дій зловмисника

Таблиця 3.6.1 – Декомпозиція факторів захищеності

Захищеність							
Цілісність			Доступність			Конфіденційність	
моніторинг цілісності	резервне копіювання	процедури відновлення даних	моніторинг доступності	наявність дублюючої системи (резерву)	процедури відкату	–	–

Протягом проєкту важливо забезпечити ефективну комунікацію між усіма зацікавленими сторонами, менеджерами, розробниками, тестувальниками, інженерами dev-ops, користувачами. Проте, перші скарги реєстр отримав не від власного персоналу, а від зовнішніх користувачів, і отримав «у неробочий час» відповідно до опублікованого пост-аналізу, тому dev-ops дізналися про наявність проб-леми тільки наступного робочого дня. Служба підтримки не вважала скарги корис-тувачів важливими, бо не знала про оновлення ПЗ і не була готова до посиленого моніторингу. Очевидним є *брак комунікацій*.

Стратегії поводження з ризиком

Якщо виникає ризик, відповідна реакція на пом’якшення наслідків повинна бути взята з уже підготовленого плану управління ризиками. Наприклад, доступні такі варіанти пом’якшення:

— «прийняти»: визнати, що ризик впливає на проєкт; це означає погодитися з можливими наслідками (таке рішення припустиме лише, якщо інші міри з пом’якшення коштуватимуть дорожче, ніж наслідки);
— «уникнути керувати наслідками»: вживання заходів для мінімізації впливу або зменшення інтенсифікації ризику;
— «передача ризику»: здійснити організаційну зміну підзвітності, відповідальності чи повноважень іншим зацікавленим сторонам, які приймуть ризик;
— «продовжити моніторинг»: часто підходить для ризиків з низьким впливом; можливо, цей було обрано в даному випадку.

Можна аргументовано показати, що в даному інциденті мала місце *відсутність чи недосконалість плану пом’якшення ризику*. Оскільки, як показано раніше, попередній ризик-аналіз був проведений недостатньо, власник системи не прийняв найкращого рішення – уникнути ризику. В даному випадку, принаймні, не проводити оновлення ПЗ реєстру маршрутизації у вечірні та нічні години, якщо вночі нікому буде спостерігати за оновленою системою.

Також є обґрунтованою думка, що не відбулося вчасної передачі ризику: черговий персонал побачив скарги користувачів, та не насмілився потурбувати більш компетентні підрозділи, оскільки то було пізно ввечері.

Окрім того, персонал реєстру не був готовий до швидкого відновлення даних. Попри значний вплив інциденту, його наслідки було усунуто більше ніж як за добу: реальне відновлення помилково видалених записів почалося на ранок 2 квітня.

Для суб'єкта глобальтної маршрутизації на цей час відсутні засоби гарантованого уникнення ризику, що витікає з вразливостей системии глобальної маршртутизації. Отже, єдиною прийнятною стратегією лишається «пом'якшення» ризику – зниження ймовірності настання ризику та зменшення масштабу наслідків.

ГЛАВА 4.
РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ БЕЗПЕКИ ТОПОЛОГІЇ ІНТЕРНЕТ

4.1. Метричні характеристики захищеності системи глобальної маршртутизації

Об’єкти глобальної маршрутизації та формальний опис відносин між ними

Телекомунікаційна мережа є невід’ємною частиною інформаційно-телекомунікаційних систем і характеризується різними за формою зв'язками, а також різними видами взаємодії. Часто математичною моделлю таких мереж може служити граф [86]. Граф можна уявити як набір точок, званих вершинами чи вузлами, з'єднаних собою лініями, які називаються дугами чи зв’язками. Кожному зв’язку і вузлу графа може відповідати певна кількість параметрів, що характеризують природні обмеження. Наприклад, мережа може бути представлена в вигляді графа, в якому дуги відповідають каналам зв'язку, а вершини – вузлам комутації. Важливі параметри включені в модель у вигляді чисел або ваг, приписаних до дуг і вершин графа. Ці ваги можуть бути фіксованими і випадковими. Так, для мережі типова вершина, що представляє вузол комутації, може мати такі ваги: максимальну пропускну здатність, обсяг запам’ятовуючого пристрою, і т. і. Типова дуга – лінія зв’язку – може мати такі ваги: максимальну пропускну здатність, середню затримку передачі по каналу зв'язку, надійність каналу зв'язку і таке інше.

Доцільність побудови моделі у вигляді графа залежить від фізичної природи досліджуваної мережі [87]. Найбільш очевидна доцільність користування моделлю у вигляді графа при вирішенні задач зв'язності [88, 89]. Так, в загальному випадку, нас може цікавити завдання доставки інформації з будь-якої точки в будь-яку. Це структурна задача, в якій необхідно встановити чи існує принаймні один шлях з будь-якої вершини в будь-яку іншу. Іншим важливим завданням є пошук найкоротшого шляху між двома, кількома, або всіма вершинами графа, а також пошук найкоротшого шляху з урахуванням різних обмежень [90 – 97]. За допомогою графів можна також вирішувати завдання синтезу топології мережі, тобто побудови оптимальної системи. Одним з можливих критеріїв оптимальності можуть бути ступінь живучості або надійності телекомунікаційної системи. Оскільки телекомунікаційній мережі властиві пошкодження і відмови (наслідком чого є порушення зв'язку), можливим завданням може бути побудова системи, в якій наслідки порушень роботи є мінімальними при заданих умовах роботи [98, 99].

Математичний апарат теорії графів, а пізніше – теорії складних мереж, у застосуванні до топології глобальної телекомунікаційної мережі Інтернет дозволяє аналізувати ступінь вузлів, розподіл ступеню, шліх між парою вузлів, середній шлях в мережі, показники кластерності, посередництва тощо. В даний

час в багатьох дослідженнях граф використовують для побудови моделі мережі Інтернет на рівні автономних систем [9, 38, 85, 86]. Мережа Інтернет в них представляється графом $G := (V, E)$, де V є множиною автономних систем (AS), а E – їхні зв‘язки, утворені протоколом маршрутизації BGP-4. При цьому пропускна спроможність зв‘язків між вузлами Інтернет не приймається о уваги і не впливає на вагу ребер, таким чином граф є незваженим. Було досліджено стосунки (node relationships) між автономними системами в Інтернеті. Було виділено декілька типів таких стосунків, зокрема «клієнт-провайдер», «партнер-партнер» та інші. У випадку взаємодії двох рівних за статусом операторів, вони анонсують один іншому власні префікси та префікси мереж своїх клієнтів. В разі взаємодії провайдера і клієнта, провайдер анонсує клієнтові всі наявні в нього префікси, а клієнт анонсує префікси власних мереж. Таким чином, зв'язки між автономними системами представляються двосторонніми, отже ребра є ненаправленими, а граф – неорієнтований.

Отже, для виявлення атак з перехоплення маршрутів, дослідження масштабів впливу на топологію, а також подальшої оцінки ризиків необхідно мати модель мережі Інтернет на рівні глобальної маршрутизації, тобто – з використанням BGP-зв’язків. Першою відмінністю від наведених в попередньому розділі підходів є те, що сам процес маршрутизації невід’ємно пов’язаний з вибором напрямку, отже при дослідженні втручання в маршрутизацію, коли результатом є несанкціонована зміна напрямку, ми не зможемо використовувати в якості моделі незважений граф. Для визначення необхідних якостей нової моделі пропонується формалізувати поняття маршрутизації.

Сформулюємо вихідні дані.

Існує адресний простір мережі Інтернет A – множина унікальних IP-адрес a, які згруповані в IP-префікси p (надалі – просто «префікси»):

$$A = \{a_1, a_2, a_3, ...a_{|A|} : a_i \neq a_j, \{i, j\} \leq |A|\};$$
$$a \in p \subset A.$$

Префікси, в свою чергу, групуються (частіше вживають термін «агрегуються») з більш специфічних в менш специфічні, як це визначено в [101] і наведено в табл.4.1.1. Повний перелік префіксів наведено в документації по CIDR. З ілюстрації зрозуміло, що будь-яка IP-адреса входить до 32 префіксів, які «інкапсулюються» входять один в одного за допомогою зміни мережевої маски. При цьому весь адресний простір A може бути описаний одним префіксом з довжиною мережевої маски 0, або об’єднанням двох префіксів з довжиною маски 1, або чотирьох з довжиною маски 2 і так далі:

$$p_3 \subset p_2 \subset p_1 \subset p_0;\ |p_0| = 2|p_1| = 4|p_2| = 8|p_3|.$$

В загальному випадку можемо так виразити відношення між підмножинами IP-адрес, визначених певними префіксами, в множині всіх IP-адрес :

$$\begin{cases} |p_i| = 2^{j-i}|p_j|; \\ i \le j; \\ 0 \le \{i, j\} \le \log_2|A| \end{cases} \qquad (4.1.1)$$

Таблиця 4.1.1 – Агрегація IPv4-префіксів згідно RFC 4632

Нотація префіксу	**Довжина netmask, біт**	**Кількість адрес в префіксі**	**Загальна кількість префіксів IPv4**
.x.x.x/32	32	1	4294967296
x.x.x.x/31	31	2	2147483648
x.x.x.x/30	30	4	1073741824
x.x.x.x/29	29	8	536870912
.....			
x.x.x.0/24	24	256	16777216
x.x.x.0/23	23	512	8388608
.....			
x.x.0.0/17	17	32768	131072
x.x.0.0/16	16	65536	65536
x.x.0.0/15	15	131072	32768
.....			
x.0.0.0/9	9	33554432	512
x.0.0.0/8	8	16777216	256
x.0.0.0/7	7	8388608	128
.....			
x.0.0.0/1	1	2147483648	2
0.0.0.0/0	0	4294967296	1

Префікси анонсуються автономними системами (в іноземній літературі використовується термін «originating», отже в кожного префіксу є свій «origin» – автономна система, що анонсує його. Приклад взаємодії AS наведено на рис.4.1.1. В нормальному стані кожен префікс анонсує лише одна автономна система.

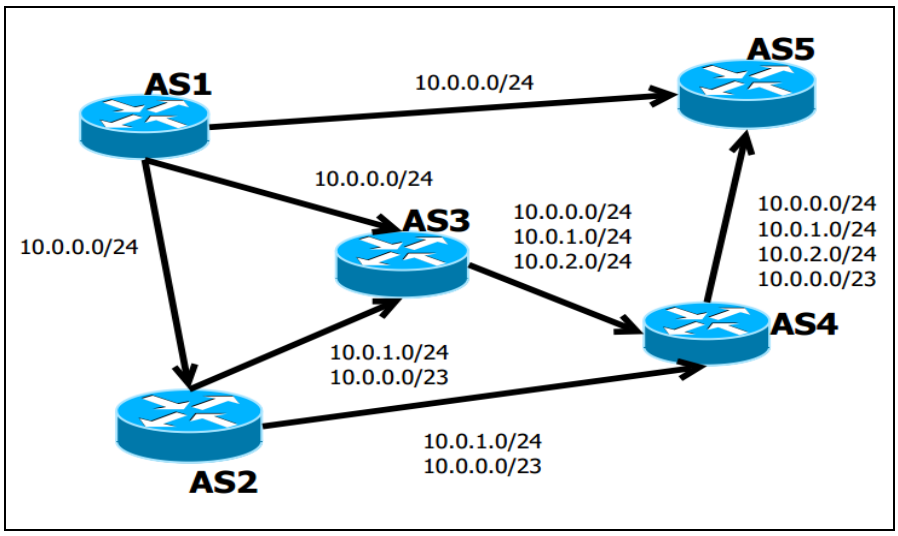


Рисунок 4.1.1 – Графічна модель експорту анонсів IP-префіксів в процесі взаємодії 5 автономних систем

До кожного префіксу p існує принаймні один маршрут $m(p)$, який складається з множини направлених ребер e_p, що відповідають напрямкам анонсів префіксу між вершинами множини v_p (автономними системами):

$$m(p) := (v_p, e_p), \qquad (4.1.2)$$

Таблиця маршрутів залежить від точки спостереження. Та, якщо обрати для спостереження вузол AS5, до нього потраплять такі маршрути:

- 10.0.0.0/24 AS1;
- 10.0.0.0/24 AS4 AS2 AS1 або AS4 AS3 AS1 (залежить від вибору на вузлі AS3);
- 10.0.1.0/24 AS4 AS2;
- 10.0.2.0/24 AS4 AS3.

До префіксу, який не анонсується, маршрутів нема, і він не може вважатись учасником Інтернету.

Сукупність маршрутів m_p до певного префікса p може бути представлена у формі зв'язного орієнтованого графа без кілець

$$M_p := (V_p, E_p), \qquad (4.1.3)$$

де V_p – зв'язки між автономними системами, по яких надходять анонси префікса p, а E_p – автономні системи, в яких присутні маршрути до префіксу p. Вершини графа по вхідних ребрах приймають анонси префіксу і по вихідних ретранслюють їх до інших вершин (чи не ретранслюють, в залежності від політики маршрутизації чи стану каналу). Одна з вершин має тільки віхідні ребра, це – origin. Інші вершини обов'язково мають вхідні ребра (бо приймають анонси) і можуть мати вихідні (якщо ретранслюють анонси).

Поєднання (ансамбль) всіх графів $M_p := (V_p, E_p)$ – це сукупність всіх маршрутів до всіх префіксів. Вона утворює такий граф

$$G := (V, E) : V = \bigcup_p V_p \; ; \; E = \bigcup_p E_p \; ,$$

який і можна інтерпретувати як мережу Інтернет, представлену на рівні глобальної маршрутизації.

Поглибимось в процес маршрутизації. Якщо префікс p_j є підмножиною префіксу p_i, тобто $p_j \subset p_i$, це не означає, що в них обов'язково однаковий origin, в загальному префікси мають origin незалежно від вкладеності. Приклад: частина великого провайдерського префіксу може санкціоновано анонсуватись одним з клієнтів провайдера в напрямку інших AS. З іншого боку, якщо в певній автономній системі відсутні анонси до префіксу p_j, це не означає, що через неї цей префікс недосяжний: наявність в якомусь вузлі анонсу до p_i означає також і можливість маршрутизації до p_j (це одностороннє твердження):

$$p_j \subset p_i \; \Rightarrow m(p_j) \subset m(p_i) \, . \qquad (4.1.4)$$

Кардинальним прикладом цього є кінцевий мережевий пристрій, підключений до мережі своїм єдиним мережевим інтерфейсом. Його таблиця маршрутизації може містити виключно маршрут до загального префіксу 0.0.0.0/0 (див. табл.4.1.1), який також зветься маршрутом за замовчанням (default route). Слід зауважити, що префікс 0.0.0.0/0 анонсується в BGP виключно для учасників, які використовують обладнання, що не здатне обробити «full view» – повну таблицю маршрутизації (зазвичай це кінцеві споживачі – невеликі за кількістю об'єднаних мереж автономні системи, яких які не є транзитерами).

Відносини між об'єктами глобальної маршрутизації і різні типи IP-адрес

На сьогоднішній день в Інтернеті використовується два типи IP-адрес, які відрізняються розрядністю. Традиційна IP-адреса складалась з 32 біт. Це наклало обмеження на кількість можливих адрес у 232 = 4294967296. Зростання Інтернету, попри впровадження економного розподілу адресного простору, призвело до нестачі адрес. Сучасна IP-адреса, яка має умовну назву «IPv6-адреса» (на відміну від традиційної, яку стали називати «IPv4-адреса») має довжину 128 біт. Ця різниця впливає на функціонування канального та мережевого рівнів (згідно моделі OSI). Однак принципи CIDR та маршрутизації в цілому не зазнали змін при впровадженні IPv6.

З точки зору CIDR, відмінність від IPv4 полягає в наступному:

максимальна довжина мережевої маски складає 128 біт замість 32;

кожна адреса входить в 128 IPv6-префіксів, включених один в одного.

Протокол BGP-4 для IPv4 та IPv6 не відрізняється – BGP-спікери використовують одні й ті самі протокольні повідомлення, атрибути шляху, критерії вибору маршруту, як для адресного простору IPv4, так і для адресного простору IPv6. Тому опис об'єктів, запропонований в даному підрозділі, зокрема вирази (4.1.1) – (4.1.4), є незмінним незалежно від типу IP-префіксів.

4.2. Формальний опис процесу утворення топології Інтернету

Формальний опис процесу обрання маршруту в IP-мережі

Знаходження оптимального маршруту є складним завданням. Для вирішення задачі має бути відомою топологія мережі, пропускні спроможності ліній зв'язку, середня довжина повідомлення. Це задача з класу цілочисельного нелінійного програмування, для яких доки не існує алгоритмів навіть з поліноміальною складністю. Відомі лише евристичні алгоритми, яке дозволяють отримувати лише приближене рішення завдання оптимізації. Тому в стеку TCP/IP прийнятий так званий однокроковий підхід до оптимізації маршруту просування пакета (next-hop routing) – кожний маршрутизатор та кінцевий вузол приймають участь виборі тільки одного кроку передачі пакета. Однокроковий підхід означає розподілене обчислення задачі вибору маршруту, і це – перевага, яка лежить в основі умовно безкінечної масштабованості мережі Інтернет.

Першим етапом обрання напрямку доставки є вибір префіксу. В таблиці маршрутизації має бути обраний з урахуванням (4.1.1) найбільш специфічний префікс:

$$p(a) = \{\min_{j}(p_j) \ : \ a \in p \subset A, \ 0 < j \le |A|\} . \qquad (4.2.1)$$

Як це пояснено в попередньому параграфі, вибір маршруту властивий не всім учасникам мережі. Суб'єктом вибору маршруту в глобальній маршрутизації є вузол графа, тобто автономна система. Передумовою для початку процесу вибору є наявність більше ніж одного маршруту до одного і того самого префікса *p*. Один з доступних маршрутів може бути визначений як шлях між двома вузлами графа (4.1.2), де початковим вузлом є автономна система, в якій приймається рішення, а кінцевим вузлом – автономна система, яка є origin для префіксу *p*. Якщо не враховувати специфічні локальні атрибути маршруту та ті, що встановлюються адміністративно, єдине, що приймається до уваги, це топологія мережі на момент прийняття рішення. Загальним критерієм обрання шляху є його довжина (best path) – кількість транзитних вузлів між початковим і кінцевим вузлом. З урахуванням (4.1.2) та (4.1.3), шляхом до префіксу буде такий маршрут $\pi_v(p)$:

$$\pi_v(p) = \{\min_v(m_v(p)) \ : \ \pi \in M_p, \ v \in V_p\}, \quad (4.2.2)$$

де v – вихідний вузол, в якому приймається рішення.

В побудові маршрутів в системі глобальної маршррутизації використовуються ті ж самі рівняння, але логіка побудови дещо інша.

На першому етапі серед маршрутів до кожного мережевого префіксу, які отримані BGP-системою від сусідів, застосовуються локальні «метрики» (атрибути, наведені в р.2.1) та обирається найкоротший маршрут відповідно до (4.2.2). Сукупність кращих маршрутів до кожного з наявних мережевих префіксів стає таблицею маршрутизації, по якій підчас відправлення IP-пакета відбувається безпосередньо маршрутизація, а саме – вибір префікса відповідно до адреси призначення (4.2.1). Перший етап вибору маршруту для кожного префіксу за мінімальною відстанню для подальшого формування таблиці маршрутизації на конкретному вузлі і є етапом, який виконується системою глобальної маршрутизації.

Якщо об'єднати обидва етапи вибору маршруту в систему, буде сформульовано математичну модель системи глобальної маршрутизації, яка дозволила описати процес формування топологічного простору окремого мережевого префікса та топологічного простору Інтернету в цілому:

$$\begin{cases} \pi_v(p) = \{\min_v(m_v(p)) \ : \ \pi \in M_p, \ v \in V_p\} \\ p(a) = \{\min_j(p_j) \ : \ a \in p \subset A, \ 0 < j \le |A|\} \end{cases} \quad (4.2.3)$$

Перехоплення, витік маршруту означають, що механізм атаки спрямований на першу частину системи (4.2.3). Атака є ефективною, якщо в її результаті в таблицю маршрутизації потрапляє інший маршрут до атакованого префіксу, ніж той, що потрапив би за відсутності атаки.

Існує підтип атаки з перехоплення (захоплення) префіксу «з деагрегацією». Суть її полягає в тому, що адресний простір певного мережевого префікса анонсується від нового джерела у вигляді дрібніших частин. Наприклад, адресний простір 193.193.0.0 – 193.193.31.255, що легітимно анонсується у вигляді префіксу 193.193.0.0/19 може бути анонсований дрібнішими частинами:

- 193.193.0.0/20;
- 193.193.0.16/20.

Або

- 193.193.0.0/21;
- 193.193.0.8/21;
- 193.193.0.16/21;
- 193.193.0.24/21.

Або ще дрібніше, у вигляді 8 префіксів з довжиною маски 22, або 16 префіксів з довжиною маски 23, або 32 префіксів з довжиною маски 24.

В такому разі хибні маршрути вже не конкуруватимуть з легітимним за потрапляння в таблицю кращих маршрутів, бо всі вони відноситимуться до різних префіксів. В цьому випадку мережевий пакет, що адресований до 193.193.15.20 попаде в маршрут до найспецифічнішого префіксу, якому може належати адреса. Порядок преференцій при деагрегації за CIDR буде такий:

1) 193.193.15.0/24
2) 193.193.14.0/23
3) 193.193.12.0/22
4) 193.193.8.0/21
5) 193.193.0.0/20

За наявності в таблиці маршрутів до будь-якого з префіксів 1)-4), мережевий трафік не піде за маршрутом 5.

Порівняння отриманої моделі з іншими моделями системи глобальної маршрутизації

Взагалі, відомо чимало підходів до моделювання, зокрема, математичного, комп'ютерних та телекомунікаційних мереж [102], а також Інтернету [103 – 107]. Зазвичай, відомі моделі, де приймаються до уваги такі властивості вузлів та гілок як пропускна здатність, навантаженість, відсоток втрат, затримка. Але розглянемо деякі запропоновані іншими дослідниками моделі, що безпосередньо стосуються системи глобальної маршрутизації.

HEAP: Reliable Assessment of BGP Hijacking Attacks.

В роботі [108] представлено формалізацію Інтернет-маршрутизації схожої концепції з запропонованою в даному розділі роботи. Модель маршрутизації також побудована на основі формальних мов. На думку авторів, за допомогою цієї моделі аномалії маршрутизації можуть бути точно вираженими, класифікованими та отримано оцінено їхній вплив та ймовірність виявлення.

В поясненні до моделі визначено, що завжди існує «точка зору» (vantage point) з якої робиться огляд маршрутів. Формальною визначено префікс як фрагмент адресного простору:

$$p \subset \prod ,$$

шлях є певним чином визначеною послідовністю AS:

$$\sum\nolimits_{AS}{}^{*} \in \sum\nolimits_{AS} ,$$

вся множина маршрутів є декартовим добутком адресного простору та множини шляхів:

$$\sum\nolimits_{AS} \times \prod$$

а маршрут визначено як кортеж «префікс, шлях» (*w*,*p*), що входить у всю множину маршрутів:

$$(w, p) \in \sum_{AS}{}^{*} \times \prod$$

Додатково до запропонованої вище моделі, автори HEAP застосовують окреме визначення AS – джерела маршруту, з метою відокремлення її від іншої частини шляху і розглядання окремо у випадках, коли перехоплення префіксу виконується з підміною джерела маршруту. За допомогою цих визначень автори моделюють зміни в множині маршрутів, що трапляються в наслідок атаки.

Недоліком запропонованого у вказаній роботі формального опису є відсутність власне рівнянь, які б показали процес та результат вибору маршруту.

Модель BGP для мережевого симулятора ns-2.

Існує програмний симулятор NS-2, який є одним з найпопулярніших мережевих тренажерів, що підтримує симуляцію TCP, маршрутизацію та багатоадресні протоколи через провідні і бездротові мережі. ns-2 написано як у на C++ і OTCL з використанням об'єктно-орієнтованої парадигми (OTCL – це мова сценаріїв), яка використовується для реалізації моделей вище ніж мережевого рівня, де гнучкість є більш важливою, ніж продуктивність. В роботі [109] представлено опис та структурно-функціональну схему моделі протоколу маршрутизації BGP-4 для симулятора ns-2, яка завдяки декомпозиції дозволяє детально представити етапи роботи протоколу, потоки даних та зв’язки між параметрами (рис. 4.2.1).

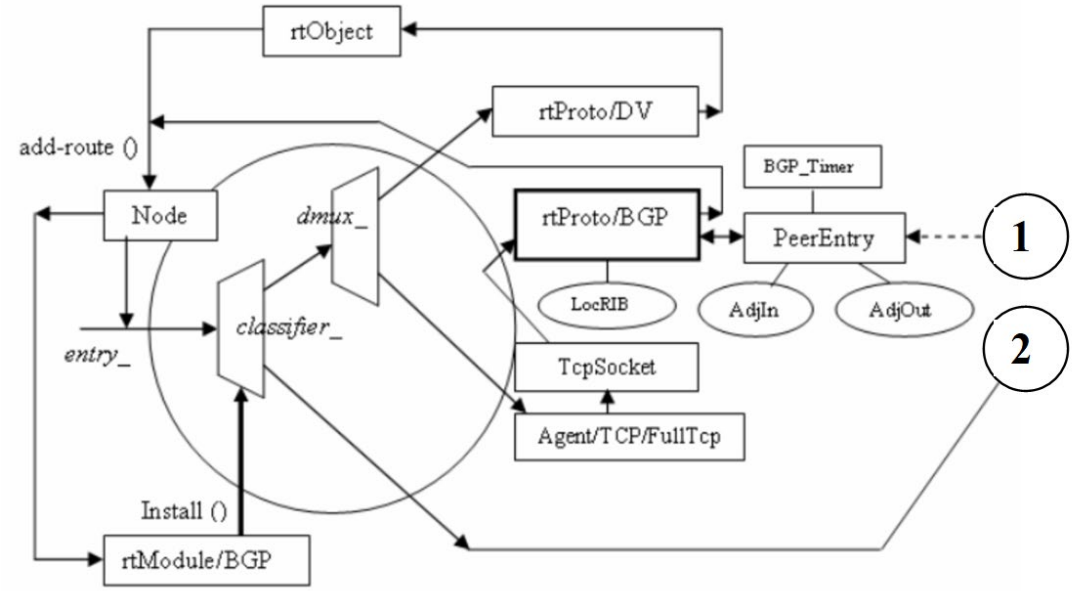


Рисунок 4.2.1 – Програмна модель BGP-системи для симулятора ns-2

.

Classifier доставляє пакет відповідному агентові чи вихідному зв’язку, rtModule – модуль маршрутизації, який керує класифікатором, RouteLogic – задана емулятору таблиця маршрутизації, rtProto – імплементує алгоритм

вибору шляху, rtPeer – зберігає параметри (метрики та преференції) кожного маршруту, rtObject керує даним екземпляром емульованої BGP-системи.

Завдяки масштабованості, в симуляторі можна представити дві та більше BGP-системи і емулювати між ними зв'язок через PeerEntry (рис.4.2.2) і певні політики маршрутизації.

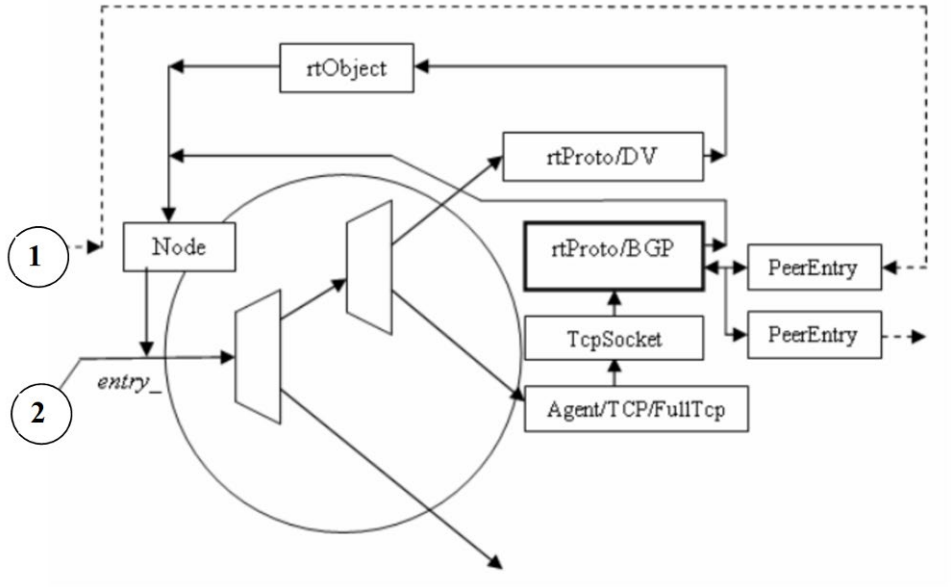


Рисунок 4.2.2 – З'єднання двох BGP-систем в емуляторі ns-2

В своїй роботі автори приводять результати тестування на схемі з 10 вузлів, та 10000 маршрутів. Для більших розмірностей були зроблені розрахунки очікуваного часу виконання.

Отже, програмна модель протоколу BGP-4 придатна для відпрацьовування взаємодії та експериментів з політиками між невеликою кількістю BGP-систем. Складно уявити взаємодію реальної кількості вузлів в емуляторі.

Модель CAIR.

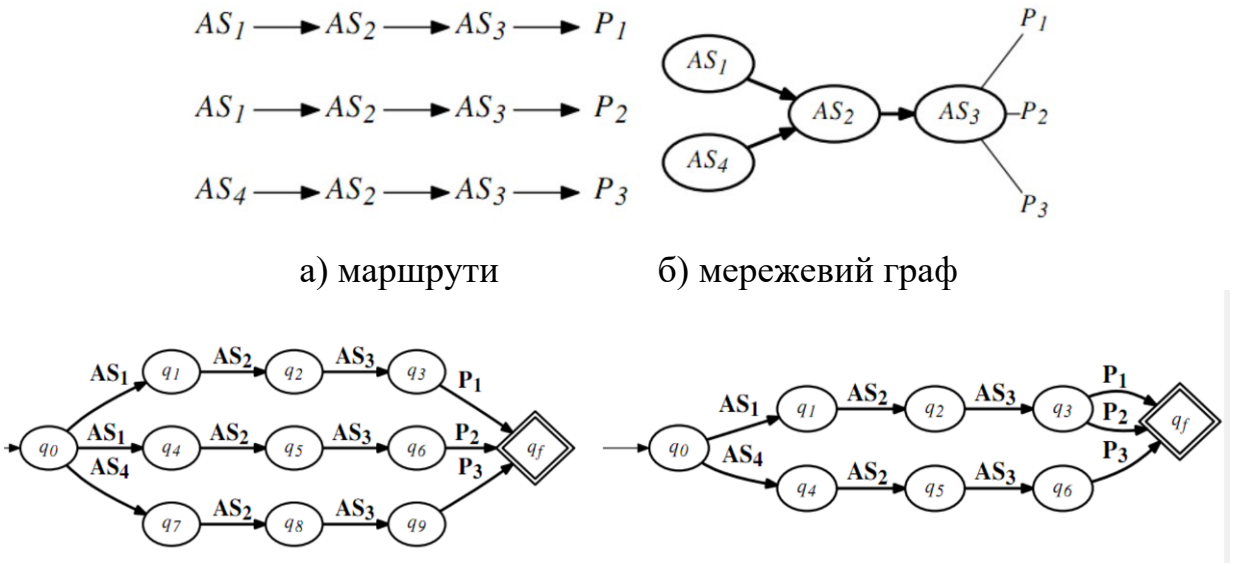
В роботі [110] зазначається, що вимірювання, моделювання та аналіз маршрутизації між автономними системами отримали більшу важливість протягом останнього десятиліття, оскільки інфраструктура Інтернету стала критичною для бізнесу, а розслідування інцидентів кібер-безпеки інтенсифікувались. Сьогодні питання про цілісність маршруту превалює в повсякденних операціях та чітке розуміння того, як дані повинні тексти дані, є критично бажаними для швидкого виявлення аномалій. Однак моделювання Інтернет маршрутизації все ще є великим викликом через складність механізмів прийняття рішень на Інтернет-магістралях. Відсутність «точок огляду» всієї системи маршрутизаціїі, складність даних роблять графовий спосіб моделювання системи маршрутизації недостатнім для відображення таких сутностей як політика маршрутизації. Автори запропонували використання методу кінцевих автоматів для побудови моделі маршрутизації (рис.4.2.3), яку вони назвали Constructible Automata for Internet Routes (CAIR).

Модель базується на такому самому формальному описі, що вже використовувався в HEAP. Крім цього, визначено поняття автомат маршруту як кортеж з 5 складових:

$$M = (Q, \sum_{AS} \bigcup \prod, \sigma, q_0, F),$$

де Q – множина маршрутів, визначена як множина кінцевих станів, q_0 – початковий вузол маршруту, визначений як початковий стан автомата, σ – якась частина маршруту, послідовність вузлів.

Всі коректні послідовності σ утворюють «правильну» мову. Автомат приймає стани, кожен з якиїх є множиною видимих з індивідуальної точки огляду маршрутів. Всі стани, які приймають таку ж правильну мову, еквівалентні і можуть бути об'єднані в єдиний стан. При ітеративному застосуванні цей процес призводить до мінімального автомату, який назвали автомат маршрутів. Цей автомат є унікальним, за винятком ізоморфізмів і вимагає мінімальної кількості станів серед усіх автоматів, які приймають однакову мову.



а) маршрути б) мережевий граф

в) детерміністичний автомат г) мінімальний автомат

Рисунок 4.2.3. Представлення розповсюдження маршрутів різними методами в моделі CAIR

Описана ідея використана при реалізації програмних засобів та публічних сервісів з виявлення атак на систему глобальної маршрутизації і покладена в основу системи ARTEMIS, яка описана в першому розділі.

Таким чином, можна зробити наступнгі висновки щодо розглянутих розглянутих формальних та функціональних моделей реалізації процесу формування та вибору маршруту в BGP-4. Розглянуті моделі без сумніву послуговують для цілей, для яких вони розроблені. Проте, вони призначені здебільшого для виявлення перехоплення маршруту за результатами

спостереження повідомлень “BGP update” на різних розгалужених точках спостереження. Моделі не задовольняють цілям підвищення захищеності за допомогою превентивного вдосконалення топології мережевого префікса, на захист якого мають бути спрямовані зусилля власника ризику.

4.3. Оцінювання ризику перехоплення маршруту

Підходи до оцінки ймовірності перехоплення

В сучасній інформаційній безпеці є чимало сучасних дослідів стосовно моделювання і оцінювання ймовірності настання негативних наслідків, зокрема, [111, 112], та дослідження ризику, пов’язані з топологією глобальної мережі, автору невідомі.

Як вже відомо з принципів організації глобальної маршрутизації, що описані в гл.2 та гл.4, основним транзитивним параметром, що характеризує привабливість маршруту, є довжина шляху (AS_PATH). Довжина шляху – це фактор, який дозволяє маршрутам до однакових префіксів конкурувати.

Якщо існує підмножина вузлів, об’єднана якоюсь сутністю, топологія цієї підмножини може розглядатись окремо. Назвемо цю підмножину цільовою групою вузлів. Такою групою можуть бути вузли – учасники будь-якої мережі обміну трафіком чи вузли-клієнти одного провайдера доступу до Інтернет. Якщо зловмисник вдало провів перехоплення маршруту чи захоплення префіксу, це означає, що для певної цільової групи вузлів маршрут до префікса жертви через вузол зловмисника став коротшим, ніж інші, природні маршрути, а отже – буде перехоплено трафік до цього префіксу від згаданої групи вузлів.

Вже згадувалось, що у сучасній практиці для формалізації ризику широко використовують моделі, які пов'язують між собою ймовірність виникнення негативних подій і можливих збитків у результаті цих подій [28, 29, 31]. Визначимо ризик перехоплення трафіку R до певного мережевого префіксу як добуток ймовірності P такого перехоплення та збитку L, пов'язаних з цим перехопленням. Збиток є в свою чергу сумою збитків від перехоплення трафіку від кожного з вузлів в цільовій групі [96], тому:

$$R = P\sum_{i}^{N} L_i$$

Якщо розподіл збитків між вузлами заздалегідь невідомий, виправданим буде вважати його однаковим для кожного вузла. Тоді збиток є пропорційним до кількості вузлів в цільовій групі. Тоді можливо оцінювати ризик як величину, пропорційну кількості вузлів N, що потрапили під вплив перехоплення:

$$R \sim NL\,.$$

Проаналізуємо, від чого залежить ймовірність перехоплення трафіку *P*. Перехоплення означає, що маршрут до префікса жертви через вузол зловмисника став коротшим, ніж істинний маршрут. З попереднього дослідження [83] відомо, що відстань між вузлами як довжина найкоротшого маршруту для мережі Інтернет – це функція:

$$d(v,u) = \min_i \left(d(v,i) + d(i,u) \right). \qquad (4.3.1)$$

З практичної точки зору це означає, що в разі перехоплення маршруту відстань (4.3.1) через фіктивний маршут стане меншою, ніж через справжній маршрут. Маніпулювати довжиною шляху тим простіше, чим цей шлях довший (в довшому шляху посередині існує більше вузлів, через які можна анонсувати фіктивний маршрут). Отже, ймовірність перехоплення $P(v,u)$ між вузлами *v,u* збільшується для далеких вузлів та зменшується для близьких:

$$P(v,u) \sim d(v,u).$$

Отже, ризик пов'язаний з кількістю вузлів, що можуть потрапити під вплив перехоплення і з відстанню до кожного з цих вузлів.

В роботі [83] представлено дослідження Інтернету з точки зору теорії складних мереж та було показано зв'язок між середнім шляхом мережі, її ефективністю та вразливістю. Для кожного конкретного вузла *v* за відомими відстанями $d(v,i)$ можна визначити суму відстаней :

$$D_v = \sum_{i=1}^{|V|} d(v,i) \qquad (4.3.2)$$

З урахуванням (4.3.2) можна отримати залежність ризику перехоплення маршрутів до вузла *v* від його положення відносно інших вузлів:

$$R_v \sim \sum_{i=1}^{|V|} d(v,i). \qquad (4.3.3)$$

де R_v – ризик перехоплення маршруту до вузла *v*.

Підходи до оцінки збитку від перехоплення

Розглянемо другий аспект ризику – розмір збитку (losses). Розмір збитку, як і ймовірність шкоди, є багатофакторної компонентою. 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 (далі – 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 L буде сумою збитків по конкретних вузлах $as_b \in \overline{AS}_b$, де переміг хибний маршрут:

$$L = \sum_i^{\left|\overline{AS}_b\right|} L_i$$

при цьому

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

Це дає змогу порівнювати потенційний збиток при моделюванні різних топологій:

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

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

4.4. Зв’язок між ризиком перехоплення маршруту та відомими метричними характеристиками складних мереж

Ступінь вузла та розподіл ступеня

Дослідженням топологічних властивостей складних мереж та, зокрема, Інтернета, приділено увагу в працях Р. Альберта та А.-Л. Барабаші, С. Строгаца та Д. Уоттса, М. Фалутсоса та П. Фалутсоса, М. Ньюмана, П. Болді, І. Євіна, О. Олємського, Д. Ланде, А. Снарського, Ш. Джина, Д. Алдерсона та інших вчених.

Відстань між вузлами, кількість транзитних маршрутів, кількість власних префіксів і ще деякі фактори впливають також і на умовну «зону ураження» – ареал розповсюдження хибного маршруту. Отже, відношення між вузлами повинні мати певні метричні характеристики [113], що характеризували б ризик перехоплення маршруту між ними як принаймні одну з двох складових ризику – ймовірності перехоплення або розміру збитків.

Проведемо дослідження відомих метричних характеристик складних мереж та вузлів, які використовуються в різних предметних областях для вивчення та моделювання поведінки мережі.

Ступенем вузла в теорії графів є кількість його вхідних та (або) вихідних ребер, в залежності від мети підрахунку.

Розподіл ступіню вузлів *P(k)* є одною з найважливіших характеристик складних мереж. Він визначається як ймовірність того, що випадково обраний вузол *i* з *N* вузлів має ступінь *k:*

$$P(k) = \frac{\langle N(k) \rangle}{N}$$

Для орієнтованих мереж окремо розраховується вхідний та вихідний ступінь вузла. Розподіл ступеня в мережі впливає на співвідношення діаметру мережі та середнього коротшого шляху, а також на живучість мережі. Мережі з різними $P(k)$ демонструють різну поведінку [37]. Однак показник розподілу ступеня не відображає ролі чи групи вузлів вузла в поширенні маршрутів та побудові коротших шляхів.

Середній коротший шлях

Шляхом між вузлами називається найкоротша відстань між ними. В зарубіжній літературі зустрічається визначення „геодезічний шлях" (geodesic path) [37, 38]. Для кожного вузла *i* можна визначити середній коротший шлях l_i між ним та всіма іншими вузлами мережі:

$$l_i = \frac{1}{N} \sum_{j}^{N} d_{ij} \,. \qquad (4.4.1)$$

Для всієї мережі теж можна визначити поняття середнього коротшого шляху l, як математичне очікування середнього коротшого шляху по всіх вузлах:

$$l = \frac{1}{N^2} \sum_{i}^{N} \sum_{j}^{N} d_{ij} \qquad (4.4.2)$$

де d_{ij} – метрична відстань між вузлами i та j.

В 4.3 показаний зв'язок ймовірності перехоплення на певному вузлі із відстанню між ним та «жертвою» – джерелом префікса, топологію якого необхідно оцінити та захищати. Якщо в джерела середня відстань (4.4.1) менша, ніж середня відстань по всій мережі (4.4.2), топологія мережевих префіксів, що походять з джерела, менше вразлива до перехоплення. Але така оцінка аж надто загальна. Оскільки кожен мережевий префікс має власну топологію, і з кожного вузла є видимою лише її частина, неможливо отримати оцінку середнього шляху по всій мережі за (4.4.2).

Посередництво

Однією з важливих характеристик вузлів є *посередництво* (betweenness, або betweenness centrality) [114]. Посередництво $\sigma(m)$ відображає роль вузла в

установленні зв'язків у мережі й показує, скільки найкоротших шляхів проходить через цей вузол:

$$\sigma(m) = \sum_{i \neq j} \frac{B(i,m,j)}{B(i,j)},$$

де $B(i,j)$ – загальна кількість найкоротших шляхів між вузлами i та j, а $B(i,m,j)$ кількість найкоротших шляхів між i та j, таких, що проходять через вузол m.

Інколи цю характеристику називають «навантаження» (load). Трактування центральності як ступеня навантаження має сенс в комп'ютерних та логістичних мережах.

Центральність може певним чином характеризвуати залученість вузла в «постачанні» кращих маршрутів. Оскільки кожний мережевий префікс має свою власну топологію, центральність має оцінюватись з однієї точки спостереження – від джерела маршруту. Тоді центральність вузла за оцінкою з точки зору джерела маршруту характеризує вплив вузла на розповсюдження маршрутів. Отримати цю оцінку можна з BGP-таблиці Adj-RIB-In, порахувавши відношення кількості маршрутів, в яких присутній ідентифікатор оцінюваної AS до загальної кількості маршрутів. Але ця характеристика не буде повною: як було показано в 4.3, ймовірність перехоплення на певному вузлі зростає з відстанню між ним та «жертвою». З цього виходить що вплив вузла на поширення маршрутів навпаки знижується з відстанню. А ця відстань не враховується в характеристиці «центральність».

Кластеризація

Кластеризація (коефіцієнт кластерності) показує, скільки найближчих сусідів заданого вузла є також найближчими сусідами один для одного [100]. Він характеризує тенденцію до утворення груп взаємопов'язаних вузлів – так званих клік (clique). Для окремого вузла мережі, який має ступінь k, тобто з якого виходить k ребер, що з'єднують його з k іншими вузлами (так званими найближчими сусідами), коефіцієнт кластерності визначається як відношення реальної кількості ребер E_m, якими з'єднані найближчі сусіди вузла, до максимально можливого, яке дорівнює, як відомо, $\frac{k(k-1)}{2}$:

$$C_i = \frac{2e_i}{k_i(k_i - 1)}$$

Рівень кластерності для всієї мережі визначається як арифметичне середнє значення коефіцієнтів кластерності по всіх вузлах мережі та вказує на ймовірність існування зв'язку між двома випадково взятими найближчими сусідами вузла, а також містить інформацію про наявність у мережі «трикутників» (циклів довжиною три).

Узагальнення аналізу відомих характеристик

Таким чином показано, що розглянуті *відомі характеристики* вузлів складних мереж *не можуть бути використані* для оцінки ризику перехоплення маршруту, оскільки не характеризують *складові цього ризику*. Дійдено висновку про необхідність розробки власних метричних характеристик для вираження відношень між вузлами Інтернет, що характеризували б ризик перехоплення маршруту між ними.

Так виникла задача знаходження інших характеристик, що зможуть характеризувати складові ризику перехоплення маршурту.

4.5. Метрична характеристика значущості

Для власника ризику важливість вибору істинного маршруту на вузлі *v* пов'язана з кількістю вихідних зв'язків вузла *v* та кількістю його власних префіксів, для яких він є джерелом маршруту. Це тому, що ці фактори прямо впливають на збиток. Масштаб збитку в разі появи на вузлі *v* хибного маршруту залежить від кількості підмереж, що маршрутизуються через цей вузол, бо їхній трафік, адресований перехопленим префіксам, буде уражено:

$$L_u = \sum_i^{|V|} L_i \quad ; \quad L_u \sim |p_v| \qquad (4.5.1)$$

Для оцінки масштабу збитку запропоновано метричну характеристику значущості S_v^u, що має характеризувати вузол *v* відповідно до кількості підмереж, які отримують маршрути за посередництва вузла *v*. Оскільки немає практичних засобів отримання даних від кожної підмережі Інтернету для з'ясування, чи не надходять до неї маршрути за посередництва певної AS, пропонується спрощена метрика значущості, а саме за підрахунком анонсованих цією AS мережевих префіксів, як власних, так і транзитних, які можна спостерігати в таблицях глобальної маршрутизації. Відомо, що мережеві префікси мають різну довжину і 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 тощо. Отже, префікси нерівнозначні і мають різну вагу. Для визначення значущості застосовано визначення ваги префіксу

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

де *w* – вага префіксу *p*, *l* – довжина префіксу *p*.

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 адресами, матиме таку саму метрику значущості, як AS, яка анонсує один префікс з 8192 адресами. Приклад розрахунку ваги для

мережевих префіксів в залежності від довжини мережевої маски, які найбільш часто зустрічаються в BGP-таблицях, наведено в табл. 4.5.1.

Крім того, слід зазначити, що цільовий вузол *v* має певний ступінь впливу на інші вузли мережі: маршрути, отримані від вузла-провайдера, ймовірніше будуть кращими, бо до провайдера відстань найменша.

Таблиця 4.5.1 – Таблиця розрахунку ваги префікса в залежності від довжини мережевої маски

Довжина маски, біт	**Десятична нотація**	**Вага префіксу**
24	255.255.255.0	1
23	255.255.254.0	2
22	255.255.252.0	4
21	255.255.248.0	8
20	255.255.240.0	16
19	255.255.224.0	32
18	255.255.192.0	64
17	255.255.128.0	128
16	255.255.0.0	256
15	255.254.0.0	512
14	255.252.0.0	1024
13	255.248.0.0	2048
12	255.240.0.0	4096
11	255.224.0.0	8192
10	255.192.0.0	16384
9	255.128.0.0	32768
8	255.0.0.0	65535

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 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 з *v* вузол, то $(1+\delta)^{-1}$=0,5. Тоді метрика значущості набуде такого вигляду:

$$S_u^v = \sum_p w_p (1+\delta_p)^{-1},,$$

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

Або у повному вигляді:

$$S_u^v = \sum_p 2^{24-l(p)} (1+\delta_p)^{-1} \qquad (4.5.2)$$

4.6. Метрична характеристика довіри

Друга складова ризику – це оцінка ймовірності, що на довільно обраному вузлі *v* «переможе» хибний маршрут до префікса, який належить вузлу *u*. Ця ймовірність зростає разом з відстанню між вузлами. Важливо зазначити, що у власника ризику нема можливості передбачити, де буде розташовано джерело атаки і який саме хибний маршрут воно запропонує. З цієї та низки інших причин власник ризику не може достовірно передбачити результат вибору маршруту в довільному вузлі *v*.

Оцінка однією стороною суб'єктивної ймовірності виконання певної дії на іншій стороні, в якій зацікавлена перша, але не може її передбачити, є одним з визначень поняття довіри [115, 116]. Оцінювання довіри, ступень довіри пов'язують з поняттям «ймовірність» [117]. Тому термін «довіра» тут і надалі буде запропоновано використання саме поняття довіри для оцінки ймовірності перехоплення маршруту.

При використанні поняття довіри необхідно визначити суб'єкта довіри, об'єкт довіри та предмет довіри.

Суб'єктом довіри в питанні визначення ймовірності перехоплення маршруту є власник ризику. Нагадаємо, що власник ризику – це особа чи група осіб, які несуть відповідальність за інформаційну безпеку інформаційного активу, який ідентифікується в мережі Інтернет за допомогою мережевого префіксу, в якого, в свою чергу, є вузол-джерело маршруту. Таким чином, це вузол *u* стає суб'єктом довіри.

Об'єктом довіри є оцінюваний вузол *v*, відносно якого робиться оцінка ймовірності перехоплення маршруту саме на ньому.

Предмет довіри – це подія, ймовірність якої оцінюється. Предметом довіри є прийняття у вузлі *v* хибного маршруту до префіксу, що належить суб'єктові довіри – вузлу *u*.

Визначимо метричну характеристику довіри *T* (від «trust») як порівняння, чи відношення відстані між суб'єктом та об'єктом довіри, порівняно з середньою відстанню між суб'єктом довіри та всіма іншими вузлами:

$$P_u^v \sim d(u,v) \quad => \quad T_u^v \sim \frac{d(u,v)}{\langle D_u \rangle},$$

$$\langle D_u \rangle = \frac{\sum_i^{|V-1|} d(u,i)}{|V-1|}, \quad i \neq u \ ;$$

$$T_u^v = \frac{d(u,v)\left(|V|-1\right)}{\sum_{i}^{|V-1|} d(u,i)} \ , \ i \neq u \quad , \qquad (4.5.1)$$

де T_u^v – показник довіри вузла *v* за оцінкою *u*; *u* – суб'єкт довіри, *v* – об'єкт довіри; *i,u,v* – автономні системи; *V* – множина всіх AS мережі Інтернет, $d(v,u)$ – метрична функція відстані між інтернет-вузлами *v,u*; $\langle D_u \rangle$ – середня відстань від суб'єкта довіри до інших вузлів.

4.7. Ризик-орієнтована модель безпеки топологічного простору Інтернету

В підрозділах 4.4 та 4.5 було сформовано такі метричні характеристики мережевих вузлів, які відображають складові ризику перехоплення маршруту. З цих метричних характеристик можна утворити ризик-орієнтовану модель топології мережевого префікса, яка основана на розподілі вузлів в просторі (R,T,S), де *R* – ризик, *T* – довіра, *S* – значущість:

$$R_u^v = T_u^v S_u^v . \qquad (4.7.1)$$

Ризик виражений через *довіру (*як оцінку ймовірності) та *значущість* (як оцінку потенційних збитків). При цьому сукупний ризик від перехоплення маршрутів по всіх цільових вузлах має вигляд

$$R_u = \sum_{i \neq u}^{|V|-1} R_i . \qquad (4.7.2)$$

Такий метод оцінювання захищеності топології через оцінювання ризику спрямований на розвиток теоретичних засад вдосконалення топології міжмережевих зв'язків в Інтернеті для поводження з ризиками кіберінцидентів глобальної маршрутизації.

Теоретичні межі метрики значущості лежать між маленькими значеннями (коли оцінюваний вузол анонсує один префікс, який він отримав через ланцюжок всіх вузлів Інтернету) та максимальною кількістю всіх префіксів (коли один вузол є джерелом для префіксів всього інтернету):

$$\frac{1}{|V|-1} \leq S_u^v < 2^{24} .$$

Але в реальності більшість автономних систем анонсують лише один префікс, і лише деякі інтернет провайдери, оператори зв'язку, мережі обміну трафіком матимуть високі показники значущості, що сягають тисяч.

Метрична характеристика довіри теоретично досягає крайніх значень коли мережа являє собою ланцюг з усіх вузлів, і власник ризику є крайнім в ланцюгу, та оцінює метрики довіри найближчого і найдальшого вузла:

$$\frac{2}{|V|-1} < T_u^v \le \frac{(|V|-1)}{2}.$$

А в реальному Інтернеті, за даними багатьох досліджень, максимальна відстань між вузлами (діаметр мережі) не перевищує 10, а середня відстань – біля 4 . Тому реальні значення метрики довіри:

$$0{,}25 < T_u^v \le 2{,}2 .$$

Щоб вирівняти вагу обох метрик при оцінюванні ризику, в моделі було вирішено метрику довіри враховувати як експоненту:

$$R_u^v = S_u^v \cdot 10^{T_u^v} \qquad (4.7.3)$$

Модель (4.7.3) базується на метричних характеристиках, що походять з топологічних характеристик вузлів Інтернет – автономних систем, та характеризують безпосередні складові ризику перехоплення маршруту – ймовірність настання збитку та потенційний розмір збитку. Така модель є адекватною для відображення характеристик вузлів з точки зору оцінювання ризику і дає можливість порівняння топологій за рівнем захищеності.

4.8. Аналіз поверхні атаки за допомогою дослідження топологічного простору мережевого префікса

4.8.1. Вектор атаки та площина атаки

В біології багато років вживається термін «вектор хвороби» (decease vector), який означає живий організм, здатний переносити збудника хвороби (наприклад, у вигляді вірусів)[1]. За аналогією, в комп'ютерній безпеці з'явився термін «вектор інфікування» (відносно класичних та мережевих комп'ютерних вірусів), а згодом його витіснив термін «вектор атаки», який широко вживається в кібербезпеці.

Отже, *вектор атаки* — це метод, який використовується зловмисником, щоб скористатися вразливістю, яка існує в системі. Поширені вектори атак – крадіжка конфіденційних облікових даних, розширення доступу до захищених ресурсів за допомогою ескалації привілеїв, неправильні конфігурації мережі,

[1] Last, James, ed. (2001). A Dictionary of Epidemiology. New York: Oxford University Press. p. 185. ISBN 978-0-19-514169-6.

які призводять до небажаного доступу до чи з Інтернету, вади криптографічних алгоритмів тощо.

Існує і набагато ширший термін, що характеризує сукупність методів експлуатації вразливостей, притаманних певній IT-системі. Він має назву «поверхня атаки».

Поверхня атаки — це умовне поняття, яким охоплюють всі потенційні вразливості, що існують в певному середовищі. Кожен вектор атаки (наприклад, шкідливе посилання в електронному листі, що призводить зловмисника до ескалації привілеїв, або невірно сконфігуровані атрибути доступу до файлу) може дозволити зловмиснику отримати несанкціонований доступ. Натомість сукупність векторів атаки складає поверхню атаки, чи, радше, поверхню, яка може бути атакована.

Відносно поверхні атаки застосовують поняття збільшення та зменшення. Такі дії, як відкриття доступу до мережевого застосунку або запровадження віддаленого доступу до чуттєвої інформації збільшують поверхню атаки, а обмеження функцій, встановлення додаткових засобів захисту – навпаки, зменшують.

Виходячи з такої практики застосувань поняття вектора та поверхні атаки, можна зробити висновок, що вектор атаки подібний не до вектора в евклідовому просторі, який характеризується довжиною (магнітудою) та направленістю, а, скоріше, матричний вектор, який описує координату певної точки в просторі. В кіберпросторі ця точка символізує конкретну вразливість системи. Природно, що сукупність точок складає якусь фігуру, яку умовно називають поверхнею атаки.

4.8.2. Зв’язок між топологічним простором мережевого префікса і поверхнею атаки

Якщо метою проведення атаки на мережевий префікс є перехоплення маршруту, в разі перехоплення префікса на певному вузлі стає вірогідним розповсюдження хибного маршруту по сусідніх вузлах, від них – до їх сусідів і так далі (як описано в розділі 1.2). Чи буде певний вузол уражений хибним маршрутом – залежить від багатьох факторів, які складаються в метрики, запропоновані в цій главі вище.

Уявімо, що кожен вузол представляє собою окремий вектор атаки. Тоді цей вектор може характеризуватись двома метричними характеристиками, запропонованими вище в цьому розділі – метрикою довіри та метрикою значущості. Разом із унікальним ідентифікатором вузла вони можуть бути використані як три координати унікальної точки. Можливо уявити, що сукупність цих точок і є поверхнею атаки на мережевий префікс.

ГЛАВА 5.
ПІДВИЩЕННЯ КІБЕРЗАХИЩЕНОСТІ ТОПОЛОГІЇ ІНТЕРНЕТУ

5.1. Формулювання вимог до вхідних даних для ризик-орієнтованої моделі топології Інтернету

В розділі 4 сформульовано двовимірну модель системи глобальної маршрутизації в Інтернеті, в основі якої лежить розподіл вузлів мережі Інтернет за зростанням ризику, де ризик виражений через метрику довіри як оцінку ймовірності, та метрику значущості 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.

Двовимірна модель розподілу вузлів має бути забезпечена даними, які дозволять виконати розрахунок метрики довіри та метрики значущості кожного оцінюваного вузла. Для цього необхідно виконати такі попередні кроки підготовки вхідних даних:

- 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.

Незалежно від формату представлення таблиць Adj-RIB-In, якими оперує BGP-система вузла u, вона міститиме наступні дані стосовно кожного маршруту:

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

Атрибут as_path в кожному маршруті має вигляд послідовності ідентифікаторів AS зліва направо від найближчого сусіда власника ризику до кінцевого вузла – джерела префіксу. Відстань d у метриці довіри буде обраховуватись по as_path зліва направо, а відстань δ для для метрики значущості – справа наліво.

5.2. Вхідні дані ризик-орієнтованої моделі кіберзахищеності топології Інтернету

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 [114]. Сама по собі інформація про маршрути в глобальній

комп‘ютерній мережі є відкритою інформацією, що визначається метою її існування та застосування [115]. 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 (рис.5.2.1). Такий запис містить наступні дані:

- версія BGP-таблиці – її унікальний "серійний номер", зміна якого однозначно дозволяє відстежувати наявність змін в BGP-таблиці. Значення «BGP Version» постійно інкрементується, коли в таблицю вносяться зміни – додаються чи вилучаються маршрути;
- всі 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
```

Рисунок 5.2.1 – Дані BGP, отримані 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.5.2.2):

- 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.

```
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
```

Рисунок 5.2.2 – Приклад даних BGP Summary

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. 5.2.3 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»).

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

Рисунок 5.2.3 – Дані про маршрути, отримані від певного учасника мережі обміну трафіком

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

5.3. Методика оцінювання ризику перехоплення маршруту

5.3.1. Загальний опис процесу оцінювання ризику перехоплення маршруту

В цьому підрозділі представлено методику як послідовність операцій, яка підлягає подальшій автоматизації шляхом створення відповідних програмних засобів. Така послідовність у вигляді функціональних блоків та зв'язків наведена на рис. 5.3.1. На цьому рисунку використані такі позначення:

БОТГМ – блок обробки таблиць глобальної маршрутизації у складі модуля збору вхідних даних (МЗТГМ), модуля виділення префіксів (МВП) та модуля виділення унікальних шляхів (МВШ);

БРМЗ – блок визначення метричної характеристики значущості у складі модуля обробки шляхів (МОШ) та модуля розрахунку метрики значущості (МРМЗ);

БРМД – блок визначення метрики довіри у складі модуля розрахунку середнього коротшого шляху в мережі (МРСШ), модуля розрахунку коротшого шляху до цільового вузла (МРКШ), модуля обчислення метрики довіри (МРМД);

БВВ – блок впорядкування вузлів у складі модуля розрахунку ризику (МРР) та модуля сортування (МС);

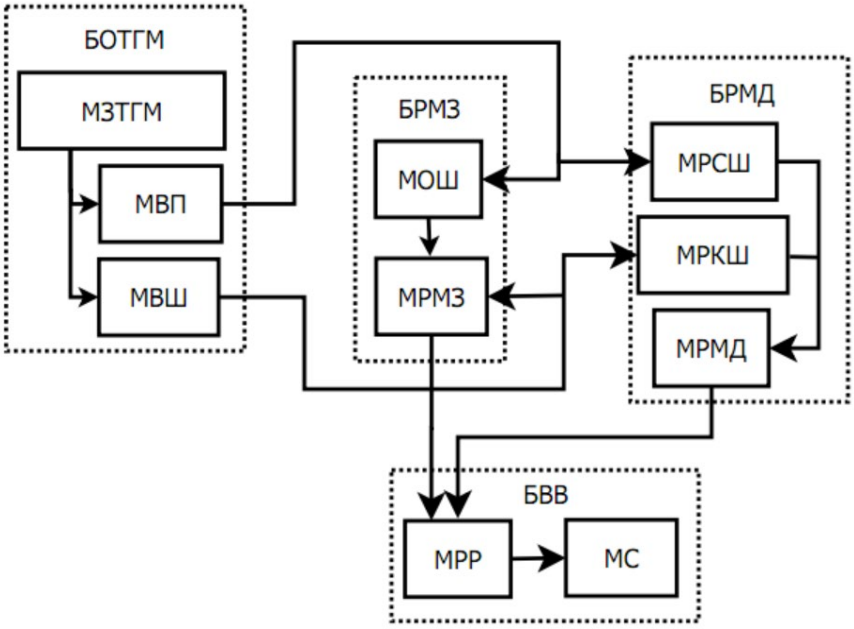


Рисунок 5.3.1 – Функціонально-логічна схема методики визначення ризику перехоплення маршруту на вузлах мережі Інтернет

5.3.2. Процедури обробки таблиць маршрутизації протоколу BGP-4

Існує декілька найчастіше вживаних форматів відображення баз маршрутів BGP, в залежності від програмного та програмно-апаратного забезпечення, яке реалізує функції BGP-системи та маршрутизацію. Найчастіше вживаними є формати:

- формат Cisco Internetwork Operating System (Cisco IOS) обладнання Cisco Systems [122];
- BIRD Internet Routing Daemon [123] – вільно розповсюджуване серверне програмне забезпечення для динамічної маршрутизації, призначене для FreeBSD, Linux та інших UNIX-подібних операційних систем;
- формат Junos OS обладнання компанії Juniper;
- формат Quagga Routin Software Suite – вільно розповсюджуване серверне програмне забезпечення для динамічної маршрутизації, призначене для FreeBSD, Linux та інших UNIX-подібних операційних систем;

На рис. 5.3.1 зображено типовий формат Cisco IOS. Таки вивід отримується за допомогою команди «show ip bgp». Команда використовується для відображення вмісту таблиці маршрутизації BGP. Вихід може бути відфільтрований, щоб відобразити записи для конкретного префікса, довжину префікса, списки префіксів, фільтри аноснів, тощо.

```
   Prefix              Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0           149.14.93.161                           174 I
* 1.0.0.0/24          149.14.93.161        2020               174 13335 I
* 1.0.4.0/22          149.14.93.161        1010               174 3356 4826 38803 I
* 1.0.4.0/24          149.14.93.161        1010               174 3356 4826 38803 I
* 1.0.5.0/24          149.14.93.161        1010               174 3356 4826 38803 I
* 1.0.6.0/24          149.14.93.161        1010               174 3356 4826 38803 I
* 1.0.7.0/24          149.14.93.161        1010               174 3356 4826 38803 I
* 1.0.16.0/24         149.14.93.161        244050             174 2519 I
* 1.0.64.0/18         149.14.93.161        142110             174 2516 7670 18144 I
* 1.0.128.0/17        149.14.93.161        146120             174 38040 23969 I
* 1.0.128.0/18        149.14.93.161        146120             174 38040 23969 I
* 1.0.128.0/19        149.14.93.161        146120             174 38040 23969 I
* 1.0.128.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.129.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.132.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.133.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.134.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.135.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.136.0/24        149.14.93.161        146120             174 38040 23969 ?
* 1.0.137.0/24        149.14.93.161        146120             174 38040 23969 ?
```

Рисунок 5.3.1 – Фрагмент вхідної таблиці маршрутів в форматі Cisco IOS

На рис. 5.3.2 наведено приклад відображення маршрутів сервером BIRD.

```
BIRD 1.5.0 ready.
168.0.168.0/24    via 77.88.200.102 on eth2.705 [datagroup 2020-09-30 04:13:38] * (100) [AS265257i]
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 3326 1299 267613 262462 265257
        BGP.next_hop: 77.88.200.102
        BGP.med: 469
        BGP.local_pref: 70
        BGP.community: (3326,3030) (3326,11001) (3326,25101)
154.0.154.0/24    via 77.88.200.102 on eth2.705 [datagroup 2020-09-28 21:01:42] (100) [AS36909i]
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 3326 37662 36930 36909
        BGP.next_hop: 77.88.200.102
        BGP.med: 1549
        BGP.local_pref: 70
        BGP.community: (3326,3101) (3326,11003) (3326,24216)
184.0.184.0/21    via 77.88.200.102 on eth2.705 [datagroup 2020-09-30 04:14:40] (100) [AS209i]
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 3326 1299 3356 2[illegible]
        BGP.next_hop: 77.88.200.102
        BGP.med: 469
        BGP.local_pref: 70
        BGP.aggregator: 205.171.203.234 AS209
```

Рисунок 5.3.2 – Фрагмент таблиці префіксів у форматі сервера маршрутизації BIRD

В кожному маршруті є елемент, що демонструє зв‘язки автономних систем. Це – атрибут AS_PATH, що характеризує довжину шляху до автономної системи, яка анонсувала префікс. Як вже згадувалось, довжина шляху вимірюється в кількості транзитних переходів від початкової AS до тієї, в якій працює BGP-система, з якої отримано базу маршрутів. Номер початкової AS, що анонсувала префікс, є окремим атрибутом шляху та має назву ORIGIN.

Як в форматі Cisco, так і в форматі BIRD атрибут AS_PATH відображається як перелік номерів автономних систем у зворотному напрямку, тобто від поточної до джерела маршруту. Оскільки AS_PATH – це шлях, то проаналізувавши AS_PATH всіх префіксів, наявних в таблиці маршрутів, можна побачити наявні зв‘язки між AS, по яких проходить обмін анонсами префіксів, майже в реальному часі. Таким чином, кожна пара сусідніх номерів ASx та ASy в AS_PATH являє собою безпосередній зв‘язок між ASx та ASy.

Для подальшої обробки в програмному блоці БРЗМ вхідні дані в будь-якому з перелічених початкових форматів мають бути оброблені в БОТГМ і представлені у вигляді «Префікс – Шлях», як наведено в табл.5.3.1.

Таблиця 5.3.1 – Приклад вхідних даних після обробки в БОТГМ

Префікс	Шлях
216.6.192.0/21	6939 3367 29907
193.7.221.0/24	6663 12975 57704 199046
46.8.14.0/23	35048
46.8.14.0/24	35048
204.9.232.0/22	6939 16904 4497
96.9.68.0/24	6939 59318 57704 131207
76.10.100.0/23	6939 26794 14090
185.10.145.0/24	6939 8902 57704 199629
217.11.245.0/24	6939 15685
103.11.75.0/24	6939 18351 57704 24532 55660
203.12.251.0/24	6939 4826
212.13.224.0/19	6939 9119
203.14.243.0/24	6939 4826 9822
72.14.112.0/22	6939 23260

Для цього розроблено парсер на мові програмування Perl. Наведемо фрагмент програмного коду на мові Perl із поясненнями у вигляді коментарів в програмному коді (в рядках, що починаються із знака «#»):

5.3.3. Розрахунок метрики значущості

Представимо загальний порядок реалізації функцій блоку розрахунку метрики значущості (БРМЗ) для вузла v:

отримується перелік мережевих префіксів 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 за формулою (4.5.2).

Нижче наведено фрагмент програмного коду на мові Perl [124 – 129] із поясненнями у вигляді коментарів в програмному коді (в рядках, що починаються із знака «#»):

```
# зчитування вхідних даних з файлу input_paths.txt,
# де вони зберігаються у форматі згідно рис.5.3.1;
# p – префікс, @path – масив-список AS_PATH, що зберігається
# в елементі геш-масиву hash, ключем якого стає префікс.
open PATHS, "./input_paths.txt";
while (<PATHS>) {
        ($p,@path)=split;
        $hash{$p}="@path";
}
close PATHS;

# ініціалізація елементу геш-масиву s{v}
# де зберігатиметься метрика значущості вузла v:
$s{$v}=0;

# Основний цикл розрахунку значущості.
 # Почерговий перебір ключів масиву hash, тобто перебір всіх префіксів
foreach $p (keys %hash) {
        # чи є вузол v в AS_PATH?
        if ($hash{$p}=~m/^$v\ / or $hash{$p}=~m/\ $v\ / or $hash{$p}=~m/\ $v$/ or $hash{$p}=~m/^$v$/) {
        @path=split(/ /,$hash{$p});

        # Пошук вузла v в усіх маршрутах до префіксів p.
        # Якщо v має відношення до p, визначається
        # довжина префікса, довжина AS_PATH, позиція v в AS_PATH:
        for ($j=0; $j<=$#path; $j++) {
                if ($v != $path[$j]) {      next;  }
                $p_len=$p;
                $p_len=~s/^.*\///;
                $p_wei=2**(24-$p_len);        #print  $p,  "       ",  $p_len,  " $p_wei\n";
               $d = $#path-$j;
                # результат додається до метрики значущості
                $s{$v}=$s{$v}+$p_wei/(1+$d);
         }
```

```
35.         }
36.     }
37.   # По закінченні всіх циклів виводиться значення s{v}:
38.     print "AS$v significance: $s{$v}\n";
```

Продемонструємо на практиці ранжування AS за метрикою значущості. Для прикладу уявімо, що власник ризику зацікавлений в поліпшенні топології з метою зниження ризику від перехоплення маршрутів саме в українському сегменті мережі Інтернет. В якості джерела даних візьмемо інформацію з сервера маршрутів міжнародного телеком-оператора Hurricane Electrics LLC (AS6939), що підключений до багатьох мереж обміну трафіком [130]. В результаті отримано інформацію про 89 автономних систем, з якими оператор взаємодіє в саме м. Києві, та мережеві префікси, анонси яких він отримує від кожної AS, з якою взаємодіє. Результати ранжування наведені на рис.5.3.1. Метрика значущості *S* представлена по логаріфмічній осі ординат. Окремо в табл.5.3.2 представлень дані про 40 AS з найвищою кількістю анонсів.

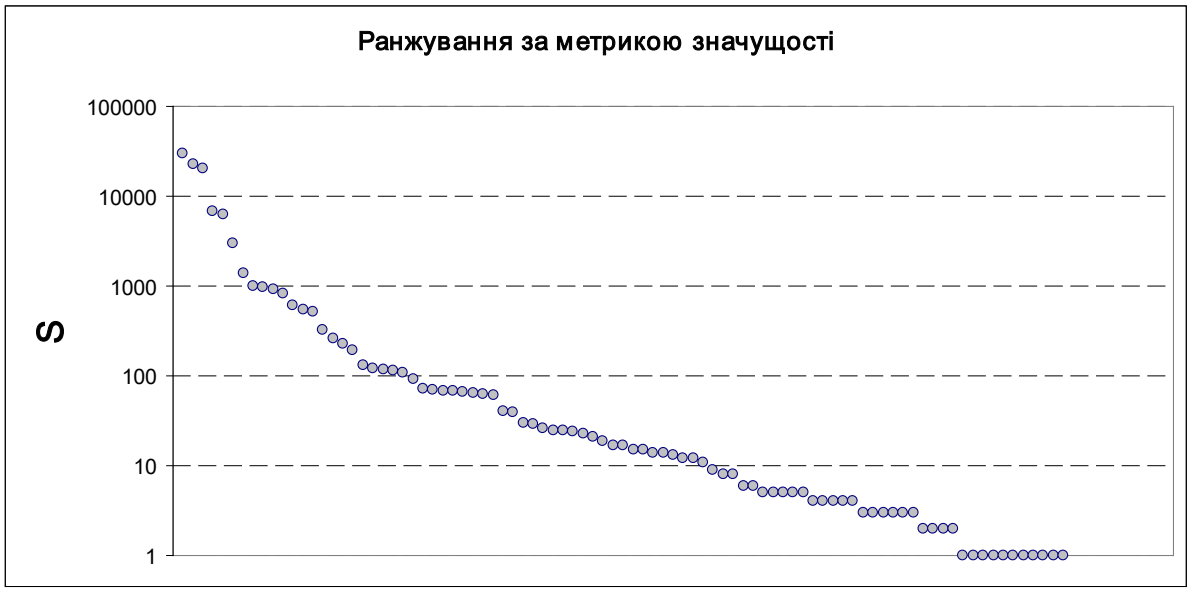


Рисунок 5.3.1 – Результат ранжування 89 AS українського сегменту Інтернет. Вісь абсцис – порядковий номер AS, вісь ординат – значення метрики значущості *S* в логарифмічному масштабі

Таблиця 5.3.2 – Ранжування «Top-40» автономних систем за кількістю анонсів.

№	Ідентифікатор AS	*S*	№	Ідентифікатор AS	*S*
1.	AS31210	29995	21.	AS29632	117
2.	AS15645	22966	22.	AS25133	114
3.	AS59613	20313	23.	AS48648	108
4.	AS29076	6892	24.	AS29107	92
5.	AS41095	6320	25.	AS60159	71

№	Ідентифікатор AS	*S*	№	Ідентифікатор AS	*S*
6.	AS43727	2956	26.	AS21500	70
7.	AS3255	1384	27.	AS34867	69
8.	AS1820	1000	28.	AS35362	69
9.	AS13249	978	29.	AS48422	66
10.	AS35297	929	30.	AS30886	64
11.	AS15169	825	31.	AS12687	62
12.	AS31148	616	32.	AS6886	61
13.	AS3303	545	33.	AS12593	41
14.	AS13335	518	34.	AS41820	39
15.	AS50581	322	35.	AS6876	30
16.	AS199995	260	36.	AS35213	29
17.	AS49544	229	37.	AS24700	26
18.	AS13188	192	38.	AS48438	25
19.	AS15895	133	39.	AS48919	25
20.	AS16276	122	40.	AS51500	24

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 та середньодобовий трафік якої складає 1.12 Тбіт/с. Зауважимо, що призначення мереж обміну трафіком та їхнє місце в функціонуванні та формуванні топології Інтернет були досліджені в [131] та [132].

З четвертого місця списку починаються AS великих українських телеком-операторів, що за вказаними характеристиками поступаються мережам обміну трафіком. Це свідчить про те, що дані, отримані з серверу маршрутів, і результат ранжування AS за метрикою значущості є адекватними.

5.3.4. Розрахунок метрики довіри

Для розрахунку метричної характеристики довіри необхідно визначити середню коротшу відстань між суб'єктом довіри u та всіма об'єктами довіри за формулою:

$$\left\langle D_u \right\rangle = \frac{\sum_{i}^{|V-1|} d(u,i)}{|V-1|}, \quad i \neq u \ , \qquad (5.3.1)$$

де u – суб'єкт довіри, v – об'єкт довіри; i,u,v – автономні системи; V – множина всіх AS мережі Інтернет, $d(v,u)$ – метрична функція відстані між інтернет-вузлами v,u; $\langle D_u \rangle$ – середня відстань від суб'єкта довіри до інших вузлів.

Представимо загальний порядок реалізації функцій блоку розрахунку метрики значущості (БРМД) для вузла v:

з повного списку атрибутів AS_PATH розраховується коротший шлях від u до інших видимих AS, та розраховується середній коротший шлях за формулою (5.3.1);

для кожного вузла – об'єкта довіри v зі списку AS, шукається найкоротша відстань між u та v з повного списку атрибутів AS_PATH;

розраховується метрика довіри u до v відповідно до формули (4.5.1).

Нижче наведено фрагмент програмного коду на мові Perl, в якому використовується пошук коротшого шляху між парою вузлів, із поясненнями у вигляді коментарів в програмному коді (в рядках, що починаються із знака «#»):

```
1.    open PATHS, "./pref_aspaths.txt";
2.
3.    #
4.    # build hash array of prefixes and ther as_path
5.    #
6.
7.    while (<PATHS>) {
8.         ($p,@path)=split;
9.
10.        # put each path into a key of hash
11.        $hash{$p}="@path";
12.   }
13.   close PATHS;
14.
15.   # головний цикл через всі вузли v – об'єкти довіри:
16.   #
17.   open AS_LIST, "./adj_hash.csv";
18.   $i=1;
19.
20.   while (<AS_LIST>) {
21.   chop;
22.   $v=$_;
23.
24.   # ініціалізація елементу геш-масива
25.   $t{$v}=0;
26.
27.    # початкова відстань до $v, заздалегідь більша за
      реальну
28.    $d=9999;
29.
30.    # Головний цикл:
31.    # 1. пошук маршрутів що містять v
32.    # 2. вибір найменшої відстані d (u,v)
33.
```

```
34.     foreach $p (keys %hash) {
35.
36.        # 1: пошук маршрутів що містять v
37.
38.        if ($hash{$p}=~m/^$v\ /
39.             or $hash{$p}=~m/\ $v$/
40.             or $hash{$p}=~m/\ $v\ /) {
41.
42.        # якщо в префіксі $p є $v - розділяємо @path на
      окремі
43.        # вузли та рахуємо позицію v
44.        @path=split(/ /,$hash{$p});
45.
46.        # 2: вибір коротшого шляху
47.        for ($j=0; $j<=$#path; $j++) {
48.         if ($v != $path[$j]) {   next;     }
49.         # якщо v присутній в шляху, порахувати його номер
      зліва
50.           if ( $d > $j+1 ) {
51.            $d=$j+1;
52.         }
53.        }
54.         }
55.    }
56.    $t{$v}=10**($d/$AD);
57.    print "$i:    AS$v -> $d\n"; $i++;
```

5.3.5. Розрахунок сумарного ризику для вузла *и*

Після розрахунку обох метричних характеристик, по всій множині вузлів для вузла *и* розраховується сумарний ризик перехоплення маршруту за формулою (4.7.3).

Якщо по горизонтальній вісі відкласти порядкові номери вузлів, а по вертикальній вісі відкласти значення рикизу, сумарний ризик від перехоплення маршруту можна візуалізовати як площу заштрихованої фігури, прикладом якої може бути рис. 6.1.3 . Зменшення її площі є зниженням ризику. Впорядкування вузлів за зменшенням ризику надає зручний спосіб до зниження рівня ризику (risk mitigating).

5.4. Підвищення кіберзахищеності топології Інтернет та порівняння результатів

5.4.1. Критерій ефективності нової топології

Поставлена задача підвищення захищеності суб'єкта глобальної маршрутизації шляхом формування ефективної топології його з'єднань за допомогою оцінювання ризику кібератак на систему глобальної маршрутизації вирішується наступним чином.

Спочатку оцінюється R_0 – початковий ризик перехоплення маршруту до мережевого префіксу, що ідентифікує цей інформаційний актив, наприклад, за вдосконаленою моделлю DREADxSTRIDE. Після цього розраховується ризик по вузлах (4) за сумарний ризик для префікса (5). Він нормується з початковим:

$$R_u = \sum_{i \neq u}^{|V|-1} R_i^v = kR_0$$

Підвищення захищеності топології мережевого префікса полягає в зниженні R_u до R'_u так, що:

$$\frac{R'_u}{R_u} < k \;\Leftrightarrow\; R'_u < kR_0 .$$

Після введення метрик довіри та значущості існує можливість впливу на ймовірність настання ризику через довіру як оцінку ймовірності, а також впливу на масштаб наслідків через значущість як оцінку потенційного збитку [133, 134]. Вплив на довіру можливий через 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, мінімізувавши таким чином метрику довіри. Для цього необхідно на моделі сегменту мережі, побудованій по реальних даних протоколу BGP-4, моделювати нові зв'язки між вузлом – власником ризику, та самим значущим вузлом з низькою метрикою довіри. В результаті прямого з'єднання відстань між вузлами $d(u,v)=1$, і це забезпечує максимальне значення T_u^v. Якщо з практичної точки зору побудова прямого BGP-з'єднання неможлива чи ускладнена, виконується або пошук вузла-посередника, щоб забезпечити $d(u,v)=2$, або береться наступний за значущістю вузол з низькою довірою та моделюється BGP-взаємодія з ним. моделювання нових топологій має на меті досягнення виконання нерівності.

5.4.2. Комбінаторна задача пошуку ефективної топології

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 .

Це – *NP*-складна комбінаторна задача [135], проте її розмірність може бути спрощена різними відомими на цей час методами, що дають наближений результат [136, 137]. Для отримання приблизних чи субоптимальних рішень *NP*-складних задач досить традиційним є метод пошуку від опорного рішення. Це може означати, що для отримання рішення для q зв'язків, спочатку шукається оптимальне рішення для q=1. Потім – для q=2, але вже при фіксованому першому з'вязку. На наступному кроці – для q=3, але при визначеному першому та другому зв'язку. Опишемо метод покрокового приєднання до q вузлів з множини $V_o : v \in V_o$:

На <u>першому кроці</u> задача вирішується для q=1. Критерієм вибору є ризик R вузла $v \in V_o$. Найкращий результат дає приєднання до вузла з найменшим ризиком.

На <u>другому кроці</u> попередній зв'язок фіксується, та перебирається множина V_o-1 вузлів, що лишились доступними. Перебором визначається другий зв'язок, який мінімізує ризик для вузла u.

Другий крок повторюється $q-1$ разів. Кількість доступних вузлів V_o при кожному кроці зменшується на 1. На першій ітерації кількість переборів дорівнює $V_o - 1$, на n-й ітерації $V_o - n$, на останній, $q-1$ ітерації – $V_o - q$. Тобто, загальна кількість переборів складає

$$|V_o|q - \sum_{n=1}^{q} n$$

за умови

$$q \le \frac{V_o}{2}.$$

В разі $\frac{V_o}{2} < q < V_o$ можна використовувати зворотній алгоритм – моделювання відключення замість підключення, і це дасть також $|V_o|q - \sum_{n=1}^{q} n$ комбінацій, а $q > V_o$ не розглядається як можлива умова задачі.

Оскільки сума членів a арифметичної прогресії S з n членів складає

$$S_n = \frac{a_1 + a_n}{2} n,$$

то

$$S_q = \frac{q + q^2}{2},$$

отже, кількість переборів становить $|V_o|q - \frac{q+q^2}{2}$, а загальна складність методу на мережі *G=(V,E)* в разі використання алгоритму широкого пошуку для розрахунку фактору віддаленості становить

$$O(|V|+|E|)(|V_o|q - \frac{q+q^2}{2}) \text{ для } q \le \frac{V_o}{2}.$$

В таблиці 2.3.1 наведено дані стосовно зростання часу пошуку рішення цим методом в залежності від кількості необхідних зв'язків та доступних вузлів.

Таким чином, рішення знаходиться за *q* кроків, тоді як на кожному кроці необхідно виконати перебір всіх доступних вузлів, з якими ще не побудовано зв'язку. Нагадаємо, що кращій варіант на кожному кроці оцінюється за мінімальним значенням ризику *R*. Загальна кількість переборних варіантів складає $\sum_{i=0}^{q-1}(|V_o|-i)$, отже таке рішення може бути отримане за поліноміальний час. На прикладі *q* та $|V_o|$ як "10 з 100", "5 з 100" та "2 з 100" можна побачити, що кількість переборів залежить від *q* майже лінійно.

Постає питання, чи можна уникнути перебору всіх доступних вузлів. Нам відомо, що є критерії привабливості вузлів мережі, за яким вони більше чи менше здатні забезпечити новому вузлу мінімальний ризитк перехоплення маршруту. Тоді можна *ввести відношення порядку* на множині вузлів V_o за ризиком. Привабливість вузла має відображати, наскільки приєднання до нього мінімізує фактор віддаленості вузла, що має бути приєднаний.

Оскільки ризик *R* може застосовуватись для оцінки якості топології мережевого префікса в мережі Інтернет, внесемо пропозицію застосовувати його як показник привабливості для моделювання нової комбінації з'єднань визначити на множині вузлів V_o відношення порядку за привабливістю.

$$R_v(i) \le R_v(j) \qquad (5.4.1)$$

Визначимо саме поняття комбінації з'єднань: це організація *q* зв'язків між вузлом-власником ризику та існуючими вузлами мережі. Тепер визначимо множину вузлів для приєднання *Q* як *q* перших вузлів з множини доступних вузлів V_o:

$$Q\{v_1, v_2, ..., v_i, ..., v_q\} \subset V_o. \qquad (5.4.2)$$

Тоді існує множина $V_o \setminus Q$, вузли з якої не використовуються до приєднання. На кордоні цієї множини та Q можливе існування таких вузлів $\{..., v_{q-2}, v_{q-1}, v_q, v_{q+1}, v_{q+2}...\}$, для яких

$$... = R_{q-2} = R_{q-1} = R_q = R_{q+1} = R_{q+2} = ... \qquad (5.4.3)$$

Через часткову впорядкованість (5.4.3) виникає неоднозначність вибору вузлів з однаковим фактором віддаленості для включення в приєднання. Це повертає необхідність перебору комбінацій з $n_P + n_{\setminus P}$ вузлів по n_Q, де n_Q – кількість вузлів з однаковим R, що входять в Q, а $n_{\setminus Q}$ кількість вузлів з однаковим R, що не входять в P. Кількість комбінацій [138] складатиме

$$\frac{(n_P + n_{\setminus P})!}{n_P!(n_{\setminus P} - n_P)!} .$$

За результатами експериментальних досліджень встановлено, що в мережі Інтернет трапляються щонайменш десятки вузлів з однаковим фактором віддаленості, тому необхідно виключити переборний метод вирішення вказаної неоднозначності. Необхідно відповісти на питання, чи призведуть приєднання до вузлів з однаковим R до однакового результату, тобто чи є еквівалентними Q та Q', якщо вони містять різні, але попарно еквівалентні елементи v_m.

Наведемо аксиоми еквівалентності [139] :

рефлексивність: $\forall x \in X, xRx$;

симетричність: $\forall x, y \in X, xRy \Rightarrow yRx$;

транзитивність: $\forall x, y, z \in X, xRy \cap yRz \Rightarrow xRz$;

Покажемо для q=1, що є еквівалентними Q та Q', якщо вони містять різні, але попарно еквівалентні елементи v_m. Виходячи з формули сумарного ризику, вузли з однаковим R мають однаковий вклад в сумарний ризик.

Отже, в разі приєднання до будь якого, але єдиного, з вузлів з однаковим ризиком, сумарний ризик у вузла власника ризику вузла буде однаковим.

Довести математично строго при q>1 навряд чи можливо для складної мережі через невизначеність її топології. Натомість, проведено ряд експериментів з наявними моделями сегментів мережі Інтернет, і це в наступному розділі буде продемонстровано. Результати, наведені в 6 розділі, надали емпіричні докази того, що результати еквівалентні принаймні для q=2 та q=3. З цього емпіричного доведення ми виходимо, коли стверджуємо, що приєднання Q та Q' є еквівалентними, якщо вони містять однакову кількість класів еквівалентності та класи множини Q дорівнюють відповідним за порядком класам Q'.

В практичній площині це означає, що ми позбавляємось необхідності застосовувати моделювання та порівняння всіх комбінацій зв’язків типу

$$P\{v_1, v_2, .., v_{q-1}, v_q\},$$
$$P'\{v_1, v_2, .., v_{q-1}, v_{q+1}\},$$
$$P''\{v_1, v_2, .., v_{q-1}, v_{q+2}\},$$

якщо v_q, v_{q+1} та v_{q+2} мають однаковий фактор віддаленості (належать до одного класу еквівалентності), і для розв'язанні задачі може бути вибиране будь-яке з них на наш вибір.

5.4.3. Методика підвищення захищеності інформаційного активу від атак на систему глобальної маршрутизації

Методика підвищення захищеності інформаційного активу від атак на систему глобальної маршрутизації включає в себе:

- отримання з відкритих джерел даних про топологію Інтернет на рівні анонсів префіксів;
- виділення цільової групи вузлів, перехоплення маршруту до яких спричинить збиток;
- розрахунок метрик довіри та значущості для цільової групи вузлів;
- розрахунок поточного ризику і порівняння його із заданим;
- пошук найбільш привабливих вузлів для скорочення шляху до них, моделювання скорочення шляху та повторний розрахунок метрик довіри та значущості;
- повторний розрахунок поточного ризику і порівняння його із заданим.

Суть способу визначення ризику перехоплення маршруту на вузлах мережі Інтернет пояснено на рис. 5.4.1, де наведено схему, яка демонструє реалізацію методики визначення ризику перехоплення маршруту на вузлах мережі Інтернет. На схемі позначено такі елементи:

1 – інформаційний актив власника ризику;
2– глобальна мережа;
AS1 – вузол власника ризику;
AS2,AS3..ASn – інші вузли;
p2,p3...pn – анонси мережевих префіксів;
3 – таблиця глобальної маршрутизації;
4 – блок розрахунку метричної характеристики значущості;
5 – блок розрахунку метричної характеристики довіри;
6 – блок розрахунку ризику та впорядкування вузлів;
7 – програмне забезпечення аналізу та моделювання нової топології.

Інформаційний актив *1*, підключений до Інтернет-вузла AS1 – власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора). AS1 разом з вузлами AS2, AS3, AS4 … AS*n* 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.

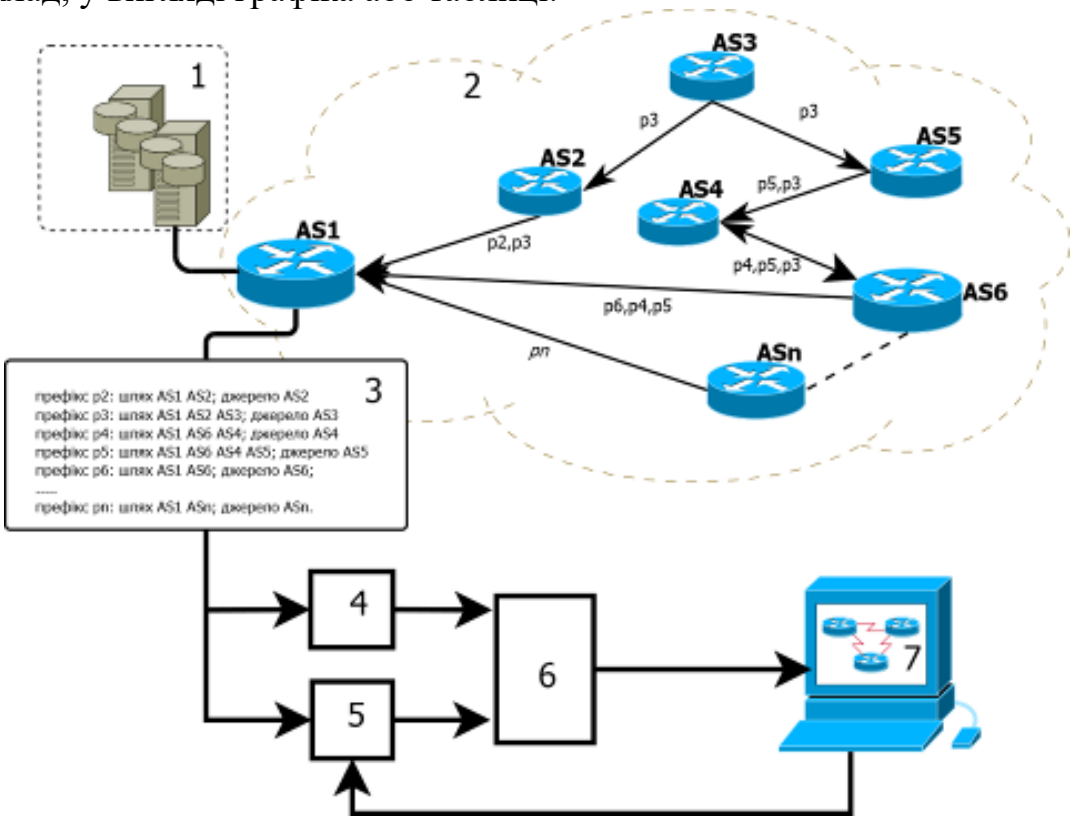


Рисунок 5.4.1 – Схема реалізації методики визначення ризику перехоплення маршруту на вузлах мережі Інтернет

Підчас моделювання ефективної топології зв’язків для зниження ризику, до блоку розрахунку метрики довіри 5 подається нова топологія міжмережевих зв'язків. З урахуванням нових зв’язків розраховується метрика довіри та ризик, який порівнюється із заданим.

Звичайною практикою є моделювання нової толпології шляхом маніпулювання з вхідними даними таблиць маршрутизації, що є поширеною практикою [102, 140 – 146]. В якості прикладу наступні рядки з табл.5.3.1:

```
193.7.221.0/24      6663 12975 57704 199046
96.9.68.0/24        6939 59318 57704 131207
185.10.145.0/24     6939 8902 57704 199629
103.11.75.0/24      6939 18351 57704 24532 55660
```

Вони демонструють, що AS57704 є досить віддаленою, але зустрічається в шляхах бахатьох префіксів. Точніше можна довідатись за допомогою розрахунку метрики значущості. Якщо AS57704 має високу значущість і доступна для побудови з нею BGP-взаємодії, для моделювання нової топології і оцінки ризику відповідні рядки у вхідній таблиці мають бути змінені наступним чином:

```
193.7.221.0/24      57704 199046
96.9.68.0/24        57704 131207
```

```
185.10.145.0/24   57704 199629
103.11.75.0/24    57704 24532 55660
```

Це еквісалентно утворенню нового елементу топологічного простору – звязку з AS57704 і, завдяки цьому, скороченню шляхів від деяких префіксів до вузла власника ризику, з точки зору якого виконується оцінювання.

5.5. Рекомендації власникам інформаційних активів з підвищення безпеки проти кібернетичних атак на систему глобальної маршрутизації

Дані рекомендації містять належні практики з оцінювання ризиків інформаційної безпеки, які спричинені кібернетичними атаками, вектором яких є система глобальної маршрутизації всесвітньої комп'ютерної мережі Інтернет, а також підвищення захищеності інформаційних активів від таких атак.

Рекомендації не містять опису заходів забезпечення кібербезпеки, мають або загальний характер, або, попри важливість, не є специфічними стосовно системи глобальної маршрутизації. Натомість, рекомендації стосуються додаткових заходів, які доповнюють чи змінюють більш загальні процедури, які виконуються в циклі забезпечення інформаційної безпеки.

В цих Рекомендаціях наведені нижче терміни вживаються в такому значенні:

Інцидент кібербезпеки (або кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

Інформаційний актив – об'єкт інформаційно-комп'ютерної та телекомунікаційної інфраструктури, який взаємодіє з глобальною

комп'ютерною мережею Інтернет, зокрема, але не тільки, електронні інформаційні ресурси.

Електронні інформаційні ресурси – будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.

5.5.1. Стислий опис загроз інформаційному активу

З вразливостей глобальної маршрутизації витікають наступні загрози інформаційному активу:

Порушення доступності. Ймовірність виникнення – висока, масштаб наслідків – великий.

Порушення цілісності (підміна даних). Ймовірність виникнення – низька, масштаб наслідків – середній.

Порушення конфіденційності. Враховуючи, що конфіденційні дані при переміщенні мережами загального користування, мають бути додатково захищені на рівні застосунків, ймовірність – середня, масштаб наслідків – низький.

Порушення спостережності. Ймовірність – висока, масштаб наслідків – середній.

5.5.2. Стислий опис механізмів реалізації загроз

Захоплення префіксу. Автономна система анонсує у якості джерела адресний простір що не належить їй. Утворений хибний маршрут конкуруватиме з істинним. При виборі маршруту BGP віддасть перевагу більш короткий, вимірюваний числом мереж між джерелом і одержувачем, маршрут. Наслідок – обмін трафіком з тими мережами, де хибний маршрут виявився кращим, неможливий (Denial of Service).

Витік префіксу. Автономна система ретранслює легально отриманий анонс мережевого префіксу в порушення політики маршрутизації, наприклад, передає одному провайдеру доступу до Інтернет маршрути, отримані від іншого провайдера, пропонуючи тим самим транзит через себе. Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, «джерело» не підмінюється і виявити такий інцидент складніше. Наслідок витоку маршруту – перенаправлення частини трафіку через непризначені для цього канали, що призводить найчастіше до неспіввідносності пропускної здатності мережі «загарбника» і обсягу трафіку, який він перемикає на себе в результаті ретрансляції чужих маршрутів. Наслідки – часткова відмова в обслуговуванні.

Захоплення підмереж. В ході кібератаки анонсуються більш специфічні префікси. При виборі маршруту BGP воліє той, який вказується більш специфічним префіксом, і таким чином атакуючий виграє незважаючи на

топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру, захоплення має глобальний ефект.

Будь-який з перелічених способів може призвести до атаки «Man-in-a-middle», в разі комбінації з іншими механізмами атак. В результаті вдалого проведення можливі перехоплення чутливої інформації, несанкціоноване залучення трафіку для проведення інших атак, використання перехопленого адресного простору для проведення інших атак тощо.

5.5.3. Традиційні заходи зменшення ризику кіберінциденту

Контроль за **налаштуванням політики маршрутизації** на зовнішніх шлюзах. Чітка реалізація прийому та передачі BGP-анонсів в залежності від статусу сусідньої автономної системи:

- клієнтам надсилати всі префікси, приймати виключно зареєстровані на цих клієнтів префікси;
- провайдерам надсилати виключно свої префікси та префікси клієнтів, приймати все;
- сусідам надсилати свої префікси і префікси клієнтів, приймати префікси сусіда та його клієнта.

Статуси префіксів, списки клієнтів визначати по об’єкту aut-num в БД регіонального Інтернет-реєстру RIPE NCC. Застосовувати готовий програмний інструментарій, який пропонується розробниками програмного та програмно-апаратного забезпечення, а також Інтернет-реєстрами.

Належна **публікація політики маршрутизації** в БД регіональних Інтернет-реєстрів. Вчасно, бажано до початку реалізації, публікувати політику маршрутизації, чітко відображати зв’язки хз іншими AS за допомогою рядків import та export. Використовувати макро-визначаення AS-SET для групування номерів AS.

Електронна **сертифікація джерела маршруту**. Для кожного окремого об’єкта маршрутизації створити та опублікувати електронний сертифікат джерела маршруту (Route Origin Authorisation). Для цього визначити і електронним підписом зафіксувати таку комбінацію: довжину префікса, номер AS – джерела маршруту, міксимальну довжину префікса (тобто чи припустимий його поділ на дрібніші об'єкти маршрутизації; бажано ніколи не допускати). Приватний ключ для підпису в найпростішому випадку зберігатиметься на сервері постачальнрика послуг RPKI (регіонального Інтернет-реєстра). Доступ в Інтернет-реєстр бажано обмежити двофакторною аутентифікацією.

Моніторинг власних мережевих префіксів. Оскільки в системі глобальної маршрутизації не існує єдиної точки спостереження всіх маршрутів, необхідно використовувати публічні сервіси з попередження перехоплення маршрутів: BGPmon, Qrator.Radar, ARTEMIS або інші.

Необхідно визначити, яким чином засобами моніторингу виявити уражений префікс; AS, на який безпосередно сталося перехоплення, технічні контакти цієї AS, її схему підключення та номери AS її провайдерів доступу.

План заходів з припинення перехоплення маршруту. Необхідно скласти чіткий і розподілений на залучених осіб план дій в разі виявлення перехоплення маршуруту. План має включати:

- інформування керівництва по лінії інформаційної безпеки;
- інформування користувачів, аб підрозділу, що забезпечує колмунікацію з користувачами;
- отримання контактів AS де сталось перехоплення, контактування всіма наявними засобами;
- отримання контактів вищіх за рівнем провайдерів тієї AS, де сталось перехоплення, контактування всіма наявними засобами;
- за потреби, завантаження конфігурації BGP-шлюзів для анонсування деагрегованого префікса (на сьогодні ефективність запобіжної деагрегації невелика).

5.5.4. Додаткові заходи зменшення ризику кіберінциденту

На сьогодні єдиним дієвим заходом зменшення ймовірності перехоплення маршруту до власних мережевих префіксів є розширення прикордонноє взаємодії з іншими AS. Цей метод «зближує» з іншими учасниками глобальної маршрутизації і ускладнює зловмиснику поширення хибних «кращих маршрутів». Оскільки побудова зв'язків між AS потребує є затратною та достить операцією, оскільки потребує розширення матеріально-технічної бази власника інформаційного активу. Для ефективного витрачання коштів необхідно скористатись методикою, викладеною в підрозділі 5.4 цього дисертаційного дослідження та визначити таку комбінацію зв'язків, яка з мінімальною кількістю зв'язків дасть найнижчий рівень ризику перехоплення маршруту.

За актуальною інформацією про безпеку та захист інформаційних активів в системі глобальної маршрутизації Інтернет, а також для оновлення методів та планів захисту необхідно звертатись до наступних актуальних джерел [147, 148]. Додаткову інформацію можна отримати з таких джерел [145-160].

5.6. Приклад програмної реалізації розрахунку факторів ризику перехоплення маршруту

В якості прикладу автоматизації запропонованої в попередніх розділах методики продемонструємо програмний засіб розрахунку факторів ризику перехоплення маршруту на Інтернет-вузлі за його топологічними характеристиками (далі Risk Metrics), опишемо склад апаратних засобів для його використання, порядок інсталяції та роботи, містить настанови користувача.

Призначення комп'ютерної програми

Програма Risk Metrics використовується в комплексі засобів для при аналізу та вдосконалення міжмережевих зв'язків в Інтернеті. Приграма призначена для розрахунку метрики довіри та метрики значущості Інтернет-вузлів за даними, отриманими з існуючих таблиць глобальної маршрутизації, побудованих за протоколом BGP (BGP routing tables).

Перетворити таблицю маршрутизації, що отримана в текстовому форматі, в таблицю бази даних в форматі «мережевий префікс маршрут джерело_маршруту»;

- задати перелік цільових мережевих префіксів, які будуть враховані при аналізі;
- отримати перелік унікальниїх маршрутів у вигляді послідовності ідентифікаторів Інтернет-вузлів;
- отримати унікальний перелік ідентифікаторів вузлів, які присутні у маршрутах заданих мережевих префіксів;
- отримати вагу кожного мережевого префікса;
- отримати метрику довіри кожного Інтернет-вузла;
- отримати метрику значущості кожного Інтернет-вузла.

Результати виводяться на дисплей та зберігаються в файлах у форматі, придатному до імпорту в MS Excel.

Вимоги до апаратного та програмного забезпечення комп'ютера

Програмний засіб Risk Metrics призначений для роботи на персональному комп'ютері користувача з частотою процесора не нижче 1 GHz та оперативною пам'яттю не менше 1024 MB.

Програмний засіб реалізовано на мові програмування Perl. Засіб працює в середовищі компілятора Perl під керуванням наступних операційних систем (але не виключно на них):

- Windows 7, 8, 8.1, 10;
- Windows Server 2012, 2012 R2, 2016, 2016 R2;
- CentOS 6,7,8;
- Ubuntu 16,17,18;
- FreeBSD 8,9,10,11.

Програмний засіб Risk Metrics не потребує інсталяції. Програмні компоненти мають запускатись в операційній системі з встановленим компілятором програмної мови Perl версії не нижче 5. Для зручності рекомендується програмні компоненти засобу Risk Metrics скопіювати в окрему директорію разом із вихідними даними (таблицею маршрутизації).

Робота з програмою

Програмний засіб Risk Metrics має інтерфейс командного рядка. Вхідними даними для роботи програмного засобу є фрагмент таблиці маршрутизації, який відноситься до цільових мережевих префіксів, у текстовому форматі, збережений у файлі adj_routes.txt. Файл повинен містити

дані в форматі «префікс шлях» у форматі Cisco IOS або BIRD, як описано в підрозділі 5.3.

Порядок запуску програмних засобів та отримання результатів наступний.

Програмний модуль Adj_build.pl:

- створює таблицю в форматі «вузол_i вузол_j» для всіх пар поєднаних вузлів та записує в файл adj_hash.txt;
- створює перелік мережевих префіксів та шляхів в форматі «префікс вузол_i вузол_j ... вузол_0» для всіх мережевих префіксів і записує у файл pref_aspaths.txt, як зображено на рис. 5.6.1.

Програмний модуль Signif.pl:

- за вхідним файлом adj_routes.txt розраховує метрику значущості для кожного вузла, присутнього в цільовій групі мережевих префіксів;
- в процесі роботи виводить на дисплей проміжні результати у вигляді лістингу відповідно до рис.5.6.2;
- результат записує результат «номер_AS ; *S*» в файл signif.csv, придатний для імпорту в MS Excel.

```
168.0.168.0/24 3326 1299 267613 262462 265257
154.0.154.0/24 3326 37662 36930 36909
184.0.184.0/21 3326 1299 3356 209
128.0.128.0/20 3326 1299 8359 25513
168.0.168.0/22 3326 1299 267613 262462 265257
131.0.131.0/24 3326 1299 12956 22927 52232
208.0.208.0/24 3326 1299 3356 26759
208.0.208.0/22 3326 1299 3356 26759
161.0.161.0/24 3326 1299 12956 7004 262237
40.0.40.0/24 3326 1299 7332 4249
186.0.186.0/24 3326 1299 3356 3549 7049 263776
188.0.188.0/24 3326 31133 49724
210.0.210.0/23 3326 9304
194.1.198.0/24 3326 31133 20632 44263
128.1.132.0/24 3326 1299 21859 135377
46.1.42.0/24 3326 1299 3257 34984 34296
202.1.206.0/23 3326 6939 7642
167.1.163.0/24 3326 1299 4775 15084
196.1.192.0/19 3326 1299 6762 15706
196.1.192.0/20 3326 1299 6762 15706
196.1.192.0/18 3326 1299 6762 15706
196.1.192.0/24 3326 1299 6762 15706
200.1.204.0/24 3326 1299 7738 8167 53062 265078 61512 52468 27795
68.1.64.0/18 3326 1299 3257 22773
```

Рисунок 5.6.1 – Результат формування даних модулем adj_build.pl програмного засобу «Risk Metrics»

```
E:\PROG\MODEL> perl  signif.pl
   AS12578 significance: 2921.66666666667
   AS13188 significance: 1618.5
   AS15645 significance: 0
   AS198401 significance: 31
   AS205103 significance: 317.916666666667
   AS210222 significance: 1514.39761904762
   AS25282 significance: 2.5
   AS262761 significance: 393.5
   AS263062 significance: 16
   AS263444 significance: 1262.13809523809
   AS263671 significance: 20
   AS28741 significance: 1
```

Рисунок 5.6.2 – Проміжні результати модуля Signif.pl програмного засобу «Risk Metrics»

Програмний модуль Trust.pl:

- за вхідними файлами adj_routes.txt розраховує метрику довіри для кожного вузла, присутнього в цільовій групі мережевих префіксів;
- в процесі роботи виводить на дисплей проміжні результати у вигляді лістингу відповідно до рис.5.6.3;
- результат записує результат у вигляді «номер_AS ; *T*» в файл trust.csv, придатний для імпорту в MS Excel.

```
E: \_PROG >perl trust1000.pl

1:      AS3356 3.11764858264486
2:      AS7018 3.11764858264486
3:      AS4134 3.11764858264486
4:      AS1299 3.11764858264486
5:      AS4837 3.11764858264486
6:      AS9808 5.50478980785497
7:      AS1239 3.11764858264486
8:      AS4766 3.11764858264486
9:      AS721 9.71973268486748
10:     AS58453 3.11764858264486
11:     AS701 3.11764858264486
12:     AS209 5.50478980785497
13:     AS6453 3.11764858264486
14:     AS7922 3.11764858264486
15:     AS17676 9.71973268486748
```

Рисунок 5.6.3 – Проміжні результати модуля Trust.pl програмного засобу «Risk Metrics»

Програмний модуль merge_metrics.pl:

- використовуючи ідентифікатор AS в якості ключа, створює асоціативний масив в форматі

$$AS_1 \{ S \} \{ T \}$$

$$AS_2 \{ S \} \{ T \}$$

....

$$AS_n \{ S \} \{ T \}$$

– обраховуючи ризик R за форумлою (4.7.3), записує результат у вигляді «номер_AS ; S; T; R» в файл merge_metrics.csv, придатний для імпорту в MS Excel.

Графічну візуалізацію результатів аналізу метричних характеристик та ризику можна виконувати за допомогою імпорту даних з файлу merge_metrics.csv в аналітичні пакети чи в електронні таблиці типу MS Exel. Імпортована таким чином таблиця результатів може буьти впорядкована за будь-якою метрикою чи за ризиком.

Методика передбачає, що варто застосовувати впорядкування за зниженням метрики значущості, та, візуально виявляючи ідентифікатори AS з високим показником метрики довіри, вивчати можливість зменшення топологічної відстані до них.

ГЛАВА 6.
ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ З ОЦІНЮВАННЯ ТА ПІДВИЩЕННЯ КІБЕРЗАХИЩЕНОСТІ СИСТЕМИ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ ШЛЯХОМ МОДЕЛЮВАННЯ ЕФЕКТИВНОЇ ТОПОЛОГІЇ ЗВ'ЯЗКІВ

6.1. Аналіз та підвищення захищеності топології для Інтернет-провайдера ElVisti (AS8258)

ТОВ «Інформаційний центр «Електронні вісті» (далі – ElVisti) є провайдером телекомунікацій, що надає послуги доступу до мережі Інтернет та внесений до державного Реєстру операторів, провайдерів телекомунікацій, і має власний ідентифікатор автономної системи AS8258 [168]. Окрім цієї діяльності, ElVisti володіє власними інформаційними ресурсами, які побудовані на веб-технологіях та підключені до вузла ElVisti. ElVisti також надає інформаційні послуги за технологіями Інтернет. В рамках цих послуг функціонує система збору інформації (сканування) з українських та світових інформаційних, насамперед новинних, ресурсів, яка є частиною програмно-технологічного комплексу InfoStream.

Однак протягом 2014-2019 років сканування інформаційних ресурсів та надання доступу до власних інформаційних ресурсів користувачам ElVisti неодноразово потерпали через кіберенетичні інциденти, які мають назву «витік маршруту» та «перехоплення маршруту», зокрема, за участі великих операторів Азії та Далекого Сходу.

За методикою, викладеною в гл.5, було оцінено двох глобальних Інтернет-провайдерів – Cogent (AS174) та Hurricane Electrics (AS6939). Порівняння продемонструвало перевагу AS6939 [169] у зниженні ризику перехоплення маршруту до регіонів Південної Азії та Далекого Сходу завдяки значному охопленню цих регіонів.

Було проведено експериментальне моделювання підвищення захищеності AS8258 від ризику атак «перехоплення маршруту». Для цього безпосередньо з маршрутизатора AS8258 отримано таблицю глобальної маршрутизації, в якій міститься інформація про маршрути до всії доступних на той момент мережевих префіксів. Кожен маршрут містить мережевий префікс та шлях (as_path). За шляхами було складено список видимих AS, що належать множині V в моделі (6.1.1).

Для кожного вузла $v \in V$ виконано розрахунок метрики значущості. Для цього для кожного v отримано множину мережевих префіксів P, до яких в AS8258 маршрути пролягають через v. Для кожного префіксу $p \in P$ визначено його джерело та відстань між джерелом та v. Також визначено вагу кожного префіксу.

Далі для кожного вузла $v \in V$ виконано розрахунок метрики довіри. Для цього з повного списку атрибутів as_path розраховано середній шляху від AS8258 до інших видимих AS за раніше складеним списком. Для кожного *v* зі списку AS знайдено коротший шлях від AS8258 серед усіх шляхів, наявних в таблиці глобальної маршрутизації.

Для кожного вузла *v* зроблено розрахунок сумарного ризику перехоплення маршруту:

$$R_u^v = S_u^v \cdot 10^{T_u^v}$$

а також сумарний ризик:

$$R^u = \sum_{i \neq u}^{|V|-1} R_i^u \qquad (6.1.1)$$

Результати візуалізовано на рис.6.1.1 – 6.1.5. На них продемонстровано розподіл метрики значущості, метрики довіри та ризику для 50 вузлів з найвищою метрикою значущості.

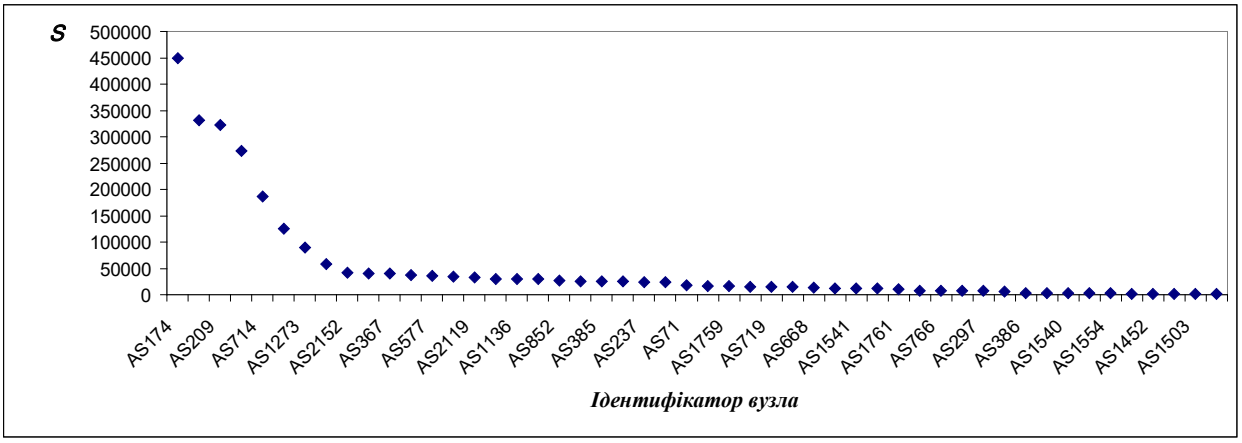


Рисунок 6.1.1 – Розподіл вузлів за метрикою значущості S

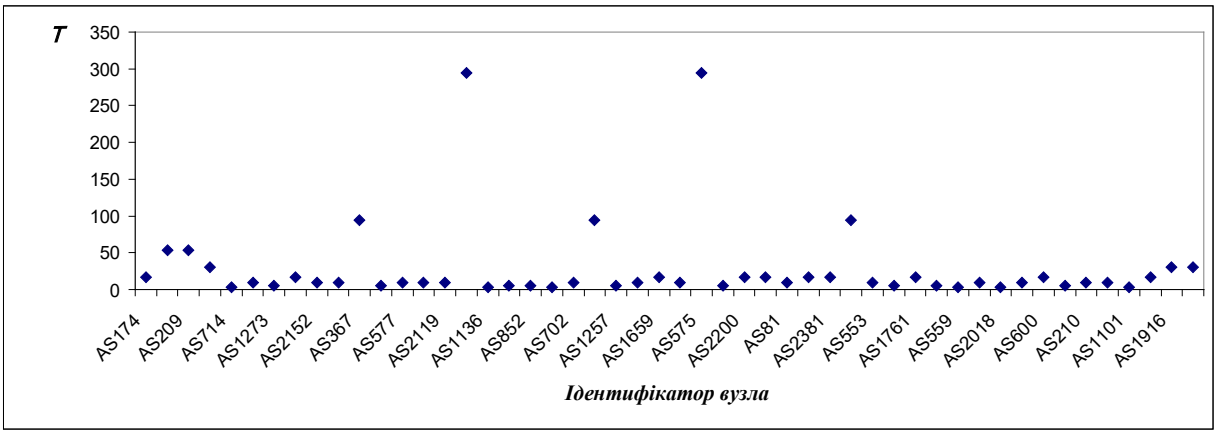


Рисунок 6.1.2 – Розподіл вузлів за метрикою довіри. Вісь ординат – метрика довіри у вигляді $10^{T_u^v}$

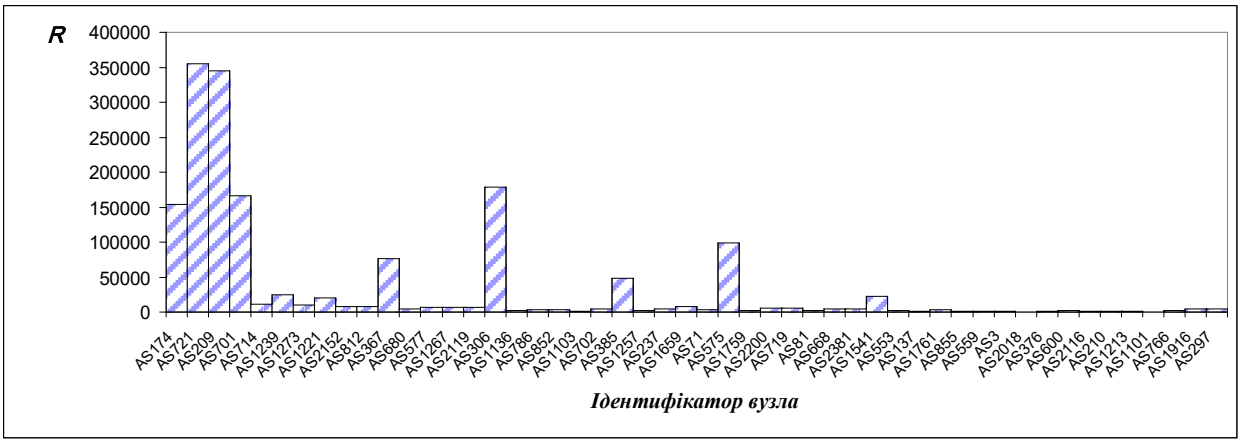


Рисунок 6.1.3 – Розподіл ризику перехоплення маршруту R серед 50 вузлів з найвищою метрикою значущості

Підрахунок дає такі результати: сумарний ризик (6.1.1) для перших 50 вузлів з найвищою значущістю $R^u = 1{,}698 \cdot 10^6$.

Далі проведено впорядкування вузлів за ризиком і виділено три вузли, що мають найвищий ризик. Це вузли AS721, AS209, AS306, через які проходить велика кількість коротших шляхів до інших мереж, при чому з цими вузлами у AS8258 відсутній безпосередній зв'язок, тож вони є концентраторами ризику перехоплення маршруту. Відповідно до методики вдосконалення топології (рис.2) на вхід модуля розрахунку метрики довіри має бути передано модифіковану таблицю глобальної маршртутизації, відповідно до якої між AS8258 та трьома концентраторами ризику присутній безпосередній зв'язок. Та в результаті предметного аналізу концентраторів ризику встановлено, що один з трьох, а саме – AS306, належить Департаменту Оборони США, тож можливість встановлення прямої BGP-взаємодії з ним для звичайного українського Інтернет-провайдера є дуже сумнівною. З урахуванням цього, замість AS306 для моделювання обрано наступний за ризиком вузол – AS701. В результаті отримано нові метрики довіри до вказаних вузлів та розраховано нові ризики по всіх вузлах. Результат продемонстровано в табл. 6.1.1.

Таблиця 6.1.1 – результати моделювання по AS8258

		Початкова топологія			Нова топологія	
№	Ідентифікатор AS	Метрика Довіри	Метрика значущості	Ризик	Метрика довіри	Ризик
1	AS721	53,51	6631	354810	1,77	11737
2	AS209	53,51	6442	344705	1,77	11403
3	AS306	294,53	605	178191	294,53	178191
4	AS701	30,30	5470	165743	1,77	9681
5	AS174	17,16	8987	154243	17,16	154243
6	AS575	294,53	337	99150	294,53	99150
7	AS367	94,47	809	76394	94,47	76394
8	AS385	94,47	511	48302	94,47	48302
9	AS1554	520,06	48	24826	520,06	24826

		Початкова топологія			Нова топологія	
№	Ідентифікатор AS	Метрика Довіри	Метрика значущості	Ризик	Метрика довіри	Ризик
10	AS1239	9,72	2512	24421	9,72	24421
11	AS1541	94,47	233	21974	94,47	21974
12	AS1221	17,16	1158	19871	17,16	19871
13	AS714	3,12	3740	11659	3,12	11659
14	AS357	294,53	36	10509	294,53	10509
15	AS1273	5,50	1803	9926	5,50	9926
16	AS1659	17,16	474	8139	17,16	8139
17	AS2152	9,72	834	8110	9,72	8110
18	AS812	9,72	809	7861	9,72	7861
19	AS577	9,72	711	6907	9,72	6907
20	AS1267	9,72	678	6592	9,72	6592
. . . . .						
48	AS2379	30,30	61	1859	30,30	1859
49	AS647	53,51	33	1786	53,51	1786
50	AS1759	5,50	317	1744	5,50	1744
	Сума			**1697539**		**865103**

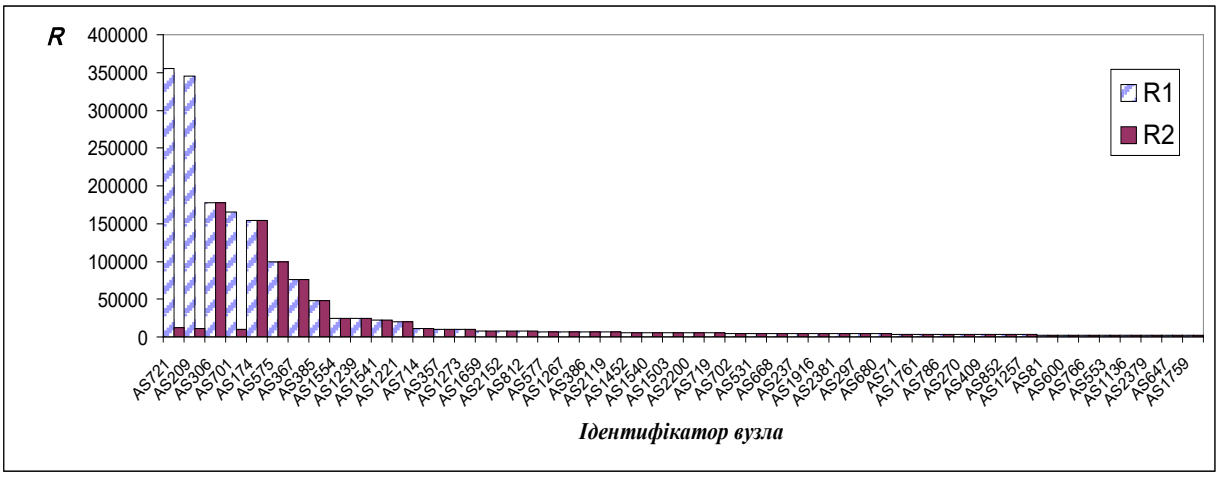


Рисунок 6.1.4 – Розподіл ризику перехоплення маршруту серед 100 вузлів з найвищою метрикою значущості для старої топології (R1) та нової топології (R2)

Візуальне та арифметичне порівняння рядів даних R1 та R2 демонструє, що запровадження окремих змін у топології зв'язків AS8258 здатно зменшити ризик перехоплення маршруту. Точний розрахунок показав, що сумарний ризик (6.1.1) для нової топології склав $R^{u} = 8{,}6 \cdot 10^{5}$, тобто R2 на 50% нижче за R1 (табл. 6.1.1).

Отже, вдалось знайти топологію зв'язків AS8258, яка на 50% більше захищена від кібератак типу перехоплення маршруту завдяки впровадженню лише трьох нових з'єднань. Пояснення такого суттєвого впливу полягає в тому,

що кожне нове з'єднання породжує велику кількість нових доступних маршрутів.

6.2. Аналіз та підвищення захищеності топології для провайдера хмарних послуг QLOUDE (AS210046)

Компанія Moris B.V. є постачальником послуг з надання в оренду віртуальної інформаційно-телекомунікаційної інфраструктури та послуг різного рівня під торгівельною маркою «Qloude» на базі власної фізичної інфраструктури, зокрема, розміщення даних «в хмарі». В компанії вважають, що загрози інформаційної безпеки, які виходять із проблем глобальної маршрутизації, в значній мірі недооцінені світовим технічним і економічним співтовариством. Фактично цією проблемою займається тільки вузьке співтовариство інженерів і регіональних Інтернет-реєстрів, при тому, що очевидно – на сьогодні і навіть на завтра не буде знайдено глобального технічного порятунку.

Компанія прагне побудувати та підтримувати сучасну надійну інфраструктуру, яка відповідає вимогам високої доступності (high availability – HA). Для цього інфраструктура має бути розгалуженою, масштабованою та з продаманими рівнями резервування. Задачі, що вирішуються за рахунок масштабування:

а) необхідність спільного та одночасного використання ресурсів і даних;

б) різнорідність ресурсів і способів їх консолідації, що обумовлена різноманітністю устаткування, розгорнутого програмного забезпечення і відмінностями в образі дій персоналу;

в) динамічність ресурсів у відповідності до обсягів завдань та даних.

г) керування пріоритетами для процесів та користувачів, відсутність якого негативно впливає на процеси, що потребують обробки в «реальному часі».

Для отримання сучасного рівня резервування, що є невід'ємною частиною забезпечення HA, інфраструктура Qloude територіально розгалужена між декількома так званими регіонами (які й насправді можуть бути географічно віддаленими). Для централізованого керування регіонами та їхньою взаємодією може бути організовано супер-ядро у складі концентратора VPN, сховища резервних копій, реєстру ключів аутентифікації, панелі керування тощо.

На рис. 6.2.1 наведено узагальнену структуру розгалуженої хмари Qloude.

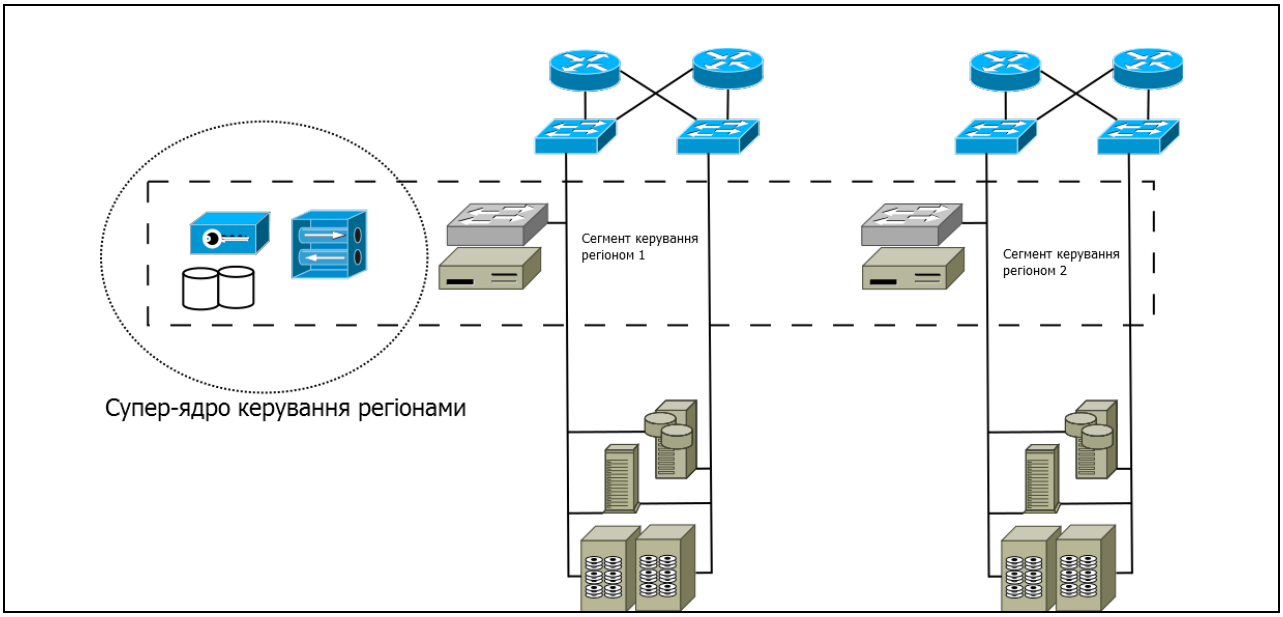


Рисунок 6.2.1 – Спрощена схема розгалуженої хмари системи Qloude із застосуванням регіонізації

Приділяючи увагу побудові ефективної топології і оптимізації витрат на транзитні канали, компанія Moris B.V. отримала власний номер автономної системи – AS210046, незалежний мережевий префікс для розгортання власної інфраструктури та віртуальної інфраструктури клієнтів – 188.66.24.0/22.

Розглядалось також питання необхідності підключення додаткового провайдера Інтернет-доступу, здатного забезпечити максимальний захист топології при мінімальній вартості експлуатації телекомунікацій. Для цього були проведені експериментальні розрахунки за методикою, викладеною в гл. 5. Для цього безпосередньо з маршрутизатора AS210046 отримано таблицю глобальної маршрутизації, в якій міститься інформація про маршрути до всіх доступних на той момент мережевих префіксів. Кожен маршрут містить мережевий префікс та шлях. За шляхами було складено список видимих AS.

Для кожної AS виконано розрахунок метрики значущості. Для цього для кожного v отримано множину мережевих префіксів P, до яких в AS210046 маршрути пролягають через v. Для кожного префіксу $p \in P$ визначено його джерело та відстань між джерелом та v. Також визначено вагу кожного префіксу.

Далі для кожної AS виконано розрахунок метрики довіри. Для цього з повного списку атрибутів as_path розраховано середній шляху від AS210046 до інших видимих AS за раніше складеним списком. Для кожного v зі списку AS знайдено коротший шлях від AS210046 серед усіх шляхів, наявних в таблиці глобальної маршрутизації.

Для кожного вузла v зроблено розрахунок сумарного ризику перехоплення маршруту, а також сумарний ризик відповідно до (6.1.1).

На рис. 6.2.2-6.2.5 продемонстровано розподіл метрики значущості, метрики довіри та ризику для 30 вузлів з найвищою метрикою значущості.

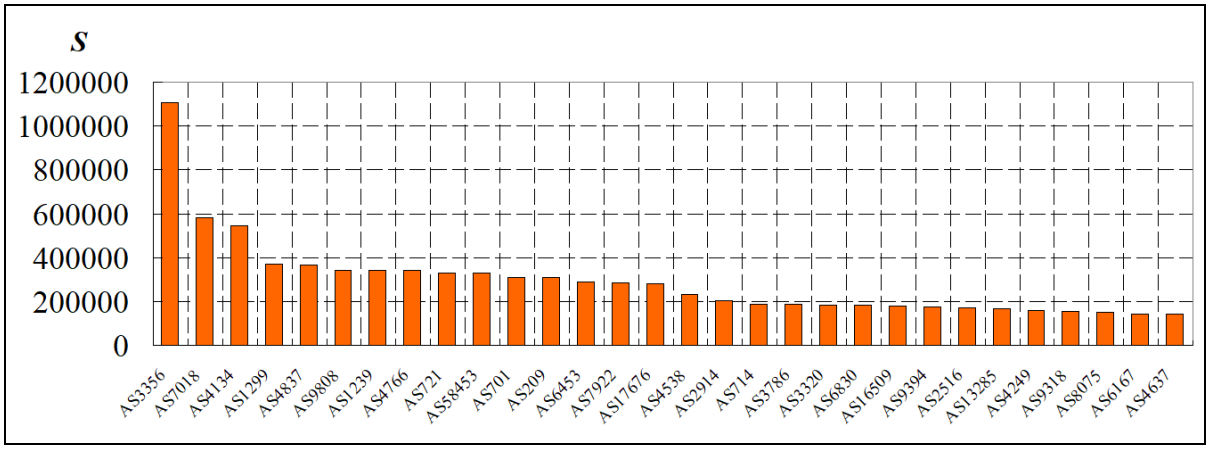


Рисунок 6.2.2 – Розподіл вузлів за метрикою значущості *S*

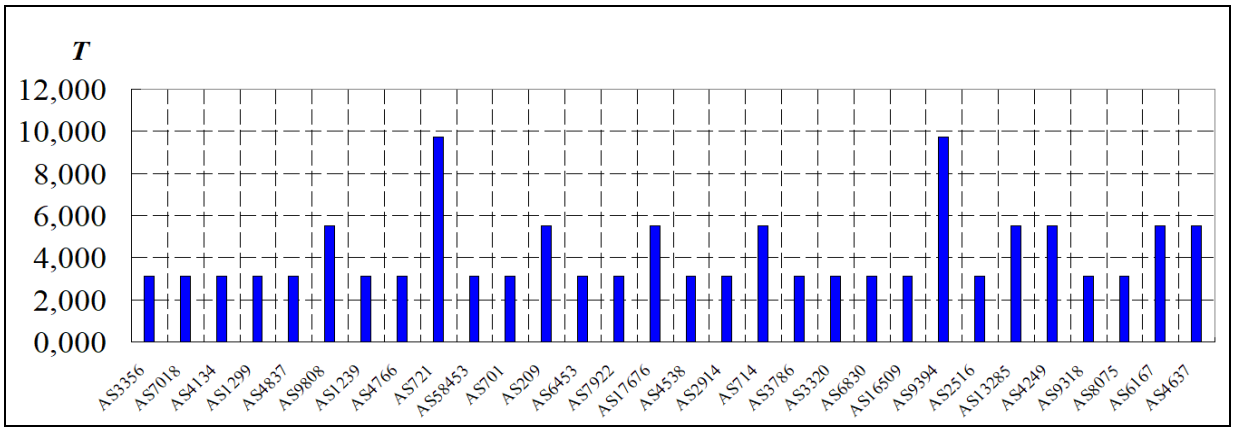


Рисунок 6.2.3 – Розподіл вузлів за метрикою довіри. Вісь ординат – метрика довіри у логарифмічному вигляді

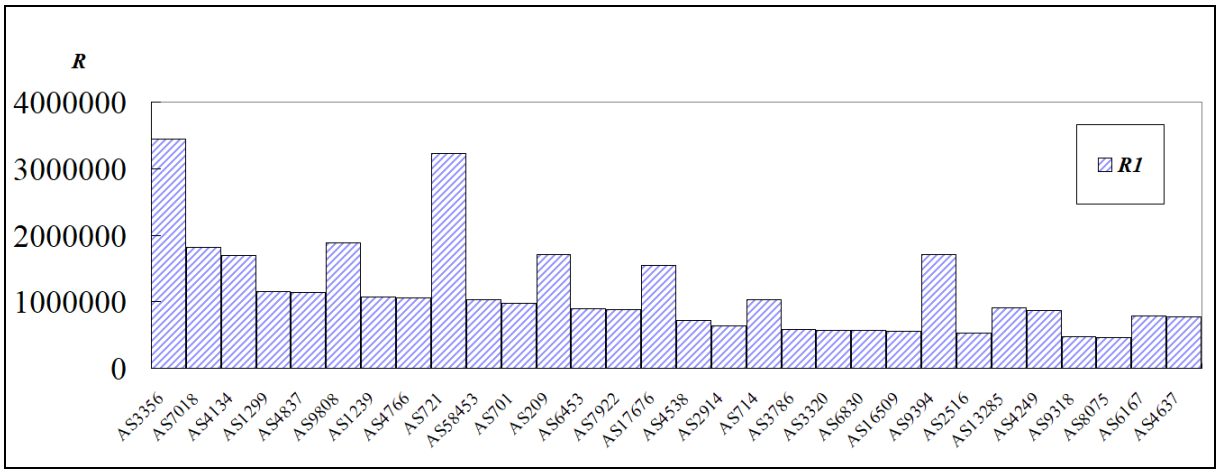


Рисунок 6.2.4 – Розподіл ризику перехоплення маршруту *R* серед 30 вузлів з найвищою метрикою значущості.

Замість BGP-таблиці, отриманої від існуючого провайдера інтернет доступу Cogent (AS174) були обраховані за вказаною методикою також таблиці від деяких інших провайдерів. Розрахунки продемонстрували, заміна на будь-якого іншого не дасть значного зміни уразливості мережевого префікса

188.66.24.0/22. Вагоме зниження ризику відбувається, якщо побудувати обмін маршрутами одночасно з декількома операторами. Для цього найбільш вигідно використовувати послугу публічного пірінгу в європейських Internet Exchanges, наприклад, територіально вигідно розташованою AMS-IX (AS6777). Дані про публічний пірінг AMS-IX отримані з серверів маршрутів AMS-IX та сервісу looking glass. В ньому приймають участь понад 240 тис мережевих префіксів IPv4 та 50 тис IPv6. Результати моделювання по перших за значущістю 20 вузлах відображено в табл. 6.2.1.

Таблиця 6.2.1 – Емпірічне дослідження ризику в AS210046

		Початкова топологія			**Нова топологія**	
№	**Ідентифікатор AS**	**Метрика Довіри**	**Метрика значущості**	**Ризик**	**Метрика довіри**	**Ризик**
1.	AS3356	1106092	3,118	3448406	3,118	3448406
2.	AS721	331341	9,720	3220543	3,118	1033004
3.	AS9808	343062	5,505	1888483	3,118	1069546
4.	AS7018	582445	3,118	1815859	3,118	1815859
5.	AS209	311011	5,505	1712053	3,118	969624
6.	AS9394	175350	9,720	1704355	3,118	546680
7.	AS4134	544921	3,118	1698873	3,118	1698873
8.	AS17676	281037	5,505	1547048	3,118	876173
9.	AS367	40578	30,303	1229635	3,118	126509
10.	AS1299	368662	3,118	1149359	3,118	1149359
11.	AS4837	366415	3,118	1142354	3,118	1142354
12.	AS1239	341435	3,118	1064474	3,118	1064474
13.	AS4766	340418	3,118	1061304	3,118	1061304
14.	AS714	187577	5,505	1032574	3,118	584800
15.	AS58453	328796	3,118	1025070	3,118	1025070
16.	AS701	311016	3,118	969639	3,118	969639
17.	AS13285	164982	5,505	908189	3,118	514355
18.	AS6453	288843	3,118	900512	3,118	900512
19.	AS7922	283953	3,118	885267	3,118	885267
20.	AS26599	89877	9,720	873576	3,118	280203
21.	AS3356	1106092	3,118	3448406	3,118	3448406
22.	AS721	331341	9,720	3220543	3,118	1033004
23.	AS9808	343062	5,505	1888483	3,118	1069546
				29277573		**21162013**

Візуалізація ризику такої топології, коли AS210046 водночас є клієнтом AS174 та учасником публічного пірінгу в AMS-IX, наведена у порівнянні на рис.6.2.6 і демонструє розрахункове зниження ризику перехоплення маршруту з $R1$=29277573 до $R2$=21162013, тобто понад 27%.

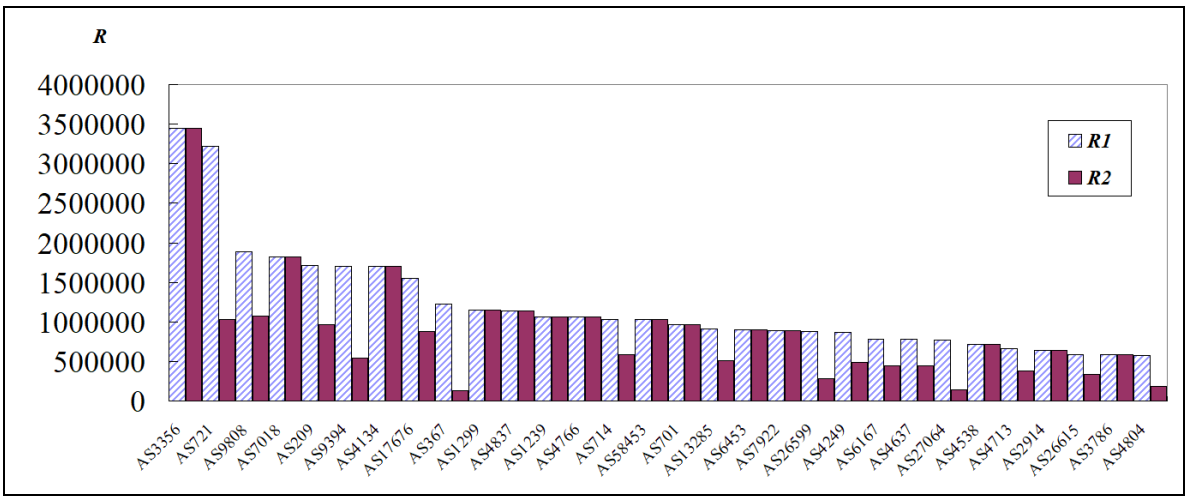


Рисунок 6.2.5 – Розподіл ризику перехоплення маршруту AS210046 серед 30 вузлів з найвищою метрикою значущості для старої топології (R1) та нової топології (R2)

6.3. Аналіз та підвищення захищеності топології для учасника мережі обміну трафіком

6.3.1. Аналіз та підвищення захищеності топології для учасника мережі UA-IX

У топології сучасного Інтернету відіграють дуже важливу роль мережі обміну трафіком чи біржі трафіка (Internet Exchange Points, IXPs). Ідея їхнього заснування – додержуватися чітко визначених процедур підключення та правил взаємодії між мережами учасників. Сьогодні в Європі функціонує багато мереж обміну трафіком. Вони мають різну кількість учасників та обсяги трафіка, різні про-цедури підключення, а головне – різну політику маршрутизації та взаємодії між учасниками. Але кожна з них має свій вплив на топологію зв’язків між автономними системами в Інтернеті.

Однією з головних послуг мереж обміну трафіком є публічний BGP-пірінг (public peering), тобто обмін маршрутами між учасниками за принципом «всі на всі». Це дозволяє кожному з учасників відкритого пірінгу обмінюватися трафіком з максимальною кількістю мереж через єдиний порт підключення до мережі обміну трафіком. Публічний піринг дозоволяє учаснику покращити зв'язність своєї мережі, оптимізувати витрати на IP-транзит, резервувати мережеві маршрути.

Популярність публічного пірінгу полягає в прагненні учасників до забезпечення надійної взаємодії з Інтернет шляхом всебічного аналізу ефективності використання існуючих транзитних каналів. В класичній мережі обміну трафіком також є послуга публічного пірингу. Однією з «класичних» мереж обміну трафіком є Українська мережа обміну трафіком (UA-IX), заснована в 2001 році. Її ідентифікатор – AS15645 [170].

Були проаналізовані ризики перехоплення маршруту для типового учасника мережі обміну трафіком UA-IX на основі BGP-таблиці маршрутів, яку Інтернет-провайдер AS8258 отримує від AS15645 як учасник мережі UA-IX. 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 (рис.6.3.1), 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.

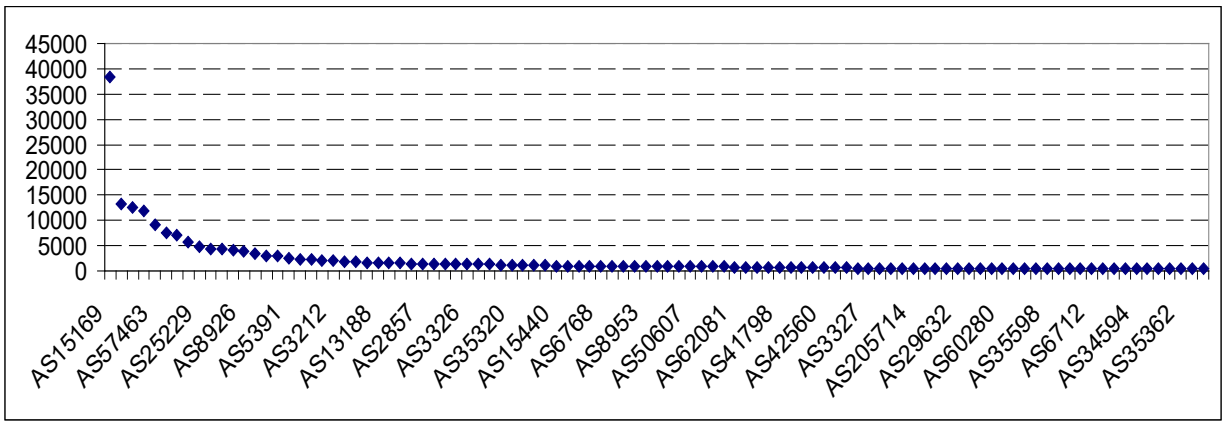


Рисунок 6.3.1 – Графік розподілу за зменшенням значущості серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика значущості *S*, вісь абсцис – порядковий номер AS в групі

Результати розрахунку метрики довіри представлені на рис.6.3.2, а розподілу ризику – на рис. 6.2.3.

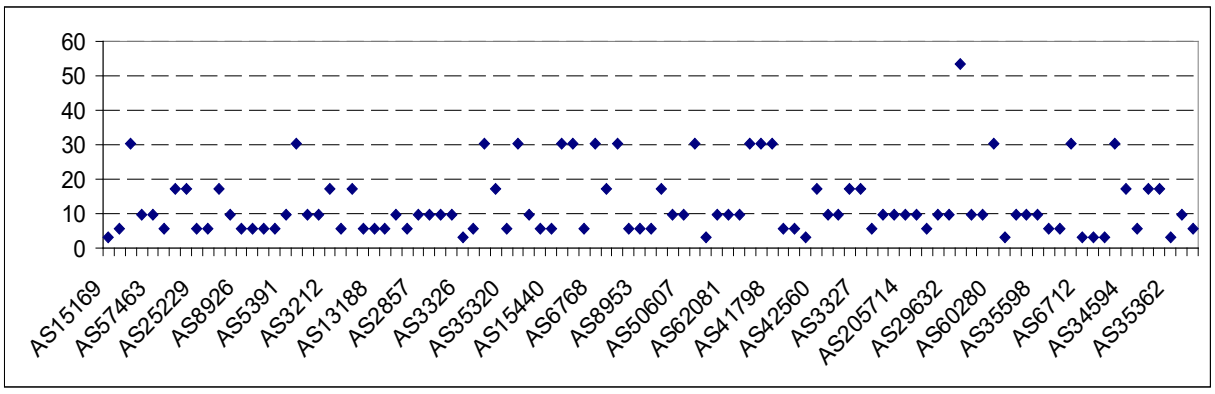


Рисунок 6.3.2 – Графік розподілу за метрикою довіри серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика довіри в логарифмічній формі

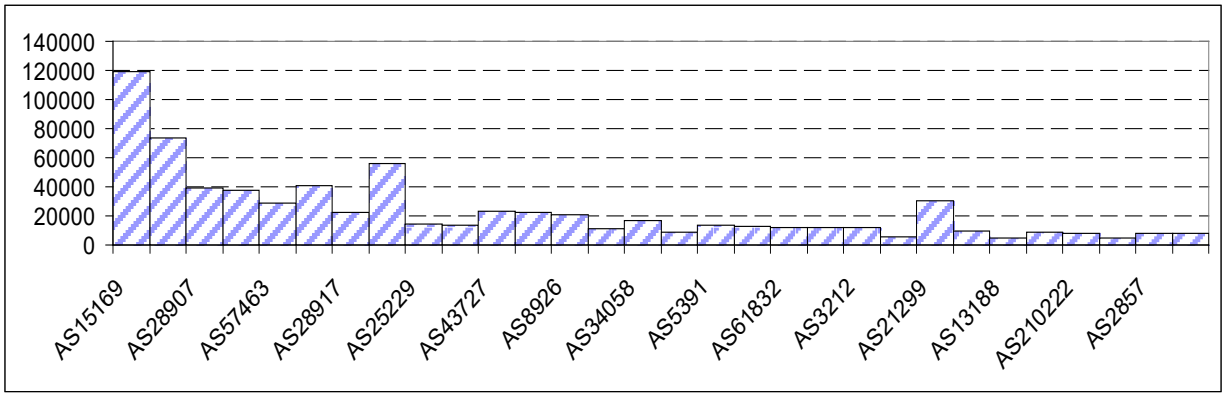


Рисунок 6.3.3 – Графік розподілу ризику серед 100 AS з максимальною метрикою значущості. Збережено впорядкування за значенням метрики значущості. Вісь ординат – ризик *R*

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.6.3.4).

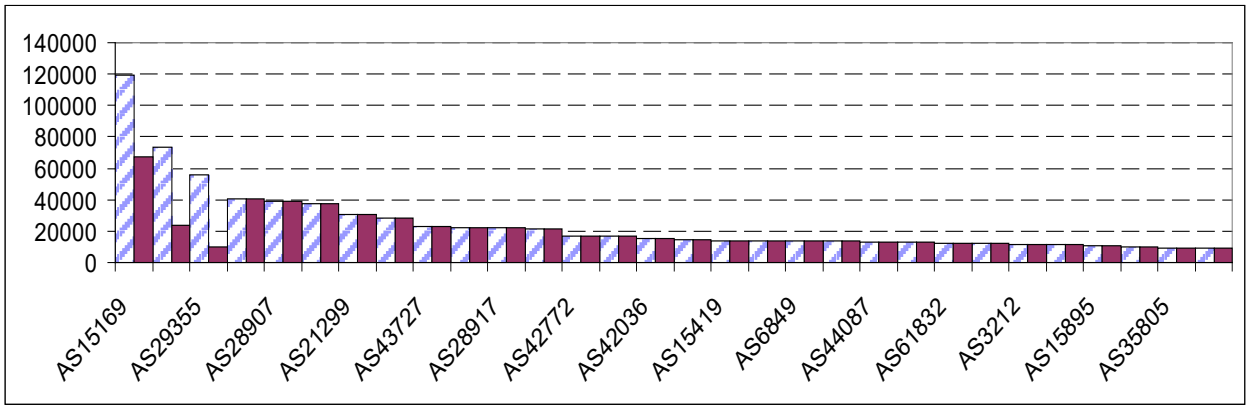


Рисунок 6.3.4 – Порівняння зниження ризику за рахунок моделювання прямих з'єднань з трьома «концентраторами ризику». Вісь ординат – ризик *R*, вісь абсцис – ідентифікатор AS

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.

6.3.2. Аналіз впливу на топологію приєднання великого оператора до мережі обміну трафіком

Станом на квітень 2013 р. в UA-IX приймали участь 132 прямі учасники, що безпосередньо підключені до цієї мережі. Вони обмінювались через UA-IX анонсували маршрути до майже 7000 мереж (чи «мережевих префіксів»), які

походять від 1984 вузлів – автономних систем, що з'єднані 2240 безпосередніми зв'язками.

Станом на жовтень 2016 року параметри UA-IX суттєво змінились. Так, кількість учасників зросла до 197, з'явились деякі досить великі учасники, такі як Google, Akamai, Яндекс та Mail.ru. В табл.6.4.1 наведені характеристики моделі UA-IX, побудованої за даними таблиць маршрутизації. Показане порівняння характеристик 2013 та 2016 року (до включення Hurricane Electric).

В UA-IX базовою і обов'язковою політикою маршрутизації є так званий «відкритий пірінг», тобто обов'язкова передача всіх маршрутів на центральний вузол і отримання всіх маршрутів інших учасників.

Таблиця 6.4.1 – Характеристики моделі UA-IX в 2013 та 2016 роках.

№	Назва параметра	2013	2016
1	Кількість прямих учасників	132	172
2	Кількість префіксів	6867	17926
3	Кількість AS, що є джерелами анонсів	1984	3469
4	Загальна кількість AS, що зустрічаються в шляхах	n/a	3535
5	Діаметр мережі	9	9
6	Кількість тупикових вузлів	1677	2689
7	Кількість транзитних вузлів	307	845
8	Середній коротший шлях	4,05	5,25

В листопаді 2016 року до мережі UA-IX приєднався міжнародний оператор Hurricane Electric, ідентифікатор AS 6939, який згадувався в 5 розділі для оцінки методики розрахунку метрики значущості. Цей оператор за багатьма даними (довжина власних мереж, кількість підключених мереж, обсяги трафіку) належить до провайдерів першого рівня (Tier 1 providers). За опублікованими відкритими даними проекту Center for Applied Internet Data Analysis (CAIDA), він безпосередньо взаємодіяв у 2016 році з приблизно 5000 автономними системами. Повна кількість префіксів, якими оперує цей провайдер, достаменно невідома, бо в різних мережах обміну трафіком він анонсує різні множини префіксів.

Hurricane Electric анонсував в мережу UA-IX 39540 префіксів, збільшивши їхню загальну кількість до понад 57000, тобто більш ніж втричі. За даними таблиці маршрутизації побудовано модель сегменту мережі, що приєдналась до UA-IX. Її характеристики наведені в табл.6.4.2.

Отже, цей сегмент подібний з характеристиками до UA-IX, але дещо щільніший, що відображується більшою транзитивністю (середній показник коефіцієнта кластеризації по мережі) та меншим середнім шляхом. Співвідношення транзитних та тупікових AS є приблизно однаковим. На рис. 6.4.1 та 6.4.2 продемонстрована різниця, як виглядало ядро (група вузлів з найбільшою кількістю зв'язків) мережі UA-IX до приєднання Hurricane Electric,

та ядро мережі Hurricane Electric, що було побудовано за даними таблиці маршрутизації.

Таблиця 6.4.2 – Характеристики сегменту Інтернет, що приєднався до UA-IX після підключення Hurricane Electric

№	Назва параметра	Значення
1	Кількість прямих учасників, підключених до Н.Е.	1028
2	Кількість префіксів	39540
3	Кількість AS, що є джерелами анонсів	5172
4	Загальна кількість AS, що зустрічаються в шляхах	5255
5	Діаметр мережі	9
6	Кількість тупикових вузлів	4213
7	Кількість транзитних вузлів	1043
8	Середній коротший шлях	4,17

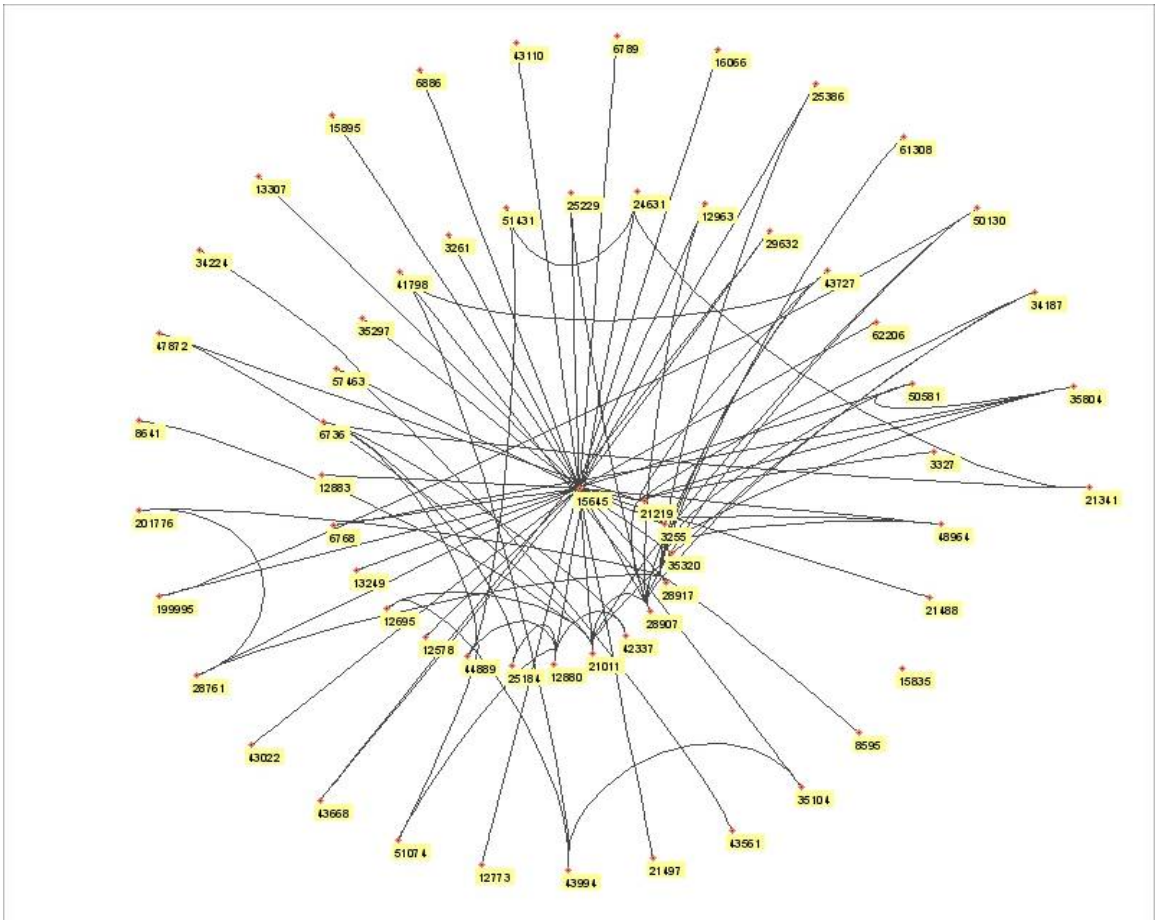


Рисунок 6.4.1 – Ядро ядро мережі Hurricane Electric

Таким чином, мережа UA-IX з моменту підключення AS6939 наче охоплює втричі більшу кількість вузлів. Протягом тижня велись спостереження за навантаженням трафіком підключення Hurricane Electric в UA-IX.

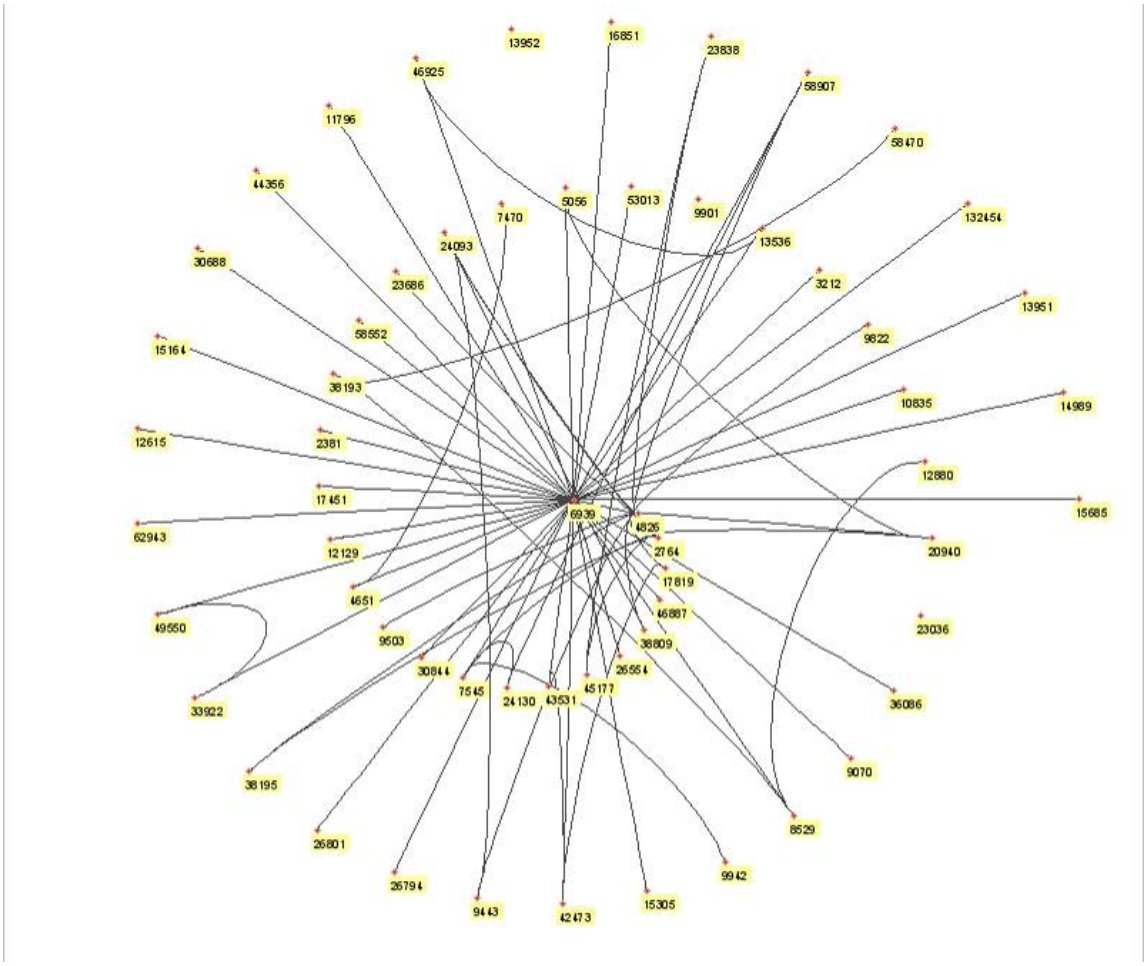


Рисунок 6.4.2 – Ядро ядро UA-IX до приєднання Hurricane Electric

Було з’ясовано, що середньодобовий вхідний та вихідний трафік не перевищують 3 Гбіт/с. Цей обсяг є дуже незначним порівняно з відомими українськими Інтернет-провайдерами. Наприклад, Датагруп (AS 21219) надсилає всього 928 префіксів, що походять від 344 автономних систем, продукує в декілька разів більше трафіку (рис.6.4.1 – 6.4.3).

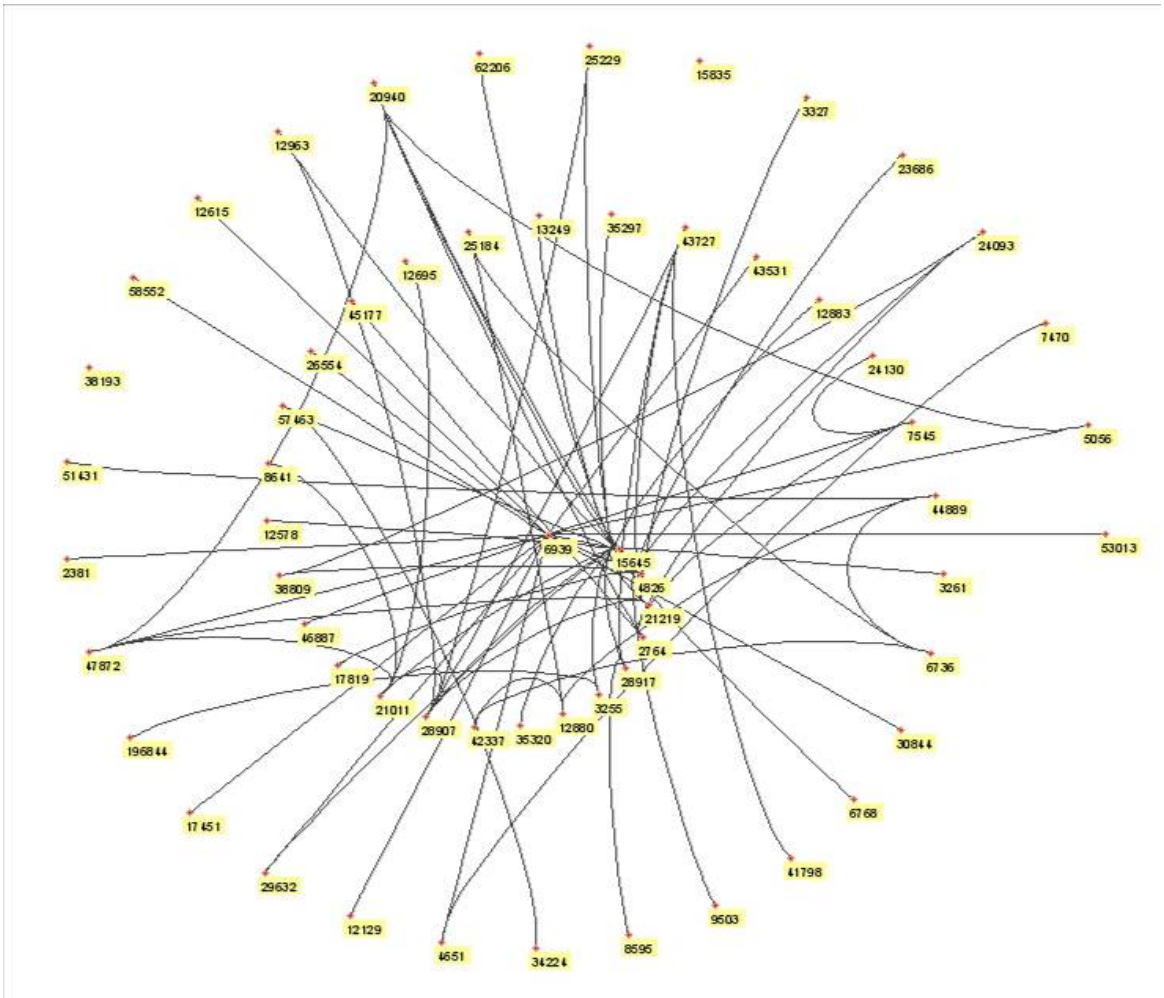


Рисунок 6.4.3 – Ядро мережі UA-IX після включення Hurricane Electric.

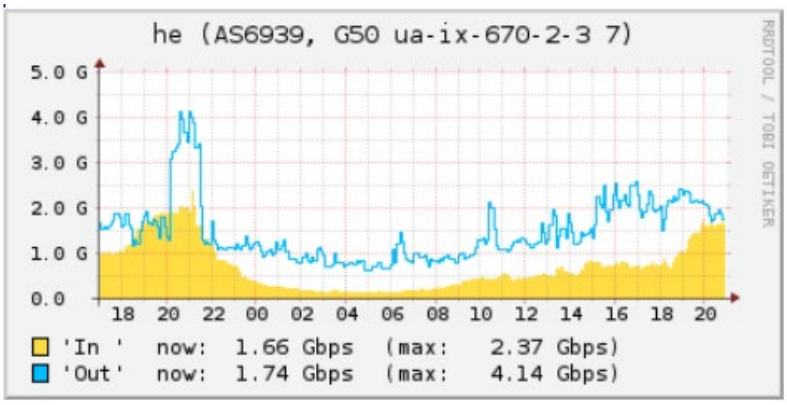


Рисунок 6.4.4 – Денний графік трафіку в UA-IX від Hurricane Electric

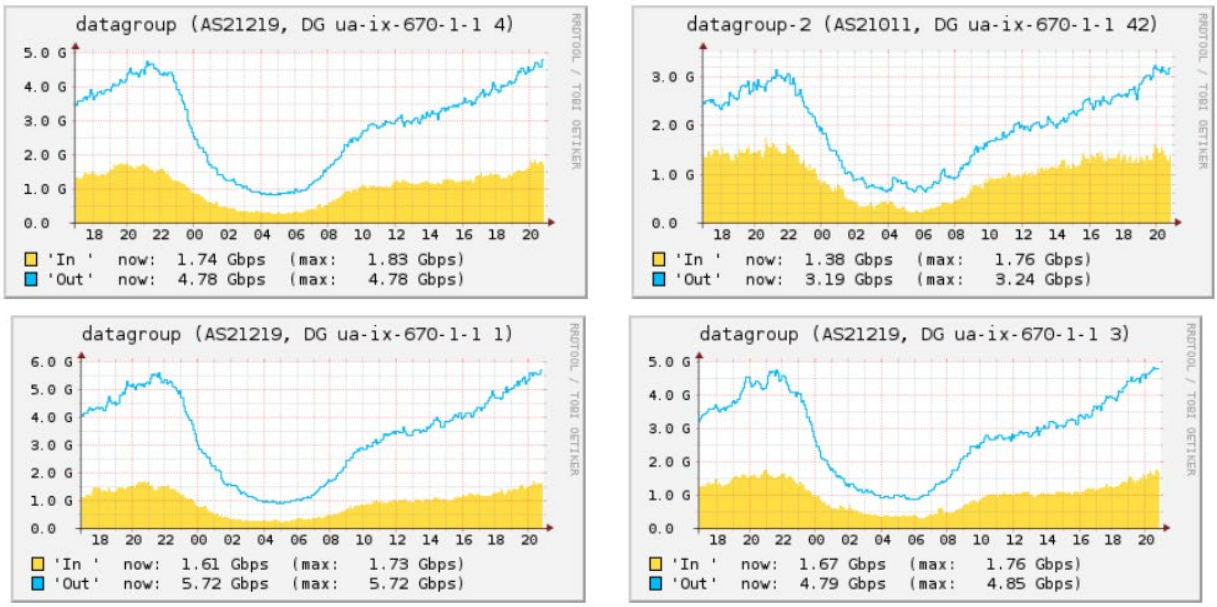


Рисунок 6.4.5 – Денний графік трафіку в UA-IX від операттора Датагруп (включення чотирма портами)

Це наштовхує на необхідність аналізу структури сегменту мережі, що підключений за Hurricane Electric, а також прогнозам використання цього підключення для певних категорій Інтернет-споживачів.

Проаналізуємо склад ядра мережі Hurriacane Electric. Він наведений в табл.6.4.3.

Таблиця 6.4.3. Опис основних мереж, що анонсуються в Hurricane Electric.

№	Номер AS	Назва, країна та основний регіон обслуговування	Кількість зв'язків	Кількість префіксів
1	6939	Hurricane Electric (Північна Америка, Південно-східна Азія, Австралія)	1029	39540 транзит, 147 власні
2	46887	Lightower (Північна Америка)	407	1126 транзит, 211 власні
3	4826	Vocus Connect Intl (Австралія)	273	4305 транзит, 102 власні
4	2764	AAPT Limited (Австралія, Нова Зеландія)	174	1939 транзит, 351 власні
5	26554	US Signal Company (Північна Америка)	84	414 транзит, 38 власні
6	7470	TrueInternet (Таіланд, Півд-Сх. Азія)	75	667 транзит, 299 власні

Перша п'ятірка за кількістю транзитних префіксів є також першою п'ятіркою за кількістю зв'язків з іншими автономними системами. Отже, це досить великі регіональні хаби. Але вони обслуговують специфічні регіони: Північну Америку, Південний Схід, Австралію та Нову Зеландію.

Вони, крім взаємодії з Hurricane Electric, є учасниками інших мереж обміну трафіком, зокрема європейських. Тому, попри анонси їхніх префіксів в

UA-IX, коротші маршрути досить часто пролягають не через UA-IX, а через інші евпропейські мережі обміну трафіком.

6.3.3. Аналіз та підвищення захищеності топології за рахунок приєднання до двох мереж обміну трафіком

Наприкінці двотисячних років мережа обміну трафіком UA-IX перестала бути монопольною мережею обміну трафіком, коли з'явилась мережа Digital Telecom IX (DTEL-IX), що на даний час налічує понад 211 учасників, а середньодобовий трафік складає 1.2 Тбіт/с. DTEL-IX не є єдиною точкою обміну Інтернет-трафіком в Україні, що пропонує послугу публічного пірінгу. Для залучення у якості клієнтів суттєвої кількості невеликих операторів та провайдерів, які вже є учасниками іншої точки обміну трафіком, було використано методологію оцінювання топології зв'язків за захищеністю від потенційного впливу атак типу «перехоплення маршруту» чи «витік маршруту».

Керівництво DTEL-IX висловило зацікавленість в аналізі захищеності мережевих префіксів учасників та порівнянні ризику перехоплення маршруту в кожній з мереж обміну трафіком, а також в більш складному експерименті із підключенням одного учасника до двох мереж одночасно і впливом такого підключення на захищеність мережевих префіксів такого учасника. Для цього персоналом DTEL-IX було надано BGP-таблицю публічного піринга [171], яка доступна типовому учаснику такого піринга в DTEL-IX. За цими даними було розраховано метрики значущості і довіри, а також розподіл ризику по вузлах, видимих в DTEL-IX.

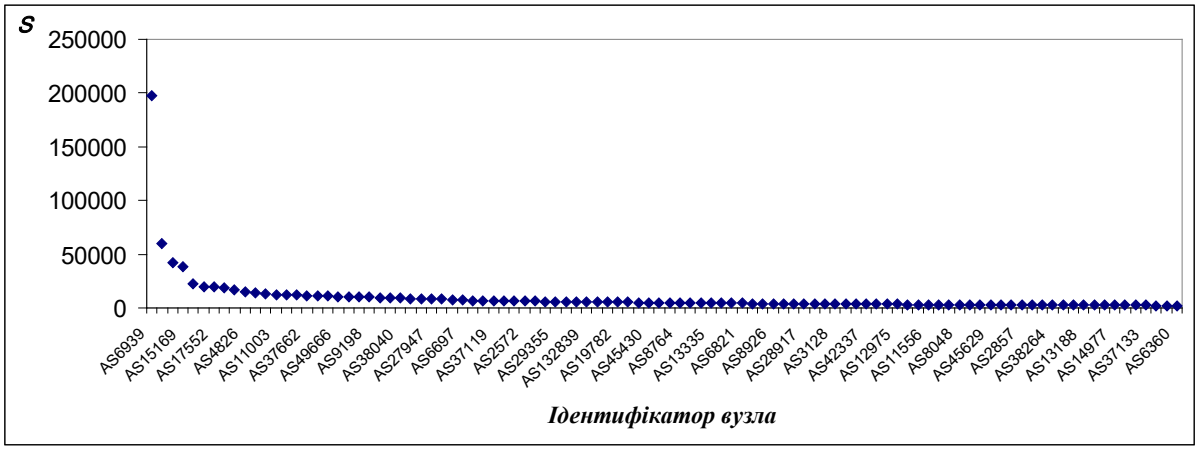


Рисунок 6.3.5 – Графік розподілу за зменшенням значущості серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика значущості *S*

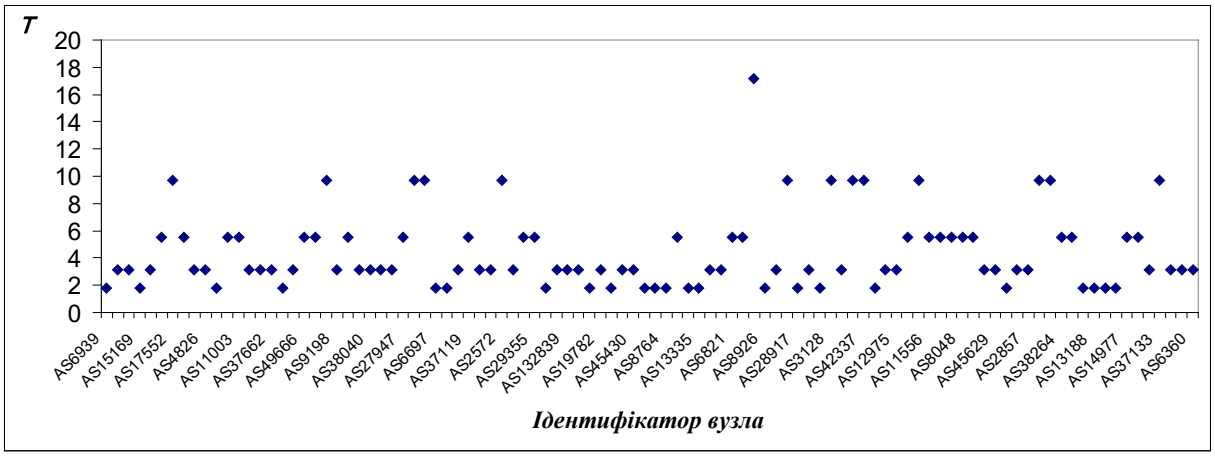


Рисунок 6.3.6. Графік розподілу за метрикою довіри серед 100 AS з максимальною метрикою значущості. Вісь ординат – метрика довіри в логарифмічній формі

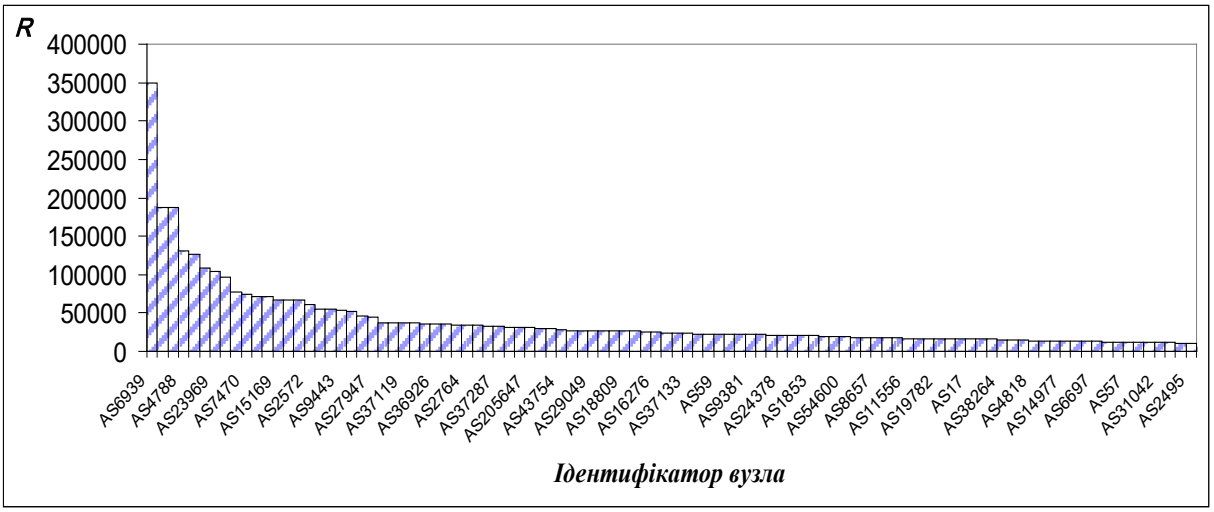


Рисунок 6.3.7 – Графік розподілу ризику серед 100 AS з максимальною метрикою значущості. Впорядкування – за ризиком *R*

Згадана в підрозділі 6.1 AS8258 є учасником UA-IX, але не є учасником DTEL-IX. Шляхом моделювання присутності AS8258 в вільному обміні маршрутами DTEL-IX проведено аналіз очікуваного підвищення захищеності маршрутів AS8258 від перехоплення. Для цього отриману таблицю маршрутів з публічного піринґу DTEL-IX об'єднано з раніше отриманою з вузла AS8258 таблицею маршрутів публічного пірінґу в мережі UA-IX. В таблиці публічного піринґу UA-IX знайдено 7647 унікальних шляхів, DTEL-IX – 21534. Після злиття в сумарній таблиці – 25768 унікальних шляхів.

Результати оцінювання початкового ризику R_1 та порівняння з ризиком нової топології R_2 у числовій формі для 100 вузлів з максимальним початковим ризиком наведено в Додатку.

На рис. 6.3.8 представлено ризик перехоплення маршрутів AS8258 на основі аналізу 50 вузлів з таблиці маршрутизації публічного піринґу в UA-IX (ряд R1) та на основі аналізу 50 вузлів з таблиці маршрутизації, отриманої в наслідок злиття з DTEL-IX (ряд R2).

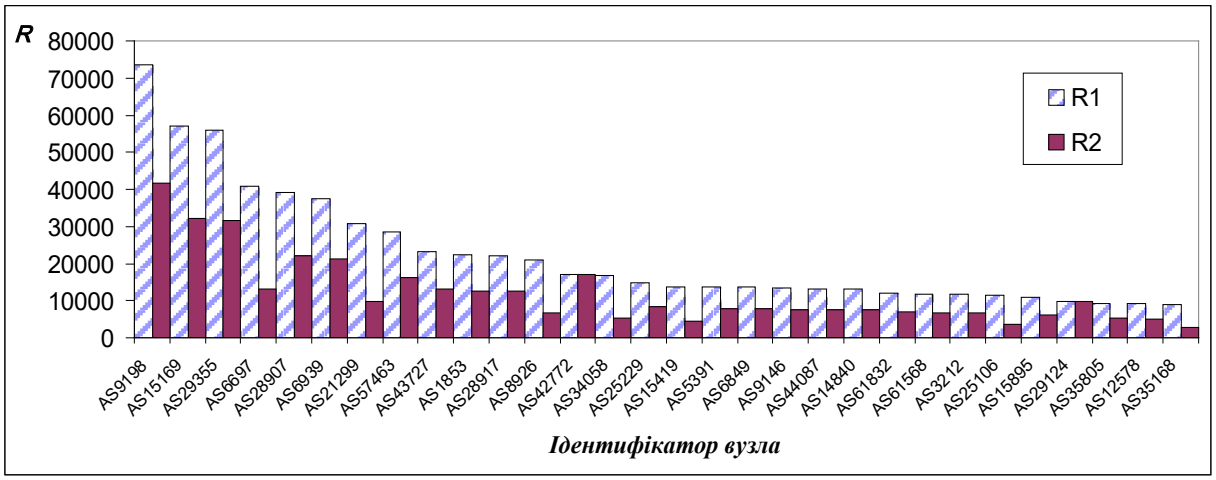


Рисунок 6.3.1 – Ризик перехоплення маршрутів AS8258 на основі аналізу 50 вузлів з таблиці маршрутизації публічного пірингу в UA-IX (R1) та після злиття з таблицею DTEL-IX (R2)

Ризик перехоплення маршруту для початкової топології, де AS8258 є лише учасником UA-IX, становить $R1 = 8{,}14 \cdot 10^5$. Моделювання приєднання AS8258 до обміну маршрутами в DTEL-IX фактично є додаванням всього одного зв'язку, та через це для AS8258 стали доступними майже 20 тисяч нових маршрутів. Це вплинуло на середню відстань до AS8258 в мережі і, відповідно, на метрику довіри. Можна спостерігати, що ризик знизився майже відносно кожного вузла, а сумарний ризик для нової топології становить $R2 = 4{,}24 \cdot 10^5$ – вдвічи менше за початковий.

ЗАКЛЮЧЕННЯ

В даній роботі нам вдалось представити та теоретично обґрунтовати розв’язання актуальної науково-прикладної проблеми підвищення захищеності інформації проти кібератак на глобальну маршрутизацію в комп’ютерній мережі Інтернет на основі ризик-орієнтованого підходу. Для цього було досліджено сучасний стан, архітектуру та топологію Інтернет. В результаті досліджень було встановлено, що що принципи, на яких базується система глобальної маршрутизації, є ключовими в забезпеченні масштабованості комп'ютерної мережі, водночас, недоліки системи глобальної маршрутизації сприяють поширенню кіберінцидентів з перехопленням маршрутів.

Особливістю і важливою перевагою маршрутизації в Інтернеті і взагалі мережах, що функціонують на базі протоколів TCP/IP, є спосіб вирішення складної обчислювальної задачі пошуку оптимального маршруту. Останні три десятиліття безперервного зростання Інтернет і розвитку технологій, що базуються на використанні Інтернет, безумовно показали масштабованість системи глобальної маршрутизації. У той же час, разом з масштабами мережі зростають загрози інформаційній безпеці, пов'язані з глобальною маршрутизацією. Дані загрози відносяться до всіх суб'єктів, чиї інформаційні активи взаємодіють з глобальною комп'ютерною мережею Інтернет. Вади інформаційної безпеки протоколу глобальної маршрутизації BGP-4 експлуатуються при атаках на маршрутизацію.

Розвиток інструментів на базі RPKI може реально вирішити проблему безпеки системи маршрутизації тільки при достатньому рівні впровадження. Зусилля окремого провайдера мають несуттєвий вплив у поліпшення системи глобальної маршрутизації і ще менш суттєвий – у поліпшення безпеки власних мережевих префіксів.

Загалом, в результаті аналізу виявлено чимало факторів, які ставлять під сумнів можливість надійного захисту системи глобальної маршрутизації. Тому для розроблюваних теоретичних засад, методів та практичних реалізації сформульовано наступні вимоги:

- універсальність: теоретичні засади та методи, що розробляються, мають бути дієвимі в разі застосування для будь-якого суб’єкта глобальної маршрутизації;
- безмасштабність: розроблювані методи мають демонструвати ефективність незалежно від того, скільки учасників глобальної маршрутизації їх використовують;
- автономність: необхідно, щоб розроблювані методи підвищення захищеності топології для одного суб'єкта глобальної маршрутизації відбувались без втручання в діяльність інших суб'єктів;
- непротирічність: необхідно, щоб розроблювані методи підвищення захищеності топології не вступали у протиріччя з існуючими,

згаданими вище, та могли доповнювати їх, не знижуючи їхню ефективність;

– сучасність: теоретичні засади та практичні методики підвищення захищеності системи глобальної маршрутизації мають роздивлятись в аспекті менеджменту ризиків інформаційної безпеки.

Топологією комп'ютерної мережі називають структуру у вигляді графа, яка може представити взаємодію елементів мережі як на так званому фізичному рівні (де демонструються розташування пристроїв та маршрути прокладання кабелів), так і на логічному, де описуються потоки даних. Оскільки відомо, що Інтернет є об'єднанням комп'ютерних мереж, і сутність його саме в цьому об'єднанні за принципами загальної логічної адресації та маршрутизації, варто розглядати «топологію Інтернет» саме на логічному рівні, де описуються потоки даних.

Основні проаналізовані дослідження не дають визначення топології Інтернет, натомість вважають топологією Інтернету щось само собою зрозуміле – з'єднання на рівні AS. Відсутність конкреного визначення топології Інтернет як поняття, та, водночас, проведення дослідження топології Інтернет, є протиріччам, що є перепоною на шляху пошуку нових методів захисту від кібернетичних атак на систему глобальної маршрутизації.

В другій главі запропоновано варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет, що утворений системою глобальної маршрутизації на множині з'єднань між вузлами, та послідовно обґрунтовано, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію Інтернету, а вразливості протоколу BGP-4 як основного елементу системи глобальної маршрутизації є вразливостями топології.

Кібернетичні атаки, вектором яких є система глобальної маршрутизації, спотворюють топологічний простір певного мережевого префіксу шляхом пропонування BGP-системам неіснуючих з'єднань, або приховуючи існуючі. Таким чином, захист системи глобальної маршрутизації є захистом топологічного простору, кожного окремого мережевого префікса в цьому просторі, шляхом зменшення ризику його спотворення в наслідок зумисних дій. При цьому критерієм захищеності топології пропонується оцінка ризику як міра захищеності інформації.

Інциденти з перехопленням маршрутів в глобальній Інтернет-маршрутизації – це результати помилки новачка, нездатність великих операторів підтримувати в актуальному стані свої фільтри маршрутів, та, безумовно, результати кібератак. З систематизованих даних можна пересвідчитись, що дедалі росте доля очевидних зумисних дій, спрямованих на скоєння атак на глобальну маршрутизацію, а наслідки атак стають більш глобальними. В якості об'єкту захисту ми розглядаємо певний інформаційний актив, функціонування якого пов'язане з Інтернет, а власником ризику є власник чи розпорядник цього активу (очевидно, що взаємодію інформаційного активу з Інтернет забезпечує інформацчйно-комунікаційна система).

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

Отримані додаткові характеристики поршника використано не тільки для уточнення моделі порушника, а і для уточнення моделі загроз інформаційному активу. Розвинуто відому модель оцінювання ризику інформаційної безпеки DREAD за рахунок уточнення складових ризику - загроз, які, в свою чергу, мают бути оцінені за методом STRIDE. Нова двовимірна модель «STRIDExDREAD» дозволяє суттєво уточнити оцінку ризику і тим самим підвищити якість рішень, що приймаються з питань кібербезпеки.

Хоча на цей час існує певна кількість моделей системи глобальних маршрутизації, попередні роботи аналогічного змісту в основному спирались на неформальні та часто суперечливі визначення. Для того, щоб мати міцну базу для широкого спектру майбутніх аналізів маршрутизації в мережі Інтернет, в даному розділі запропоновано нову модель глобальної маршрутизації, яка концептуально базується на описі суб'єктів, об'єктів системи глобальної маршрутизації та відносин між ними за допомогою формальної мови.

Для формалізації ризику широко використовують моделі, які пов'язують між собою ймовірність виникнення негативних подій і можливих збитків у результаті цих подій. Можна отримати залежність ризику перехоплення маршрутів до вузла від його положення відносно інших вузлів. Відстань між вузлами, кількість транзитних маршрутів, кількість власних префіксів і ще деякі фактори впливають також і на умовну «зону ураження» – ареал розповсюдження хибного маршруту. Отже, відношення між вузлами повинні мати певні метричні характеристики, що характеризували б ризик перехоплення маршруту між ними як принаймні одну з двох складових ризику – ймовірності перехоплення або розміру збитків.

Відомі характеристики, які походять з топології складних мереж, не можуть бути використані для оцінки ризику перехоплення маршруту, оскільки не характеризують складові цього ризику. Було розроблено власні метричні характеристики мережі, що отримали назву «метрика значущості» та «метрика довіри». Вони походять з топологічних характеристик вузлів та характеризують безпосередні складові ризику перехоплення.

Розроблено ризик-орієнтовану модель топологічного простору Інтернет, яка базується на запропонованих метричних характеристиках, та дає

можливість порівняння різних топологій за рівнем захищеності шляхом розрахунку оцінки ризику перехоплення маршруту. Така модель адекватність моделі для відображення характеристик вузлів з точки зору оцінювання ризику і дає можливість порівняння топологій за рівнем захищеності.

Запропонований розвиток теоретичних засад формування метричних характеристик для оцінювання захищеності системи глобальної маршрутизаці дозволив сформулювати такі метричні характеристики мережевих вузлів, які відображають обидві складові ризику перехоплення маршруту – ймовірність перехоплення маршруту до певного мережевого префікса та масштаб впливу перехоплення на топологічний простір мережевого префіксу. Ці метрики покладено в основу ризик-орієнтованої моделі топології Інтернет, яка дає можливість порівняння різних топологій за рівнем захищеності шляхом розрахунку оцінки ризику перехоплення маршруту.

Запровадження оцінки ризику кібератак на систему глобальної маршрутизації розширює розширенню критерії ефективності топології, що дає подальший розвиток методиці формування ефективних міжвузлових зв'язків комп'ютерної мережі Інтернет. Оже, природно, шо ми запропонували підходи до створення програмних засобів розрахунку ризику перехоплення маршруту в топологічному просторі окремого мережевого префіксу, моделювання нової топології та оцінювання результатів. Запропонована методика оцінювання ризику перехоплення маршруту до інформаційного активу дозволяє автоматизувати аналіз топології, розрахунок ризику перехоплення маршруту в топологічному просторі окремого мережевого префіксу та моделювання нової топології для підвищення захищеності мережевого префікса від атак на систему глобальної маршрутизації.

Методика підвищення захищеності від кібернетичних атак на систему глобальної маршрутизації призначена для формування ефективної топології мережевого префікса. Критерієм ефективності є оцінка ризику кібератак на систему глобальної маршрутизації. Методика складається з двох етапів: розрахунку оцінок ризику перехоплення маршруту та моделювання змін топології. В ході дослідження було проведено експерименти на реальних даних з глобальної таблиці маршрутизації отриманих від декількох різних автономних систем. Було отримано розподіл вузлів за метрикою значущості, визначено розподіл метрики довіри, продемонстровано її вплив на ризик. Ризики перехоплення на окремих вузлах можна просумувати і отримати інтегральний ризик для всієї мережі. В результаті експериментів, проведених з реальними таблицями глобальної маршрутизації, отримано емпіричне підтвердження того, що мінімальні зміни в топології, запроваджені власником інформаційного активу в інтересах підвищення захищенності від атак типу «перехоплення маршруту» здатні суттєво вплинути на ризик перехоплення маршруту. Вибір нової топології є складною комбінаторною задачею, для дозв'язання якої вже існує чимало точних та наближених методів.

Таким чином, представлені дані емпіричних досліджень свідчать про результативність запропонованої методики, а отже, і теоретичних результатів, що покладено в її основу, для підвищення захищеності топології зв'язків

певного вузла Інтернет від кібератак, вектором яких є перехоплення маршруту до мережевих префіксів, що належать цьому вузлу. Експерименти продемонстрували ефективність застосування власниками комп'ютерних систем та мереж, функціонування яких пов'язане з Інтернетом, запропонованого програмного засобу автоматизації дослідження захищеності топології, а саме – зниження ймовірності та наслідків успішного проведення кібернетичних атак, вектором яких є система глобальної маршрутизації. У додатках наведено відповідні документи, що підтверджують практичне значення та впровадження отриманих результатів.

Методика оцінювання ризиків інформаційної безпеки, що спричинені кібернетичними атаками, вектором яких є система глобальної маршрутизації Інтернет, а також підвищення захищеності інформаційних активів від таких атак, має стати важливим доповненням до відомих рекомендацій та належних практик кіберзахисту інформаційних активів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Y.Rekhter, D. Estrin, and S.Hots. A Unified Approach to Inter-Domain Routing. [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc1322. Дата доступу: Чер.29, 2018.

[2] Hawkinson, J., Bates, T. Guidelines for creation, selection, and registration of an Autonomous System (AS). IETF. sec. 3. March, 1996. DOI:10.17487/RFC1930.

[3] Y.Rekhter, T.Li and S.Hares. A Border Gateway Protocol 4 (BGP-4). [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc4271. Дата доступу: Чер.29, 2018.

[4] G. Huston. "Why Securing BGP is So Damn Hard". [Електронний ресурс] Режим доступу: https://blog.apnic.net/2019/09/19/why-is-securing-bgp-just-so-damn-hard/. Дата звернення: Sep.15, 2019.

[5] Cybercrime Magazine (2018), "Global Ransomware Damages Predicted To Exceed $5 Billion In 2017". [Електронний ресурс] Режим доступу: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/. Дата звернення: Тра.05, 2018.

[6] Internet Security Threat Report 2018. [Електронний ресурс]. Доступно: https://www.symantec.com/security-center/threat-report. Дата звернення: Тра.10, 2018.

[7] K. Sriram, D. Montgomery, et al. "Problem Definition and Classification of BGP Route Leaks". [Електронний ресурс] Режим доступу: https://www.rfc-editor.org/rfc/rfc7908.html. Дата звернення: Тра.05, 2018.

[8] Pilosov, A. and T. Kapela, "Stealing The Internet. An Internet-Scale Man In The Middle Attack". Defcon 16, Las Vegas, NV – 2008. [Електронний ресурс] Режим доступу: https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf/. – Дата звернення: Жов.1, 2019.

[9] Zhou S. The Rich-club Phenomenon in the Internet Topology / S. Zhou // Communication Letters, IEEE. – 2004. – Vol.8, issue 3. – С.180-182.

[10] P.Sermpezis, V. Kotronis, P. Gigis et al., "ARTEMIS: Neutralizing BGP HijackingWithin a Minute". IEEE/ACM Transactions On Networking . – 2018. – DOI:10.1109/TNET.2018.2869798

[11] G. Chaviaras, P. Gigis et al. "ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking". SIGCOMM '16: Proceedings of the 2016 ACM SIGCOMM Conference. – 2016. – Pages 625–626. – DOI:10.1145/2934872.2959078

[12] M.Lepinski, S.Kent, "An Infrastructure to Support Secure Internet Routing". Request for Comments: 6480. – [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc6480 – Дата звернення: Жов.10, 2018.

[13] RIPE NCC. BGP Origin Validation. [Електронний ресурс] Режим доступу: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/bgp-origin-validation. Дата звернення: Чер.29, 2018.

[14] "Eliminating opportunities for traffic hijacking". Qrator.Radar Blog. – 2019. – [Електронний ресурс] Режим доступу: https://radar.qrator.net/blog/eliminating-traffic-hijacking_36. – Дата звернення: Чер.2, 2019.

[15] MERIT. List of Routing Registries. [Електронний ресурс] Режим доступу: http://www.irr.net/docs/list.html. Дата звернення: Чер.29, 2018.

[16] G.Huston, G.Michaelson, “Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)”. Request for Comments: 6483. – [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc6483 – Дата звернення: Жов.10, 2018.

[17] P. Mohapatra, J. Scudder et al., “BGP Prefix Origin Validation”. Request for Comments: 6811. – [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc6811 – Дата звернення: Жов.10, 2018.

[18] NTT Peer Locking Technical Details. [Електронний ресурс] Режим доступу: http://instituut.net/~job/peerlock_manual.pdf. – Дата звернення: Бер.10, 2019.

[19] Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization. https://tools.ietf.org/id/draft-ietf-sidrops-aspa-verification-05.html

[20] RPKI ROA Deletion: Post-mortem. [Електронний ресурс] Режим доступу: https://www.ripe.net/ripe/mail/archives/routing-wg/ 2020-April/004072.html. – Дата звернення: Кві.21, 2020).

[21] This is how you deal with route leaks. Qrator Labs corporate blog. . [Електронний ресурс] Режим доступу: https://habr.com/en/company/qrator/blog/495260/ . – Дата звернення: Кві.21, 2020.

[22] Russian Telco Hijacked Internet Traffic of Major Networks – Accident or Malicious Action? [Електронний ресурс]. – Режим доступу: https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action. – Дата звернення: Кві.21, 2020.

[23] SIDR BOF Agenda – IETF 64 [Електронний ресурс]. Доступно: https://tools.ietf.org/agenda/64/sidr.html. – Дата доступу: Тра.13,2020.

[24] M.Lepinski, K.Sriram. BGPsec Protocol Specification [Електронний ресурс]. Доступно: https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-23. – Дата доступу: Тра.13,2020.

[25] K.Sriram. BGPsec Design Choices and Summary of Supporting Discussions Specification [Електронний ресурс]. Доступно: https://tools.ietf.org/html/rfc8374. – Дата доступу: Тра.13,2020.

[26] Ke Wang. Anomalous Payload-Based Network Intrusion Detection / Ke Wang, Salvatore J. Stolfo // RAID 2004: Recent Advances in Intrusion Detection. – Pages 203-222

[27] A.S.Syed Navaz. Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud / A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi // International Journal of Computer Applications (0975 – 8887). – Vol.62. – No.15. – Jan.2013

[28] Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) : ДСТУ ISO/IEC 27001:2015. – К.:УкрНДНЦ. – 2016. – 22с.

[29] Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments [Електронний ресурс]. Доступно: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ /nistspecialpublication800-30r1.pdf. – Назва з екрану. – Дата доступу:Бер.01,2019.

[30] A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies (Recommendation ITU-T X.1208). – Женева. – 2014.

[31] Закон України «Про основні засади забезпечення кібербезпеки України». – К.: Відомості Верховної Ради. – 2017. – № 45. – с.403.

[32] В. Г. Олифер, Н. А. Олифер. 54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд, 2006

[33] He Y., Siganos G., Faloutsos M., “Internet Topology” In: Meyers R. (eds) Encyclopedia of Complexity and Systems Science. Springer. – 2009.

[34] K. L. Calvert, M. B. Doar and E. W. Zegura, "Modeling Internet topology," in IEEE Communications Magazine, vol. 35, no. 6, pp. 160-163, June 1997, doi: 10.1109/35.587723

[35] Faloutsos M. On Power Law Relationships of the Internet Topology / Faloutsos M., Faloutsos P., Faloutsos C .// Comput. Commun. Rev. – 1999. – №.29. – С.251-263

[36] Krioukov D. The Internet AS-Level Topology: Three Data Sources and One Definitive Metric / D. Krioukov // SigComm Computer Communication Review. – Vol.36,issue 1. – С.17-26.

[37] Newman M. The structure and function of complex networks / M.E.J. Newman // SIAM Review. – 2003. – Vol.45. – С.167–256.],

[38] Barabasi A.-L. Scale-Free Networks / A.-L. Barabasi, E. Bonebau // Scientific American. – 2003.- Vol.5. – С.50-59.

[39] Живицкая Е. Топологические свойства сложных логистических систем / Е.Н. Живицкая // Доклады БГИУР. – №8. – 2012.

[40] Інтернет [Електронний ресурс]. Доступно: https://uk.wikipedia.org/wiki/Інтернет/ – назва з екрану. Дата доступу: Жов.1,2020.

[41] Risk Management – Vocabulary (ISO Guide 73:2009, IDT) : ДСТУ ISO Guide 73:2013. – К. : Мінекономрозвитку України. – 2014. – 13с.

[42] Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ISO/IEC 27005:2018, IDT) : ДСТУ ISO/IEC 27005:2019

[43] Information technology – Security techniques – Evaluation criteria for IT security. Part 1: Introduction and general model (ISO/IEC 15408-1:2009)

[44] Vincent J. Bono. 7007 Explanation and Apology. [Електронний ресурс] Режим доступу: https://seclists.org/nanog/1997/Apr/444. Дата звернення: Лип.12,2019.

[45] Larry J. Blunk. New BGP analysis tools and a look at the AS9121 Incident. – Merit Network, Inc. – IEPG Meeting – 62nd IETF. – Minneapolis. – March 6, 2005.

[46] YouTube Hijacking: A RIPE NCC RIS case study (назва з екрана) [Електронний ресурс]. Доступно: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (Дата звернення: 21.04.2020)

[47] This is how you deal with route leaks. Qrator Labs corporate blog. Information Security, Network technologies. URL: https://habr.com/en/company/qrator/blog/495260/ (Дата звернення: 21.04.2020)

[48] Russian Telco Hijacked Internet Traffic of Major Networks – Accident or Malicious Action? URL: https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action (Дата звернення: 21.04.2020)

[49] Hijacking Bitcoin: routing attacks on cryptocurrencies. [Електронний ресурс] Режим доступу: https://blog.acolyer.org/2017/06/27/hijacking-bitcoin-routing-attacks-on-cryptocurrencies/. Дата звернення: Гру.1, 2017.

[50] D. Goodin (2017), “Russian-controlled telecom hijacks financial services’ Internet traffic” [Електронний ресурс] Режим доступу: https://arstechnica.com/information-

technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/. Дата звернення: Гру.1, 2019.

[51] BGPStream and Curious Case of AS12389 (назва з екрану) [Електронний ресурс] Режим доступу: https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/. Дата звернення: Гру.1, 2019.

[52] The Next Web (2017), ”Google made a tiny error and it broke half the Internet in Japan” [Електронний ресурс] Режим доступу: https://thenextweb.com/google/2017/08/28/google-japan-internet-blackout/. Дата звернення: Кві.20, 2018.

[53] История одного BGP hijack, или необходимо ли фильтровать full-view от аплинков (назва з екрана). [Електронний ресурс] Режим доступу: https://nag.ru/articles/article/101232/istoriya-odnogo-bgp-hijack-ili-neobhodimo-li-filtrovat-full-view-ot-aplinkov.html. Дата звернення: Січ.20,2019.

[54] Internet Vulnerability Takes Down Google. [Електронний ресурс] Режим доступу: https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/. Дата звернення: Січ.20,2019.

[55] China Telecom's Internet Traffic Misdirection. [Електронний ресурс] Режим доступу: https://internetintel.oracle.com/blog-single.html?id=China+Telecom%27s+Internet+Traffic+Misdirection. Дата звернення: Січ.15,2019.

[56] How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/

[57] Зубок В. Оцінювання ризиків кібернетичних атак на глобальну маршрутизацію в мережі Інтернет // Збірка праць конференції «Моделювання-2018», 12-14 вересня, Київ. – К., «Академперіодика».- с. 147-150.

[58] Буров Є., Комп‘ютерні мережі. Львів. БаК, 1999. – 468 с.

[59] Слепов Н.Н. Современные технологии цифровых оптоволоконных сетей связи (ATM, PDH, SDH, SONET и WDM). – М.: Радио и связь, 2000.

[60] MEF 3 Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks [online]. Available: https://www.mef.net/resources/mef-3-circuit-emulation-service-definitions-framework-and-requirements-in-metro-ethernet-networks/. – Accessed: Oct.10,2020.

[61] MEF 4 Metro Ethernet Network Architecture Framework Part 1: Generic Framework [online]. Available: https://www.mef.net/resources/mef-4-metro-ethernet-network-architecture-framework-part-1-generic-framework/. – Accessed: Oct.10,2020.

[62] Rosen, E., Viswanathan, A., Callon, R. “Multiprotocol Label Switching Architecture (RFC3031)” (назва з екрану) [Електронний ресурс]. Доступно: https://tools.ietf.org/html/rfc3031 . Дата доступу: 01 жовтня, 2019 р.

[63] Хмелёв К. Ф. Основы SDH: Монография. – К.: ІВЦ «Видавництво "Політехніка"», 2003. – 584 с.

[64] Слепов Н.Н. Синхронные цифровые сети SDH. – М.: Эко Трендз, 1997

[65] Dodonov, A. Increasing the survivability of automated systems of organizational management as a way to security of critical infrastructures / A Dodonov, O Gorbachyk, M Kuznietsova // Information Technologies and Security (CEUR-WS). – 2018. – Vol.2318.

[66] Dodonov O. Survivability Mechanisms of Complex Computer Systems Based on Common Information Space / DODONOV O., JIANG B., DODONOV V. // Computer Science. – ISSN:1000-3428. – 2019. – Vol.45. – №7. –p. 41-45. DOI:10.19678/j.issn.1000-3428.0053440

[67] Виро О.Я., Иванов О.А., Нецветаев Н.Ю., Харламов В.М. Элементарная топология. – М.: МЦНМО. – 2010. – 352 с.

[68] John L. Kelley. General Topology . – Dover Books on Mathematics (Reprint Edition). – 2017.- 320p.

[69] Корченко А. Система выявления аномального состояния в компьютерных сетях / А. Корченко // Безпека інформації. – 2012. – № 2. – С. 80-83.

[70] Ланде Д. В. Контури сучасних технологій побудови глобальних інформаційних мереж : метод. посібн. / Д. В. Ланде, В. Ю. Зубок, В. В. Мохор. – К. : Вид-во ІСЗЗІ НТУУ "КПІ", 2009. – 195 с.

[71] Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. - К.: ИПРИ НАН Украины, 2013. - 248 с. ISBN 978-966-2944-96-9.

[72] Юдін О. Підходи до оцінювання ефективності захисту інформації в інформаційно-телекомунікаційних системах на стадії модернізації / О.К. Юдін, М.А. Стрельбіцький // Під заг. ред. ВМ Безрука, ВВ Баранника. – 2017. – 582с.

[73] О. І. Алєнін, А. В. Габінет, О. П. Роковий, С. Г. Стіренко, О. О. Ілляшенко, А. А. Стрєлкіна. Методи та засоби технічного аудиту інформаційної безпеки комп'ютерних систем та мереж / под ред. В.С. Харченко – Министерство освіти та науки України, Національний аэрокосмічний університет ім. М .Є. Жуковського «ХАІ». 2017. – 136 с.

[74] Бондаренко І. Аналіз проблем побудови критичної іт-інфраструктури міністерства / І. Бондаренко, Я. Дорогий, С. Стіренко, Т. Шемсединов // Information Technology and Security. – 2018. – Т.6. – №1. – С.96-107

[75] ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

[76] НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

[77] НД ТЗІ 2.5-004-99. Критерії оцінювання захищеності в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

[78] Грайворонський М. В. Безпека інформаційно-комунікаційних систем : підручник / М. В. Грайворонський, О. М. Новіков. – К. : Вид. група BHV, 2009. – 608 с.

[79] Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model / ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009). – Національний стандарт України. – Чинний. – Наказ №04.08.2017.- №207.

[80] Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements / ДСТУ ISO/IEC 15408-2:2017 (ISO/IEC 15408-2:2008). – Національний стандарт України. – Чинний. – Наказ №04.08.2017.- №207.

[81] Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements requirements / ДСТУ ISO/IEC 15408-3:2017 (ISO/IEC

15408-3:2008). – Національний стандарт України. – Чинний. – Наказ №04.08.2017.-№207.

[82] L. Kohnfelder, P. Garg. The threats to our products. [Електронний ресурс] Режим доступу: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx. Дата звернення: Лют.21,2019.

[83] Howard M., LeBlanc D. Writing Secure Code, 2nd edition. Microsoft Press, 2003, 768 p.

[84] NASA-GB-9719.13: NASA Software Safety Guidebook. NASA Technical Standard. – Washington D.C. National Aeronautics and Space Administration, 2004.

[85] Measuring and Managing Information Risk: A FAIR Approach. (назва з екрана) [Електронний ресурс]. Доступно: https://www.fairinstitute.org/fair-book (Дата звернення: 10.06.2020).

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

[87] Зыков А. Теория конечных графов / А. Зыков // Новосибирск : Наука. – 1969.

[88] Ландэ Д.В., Снарский А.А., Безсуднов И.В. Интернетика: Навигация в сложных сетях: модели и алгоритмы. – М.: Либроком (Editorial URSS), 2009. – 264 с.

[89] Poryev G. CARMA: A Distance Estimation Method for Internet Nodes and its Usage in P2P Networks / G. Poryev, H. Schloss, R. Oechle // Internatonal Journal on Advances in Telecommunications. – 2010. – vol.3. – С.114-128.

[90] Fox G. Peer-to-peer networks // G. Fox / Computing in science & engineering. – 2001, May/June. – С.2-4.

[91] Ткаченко А.А. Математическое моделирование режимов работы сетей с протоколом TCP / Ткаченко А.А. Карпухин А.В., Кобзев В.Г., Грицив Д.И.// Материалы Международной научно-практической конференции «Проблемы инфокоммуникаций» – Харьков: ХНУРЭ, 2013. – с.150-152.

[92] Вишневский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. -512 с.

[93] Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 3-е изд. – СПб.: Питер, 2006 – 958 с.

[94] Хинчин А. Я. Работы по математической теории массового обслуживания. –М.: Физматгиз, 1963. – 236 с.

[95] Клейнрок Л. Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с

[96] Хелеби С., Мак-Ферсон Д., Принципы маршрутизации в Интернет. 2 издание. – М., Издательский дом «Вильямс», 2001. – 448 с.

[97] Березко М.П., Вишневский В.М., Левнер Е.В., Федотов Е.В. Математические модели исследования алгоритмов маршрутизации в сетях передачи данных // Информационные процессы, Том. 1, № 2, 2001. – С. 103-125.

[98] Nakao A. A Routing Underlay for Overlay Networks / A. Nakao, L.Peterson, A. Bavier // SigComm'2003 Proceedings. – 2003. – С.11-18.

[99] Кутузов О.И. Распределенные информационные системы управления. Учебное пособие по курсовому проектированию. / Кутузов О.И. Татарникова Т.М., Петров К.О. – СПб.: СПбГУТ, 2006. – 40 с.

[100] Watts, D. Collective dynamics of "small-world" networks / D.J. Watts, S.H.Strogaz // Nature. – 1998. – Vol. 393. – С.440-442.

[101] Fuller, V., Li, T.: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (назва з екрану) [Електронний ресурс]. Доступно: https://tools.ietf.org/html/rfc4632 . Дата доступу: 01 жовтня, 2019 р.

[102] В. Зубок. Практические аспекты моделирования изменений в топологии глобальных компьютерных сетей // Реєстрація, зберігання і оброб. даних. – 2012.- Т. 14, № 2.

[103] IPv4 and IPv6 AS Core: Visualizing IPv4 and IPv6 Internet Topology at a Macroscopic Scale (назва з екрану) [Електронний ресурс]. Доступно: http://www.caida.org/research/topology/as_core_network/ . Дата доступу: 20 жовтня, 2019 р.

[104] Лосев Ю. «Сравнительный анализ математического аппарата моделирования телекоммуникационных сетей» / Ю.И. Лосев, К.М. Руккас // Системи обробки інформації. – 2007. – вип.8 (66). – с.55-60.

[105] CAIDA, Macroscopic Topology AS-Adjacencies Data set (назва з екрану) [Електронний ресурс]. Доступно: http://www.caida.org/tools/measurement/skitter/as adjacencies.xml.

[106] CAIDA, Router-Level topology Measurements (назва з екрану) [Електронний ресурс]. Доступно: http://www.caida.org/tools/measurement/skitter/router_topology

[107] A.K. Singh, and V.K. Singh, “Formal Modeling of Distance Vector Routing Protocol using Event-B”, Advance in Electronic and Electric Engineering, Volume 3, Number 1 (2013), pp. 91-98.

[108] J. Schlamp, R. Holz, Q. Jacquemart et al., “HEAP: Reliable Assessment of BGP Hijacking Attacks.”, IEEE Journal on Selected Areas in Communications, Vol.34, Iss.6. Available: https://ieeexplore.ieee.org/document/7460217 (Accessed Jan,21,2020).

[109] T. D. Feng, R. Ballantyne, dhe L. Trajkovi. Implementation of BGP in a network simulator. Advanced Simulation Technologies Conference 2004 (ASTC’04). – 2004.

[110] J. Schlamp, M. Wählisch, T. C. Schmidt, at al., “CAIR: Using Formal Languages to Study Routing, Leaking, and Interception in BGP.”, [Onine] Available: https://arxiv.org/abs/1605.00618. – Accessed: Mar,3, 2019.

[111] Мохор В. Функціональне моделювання системи керування ризиком безпеки інформації / В. Мохор, В. Цуркан, Я. Дорогий, О. Крук // Захист інформації. – 2016. – Т. 18, № 1. – С. 74-80.

[112] Мохор В. В. Геометрический подход к оцениванию вероятности приемлемых рисков информационной безопасности / В. В. Мохор, А. О. Бакалинский, В. В. Цуркан // Захист інформації. – 2016. – Т. 18, № 3. – С. 210-217.

[113] A.Jamakovic, S.Uhlig and I.Theisler, “On the relationships between topological metrics in real-world networks”, Networks and Heterogeneous Media (2008), №3(2):pp.345-359

[114] Ланде Д. Порівняльна оцінка критеріїв центральності в ієрархічних мережах / Д. Ланде, О. Сулема // Information Technology and Security. – 2015. – Vol. 3, № 2. – С. 80-87.

[115] Mui L., Mohtashemi M., Halberstadt A. (2002) A computational model of trust and reputation. – System Sciences. – 2002. – P.2431-2439.

[116] March, S.P.,”Formalizing Trust As Computational Concept.”, Thesis or Dissertation [online]. Available: http://hdl.handle.net/1893/2010. Accessed: May,11,2020.

[117] Z.M. Aljazzaf, M.Perry, M.A.M. Capretz, “Trust Metrics for Services and Service Providers.”, ICIW 2011 : The Sixth International Conference on Internet and Web Applications and Services (2011) [online]. – Available: https://www.researchgate.net/publication/229041354_Trust_Metrics_for_Services_and_Service_Providers. – Accessed Jun.1,2020.

[118] Tran, Muoi and Kang, Min Suk and Hsiao, Hsu-Chun and Chiang, Wei-Hsuan and Tung, Shu-Po and Wang, Yu-Su, “On the Feasibility of Rerouting-based DDoS Defenses,”. – IEEE Symposium on Security and Privacy 2019. – 2019. – Vol.1. – Pages: 798-813. DOI:10.1109/SP.2019.00055

[119] K. Sriram, O. Borchert, O. Kim, P. Gleichmann, and D. Montgomery, "Routing Data Quality and Its Impact on BGP Anomaly Detection Algorithms". Invited presentation given at the ISOC Routing Resiliency Measurements Workshop, Atlanta, November 2012. [Електронний ресурс]. Доступно: https://www.nist.gov/document/isoc-rrm-workshop-sriram-nov2012-2pdf. Дата: Січ.15,2020.

[120] T. Bates, E. Gerich etc. Representation of IP Routing Policies in a Routing Registry (ripe-181). – 1994 ; [електронний ресурс]. – ftp://ftp.ripe.net/ripe/docs/ripe-181.txt.

[121] K. Sriram, O. Borchert, O. Kim, D. Cooper, and D. Montgomery, "RIB Size Estimation for BGPSEC," Presented at the IETF-81, SIDR WG Meeting, July 2011. [Електронний ресурс]. Доступно: https://www.nist.gov/document/bgpsecribestimationpdf. Дата:Січ.15, 2020.

[122] Cisco IOS IP Routing: BGP Command Reference [Електроний ресурс]. – Режим доступу : URL : http://www.cisco.com/en/US/docs/ios/iproute_bgp/ command/reference/irg_bgp5.html – Назва з екрана.

[123] BIRD Internet Routing Daemon. About Routing Tables [Електроний ресурс]. – Режим доступу : URL : http://bird.network.cz/?get_doc&f=bird-2.html – Назва з екрана.

[124] Торкингтон Н., Кристиансен Т. Библиотека программиста: Perl. – М.: Питер, 2001. – 736 с.

[125] Полянский А. Учебное пособие по CGI-программированию. – М.: Познавательная книга плюс, 2000. – 176 с.

[126] Гошко В. Регулярные выражения и поиск текста в Perl // «Системный администратор». – № 8, 2003. – С. 78-86.

[127] Padala, P., “Exploring Perl Modules – Part 1: On-The-Fly Graphics with GD” // Linux Gazette. – 2002. – Iss.81.

[128] Collected Algorithms from CACM. [Електронний ресурс]. Доступно: http://www.acm.org/– назва з екрану. – Дата доступу: Вер.4,2018.

[129] Федосеева А. Спецификация языка Perl. [Електронний ресурс]. Доступно: http://lib.luksian.com/ programming/perl/spec/. – назва з екрану. – Дата доступу: Вер.4,2018.

[130] Zubok V. Y. Всесвітні інтернет-провайдери в українській мережі обміну трафіком: виклики та можливості (Worldwide Internet Service Providers in Ukrainian Internet Exchange: Threats and Opportunities) / Vitalii Zubok // Information Technologies and Security (CEUR). – ISSN:1613-0073. – 2016. – №1813. – С. 68–72.

[131] Зубок В. Ю. Європейські мережі обміну Інтернет-трафіком та їхній вплив на зв’язність між автономними системами / В. Ю. Зубок // Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. – 2011. – №58. – С.34-43.

[132] Зубок В. Ю. Аналіз характеристик нових мереж обміну Інтернет-трафіком / В. Ю. Зубок // Реєстрація, зберігання і обробка даних. – 2013. – Том 15,№2. – С.48 54.

[133] V.Zubok. Empirical Study of New Metrics For the Internet Route Hijack Risk Assessment. Інформаційні технології і безпека: Матеріали XX Міжнародної науково-практичної конференції ІТБ-2020. – Київ: Інжиніринг. – С. 110-115.

[134] Мохор В. В. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури / В. В. Мохор, С. Ф. Гончар, О. М. Дибач // Ядерна та радіаційна безпека. – 2019. – Вип. 2. – С. 4-8.

[135] Karp R. M. Reducibility Among Combinatorial Problems / R.M. Karp // The IBM Research Simposia. – 1972. – С.85-103.

[136] Зубок В. Ю. Оптимізація зв'язків між вузлами інтернет як окремий випадок задачі Штейнера / В. Ю. Зубок // XXXIII наук.-техн. конф. "МОДЕЛЮВАННЯ" : 15-16 січня 2014 р. : тези доп. – К.: ІПМЕ ім. Г. Є. Пухова, 2014. – С.7.

[137] Берн М. У. Поиск кратчайших сетей / М.У. Берн, Р.Л. Грэм // Scientific American. Издание на русском языке. – 1989. – №3. – С.64-70.

[138] Melzak Z.A. Companion To Concrete Mathematics (Pure And Applied Mathematics S.), Vol. 1 / Z.A. Melzak. – John Wiley & Sons Inc. – 1973.

[139] Шрейдер Ю.А. Равенство, сходство, порядок / Ю.А. Шрейдер. – М.: Наука, 1971.

[140] Hernando C. Extremal Graph Theory for Metric Dimension and Diameter / C. Hernando, M. Mora, I. Pelayo, C. Seara, D.R. Wood // Cond-Math. – 2007. – Режим доступу : http://arxiv.org/pdf/0705.0938

[141] X. A. Dimitropoulos and G. F. Riley. Large-scale simulation models of BGP. In Proceedings of the Twelvth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'04). – 2004.

[142] X. Dimitropoulos and G. Riley. Creating realistic bgp models. In Proceedings of Eleventh International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'03). – 2003. – pages 64 – 69..

[143] R. Oliveira, B. Zhang, D. Pei, and L. Zhang, "Quantifying path exploration in the internet," IEEE/ACM Transactions on Networking. 2009. – vol. 17, no. 2. – pp. 445–458.

[144] R. Hiran, N. Carlsson, and P. Gill, "Characterizing large-scale routing anomalies: A case study of the china telecom incident," in Passive and Active Measurement Conf. Springer, 2013, pp. 229–238.

[145] V. Raghavan, G. Riley and T. Jaafar, "Realistic Topology Modeling for the Internet BGP Infrastructure," 2008 IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems, Baltimore, MD, USA. – 2008. – pp. 1-8, DOI:10.1109/MASCOT.2008.4770576.

[146] P. Richter, G. Smaragdakis, A. Feldmann, N. Chatzis, J. Boettger, and W. Willinger, "Peering at peerings: On the role of IXP route servers," in ACM SIGCOMM Conf. on Internet Measurement. ACM. – 2014. – pp. 31–44.

[147] MANRS – Mutually Agreed Norms for Routing Security [Електронний ресурс]. Доступно: http://www.manrs.org. – назва з екрану. – Дата доступу: Вер.14,2019.

[148] "A Guide to Border Gateway Protocol (BGP) Best Practices. A Technical Report from System Analysis Branch". NSA Cybersecurity Report. – PP-18-0645 (2018).

[149] D. McPherson. BGP Security Techniques. [Електронний ресурс]. Доступно: http://www.arbornetworks.com/en/research.html. – назва з екрану. – Дата доступу: Вер.4,2018.

[150] Зубок В. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електронне моделювання. – К.,2018. Т.40, №5.

[151] T. McDaniel. Peerlock: Flexsealing BGP / T. McDaniel, J.M. Smith, M. Schuchard // arXiv:2006.06576v3 [cs.NI] 17 Jul 2020.

[152] Zh. Zhang. “Practical Defenses Against BGP Prefix Hijacking” / Zheng Zhang, Ying Zhang, Y.Charlie Hu, Z.Morey Mao // CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference. – Dec. 2007. – p.1–12. DOI:10.1145/1364654.1364658

[153] J. M. Smith, K. Birkeland, T. McDaniel, and M. Schuchard, “Withdrawing the BGP re-routing curtain: Understanding the security impact of BGP poisoning through real-world measurements,”. – Conference Proceedings. – Network and Distributed Systems Security Symposium (NDSS). – 2020.

[154] J. M. Smith and M. Schuchard, “Routing around congestion: Defeating DDoS attacks and adverse network conditions via reactive bgp routing,” in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 599–617.

[155] Snijders, J., Heasley, J. and Schmidt, M., “Use of bgp large communities,” [Електронний ресурс]. – Доступно: https://tools.ietf.org/html/rfc8195 . –Дата доступу: Чер.,17, 2019.

[156] Sriram, K., and Azimov, A., “Methods for detection and mitigation of BGP route leaks,” [Електронний ресурс]. – Доступно: https://bit.ly/2Z7NlkW. – Дата доступу: Лис.10, 2020.

[157] Sriram, K., and Montgomery, D.C., “Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation,” Special Publication (NIST SP) №800-189,” [Електронний ресурс]. – Доступно: https://www.nist.gov/publications/resilient-interdomain-traffic-exchange-bgp-security-and-ddos-mitigation. – Дата доступу: Чер.1,2020.

[158] Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Изд-во «Яхтсмен», 1996. – 187 с.

[159] Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. : Изд-кий центр «Академия», 2005. – 144 с.

[160] Теоретические основы компьютерной безопасности / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. – М. : Радио и связь, 2000. –192 с.

[161] Щербаков А .Ю. Введение в теорию и практику компьютерной безопасности. – М. : Изд-во Молгачева С.В., 2001. – 352 с.

[162] C. McNab. Network Security Assessment, 3rd Edition / Chris McNab. – O’Reilly. – 2016. – 494p.

[163] Bellovin, S. M., Cheswick W. R. Firewalls and Internet Security, Repelling the Wily Hacker . – Addison-Wesley Publishing Company. – 2003. – 464p.

[164] Harrison M., Ruzzo W., Ullman J. Protection in operation systems. Communications of the ACM, 19(8): 1976. – P. 461-471. DOI:10.1145/360303.360333

[165] Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman. “Building Internet Firewalls. Second Edition”. - O’Reilly. – 2000

[166] Garfinkel, S. Practical Unix & Internet Security, 3rd Edition / Simson Garfinkel, Alan Schwartz, Gene Spafford. – O’Reilly. – 2003.

[167] Hunt, C. TCP/IP Network Administration. Third Edition / Craig Hunt . – O'Reilly. – 2002. – 746p.

[168] Visti.Net Looking Glass [Електронний ресурс]. Доступно: https://noc.visti.net/l-g/. – Назва з екрану. – Дата доступу: Лис.1,2020.

[169] Hurricane Electric Looking Glass [Електронний ресурс]. Доступно: https://lg.he.net/. – Назва з екрану. – Дата доступу: Кві.11,2019.

[170] UA-IX Looking Glass Company [Електронний ресурс]. Доступно: https://lg.ix.net.ua/. – Назва з екрану. – Дата доступу: Гру.11,2019.

[171] DTEL-IX. The Peering Company [Електронний ресурс]. Доступно: https://dtel-ix.net/ix/looking-glass. – Назва з екрану. – Дата доступу: Лип.1,2020.

ДОДАТОК

Таблиця результатів експерименту з приєднанням до двох мереж обміну трафіком (підрозділ 6.3)

№	Ідентифікатор AS	Метрика Довіри, T_1	Метрика значущості, S	Ризик, R_1	Метрика довіри, T_2	Ризик, R_2
		Початкова топологія			Нова топологія	
1	AS9198	5,505	13347,3	73474	3,118	41612
2	AS15169	3,118	18278,8	56987	1,766	32275
3	AS29355	9,720	5757,0	55957	5,505	31691
4	AS6697	5,505	7433,9	40922	1,766	13126
5	AS28907	3,118	12577,4	39212	1,766	22208
6	AS6939	3,118	11982,4	37357	1,766	21157
7	AS21299	17,162	1790,3	30726	5,505	9855
8	AS57463	3,118	9190,3	28652	1,766	16227
9	AS43727	5,505	4227,6	23272	3,118	13180
10	AS1853	5,505	4058,6	22342	3,118	12653
11	AS28917	3,118	7071,5	22046	1,766	12486
12	AS8926	5,505	3835,3	21112	1,766	6772
13	AS42772	17,162	988,3	16960	17,162	16960
14	AS34058	5,505	3059,0	16839	1,765	5399
15	AS25229	3,118	4741,0	14781	1,766	8371
16	AS15419	9,720	1405,5	13661	3,118	4382
17	AS5391	5,505	2477,9	13640	3,118	7725
18	AS6849	3,118	4361,6	13598	1,766	7701
19	AS9146	9,720	1383,0	13442	5,505	7613
20	AS44087	30,303	436,0	13212	17,162	7483
21	AS14840	5,505	2379,6	13099	3,118	7419
22	AS61832	5,505	2207,5	12152	3,118	6882
23	AS61568	5,505	2155,4	11865	3,118	6720
24	AS3212	5,505	2126,4	11705	3,118	6629
25	AS25106	9,720	1189,8	11565	3,118	3709
26	AS15895	3,118	3468,0	10812	1,766	6123
27	AS29124	17,162	569,2	9768	17,000	9676
28	AS35805	5,505	1700,0	9358	3,118	5300
29	AS12578	3,118	2921,7	9109	1,766	5159
30	AS35168	9,720	909,3	8838	3,118	2835
31	AS6877	5,505	1562,7	8602	3,118	4872
32	AS12406	9,720	882,0	8573	3,118	2750
33	AS210222	5,505	1514,4	8336	1,766	2674
34	AS25144	9,720	849,2	8254	5,505	4674
35	AS2857	5,505	1447,5	7968	3,118	4513
36	AS6661	5,505	1413,8	7783	3,118	4408
37	AS28220	9,720	763,0	7416	5,505	4200

38	AS34123	9,720	723,9	7036	1,766	1278
39	AS8595	9,720	718,3	6981	3,118	2239
40	AS263444	5,505	1262,1	6948	3,118	3935
41	AS41798	9,720	703,3	6836	3,118	2193
42	AS39824	17,162	391,3	6716	5,505	2154
43	AS42560	9,720	657,8	6394	5,505	3621
44	AS8641	5,505	1114,0	6132	3,118	3473
45	AS35297	3,118	1913,2	5965	1,766	3378
46	AS28186	5,505	1077,8	5933	3,118	3360
47	AS36384	5,505	1031,0	5675	3,118	3214
48	AS15440	5,505	1018,7	5608	1,766	1799
49	AS42861	5,505	1010,8	5564	3,118	3151
50	AS12530	5,505	962,5	5298	3,118	3001
51	AS34602	9,720	542,5	5273	9,720	5273
52	AS13188	3,118	1618,5	5046	3,118	5046
53	AS679	9,720	516,0	5015	9,720	5015
54	AS205714	9,720	512,0	4977	9,720	4977
55	AS34665	9,720	512,0	4977	9,720	4977
56	AS8585	9,720	502,8	4887	9,720	4887
57	AS6703	5,505	874,0	4811	5,505	4811
58	AS28910	9,720	486,6	4730	9,720	4730
59	AS24689	9,720	484,0	4704	9,720	4704
60	AS33922	5,505	844,0	4646	5,505	4646
61	AS12684	9,720	468,5	4554	9,720	4554
62	AS50607	5,505	825,5	4544	5,505	4544
63	AS21497	3,118	1452,5	4528	3,118	4528
64	AS25454	5,505	817,5	4500	5,505	4500
65	AS31252	5,505	810,2	4460	5,505	4460
66	AS60330	9,720	451,6	4389	9,720	4389
67	AS62081	5,505	768,7	4231	5,505	4231
68	AS3326	3,118	1305,7	4071	3,118	4071
69	AS39608	3,118	1275,7	3977	3,118	3977
70	AS21412	5,505	700,0	3853	5,505	3853
71	AS262761	9,720	393,5	3825	9,720	3825
72	AS760	9,720	389,5	3786	9,720	3786
73	AS396982	5,505	677,0	3727	5,505	3727
74	AS20875	9,720	374,5	3640	9,720	3640
75	AS264556	5,505	655,1	3606	5,505	3606
76	AS35320	3,118	1154,1	3598	3,118	3598
77	AS50509	5,505	604,3	3327	5,505	3327
78	AS3327	5,505	568,7	3130	5,505	3130
79	AS31514	5,505	547,0	3011	5,505	3011
80	AS6768	3,118	921,8	2874	3,118	41612
81	AS43561	5,505	503,9	2774	1,766	32275
82	AS8953	3,118	873,4	2723	5,505	31691

83	AS12883	3,118	856,8	2671	1,766	13126
84	AS9119	5,505	483,8	2663	1,766	22208
85	AS60280	5,505	479,8	2641	1,766	21157
86	AS50923	5,505	464,2	2555	5,505	9855
87	AS3255	3,118	812,1	2532	1,766	16227
88	AS35598	5,505	459,3	2529	3,118	13180
89	AS34224	5,505	459,0	2527	3,118	12653
90	AS34594	5,505	419,8	2311	1,766	12486
91	AS31148	3,118	674,0	2101	1,766	6772
92	AS29632	3,118	499,5	1557	17,162	16960
93	AS31272	3,118	474,0	1478	1,765	5399
94	AS49544	3,118	459,0	1431	1,766	8371
95	AS6712	3,118	444,0	1384	3,118	4382
96	AS25133	3,118	438,0	1366	3,118	7725
97	AS6876	3,118	436,5	1361	1,766	7701
98	AS34700	3,118	407,0	1269	5,505	7613
99	AS35362	3,118	391,0	1219	17,162	7483
100	AS15377	3,118	382,7	1193	3,118	7419

Наукове видання

ЗУБОК Віталій Юрійович
МОХОР Володимир Володимирович

Кібербезпека топології INTERNET

Монографія

Підп. до друку 17.06.2022. Формат 16х84/16
Папір офсетний. Друк цифровий.
Ум. друк. арк. 11,16. Зам. №1706-22
Наклад 300 прим.

Видавець:
Інститут проблем моделювання в енергетиці ім Г. Є. Пухова НАН України. Київ, 03164, вул. Генерала Наумова, 15. тел.: 380 (44) 424-10-63, e-mail: ipme@ipme.kiev.ua.
Свідоцтво суб'єкта видавничої справи ДК №6063 від 05.03.2018р.

Виготовлювач:
ТОВ «7БЦ»
03067, м. Київ, вул. Олекси Тихого, 84
тел: 380 (44) 592-00-80, e-mail: 7bc@ukr.net
Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017