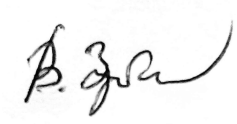
Національна академія наук України
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова

Зубок Віталій Юрійович



УДК 004[413.3+738.5.057.4] : 519.173

РОЗВИТОК ТЕОРІЇ ЗАХИЩЕНОСТІ ТОПОЛОГІЇ ГЛОБАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД КІБЕРАТАК НА СИСТЕМУ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ

Спеціальність 05.13.05 – комп‘ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Науковий консультант

чл.-кор. НАН України,
доктор технічних наук, професор
Мохор Володимир Володимирович,
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова, директор

Офіційні опоненти:

доктор технічних наук, професор
Додонов Олександр Георгійович,
Інститут проблем реєстрації інформації НАН України, заступник директора з наукової роботи

доктор технічних наук, професор
Стіренко Сергій Григорович,
НТУУ «КПІ імені Ігоря Сікорського»,
завідувач кафедри обчислювальної техніки

доктор технічних наук, професор
Юдін Олександр Костянтинович,
Національна академія Служби безпеки України,
завідувач спеціалізованої кафедри СК-31

Захист дисертації відбудеться "28" квітня 2021 р. о 14^{00} годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитись у бібліотеці Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий "27" березня 2021 р.

Вчений секретар спеціалізованої вченої ради
кандидат технічних наук, доцент В. В. Душеба

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Як відомо, існує умовний розподіл комп’ютерних мереж на локальні та глобальні. Для глобальних мереж є типовим широкий територіальний розподіл вузлів, розташування в різних країнах та різне підпорядкування. Це є основною причиною неможливості розробки та впровадження уніфікованих систем захисту інформації, що реалізували б єдину політику безпеки для цілої мережі.

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 Інтернет, який був створений і 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.

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* BGP-4, 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». 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 викривлення маршрутів до певних мережевих префіксів, а отже, вони змінюють топологічний простір мережі.

Проблема відома вже 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.

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, 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 спосіб здатен дієво зменшити 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, К. Шрирама, 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 методом протидії перехопленню маршрутів є напрям криптографічного захисту. Він потребує 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 маршрутизаціїї.

Ці недоліки мають бути вирішені в новому протоколі глобальної маршрутизації (робоча назва – «Secure BGP»), та, поряд з невизначеністю критеріїв достатності засобів для надійного захисту маршрутів, дослідники зауважують майбутні проблеми його глобального впровадження.

Таким чином, на сьогодні та в осяжній перспективі перелічені 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. 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, О. Юдіна, С. Стіренка, С. Гончара, Ф. Крамера, О. Боршера, Д. Монтгомери та інших вітчизняних та закордонних вчених.

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 даному дослідженні 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.

Зв'язок з науковими програмами, планами, темами. Дослідження, що проводились при виконанні дисертаційної роботи, здійснювалися у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в рамках науково-дослідних робіт:

«Розвиток наукових засад забезпечення інформаційної безпеки об'єктів критичної інфраструктури електроенергетичної галузі на основі методології системних досліджень» (шифр: Бескіди), що виконується у 2018-2022 рр. (номер державної реєстрації 0117U005467);

«Розроблення методів забезпечення кібернетичної безпеки функціонування об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр: Інтеленерго), що виконується в 2019-2021 рр. (номер державної реєстрації 0119U101856).

Метою дисертаційної роботи є розробка методів, моделей, методик підвищення захищеності топології глобальної комп'ютерної мережі Інтернет від атак на систему глобальної маршрутизації шляхом вдосконалення міжмережевих зв'язків на основі ризик-орієнтованого підходу.

В ході досягнення мети були поставлені та вирішувались такі *основні задачі*:

1) дослідити сучасний стан архітектури глобальної комп'ютерної мережі Інтернет, системи глобальної маршрутизації, та виокремити фактори, що формують переваги та недоліки цієї системи; провести аналіз відомих кібернетичних атак на систему глобальної маршрутизації, існуючих сучасних та перспективних напрямків розвитку методів захисту інформації, що застосовуються для протидії атакам на систему глобальної маршрутизації в комп'ютерній мережі Інтернет; сформулювати вимоги до розроблюваних моделей, методів, методик підвищення захищеності системи глобальної маршрутизації;

2) дослідити топологічний простір, на якому функціонує система глобальної маршрутизації Інтернету;

3) провести аналіз ризиків інформаційної безпеки системи глобальної маршрутизації, визначити пріоритети стратегії оброблення ризику в інтересах власників ризику та запропонувати теоретичні засади та практичні заходи з підвищення захищеності топології Інтернет, що здатні поліпшити якість рішень з питань інформаційної безпеки в мережі Інтернет;

4) розробити теоретичні засади формування метричних характеристик оцінки захищеності системи глобальної маршрутизації;

5) розробити ризик-орієнтовану модель топології Інтернет, яка б дозволила проводити аналіз та вдосконалення зв'язків суб'єкта глобальної маршрутизації шляхом зниження ризику перехоплення маршруту;

6) розвинути методику підвищення захищеності суб'єкта глобальної маршрутизації шляхом формування ефективної топології його з'єднань за допомогою оцінювання ризику кібератак на систему глобальної маршрутизації;

7) запропонувати підхід до побудови засобів автоматизації дослідження захищеності топології комп'ютерних систем, функціонування яких пов'язане з Інтернет і які є суб'єктами глобальної маршрутизації.

Об'єктом дослідження є глобальна маршрутизація Інтернет.

Предметом дослідження є процес формування топології системою глобальної маршрутизації Інтернет.

Основними *методами дослідження* є методи системного аналізу, дискретної математики, комбінаторики, теорії графів, теорії складних мереж, теорії множин, а також методи управління інформаційною безпекою.

Наукова новизна отриманих результатів полягає у наступному:

1. Вперше запропоновано варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет, що утворений системою глобальної маршрутизації на множині з'єднань між вузлами, завдяки чому обґрунтовано, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію Інтернет, а вразливості системи глобальної маршрутизації є вразливостями топології Інтернет. Це також відкриває можливість застосування теорії топологічних просторів в дослідженнях системи глобальної маршрутизації.

2. Запропоновано вдосконалену модель оцінювання ризику інформаційної безпеки на базі відомої моделі DREAD, яка завдяки додатковій деталізації критеріїв забезпечує підвищення якості рішень, що приймаються з питань захисту інформації в комп'ютерній мережі Інтернет.

3. Сформульовано математичну модель системи Інтернет-маршрутизації, яка спирається на запропонований в роботі формальний опис елементів системи глобальної маршрутизації та відношень між ними. Така модель, на відміну від існуючих моделей маршрутизації, дозволила описати процес формування топологічного простору окремого мережевого префікса та топологічного простору Інтернету в цілому. Це дозволило, в свою чергу, синтезувати такі метричні характеристики мережевих вузлів, які, на відміну від відомих характеристик, відображають складові ризику перехоплення маршруту.

4. Вперше створено ризик-орієнтовану модель системи глобальної маршрутизації, яка, завдяки запропонованим метричним характеристикам вузлів, що дозволяють оцінювати складові ризику перехоплення маршруту, надає можливість оцінювання і порівняння топологій за рівнем захищеності за допомогою повторної оцінки ризиків інформаційної безпеки.

5. Отримала подальший розвиток методика формування ефективних міжвузлових зв'язків комп'ютерної мережі Інтернет завдяки розширенню критеріїв ефективності шляхом запровадження оцінки ризику кібератак на систему глобальної маршрутизації, що дає можливість автоматизації аналізу топології, розрахунку ризику перехоплення маршруту в топологічному просторі окремого мережевого префіксу, моделювання нової топології та оцінювання результатів.

Практичне значення одержаних результатів полягає в наступному:

1. Шляхом аналізу ланцюжка «подія – причина – наслідки» по відомих кіберінцидентах з системою глобальної маршрутизації отримано характеристики, необхідні для складення моделі порушника та моделі загроз, які повинні використовуватись для проєктування системи керування інформаційною безпекою інформаційного активу, функціонування якого пов'язане з Інтернет.

2. Розроблено методику оцінювання захищеності топології зв'язків суб'єкта глобальної маршрутизації, яка доповнює існуючі методи протидії атакам на систему глобальної маршрутизації та спирається на сучасні методи управління інформаційною безпекою.

3. Відповідно до розробленої методики підвищення захищеності інформаційного активу створено програмний засіб визначення ризику перехоплення маршруту на вузлах мережі. Отримано патент України на корисну модель UA145947U та авторське свідоцтво на програмний модуль розрахунку факторів ризику перехоплення маршруту на Інтернет-вузлі за його топологічними характеристиками №101657.

Результати дослідження і розроблені методики були використані:

- компанією Moris B.V. (Нідерланди) для визначення апстрім-провайдерів для хмарного сервісу Qloude (довідка про впровадження результатів дисертаційного дослідження);
- ТОВ «Інформаційний центр «Електронні вісті» підчас винесення окремих функцій сервісу Infostream до зовнішніх датацентрів (акт впровадження результатів дисертаційного дослідження);
- ТОВ «ДІДЖИТАЛ ТЕЛЕКОМ-АЙ ІКС» для порівняльної оцінки топології з'єднань учасників мережі обміну трафіком DTEL-IX (акт впровадження результатів дисертаційного дослідження);
- Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України в ході виконання науково-дослідних робіт шифр «Інтеленерго» та шифр «Бескіди» (акт впровадження результатів дисертаційного дослідження).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. В роботах, опублікованих у співавторстві, автору належать: [17] обґрунтування зв'язку між топологією та ризиком кібератак на глобальну маршрутизацію; [20] збір даних та

аналіз можливості використання відхилень стану працездатності для виявлення кібернетичних інцидентів; [21] аналіз топології Інтернет, метод наближеного вирішення комбінаторної задачі пошуку оптимальної комбінації зв'язків, матеріали експериментальних досліджень; [28] обґрунтування використання метричної функції відстані для оцінки ймовірності перехоплення маршруту; [37] спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет.

Апробація результатів дисертаційної роботи. Основні результати роботи доповідались на 15 наукових та науково-практичних конференціях, в тому числі: XV – XX міжнародні науково-практичні конференції «Інформаційні технології та безпека» (Київ, 2015 – 2020); VI міжнародна науково-практична конференція «Моделювання-2018» (Київ, 2018); Науково-практична конференція «Кібербезпека енергетики» (Одеса, 2019); Міжнародна науково-практична конференція «Перспективні напрями захисту інформації» (Затока, 2020); Міжнародна науково-практична конференція «Science, Engineering and Technology: Global Trends, Problems and Solutions» (Прага, Чеська республіка, 2020); IX Міжнародна науково-технічна конференція ІСТ-2020, присвячена 90-річчу ХНУРЕ (Харків, 2020).

Публікації. Матеріали дисертації опубліковано в 39 наукових роботах, в тому числі – 18 статей в наукових фахових журналах та збірниках наукових праць України, 5 публікацій в закордонних виданнях (з яких 4 публікації проіндексовані в наукометричній базі Scopus), 1 патент України на корисну модель, 1 авторське свідоцтво на програмний твір.

Структура та обсяг дисертації. Дисертаційна робота складається з анотації, вступу, 6 розділів, висновків, списку використаних джерел (171 найменування на 19 сторінках), та 3 додатків (на 18 сторінках). Загальний обсяг дисертації становить 323 сторінок. Основний зміст викладено на 266 сторінках, включаючи 19 таблиць та 59 рисунків.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано мету і задачі дослідження, визначено наукову новизну і практичну цінність отриманих результатів, наведені дані про публікації й апробацію результатів досліджень, показано зв’язок роботи з науковими темами. Також у вступі наведено дані про особистий внесок здобувача в оприлюднених у співавторстві наукових працях, надано інформацію про структуру дисертації.

Перший розділ роботи присвячено дослідженню сучасного стану архітектури і топології глобальної комп'ютерної мережі Інтернет, та виокремлено фактори, що формують переваги та недоліки цієї системи. Загрози, пов'язані з глобальною маршрутизацією, описані як один з окремих випадків загроз інформаційної безпеки. 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. Суб'єктами глобальної маршрутизації є так звані автономні системи. Автономна система (AS) – це комп'ютерна мережа або сукупність мереж під загальним управлінням. 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.

В розділі описано дослідження процесів глобальної маршрутизації в Інтернеті. Виділено проблемні аспекти функціонування протоколу глобальної маршрутизації BGP-4. 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. Обидві цих властивості експлуатуються при атаках на маршрутизацію. BGP-система може задати тільки наступний крок (next hop), покладаючись на дані, отримані від інших систем. Зловмисник, який отримав управління над одним з прикордонних маршрутизаторів, може постачати сусідні AS хибною інформацією тому, що протокол BGP-4 заснований на довірі між з'єднаними мережами, і довіра має транзитивну властивість: сусідні BGP-системи довіряють одна одній, ті, в свою чергу, довіряють своїм сусідам і в підсумку всі довіряють всім. 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. Таким чином, основні вразливості BGP-4 пов'язані з відсутністю вбудованих механізмів авторизації учасників обміну маршрутами і верифікації інформації про маршрути.

На рис.1 приведено функціональну схему BGP-4. Виділено основну вразливість BGP-4 – відсутність механізмів для авторизації джерел вхідної інформації та валідації самої інформації.

Відомо кілька сценаріїв кіберінцідентов, пов'язаних з глобальною маршрутизації. «Викрадення маршруту», чи «викрадення префіксу» — це явище, при якому AS нелегітимно оголошує себе як джерело маршруту (route origin) замість справжнього джерела. «Витік маршруту» означає, що AS нелегітимно, з порушенням політики маршрутизації, пропонує маршрути до чужих префіксів через себе. Ці нелегітимні маршрути забруднюють таблиці маршрутизації BGP, спотворюють шляхи проходження мережевого трафіку та впливають на конфіденційність, цілісність ті доступність IP-комунікацій. Такі атаки використовуються для маніпуляцій з трафіком з метою дестабілізації телекомунікаційної мережі Інтернет, перехоплення трафіку, шпигунства, крадіжок даних, нанесення матеріальної шкоди, дезінформації тощо.

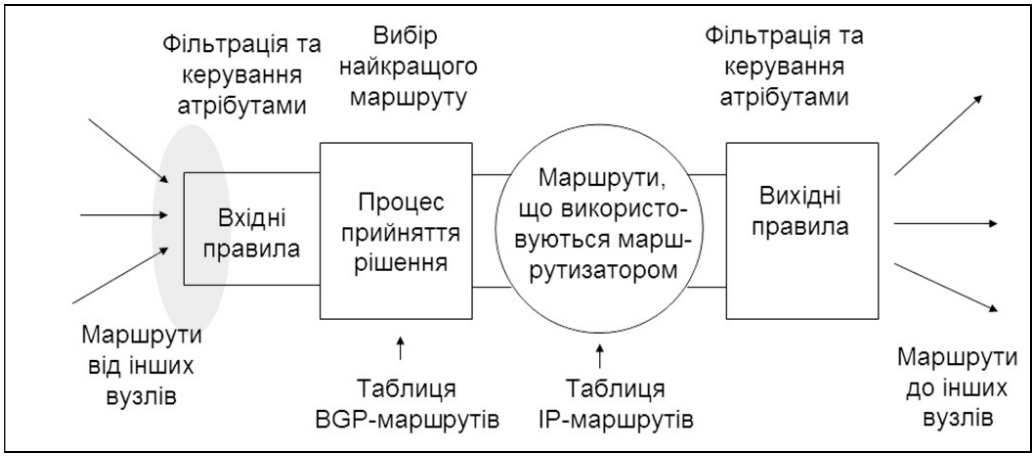


Рисунок 1 – Функціональна схема протоколу маршрутизації BGP-4

Огляд існуючих і розроблюваних захисних механізмів і механізмів удосконалення системи глобальної маршрутизації (табл.1) показав, що нині деякі захисні механізми, що функціонують як додаткова система поза протоколом BGP-4, знаходяться на різній мірі впровадження. Це, перш за все, реєстри маршрутизації (routing registries), які покликані бути офіційними джерелами про прикордонний взаємодії AS. По-друге, це механізм інфраструктури публічних ключів для маршрутизації (RPKI), за допомогою якого стало можливим постачати електронним підписом один з атрибутів маршруту – джерело маршруту (ROA), а також затверджувати цей електронний підпис. На жаль, застосування RPKI на всіх вузлах мережі є далекою перспективою, а часткове застосування дає частковий результат. До того ж, захист одного атрибута не усуває в цілому проблем перехоплення маршруту. Більш фундаментальні зміни в сам протокол BGP-4, які дозволяють захистити криптографічно не тільки джерело маршруту, а й легітимний шлях, все

ще знаходяться в розробці. На шляху реалізації цих змін знаходяться проблеми обчислювальної складності і необхідності глобальної імплементації. Таким чином, уразливості глобальної маршрутизації є загрозами інформації, для захисту від яких потрібні нові підходи, ефективні для конкретних учасників глобальної маршрутизації.

Таблиця 1 – Характеристики відомих захисних механізмів 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	(+) Сприяє запобіганню більшості інцидентів (-) Проблеми якості інформації в реєстрах (-) Нема 100% впровадження
	валідація атрибутів шляху екстрапротокольними засобами	PeerLock ROA ASPA	(+) Забезпечує цілісність головних атрибутів маршруту (-) ASPA не стандартизовано (-) проблеми з 100% впровадженням (-) утворення нових точок відмови
	криптографічний захист атрибутів шляху в протоколі маршрутизації	BGPsec	(+) захист атрибутів інтегровано в протокол (-) проблеми реалізації, дискусії про обчислювальну складність (-) неможливість 100% впровадження

Враховуючи вказані недоліки, було визначено *вимоги до розроблюваних методів, моделей, методик*:

1. Універсальність: результати дослідження мають бути дієвими в разі застосування для будь-якого суб’єкта глобальної маршрутизації.

2. Безмасштабність: розробки мають демонструвати ефективність незалежно від того, скільки учасників глобальної маршрутизації їх використовують.

3. Автономність: підвищення захищеності топології для одного суб'єкта глобальної маршрутизації повинно відбуватись без втручання в діяльність інших суб'єктів.

4. Непротирічність: мають не протирічити і не знижувати ефективність існуючих методів, які вже використовуються в світі, та призводити до появи нових вразливостей у вигляді створення нової єдиної точки відмови.

Сучасне управління інформаційною безпекою базується на управлінні ризиками (ДСТУ ISO/IEC 27001, NIST SP800-30, Закон України «Про основні засади забезпечення кібербезпеки України»). Ризик кількісно прийнято виражати як добуток суми збитку від реалізації певної загрози на ймовірність реалізації цієї. Найважливішою стадією управління ризиками є ідентифікація ризику та кількісна оцінка збитку від реалізації кожної загрози. Для кількісної оцінки ризику потрібно метод оцінювання ймовірності настання збитку. При наявності такого методу підвищення захищеності інформації від загроз, пов'язаних з глобальною маршрутизацією, можна буде вирішувати шляхом поводження з ризиками. Було

зроблено припущення, що ризик перехоплення маршрутів може бути оцінений шляхом аналізу міжмережевих зв'язків. Тоді керування ризиком можливо шляхом підвищення захищеності системи глобальної маршрутизації.

В другому розділі роботи систему глобальної маршрутизації розглянуто як таку що утворює топологію комп'ютерної мережі, та послідовно обґрунтовано, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію Інтернету.

На рис.2 зображено основні елементи системи глобальної маршрутизації.

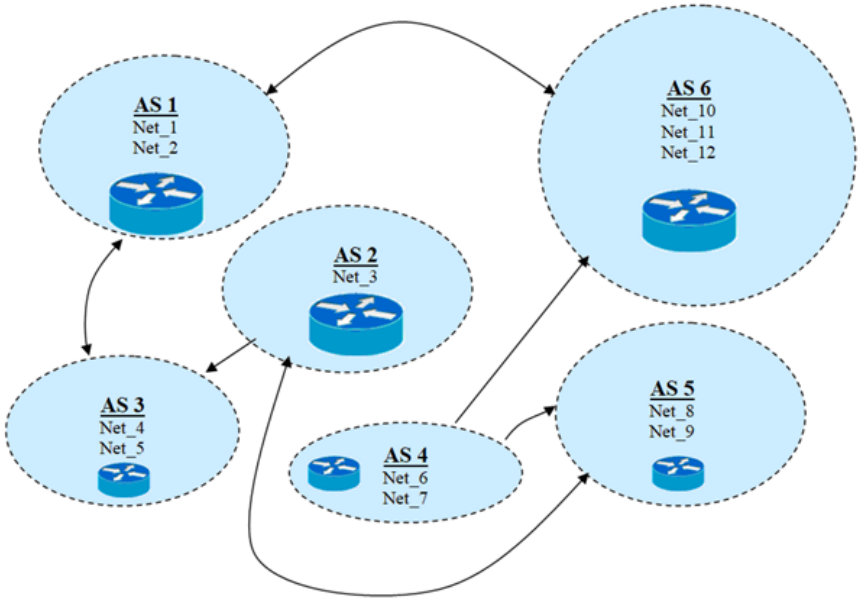


Рисунок 2 – Система глобальної маршрутизації

До системи глобальної маршрутизації Інтернет 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*":
$$\forall p : p \in v_1 \Leftrightarrow p \notin v_2,\ v_1, v_2 \in V;$$
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) $l = \{AS_i, AS_j\} \neq \{AS_j, AS_i\}$– **з'єднання суміжних AS, *l,*** по яких *анонсуються* префікси p;
4) {Net_1, Net_2,..Net_10} – множина **мережевих префіксів *p***, кожен префікс прив'язаний до певного та єдиного вузла v, званого "*джерелом*":
$$\forall p : p \in v_1 \Leftrightarrow p \notin v_2,\ v_1, v_2 \in V;$$
5) {AS1,AS2,..AS5} – множина **вузлів** V, кожен вузол є джерелом для певних префіксів:
$$\forall v \in V : \exists\{p_1, p_2, ..., p_n\} \in v;$$

6) {AS1,AS3},{AS3,AS1},{AS2,AS3},... – **з'єднання суміжних AS, *l,*** по яких *анонсуються* префікси *p*:

$$l = \{AS_i, AS_j\} \neq \{AS_j, AS_i\}.$$

Крім того, до системи глобальної маршрутизації належать і процеси, які виконуються алгоритмами протоколу BGP-4. Основною функцією протоколу BGP-4 є обмін інформацією про доступність окремих мереж. Обмін відбувається по зв'язках, які визначені адміністративно заданими налаштуваннями BGP-систем на певних AS, і ці AS отримують назви сусідніх AS (peer AS). Маршрут – це одиниця інформації, яка відображає шлях до окремої мережі (яка ідентифікована за допомогою мережевого префікса), і представлений у вигляді списку AS, крізь які проходить інформація про доступність мережі.

Будь-який мережевий префікс *p*, що ідентифікує мережу, яка входить до Інтернет, закріплений за власним джерелом – певною AS.

Нехай існує множина всіх з'єднань між вузлами $\exists L: l \in L$. Нехай існує система елементів множини цих з'єднань, 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:

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

$$\forall m(p'), m(p'') \in T : \left(m(p') \cup m(p'') \in L \subset T; \ m(p') \cap m(p'') \in (\varnothing, L) \subset T\right)$$

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:

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

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»:

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

В результаті алгоритм маршрутизації, використовуючи хибну топологію, дає хибний результат вибору маршруту.

Таким чином, *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.*

Отже головну проблему і мету роботи уточнено як підвищення захищеності топологічного простору кожного окремого мережевого префікса шляхом зменшення ризику його спотворення в наслідок зумисних дій. При цьому критерієм захищеності слугуватиме оцінка ризику як міра захищеності інформації.

В третьому розділі висвітлено результати застосування та розвитку методів інформаційної безпеки для захисту системи глобальної маршрутизації. Для цього на основі ретроспективного аналізу кіберінцидентів з використанням атак на систему глобальної маршрутизації, було досліджено ланцюжок «Подія-Причина-Наслідки». Аналіз інцидентів кібербезпеки, пов'язаних з перехопленням маршрутів, які отримали широкий резонанс (табл.2), показав їх глобальні масштаби як за областю поширення, так і за розміром наслідків.

Було ідентифіковано загрози інформаційної безпеки та визначено об'єкт впливу цих загроз – інформаційний актив, тобто комп'ютерна система чи комп'ютерна мережа, функціонування якої пов'язане із взаємодією з глобальною мережею Інернет. Власник цієї інформаційного активу є основною зацікавленою стороною (так званий stakeholder) в управлінні ризиками, і він є власником ризику.

В результаті було встановлено наступне:

Метод реалізації загроз – несанкціоновані зміни множині з'єднань, які призводять до нелегітимного розширення бази топології.

Засіб – експлуатація вразливостей протоколу BGP-4.

Результат – утворення нових елементів топології (в т.ч. хибних маршрутів).

Наслідки – втрати цілісності, доступності, конфіденційності, спостережності.

Таблиця 2 – Фрагмент результату ретроспективного аналізу інцидентів

Назва інциденту	**Джерело**	**Подія**	**Причина**	**Наслідки**
Інцидент з Youtube, 2008	державний оператор	перехоплення маршруту з деагрегацією	зумисні дії	Постраждав сервіс YouTube та користувачі
Canadian Bitcoin Hijack, 2014	приватні особи	перехоплення маршруту	зумисні дії	Постраждалі – користувачі 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

На основі ретроспективного аналізу кіберінцидентів з глобальною маршрутизацією було систематизовано *основні сценарії проведення атаки*, включно з джерелом виникнення загрози, механізму реалізації. Було виявлено наступні сценарії.

1) Перехоплення префіксу (prefix hijack): вузол зловмисника пропонує себе як джерело маршруту до адресного простору, що не належить йому. Таким чином цей маршрут буде конкурувати з істинним на всіх інших вузлах мережі. Подібна атака може бути відносно швидко виявлена, бо анонсування того самого адресного простору від різних вузлів порушує вимоги стандарту RFC1930.

2) Витік маршруту (route leak): вузол зловмисника ретранслює легально отриманий анонс адресного простору всупереч політиці маршрутизації, що визначає відносини між вузлами («клієнт-провайдер», «сусід-сусід»), 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 підмереж (subnet hijack): вузол зловмисника анонсує чужий адресний простір, поділивши його на дрібніші підмережі і анонсувавши більш специфічні префікси. За відсутності конкуруючих префіксів такого ж розміру, захоплення має глобальний ефект.

4) Захоплення нерозподіленого або невикористаного адресного простору. В цьому випадку анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.

Будь-який з варіантів атаки призводить до «перетягування» мережевого трафіку на інший маршрут. В більшості випадків цей трафік втрачається, факт порушення доступності інформації викривається досить швидкою. Така стратегія має назву створення «чорної діри» (blackholing). Але 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. Найскладніший сценарій атаки передбачає повернення перенаправленого трафіку назад в мережу, де він може просуватись далі легітимним маршрутом. До повернення на легітимний маршрут трафік перехоплюється з метою аналізу, прослуховування та модифікації переданих даних.

Було складено модель загроз та модель порушника. Встановлено, зокрема, що на відміну від більшості відомих моделей порушника, найвищий рівень загрози може спричинити зовнішній порушник, не використовуючи проникнення в середину інформаційного активу. В інтересах власника ризику для підвищення захищеності інформації необхідно розробити стратегію, спрямовану на зниження ризику перехоплення маршруту до його інформаційного активу.

Для складення моделі загроз було використано відому модель STRIDE, яка враховує вагу інформаційних загроз по окремих типах (Spoofing, Tampering, Repudiation, Denial of Service, Elevation of Privilege). Для поліпшення якості рішень стосовно інформаційної безпеки, було запропоновано вдосконалену модель оцінки ризиків DREAD. DREAD – це фактори, за яким оцінюється ризик інформаційної безпеки (damage, reproducibility, exploitability, affected users, disclosure):

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

Запропоновано вдосконалення за рахунок поєднання її з моделлю ідентифікації загроз STRIDE. 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

Крім цього, результуюча оцінка ризику за комбінованою моделлю STRIDExDREAD стає фактично на 80% точнішою за просто DREAD:

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

$$R_D = \frac{R_{DS} + R_{DT} + R_{DR} + R_{DI} + R_{DD} + R_{DE}}{6}; \quad \text{так само для } R_R, R_E, R_A, R_{Dx};$$

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

Отже, *проведено структуроване ідентифікування загроз та ризиків інформаційної безпеки, що стосуються системи глобальної маршрутизації. Отримано додаткові характеристики для уточнення моделі порушника та моделі загроз інформаційному активу, а також розвинуто відому модель оцінювання ризику інформаційної безпеки DREAD за рахунок уточнення складових ризику.*

Ці результати спрямовані на підвищення якості рішень, які приймаються з питань захисту інформації і їх використано пізніше в роботі при створенні методики оцінки захищеності топології.

В **четвертому розділі** було розроблено теоретичні засади формування метричних характеристик оцінки захищеності системи глобальної маршрутизації.

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, що базується на BGP-зв'язках. Для визначення необхідних якостей нової моделі було формалізовано поняття маршрутизації. Для цього спочатку було зроблено формальний опис перелічених раніше мережевих об'єктів та процесів – мережева адреса та адресний простір як безперервна множина унікальних адрес:

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

IP-префікс як послідовність адрес, кількість яких кратна ступеню двійки:

$$\begin{cases} p_i = 2^{j-i} p_j, \\ i \leq j, \\ 0 \leq \{i, j\} \leq \log_2 |A|. \end{cases}$$

Маршрут як послідовність з'єднаних вузлів до місця призначення:

$$m(p) := \left(v_p, e_p\right).$$

Відносини між префіксом та маршрутом, як такі, що якщо префікс j вкладений в префікс i, то маршрут до префікса i є також маршрутом до j:

$$p_j \subset p_i \Rightarrow m(p_j) \subset m(p_i)$$

За допомогою наведених вище визначень сформульовано математичну модель системи глобальної маршрутизації, яка базується на тих самих алгоритмах, що реалізовані в протоколі BGP, та на відміну від існуючих моделей, позбавлена від нетранзитивних параметрів. В ній маршрутизація представлена як процес, що складається з двох незалежних етапів:

$$\begin{cases} \pi_v(p) = \{\min_v(m_v(p)) \ : \ \pi \in M_p, \ v \in V_p\} \\ p(a) = \{\min_j(p_j) \ : \ a \in p \subset A, \ 0 < j \le |A|\} \end{cases} \quad (1)$$

На першому етапі системи (1) серед маршрутів до кожного мережевого префіксу обирається найкоротший маршрут. Сукупність кращих маршрутів до кожного з наявних мережевих префіксів стає таблицею маршрутизації, по якій підчас відправлення IP-пакета відбувається другий етап системи (1), а саме – вибір префікса відповідно до адреси призначення. 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.

Таким чином, *сформульовано математичну модель системи глобальної маршрутизації, яка дозволила описати процес формування топологічного простору окремого мережевого префікса та топологічного простору Інтернету в цілому*.

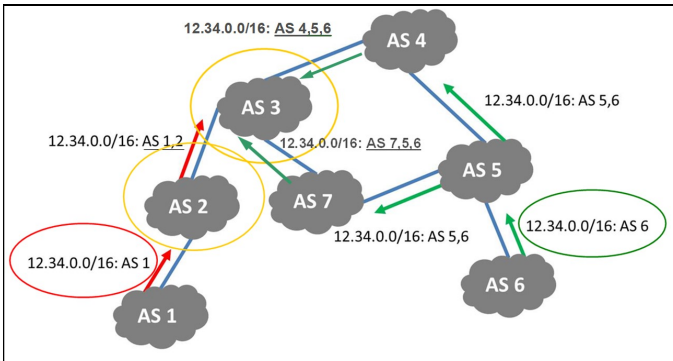
Перехоплення, витік маршруту означають, що механізм атаки спрямований на першу частину системи (1). Атака є ефективною, якщо в її результаті в таблицю маршрутизації потрапляє інший маршрут до атакованого префіксу, ніж той, що потрапив би за відсутності атаки.

В цьому розділі було досліджено вплив взаємного розташування вузлів на ризик перехоплення маршруту. Загально прийнятим в інформаційній безпеці є вираз ризику R через добуток збитку, та ймовірності настання цього збитку:

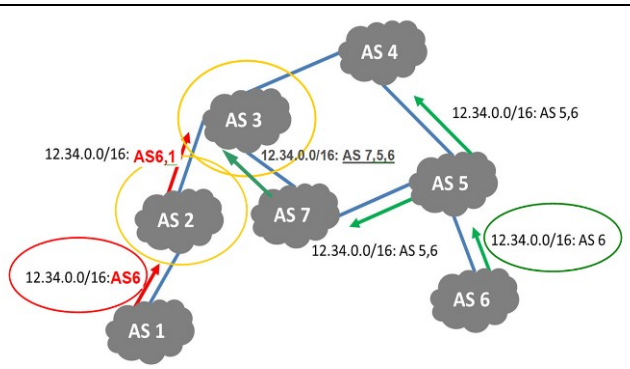
$$R = L \cdot P,$$

де L – збиток, P – ймовірність настання збитку.

Прості моделювання та аналіз відомих інцидентів продемонстрували, що чим більша відстань між вузлом власника інформаційного активу та його потенційною аудиторією, тим легше фальсифікувати маршрут по дорозі. На рис.3 наведено приклад, як хибний анонс маршруту впливатиме на розповсюдження істинного маршруту, конкуруючи з ним (вузли, «уражені» хибним маршрутом, окреслені жовтим колом).



AS1 перехоплює маршрут до 12.34.0.0/16 який належить AS6.



AS1 підроблює джерело маршруту до 12.34.0.0/16, в той час як AS2 не застосовує необхідну фільтрацію анонсів BGP.

Рисунок 3 – вплив відстані на поширення хибного маршруту

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.

Було проаналізовано декілька відомих метричних характеристик складних мереж та вузлів, які використовуються в різних предметних областях для вивчення та моделювання поведінки мережі. Серед цих характеристик:

1) ступінь вузла: характеризує кількість зв'язків вузла (вхідних чи вихідних), та не відображає ролі вузла в побудові коротших шляхів;
2) розподіл ступеню в мережі: топологічна властивість, яка впливає на співвідношення діаметру мережі та середнього коротшого шляху, а також на живучість мережі;
3) кластеризація: характеризує наявність в мережі структур, де вузли зв'язані значно щільніше, ніж в середньому в мережі;
4) посередництво, навантаження, центральність: характеристики конкретного вузла, які відображають його роль як транзитера, присутність в коротших шляхах між іншими парами вузлів.

Було встановлено, що відомі характеристики 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.

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:

$$L_u = \sum_{i}^{|V|} L_i \quad ; \quad L_u \sim |p_v|$$

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.

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. 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:

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

де δ_π – відстань між джерелом префіксу та вузлом v.

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. Тому термін «довіра» було використано для оцінки ймовірності перехоплення маршруту. Тут власник ризику u стає суб'єктом довіри, оцінюваний вузол v – об'єктом довіри, а предметом довіри – прийняття у вузлі v хибного маршруту.

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:

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

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

$$T_u^v = \frac{d(u,v)\left(|V|-1\right)}{\sum_{i}^{|V-1|} d(u,i)} \ , \ i \neq u \qquad (3)$$

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*; $\left\langle D_u \right\rangle$ – середня відстань від суб'єкта довіри до інших вузлів.

Таким чином було сформовано такі метричні характеристики мережевих вузлів, які відображають складові ризику перехоплення маршруту. З цих метричних характеристик утворено ризик-орієнтовану модель міжмережевих зв'язків, яка основана на розподілі вузлів в просторі (R,T,S), де *R* – ризик, *T* – довіра, *S* – значущість.

$$R_u^v = T_u^v S_u^v \qquad (4)$$

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

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

Такий метод 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:

$$R_u^v = S_u^v \cdot 10^{T_u^v} \qquad (6)$$

Таким чином, *розроблено ризик-орієнтовану модель топології Інтернет, яка базується на запропонованих метричних характеристиках мережі, що походять з топологічних характеристик вузлів та характеризують безпосередні складові ризику перехоплення маршруту – ймовірність настання збитку та потенційний розмір збитку, що дає можливість порівняння топологій за рівнем захищеності.*

Продемонстровано адекватність моделі для відображення характеристик вузлів з точки зору оцінювання ризику.

В **п’ятому розділі** роботи розвинути методику підвищення захищеності інформаційного активу від атак на систему глобальної маршрутизації. 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:

$$R_u = \sum_{i \ne u}^{|V|-1} R_i^v = kR_0$$

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. 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. Це *NP*-складна комбінаторна задача, проте її розмірність може бути спрощена різними відомими на цей час методами, що дають наближений результат.

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;

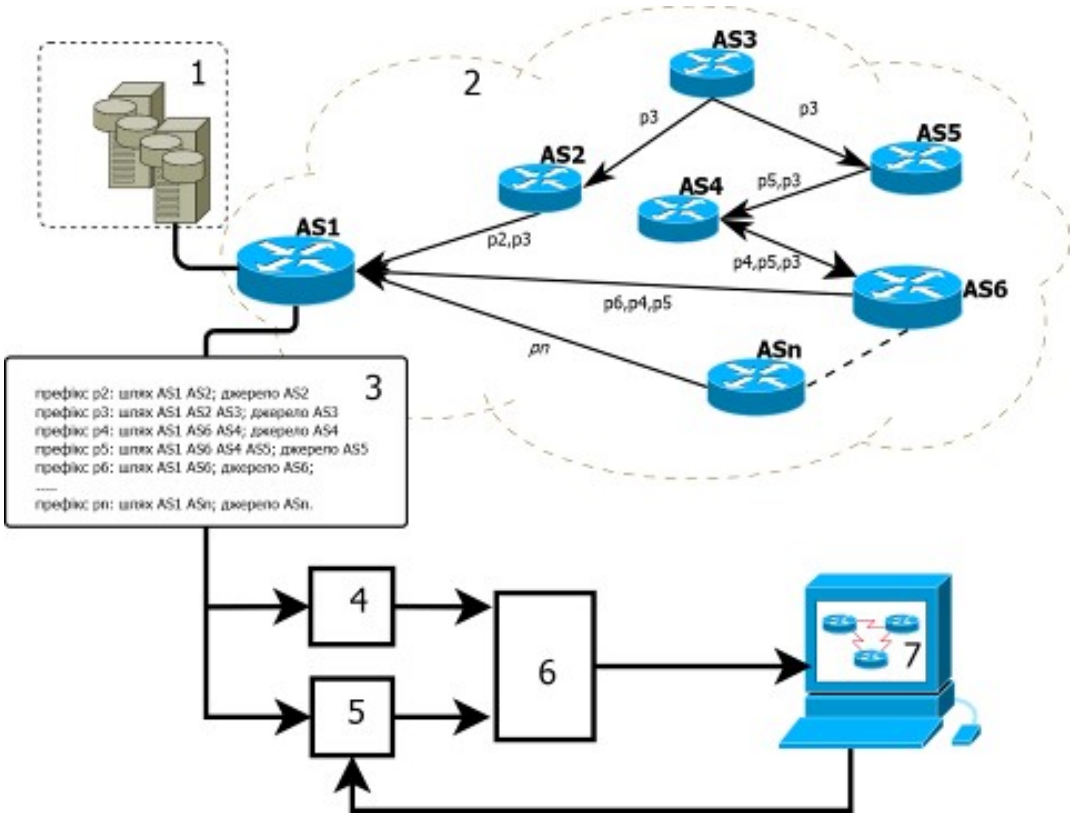
– розрахунок метрик довіри та значущості для цільової групи вузлів;

– 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. 4, де наведено схему, яка демонструє реалізацію методики визначення ризику перехоплення маршруту на вузлах мережі Інтернет. На схемі позначено інформаційний актив *1*, підключений до Інтернет-вузла AS1 – власного обладнання, задіяного для забезпечення глобальної маршрутизації (BGP-маршрутизатора). 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. Підчас моделювання ефективної топології зв’язків для зниження ризику, до блоку розрахунку метрики довіри подається нова топологія міжмережевих зв'язків, що містить нові зв’язки.



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.

Рисунок 4 – схема реалізації методики визначення ризику перехоплення маршруту на вузлах мережі Інтернет

З урахуванням нових зв’язків розраховується метрика довіри та ризик, який порівнюється із заданим.

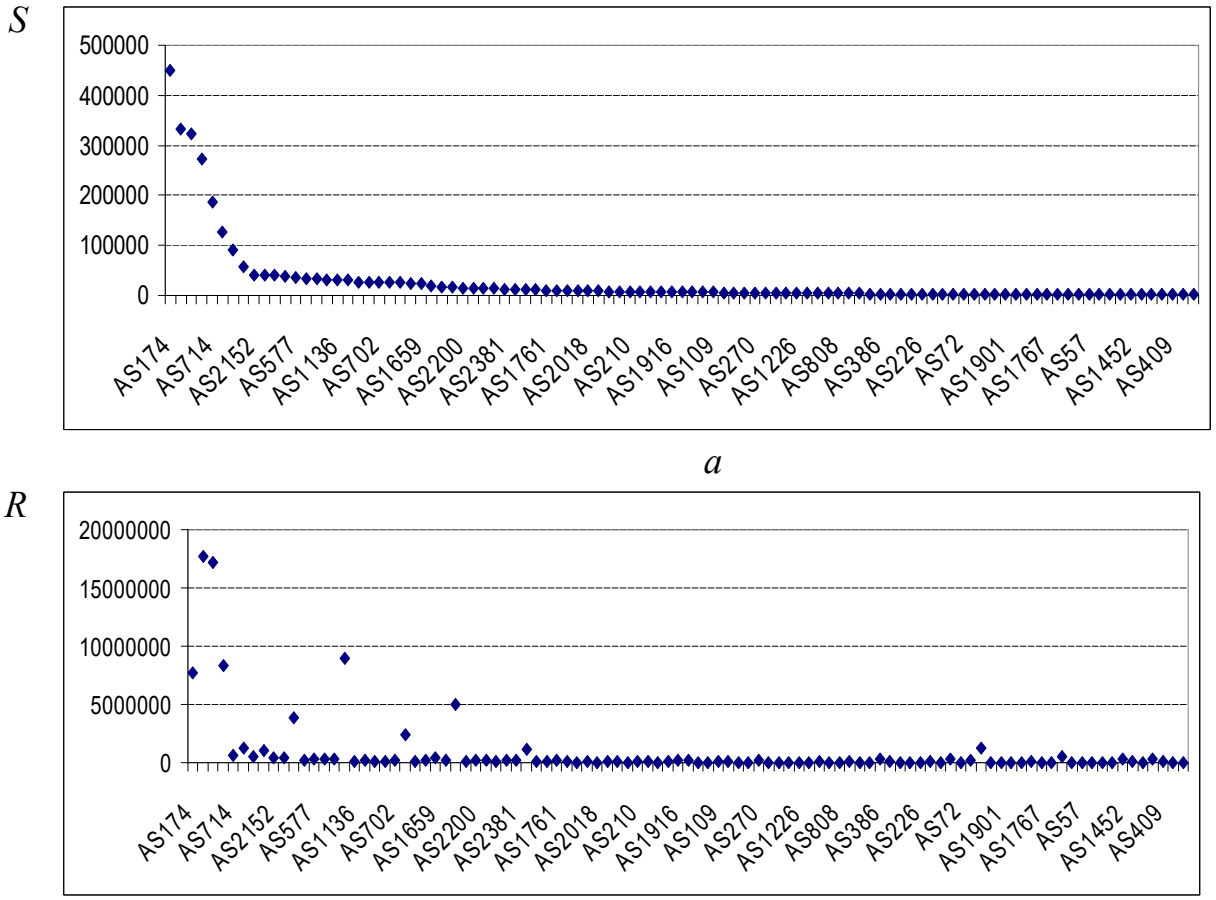
В **шостому розділі** продемонстровано результати експериментальних досліджень розробленого програмного засобу, в якому автоматизовано всі етапи методики формування топології комп’ютерної мережі Інтернет на основі оцінок ризику кібератак на глобальну маршрутизацію, а саме – аналіз топології, розрахунок ризику перехоплення маршруту в топологічному просторі окремого мережевого префіксу, моделювання нової топології, порівняння та оцінювання результатів.

В першому експерименті обраховано ризик перехоплення маршруту до префікса 195.64.224.0/22, джерелом якого є Інтернет-вузол AS8258. Для цього з прикордонних маршрутизаторів AS8258 отримано BGP-таблицю маршрутизації і виконано розрахунки метрики значущості та метрики довіри. З BGP надійшла інформація про 811143 мережевих префікса. В маршрутах були присутні ідентифікатори 68803 автономних систем, які утворили 101000 унікальних шляхів.

Після розрахунку метрики значущості S перелік AS було впорядковано

зменшення значення S. З'ясовано, що таке впорядкування має експоненційний розподіл з «важким хвостом» AS, що мають мінімальну значущість. Так, 10841 з 68803 AS мають метрику значущості 1 та менше, тому що анонсують один мережевий префікс довжиною 24 біта або взагалі лише зустрічаються у шляхах одного чи двох префіксів, що належать іншим AS.

Для подальшого аналізу відібрано 100 AS з максимальною метрикою значущості. В цій групі $1557 \le S_v^u \le 786647$. Для впорядкованої за S множини AS розраховано довіру та ризик. На рис.5,*а* на прикладі 100 вузлів з найвищою значущістю показано, як початкове ранжування вузлів змінюється під в пливом метрики довіри (рис.5,*б*).



а

б

Рисунок 5 – графіки розподілу вузлів за зменшенням значущості серед 100 AS з максимальною метрикою значущості

Впорядкування вузлів за зменшенням ризику (рис.8) уможливлює зручний спосіб зниження рівня ризику. Сумарний ризик від перехоплення маршруту можна візуалізувати як площу заштрихованої фігури. Зменшення її площі відповідає зниженню ризику.

Це продемонстровано в другому експерименті при розрахунку ризик перехоплення маршруту до префіксу 195.64.224.0/22 серед AS що є учасниками Української мережі обміну трафіком (UA-IX). З BGP надійшла інформація про 6580 AS та 31420 мережевих префікси.

Запропоновано три нових з'єднання з вузлами, що мають максимальний рівень ризику, та на новій топології повторно розраховано ризики вузлів. Сумарний ризик в новій топології виявився на 50% нижче (рис.6):

$$R1^u = 1{,}698 \cdot 10^6 \; ; \; R2^u = 8{,}6 \cdot 10^5$$

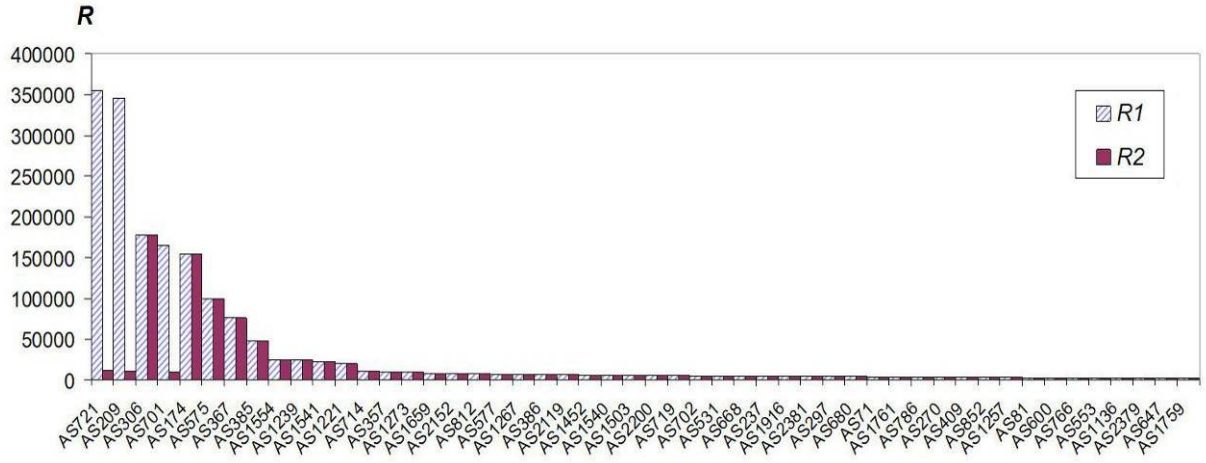


Рисунок 6 – візуалізація результатів розрахунку ефективної топології для префіксу 195.64.224.0/22

Другий експеримент проводився за участі так званих мереж обміну трафіком (Internet Exchanges, IX). IX – загальні точки підключення для суб'єктів глобальної маршрутизації, де пропонується, зокрема, вільний обмін маршрутами, що значно зменшує відстань між вузлами-учасниками. Участь інформаційних ресурсів в таких точках корисна для зниження ризику перехоплення маршруту. В Україні функціонує декілька таких мереж.

У другому експерименті було проаналізовано ризик перехоплення маршруту з точки зору учасника мережі обміну трафіком UA-IX, а потім – з точки зору учасника DTEL-IX, а на третьому етапі змодельовано топологію, коли певний вузол є учасником обох мереж. Такий уявний учасник об'єднаної топології мав ризик перехоплення маршруту майже вдвічі нижче, у порівнянні з учасником UA-IX (рис.7).

$$R1^u = 8{,}14 \cdot 10^5 \; ; \; R2^u = 4{,}24 \cdot 10^5$$

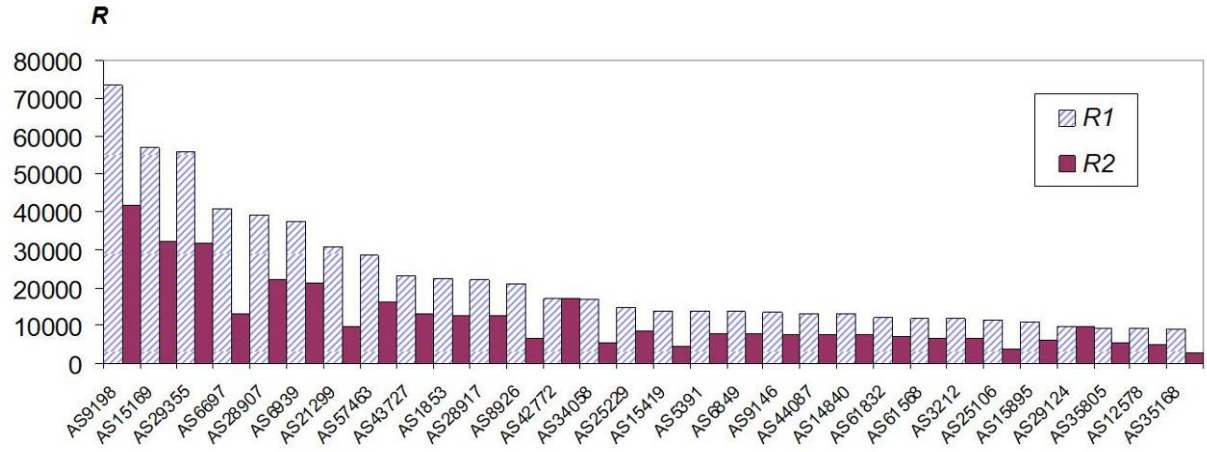


Рисунок 7 – візуалізація результатів розрахунку ризику перехоплення маршруту в результаті моделювання злиття UA-IX та DTEL-IX

Таким чином, *експериментальні дослідження 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.

За результатами розробки методики та програмного засобу отримано патент України на корисну модель та авторське свідоцтво на програмний модуль розрахунку факторів ризику перехоплення маршруту на Інтернет-вузлі за його топологічними характеристиками.

У **додатках** наведено документи, що підтверджують практичне значення та впровадження отриманих результатів.

ВИСНОВКИ

У дисертації наведено та теоретично обґрунтовано розв'язання актуальної науково-прикладної проблеми підвищення захищеності інформації проти кібернетичних атак на глобальну маршрутизацію в комп'ютерній мережі Інтернет на основі ризик-орієнтованого підходу. Це дало змогу отримати такі наукові та практичні результати:

1. Досліджено сучасний стан, архітектуру та топологію Інтернет. Встановлено, що принципи, на яких базується система глобальної маршрутизації, є ключовими в забезпеченні масштабованості комп'ютерної мережі. Виокремлено недоліки системи глобальної маршрутизації, що сприяють поширенню кіберінцидентів з перехопленням маршрутів.

Проведено аналіз і систематизацію існуючих методів протидії кібернетичним атакам на систему глобальної маршрутизації та реагування на інциденти з перехопленням маршрутів. Встановлено, що існуючі та розроблювані засоби та методики запобігання таким інцидентам мають недоліки у вигляді небажаних побічних ефектів та невизначеності стосовно можливості глобального впровадження. З урахуванням недоліків існуючих засобів та методик визначено вимоги до захисту системи глобальної маршрутизації, а саме – незалежність від масштабів впровадження, автономність при реалізації, універсальність по відношенню до суб'єктів глобальної маршрутизації, непротирічність до існуючих методів захисту системи глобальної маршрутизації, та спирання на сучасні методи управління інформаційною безпекою.

2. Вперше запропоновано варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет, що утворений системою глобальної маршрутизації на множині з'єднань між вузлами. Приведено обґрунтування того, що маршрути є елементами топології топологічного простору Інтернету, і, таким чином, кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію Інтернет, а отже – захист системи глобальної маршрутизації спрямований

на захист топології. Це в подальшому відкриває можливість застосування теорії топологічних просторів в дослідженнях системи глобальної маршрутизації.

3. Проведено структуроване ідентифікування загроз та ризиків інформаційної безпеки, що стосуються системи глобальної маршрутизації. Визначено фактори ризику, власника ризику та об’єкта захисту – інформаційного активу, функціонування якого пов'язане з Інтернет. Окреслено прийнятні для захисту методи оброблення ризику.

Отримано додаткові характеристики для уточнення моделі порушника та моделі загроз інформаційному активу. Розвинуто відому модель оцінювання ризику інформаційної безпеки DREAD за рахунок уточнення складових ризику. Ці результати спрямовані на підвищення якості рішень, які приймаються з питань захисту інформації.

4. Розроблено теоретичні засади формування метричних характеристик для оцінювання захищеності системи глобальної маршрутизаці. Сформульовано математичну модель системи глобальної маршрутизації, яка дозволила описати процес формування топологічного простору окремого мережевого префікса та топологічного простору Інтернету в цілому. Це дозволило сформувати 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.

5. Розроблено ризик-орієнтовану модель топології Інтернет, яка базується на запропонованих метричних характеристиках мережі, що походять з топологічних характеристик вузлів та характеризують безпосередні складові ризику перехоплення. Ця модель дає можливість порівняння різних топологій за рівнем захищеності шляхом розрахунку оцінки ризику перехоплення маршруту.

6. Завдяки розширенню критеріїв ефективності топології шляхом запровадження оцінки ризику кібернетичних атак на систему глобальної маршрутизації, отримала подальший розвиток методика формування ефективних міжвузлових зв'язків комп’ютерної мережі Інтернет, що дозволило автоматизувати аналіз топології, розрахунок ризику перехоплення маршруту в топологічному просторі окремого мережевого префіксу, моделювання нової топології та оцінювання результатів.

7. Відповідно до розробленої методики підвищення захищеності інформаційного активу створено програмний засіб визначення ризику перехоплення маршруту на вузлах мережі. Отримано патент України на корисну модель UA145947U та авторське свідоцтво на програмний модуль розрахунку факторів ризику перехоплення маршруту на Інтернет-вузлі за його топологічними характеристиками №101657.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації.

1. Зубок В.Ю. Поводження з ризиками від перехоплення маршруту в мережі інтернет з використанням ризик-орієнтованої моделі глобальної маршрутизації /

В.Ю. Зубок // Проблеми інформатизації та управління. – ISSN:2073-4751. – 2020. – №63. – С.34-42.

2. Зубок В.Ю. Вдосконалення топології міжмережевих зв'язків шляхом оцінки ризику / В.Ю. Зубок // Сучасні інформаційні технології у сфері безпеки та оборони. – ISSN:2311-7249. – 2020. – №3(39). – С.62-66.

3. Зубок В.Ю. Побудова та візуалізація нової ризик-орієнтованої моделі глобальної маршрутизації в комп'ютерній мережі Інтернет/ В.Ю. Зубок // Електронне моделювання. – ISSN:0204-3572. – 2020. – №42(6). – С.108-115.

4. V. Zubok. Determination Of Route Hijack Risk Components By Analysis Of The Internet Connections Topology / Vitalii Y. Zubok // Information Technology and Security. – ISSN:2411-1031. – 2020. – №7(2). – С.232-239.

5. Зубок В.Ю. Факторний аналіз ризиків на прикладі інциденту з програмним забезпеченням реєстру глобальної маршрутизації. / В.Ю. Зубок // Реєстрація, зберігання і обробка даних. – ISSN: 1560-9189. – 2020. – Т.22. – №1. – С.49-55.

6. Зубок В.Ю. Нові метрики для ризик-орієнтованого підходу до протидії атакам на глобальну маршрутизацію в Інтернеті. / В.Ю. Зубок // Електронне моделювання. – ISSN:0204-3572. – 2020. – №42(5). – С.111-119.

7. Зубок В.Ю. Аналіз захищеності інтернет-вузлів від кібератак типу перехоплення маршруту . / В.Ю.Зубок // Реєстрація, зберігання і обробка даних. – ISSN: 1560-9189. – 2020 . – Т.22. – №3. – С.58-67.

8. Зубок В.Ю. Побудова та візуалізація нової ризик-орієнтованої моделі глобальної маршрутизації в комп'ютерній мережі Інтернет. / В.Ю.Зубок // Електронне моделювання. – ISSN:0204-3572. – 2020. – №42(6). – С.108-115.

9. Зубок В.Ю. Оцінювання ризику кібератак на глобальну маршрутизацію. / В.Ю.Зубок // Електронне моделювання. – ISSN:0204-3572. – 2019. – №41(2). – С.97-110.

10. Зубок В.Ю. Поєднання традиційних методів та метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію / В.Ю. Зубок // Реєстрація, зберігання і обробка даних. – ISSN:1560-9189. – 2019 . – Т.21. – №2. – С. 41-48.

11. Зубок В.Ю. Особливості моделі порушника при аналізі атак на глобальну маршрутизацію в Інтернеті / В.Ю.Зубок // Реєстрація, зберігання і обробка даних. – ISSN: 1560-9189. – 2019 . – Т.41. – №5. – С. 59-70

12. Зубок В.Ю. Ретроспективний аналіз інцидентів кібербезпеки, пов'язаних з атаками на глобальну маршрутизацію. / В.Ю. Зубок // моделювання та інформаційні технології. – ISSN:2309-7647. – 2019. – №86. – С. 41-49.

13. Зубок В.Ю. Формальний опис об'єктів і процесів глобальної маршрутизації у мережі Інтернет для оцінки впливу кібератак на маршрутизацію / В.Ю.Зубок // Реєстрація, зберігання і обробка даних. – ISSN:1560-9189. – 2019 . – Т.21. – №4. – С.67-74.

14. Zubok V. Building Formal Model of the Internet Routing for Risk Evaluation of Cyberattacks on Global Routing / Vitalii Zubok // Information Technologies and Security (CEUR). – ISSN:1613-0073. – 2019. – №2577. – С.292-301.

15. Зубок В.Ю. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет / В.Ю. Зубок // Електронне моделювання. – ISSN:0204-3572. – 2018. – №40(5). – С.67-76.

16. Зубок В.Ю. Розпізнавання аномалій в глобальній Інтернет-маршрутизації при нечіткому описі подій / В.Ю. Зубок // моделювання та інформаційні технології. – ISSN: 2309-7647. – 2018. – №84. – С.20-27.

17. Зубок В.Ю. Дослідження зв'язку між топологією та ризиком в наслідок кібератак на глобальну маршрутизацію / В.Ю. Зубок, В.В. Мохор // моделювання та інформаційні технології. – ISSN: 2309-7647. – 2018. – №85. – С.23-26.

18. Zubok V. Метричний підхід до оцінки ризику кібератак на глобальну маршрутизацію (Metric Approach to Risk Evaluation of Cyberattacks on Global Routing) / Vitalii Zubok // Information Technologies and Security (CEUR). – ISSN:1613-0073.– 2018. – №2318. – С. 251–260.

19. Зубок В.Ю. Використання технології DNSSec для захисту доменних імен в українському сегменті мережі Інтернет / В.Ю.Зубок // Information Technology and Security. – ISSN:2411-1031. – 2017. – Vol.5 №2(9). – С.43-50.

20. Zubok V.Y. Розпізнавання аномальних станів в інформаційно-телекомунікаційних системах при нечіткому описі подій (Recognition of Abnormal State in Computer Network Systems with Fuzzy Description of Events) / Vitalii Y. Zubok, Oleksandr I. Zakharchenko, Yurii O. Belanov // Information Technologies and Security (CEUR). – ISSN:1613-0073. – 2017. – №2067. – С.41-46.

21. Мохор В.В., Зубок В.Ю. Формування міжвузлових зв'язків в Інтернет з використанням методів теорії складних мереж. - К.: Прометей, 2017. – 175С.

22. 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.

Праці апробаційного характеру.

23. Зубок В.Ю. Оцінювання стану мережі Інтернет стосовно загроз зміни її топології. *Информационные технологии и безопасность*: Материалы XV Международной научно-практической конференции. Выпуск 15. – К.: ИПРИ НАН Украины, 2015. – С.100-105. Зубок В.Ю.

24. Зубок В.Ю. Всесвітні Інтернет-провайдери в українській мережі обміну трафіком: виклики та можливості. *Информационные технологии и безопасность*. Материалы XVI Международной научно-практической конференции. Выпуск 16. – К.: ИПРИ НАН Украины, 2017. – С.156-162.

25. Зубок В.Ю., Захарченко О.І. Виявлення аномальних станів в ІТС під впливом кібернетичних атак. *Безпека в інформаційно-телекомунікаційних системах* : матеріали міжнар. наук.-практ. конф. (Київ, 25-26 травня 2017). Вип. 19. ДССЗЗІ. – Київ. – 2017.

26. Зубок В.Ю., Захарченко О.І., Бєланов Ю.О. Розпізнавання аномальних станів в інформаційно-телекомунікаційних системах при нечіткому описі подій. *Информационные технологии и безопасность* : материалы XVII международной

научно-практической конференции. Выпуск 17. – К.: ИПРИ НАН Украины, 2017. – С.92-96.

27. Зубок В.Ю. Кібератаки на глобальну маршрутизацію в Інтернеті: визначення можливих масштабів та наслідків. *Науково-технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України (до 100-річчя Національної академії наук України)* : Збірник тез конференції (Київ, 16 травня 2018). 16 травня 2018 р. – К.: ІПМЕ ім. Г.Є. Пухова НАН України. – 2018. – С.20-22

28. Зубок В.Ю., Мохор В.В. Оцінювання ризиків кібернетичних атак на глобальну маршрутизацію в мережі Інтернет. *Моделювання-2018* : Збірка праць конференції (Київ, 12-14 вересня 2018). – Київ. – К., Академперіодика.- С. 147-150.

29. Зубок В.Ю. Метричний підхід до оцінки ризику кібератак на глобальну маршрутизацію. *Информационные технологии и безопасность* : Материалы XVIII Международной научно-практической конференции (ИТБ-2018, 27 ноября 2018 года, Киев, Украина). Вип. 18, С. 43-47.

30. Зубок В.Ю. Використання моделей загроз та оцінка ризиків кібератак на глобальну маршрутизацію в Інтернеті. *XXXVIII Науково-технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України* : Збірник тез конференції (Київ, 15 травня 2019). 16 травня 2018 р. – К.: ІПМЕ ім. Г.Є. Пухова НАН України. – 2019. – С.15-18

31. Зубок В.Ю. моделювання загроз та оцінка ризиків кібератак на глобальну маршрутизацію в інтернеті. *Кібербезпека енергетики:* Збірка праць конференції. 28 травня 01 червня 2019. Одеса. – К.: Інститут проблем моделювання в енергетиці ім.. Г.Є. Пухова Національної академії наук України, 2019. – С.7-11.

32. Зубок В.Ю. Побудова формальної моделі Інтернет-маршрутизації для оцінки впливу атак з перехопленням маршрутів. *Информационные технологии и безопасность* : Материалы XIX Международной научно-практической конференции (ИТБ-2019, 28 ноября 2019 года, Киев, Украина). Вип. 19, С.196-200.

33. Зубок В.Ю. Застосування ризик-орієнтованого підходу до протидії атакам на глобальну маршрутизацію в Інтернеті. *Перспективні напрями захисту інформації*: матеріали шостої міжнародної наук.-пр. конф. (м. Одеса, 02 – 06 вересня 2020 р.). – Одеса: Бондаренко М.О., 2020. –С. 50-54.

34. V. Zubok. Topological Approach To The Risk Assessment Against The Internet Route Hijack Cyberattacs. *Science, Engineering And Technology: Global Trends, Problems And Solutions*: Conference Proceeding (Прага, Чеська Республіка, 25-25 вересня 2020). Prague: Izdevnieciba «Baltija Publishing», 2020. – p.32-37.

35. V. Zubok. New Metrics For Assessment the Risks Of the Internet Route Hijack Cyberattacs. *Інформаційні системи та технології ICT-2020* : 9-та Міжнародна науково-технічна конференція (Харків, 17-20 листопада 2020 року). – Секція 7. – С.210-213.

36. 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.

37. В. Зубок. Формування ефективної топології зв'язків в комп'ютерній мережі Інтернет на основі оцінок захищеності від кібератак на систему глобальної маршрутизації. *Безпека енергетики в епоху цифрової трансформації, Друга науково-*

практична конференція ІПМЕ ім. Г.Є. Пухова Національної академії наук України : програма та матеріали (Київ, 28-29 грудня 2020 р.). – Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2020. – С. 37-41.

Праці, які додатково відображають наукові результати дисертації.

38. Патент UA145947 U; спосіб визначення ризику перехоплення маршруту на вузлах мережі Інтернет / Зубок В.Ю., Мохор В.В., Ланде Д.В.; Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України. – заяв. u 2019 07198, 11.11.2020 р. – Опубл. 06.01.2021, Бюл. № 1.

39. Свідоцтво про реєстрацію авторського права на твір № 101657, 11.01.2021 р. Комп'ютерна програма «Програмний модуль розрахунку факторів ризику перехоплення маршруту на Інтернет-вузлі за його топологічними характеристиками» / Мохор В.В., Зубок В.Ю. – опубл. 31.03.2021, Бюл. № 63.

АНОТАЦІЯ

Зубок В.Ю. Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршрутизації. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2021.

Дисертаційна робота присвячена розвитку теоретичних засад та розробці методик підвищення захищеності топології глобальної комп'ютерної мережі Інтернет від атак на систему глобальної маршрутизації шляхом вдосконалення міжмережевих зв’язків на основі ризик-орієнтованого підходу, в якому оцінка ризику інформаційної безпеки послуговує критерієм захищеності топології.

Для досягнення поставленої мети було проведено аналіз і систематизацію існуючих методів протидії кібернетичним атакам на систему глобальної маршрутизації та реагування на інциденти з перехопленням маршрутів. З урахуванням недоліків існуючих засобів та методик визначено вимоги до захисту системи глобальної маршрутизації. Вперше 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.

Розроблено ризик-орієнтовану модель топології Інтернет, яка базується на запропонованих метричних характеристиках мережі, що походять з топологічних характеристик вузлів та характеризують безпосередні складові ризику перехоплення маршруту – ймовірність перехоплення та розмір втрат. Ця модель дозволила вдосконалити методику формування ефективних міжвузлових зв'язків комп’ютерної мережі Інтернет завдяки автоматизуванню. З метою спрощення практичного застосування запропонованої методики, її було реалізовано у вигляді програмного засобу.

Ключові слова: глобальна маршрутизація, топологічний простір Інтернет, захищеність топології, перехоплення маршруту, модель оцінки ризиків.

АННОТАЦИЯ

Зубок В.Ю. Развитие теории защищенности топологии глобальных компьютерных сетей от кибератак на систему глобальной маршрутизации. – На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Институт проблем моделирования в энергетике им. Е. Пухова НАН Украины, Киев, 2021.

Диссертация посвящена развитию теоретических основ и разработке методик повышения защищенности топологии глобальной компьютерной сети Интернет от атак на систему глобальной маршрутизации путем совершенствования межсетевых связей на основе риск-ориентированного подхода, в котором оценка риска информационной безопасности служит критерием защищенности топологии.

Для достижения поставленной цели был проведен анализ и систематизацию существующих методов противодействия кибернетическим атакам на систему глобальной маршрутизации и реагирования на инциденты с перехватом маршрутов. С учетом недостатков существующих средств и методик определены требования к защите системы глобальной маршрутизации. Впервые предложен вариант представления топологического пространства глобальной компьютерной сети Интернет, образованный системой глобальной маршрутизации на множестве соединений между узлами, и обосновано, что кибернетические атаки на систему глобальной маршрутизации являются атаками на топологию компьютерной сети.

Разработана риск-ориентированная модель топологии Интернет, основанная на ранее неизвестных метрических характеристиках сети, происходящих из топологических характеристик узлов и характеризующая составляющие риска перехвата маршрута – вероятность перехвата и размеры ущерба. Эта модель позволила усовершенствовать методику формирования эффективных связей между узлами компьютерной сети Интернет. С целью упрощения практического применения предложенной методики, она была реализована в виде программного средства.

Ключевые слова: глобальная маршрутизация, топологическое пространство Интернет, защищенность топологии, перехват маршрута, модель оценки рисков.

ABSTRACT

Zubok V.Yu. Development of the Theory of Topology Security of Global Computer Networks against Cyber Attacks on Global Routing System. – As the manuscript.

Thesis for the scientific degree of doctor of technical sciences in the specialty 05.13.05 – Computer systems and components. – Pukhov Institute for Modelling in Energy Engineering, National Academy of Sciences of Ukraine, Kyiv, 2021.

The thesis is devoted to the development of the theoretical foundations and development of methods for improving the protection of the topology of the global

computer network of the Internet from attacks on the global routing system by improving routing security with risk-based approach, in which the information security risk assessment is the criterion for efficiency of the network topology.

In the **first chapter**, an analysis and systematization of existing methods for countering cyber attacks on the global routing system. Possibility of dynamic routes change between nodes which are not physically connected is a key feature of the Internet routing. With two key concepts – one-hop forwarding in routing process and possibility of address space aggregation for routing purposes, the Internet became global and can grow virtually unlimited. However one of the most significant problems of the Internet connectivity is deriving from the Border Gateway Protocol (BGP) weaknesses – lack of verification of input routing data. It leads to so known route leaks and route hijacks. None of proposed and partially implemented upgrades and add-ons which are referred as MANRS can not deliver reliable defense against those types of attacks. Route hijack detection services are mainly provided by third-party services such as BGPMon. They track worldwide routes by tracing and keep track of route announcements in BGP and notify the network administrator of suspicious events related to their prefixes based on routing information. And the main problem is that monitoring alert is post-mortem reaction after the routing accident already happened or happening at this time. That's why it is necessary to learn how to manage risks arising from cyberattacks on global routing. As a result of the analysis, the requirements for protecting the global routing system are defined: universality – for being efficient for any global routing party, scalability – for being efficient for any number of applications on the network, self-sufficiency – for being effective for implying party independently from other parties' deeds, and non-contradictory – for being effective and supplemental to current methodology and practices.

In the **second chapter** was represented a version of the presentation of the topological space of the global computer network, formed by the global routing system on a plurality of connections between nodes. Any route to network prefix can be depicted as a topology element, and a tuple all routes provide a topology of the whole network. AS inter-AS links are the elements of topological space, spoofing links leads to emerging false topologies which could be selected by routing algorithm and become fake routes. Thus, it is reasonable that cyber attacks on the global routing system are equal to the attacks on the Internet topology.

In the **third chapter**, as a result of a complex of measures to identify threats and information security risks regarding the global routing system, additional characteristics were obtained to clarify the model of the intruder and the threat models of the information asset. The well-known risk assessment model DREAD was improved by merging with threats evaluation model STRIDE, which made it possible to make more accurate assessment and improve the quality of solutions made to information security area.

Assessing the risks of route interception requires quantitative measurement of the impact of an attack on the routing distortion, and therefore, the breach of information security. In the **fourth chapter** offered a way of exploring the topology of connections between Internet nodes to further solve the risk management task with a topology methods. In previous papers we used the knowledge of the features of the Internet topology to find the relationship between topology and global routing vulnerability. One of the most important steps was to build a formal model of global Internet routing with

formal description for objects, relations and processes of the Internet routing such as the IP address, address space, network prefix and their incapsulation, route, best path, and routing itself. In this paper we offer new node metrics for representation of both components of information security risk – possible losses and likelyhood of losses. First metrics we called 'significance' and tied it to importrance of node in routes distribution, with impact of number and weight of announced prefixes. The second metrics we called 'trust' and it reflects likelyhood of hijacking a route on a particular node. At the final, we demonstrate some empirical results of how these metrices can model the effective network topology regarding to relaxating risks of route hijack.

To assess the security of the computer network topology from attacks on the global routing system, a risk-oriented model of the topology of the Internet, based on the proposed metric characteristics of the network originating from the topological characteristics of nodes was proposed. Model characterizes the direct components of the risk of the route hijack. This model made it possible to improve the methodology for the formation of effective links between the computer network nodes through the automation of the topology analysis, calculating the risk of hijack in the topological space of a specified network prefix, modeling a new topology and evaluation of results. In order to simplify the practical application of the proposed technique, it was implemented as a software. The **fifth** and **sixth chapter** regardingly devoted to description of the metodics, its automation and empirical studies of its implementation.

Keywords: global routing, topological space of the Internet, topology security, route interception, risk assessment model.

Підписано до друку 25.03.2021 р. Формат 60x90 1/16.
Ум. друк. арк. 0,9. Обл.-вид. арк. 0,9
Наклад 100 прим. Замовлення № 638.
Віддруковано на ризографі в видавничому центрі «Принт-центр»
04053, м.Київ, вул. Січових Стрільців, 26А
Тел./факс: 486-50-88, (050)712-40-80, (097)182-07-07, 277-40-16
http://www.printc.kiev.ua; E-mail: printcentr@ukr.net