ВІДГУК

офіційного опонента про дисертаційну роботу Зубка Віталія Юрійовича «Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршртутизації», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми дисертації

Всесвітня комп'ютерна інформаційна система Інтернет, яка є найбільшою комп'ютерною мережею, розбудовувалась багато десятиліть, тобу деякі її основоположні архітектурні засади, розроблені 25 і більше років тому, не відповідають сучасному рівню кібербезпеки. Суттєві архітектурні вади єдиного протоколу глобальної маршрутизації BGP-4 впливають на безпеку функціонування Інтернет, призводять до систематичних масштабних кіберінцидентів та несуть загрозу будь-якій іншій інформаційно-телекомунікаційній системі, функціонування якої невідривно пов'язане з Інтернетом. Такими системами, зокрема, є комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу, які визначені в Законі України «Про основні засади забезпечення кібербезпеки України» як об'єкти кіберзахисту.

Кіберінциденти в глобальній маршрутизації спричинені специфічними атаками, в результаті яких «перехоплюються маршрути» - порушується зв'язність мережі, утворюються хибні маршрути та зникають легітимні шляхи. Значна частина таких атак є зумисними діями, спрямованими на порушення доступу до інформаційних ресурсів, перехоплення конфіденційної інформації, приховані дії в мережі, і т.і.

ЗПМЕ вх. 158
16.04.2021р.

Інтернет складається з мільярдів мережевих пристроїв та десятків мільйонів вузлів мережевого рівня, з яких на сьогодні понад 80000 приймають участь в глобальній маршрутизації. Ці вузли територіально розподілені по всіх континентах, розташовані в різних країнах та не мають жодного загального підпорядкування. Ця основна причина ускладнює розробку та, головне, унеможливлює загальне впровадження уніфікованих методик та засобів кіберзахисту, що реалізували б єдину політику безпеки для системи глобальної маршрутизації.

Дисертаційна робота Зубка В. Ю. «Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршртутизації» присвячена пошуку шляхів підвищення захищеності інформаційно-комп’ютерних систем, що взаємодіють з глобальною комп’ютерною мережею Інтернет, від атак на глобальну маршрутизацію в умовах відсутності в осяжній перспективі розробки та впровадження нового єдиного захищеного протоколу глобальної маршрутизації. Метою роботи є 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.

Таким чином, дисертаційна робота В.Ю. Зубка присвячена актуальній науково-прикладній проблемі.

1. Огляд змісту дисертації

В першому розділі для досягнення поставленої в дослідженні 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.

В другому розділі проведено на основі дослідження топологічної організації глобальних інформаційно-телекомунікаційних систем запропоновано варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет. В термінах системи глобальної маршрутизації визначено базу топології, описано процес утворення топології системою глобальної маршрутизації, та обґрунтовано, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію комп'ютерної мережі.

Третій розділ присвячений розвиту сучасних підходів до управління інформаційною безпекою. Узагальнені дані про кіберінциденти з системою глобальної маршрутизації, отримані в результаті ретроспективного аналізу кіберінцидентів, дозволили встановити метод, засіб, результат та наслідки кібератак, ідентифікувати ризики, конкретизувати власника ризику та об'єкт захисту – певний інформаційний актив, ідентифікований за допомогою глобальної системи адресації Інтернету.

Також запропоновано уточнення до відомих методів оцінювання ризику.

В четвертому розділі запропоновано формальний математичний опис елементів глобальної маршрутизації та їхньої взаємодії. Завдяки ним знайдено такі метричні характеристики мережевих вузлів, які, з точки зору відображають обидві складові ризику перехоплення маршруту – ймовірність перехоплення маршруту до певного мережевого префікса та збитки (масштаб перехоплення). Розроблено ризик-орієнтовану модель топології Інтернет, яка базується на запропонованих метричних характеристиках мережі і представляє розподіл вузлів за рівнем ризику перехоплення маршруту до об'єкта захисту.

В п'ятому розділі викладено методику оцінювання ризику перехоплення маршруту, запропоновано підходи до зниження ризику (а отже – підвищення захищеності) топології шляхом вирішення комбінаторної задачі вибору нової топології, оцінки та порівняння ризку з початковим значенням.

В шостому розділі приведено результати декількох експериментів із залученням реальних суб'єктів галузі надання послуг доступу до Інтернет.

2. Науковий рівень дисертації

Матеріали, викладені в дисертації, свідчать, що в ході дослідження Зубок В.Ю. отримав нові наукові результати, зокрема:

- *Вперше запропоновано* варіант представлення топологічного простору глобальної комп'ютерної мережі Інтернет, що утворений системою глобальної маршрутизації на множині з'єднань між вузлами, завдяки чому обгрунтовано, 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.
- *Вдосконалено* модель оцінювання ризику інформаційної безпеки завдяки додатковій деталізації загроз та критеріїв ризику, що забезпечує підвищення якості рішень, які приймаються з питань захисту інформації в комп'ютерній мережі Інтернет.
- *Запропоновано* новий формальний опис елементів системи глобальної маршрутизації та відношень між ними, завдяки якому *створено* математичну модель системи Інтернет-маршрутизації, яка, на відміну від існуючих моделей, дозволила описати процес формування топологічного простору окремого мережевого префікса та топологічного простору Інтернету в цілому.
- *Вперше запропоновано* ризик-орієнтовану модель топології Інтернет, яка, завдяки використанню метричних характеристиках мережі, що походять з топологічних характеристик вузлів та характеризують безпосередні складові ризику перехоплення маршруту, дозволяє досліджувати розподіл вузлів за рівнем ризику перехоплення маршруту до об'єкта захисту.

– *Розвинуто* методику формування ефективних міжвузлових зв'язків комп'ютерної мережі Інтернет, де комбінаторна задача пошуку ефективної топології вирішується шляхом запровадження відношення порядку за ризиком перехоплення маршруту.

3. Обґрунтованість і достовірність наукових результатів

Наукові положення, висновки і рекомендації, викладені в дисертаційній роботі, обґрунтовані шляхом коректного застосування методів і моделей з теорії множин, теорії графів, теорії складних мереж, теорії захисту інформації, використання відомих принципів організації комп'ютерних мереж.

Достовірність основних наукових результатів дисертаційної роботи підтверджується успішними результатами обчислювальних експериментів та досвідом практичного впровадження результатів досліджень .

4. Повнота представлення основних результатів дисертації в публікаціях

Хід дисертаційного дослідження та його основні положення достатньо повно викладено в 39 публікаціях, в тому числі 22 публікації в фахових періодичних виданнях (з них 4 – в закордонних, які проіндексовано в базі Scopus), 15 робіт апробаційного характера, один державний патент на корисну модель та одне авторське свідоцтво на програмний модуль. 5 публікацій видано англійською мовою.

Автореферат дисертації відповідає вимогам щодо його оформлення і містить дані про дисертаційне дослідження для оцінки його фахівцями.

5. Значущість результатів для науки і практики

На думку офіційного опонента, значущість проведеного дослідження в теоретичному плані полягає в розвитку відомих методів та моделей дослідження зв'язків складних комп'ютерних систем, а також методів

управління інформаційною безпекою. Крім того, в результаті дослідження отримані важливі дані, що уточнюють параметри моделі загроз та моделі порушника.

Основна практична цінність роботи полягає в розробці та впровадженні методики зниження ризику перехоплення маршруту, яка може застосовуватись незалежно кожним суб'єктом глобальної маршрутизації і не конфліктує з іншими сучасними методиками захисту глобальної маршрутизації.

Спосіб вдосконалення міжмережевих зв'язків шляхом визначення ризику перехоплення маршруту на вузлах мережі та розроблений програмний засіб оформлено патентом України на корисну модель та авторським свідоцтвом на програмний модуль.

Практичну цінність роботи підтверджують документи про впровадження результатів дисертації, які виконано у відповідних галузевих підприємствах.

6. Зауваження до дисертаційної роботи

В результаті вивчення рукопису дисертації варто, на думку опонента, привернути увагу до таких недоліків.

1. У вступній частині наводяться аргументи актуальності та масштабності проблеми безпеки системи глобальної маршрутизації. Відомо, що в Інтернеті існує ще принаймні дві масштабні проблеми, шляхи вирішення яких ускладнені з тих самих причин, що і безпека системи глобальної маршрутизації. Це, по-перше, незахищеність системи доменних імен і надто повільне впровадження технології DNSSEC, по-друге – глобальне вичерпання адресного простору IPv4 і дуже повільне впровадження IPv6. Відсутність порівняння потенційних наслідків невирішення цих трьох глобальних проблем є недоліком при обгрунтуванні актуальності.
2. В п. 2.3 за допомогою ряду тверджень пропонується встановити відповідність між маршрутами в Інтернет та топологією на множині

всіх з’єднань, що належать до маршрутів. Обгрунтовано, що будь-який маршрут належить до топології. Проте, до топології, відповідно до математичного визначення, належать і інші комбінації з’єднань, які не є маршрутами за визначенням. Бракує аналізу сутності таких елементів та їхньої відмінності від хибних маршрутів.

3. В пункті 4.7 запропоновано вирівняти вплив метрики довіри та метрики значущості на оцінку ризику за допомогою експоненти. Але за даними, представленими в експериментах, попри намагання автора, вказані метричні характеристики все одно відрізняються на 1-2 порядки. Це наводить на думку, що розмірність принаймні якоїсь однієї метрики обрано невдало.
4. Поясненню та аргументації співвідношення двох метричних характеристик в загальній оцінці ризику в розділі 4 приділено замало уваги.
5. Не надано оцінки алгоритмічної складності методу розрахунку ризику перехоплення маршруту, приблизних характеристик обчислювальних засобів для виконання методики, що є важливим для практичної реалізації та застосування результатів.
6. В експериментальній частині не згадується, які інші методи захисту топології застосовують (чи не застосовують) учасники експериментів до своїх інформаційних активів, через що неможливо пересвідчитись у відповідності розроблених підходів «вимозі непротирічності» - відсутності конфліктів з відомими методами та заходами.

Перелічені недоліки, на думку офіційного опонента, не впливають на сутність отриманих наукових результатів та не знижують наукової цінності роботи в цілому.

8. Загальний висновок

За результатами вивчення дисертації Зубка В. Ю. «Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршртутизації» та публікацій за темою дисертації, вважаю, що дана дисертаційна робота є завершеною науковою працею, в якій вирішується актуальна науково-прикладна проблема підвищення захищеності топології глобальних комп'ютерних мереж, виконаною в цілому на високому науковому рівні. Дисертаційна робота відповідає вимогам «Порядку присудження наукових ступенів», що висуваються до докторських дисертацій, а її автор Зубок Віталій Юрійович гідний присудження йому ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
завідувач кафедри обчислювальної техніки
НТУУ «КПІ імені Ігоря Сікорського»
д.т.н., проф. С.Г. Стіренко