В І Д Г У К

офіційного опонента

доктора технічних наук, професора

Юдіна Олександра Костянтиновича

на 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

Найбільшою глобальною комп'ютерною мережею та інформаційною системою є Інтернет. Її фундамент,що забезпечує постійне зростання протягом багатьох десятків років – це система глобальної маршрутизації. Але ця система не відповідає сучасному рівню кібербезпеки, що призводить до можливості проведення кібератак на маршрутизаію, тобто – несанкціонованої зміни шляхів пересилання пакетів. Такі кібернетичні атаки мають назву «перехоплення маршруту» і «витік маршруту». Механізми атак спрямовані на викривлення маршрутів до певних мережевих префіксів, а наслідками – порушення доступу до інформаційних ресурсів, порушення спостережності, несанкціонований доступ до даних, несанкціоноване використання чужого адресного простору і т.і.

Забезпечення інформаційної безпеки – це безперервний цикл моніторингу стану безпеки, виявлення інцидентів, реагування, аналізу. Системи моніторингу та виявлення інцидентів безпеки в системі глобальної маршрутизації отримали чималий розвиток, широко і вдало застосовуються учасниками глобальної маршрутизації. Але в результаті аналізу мали б бути розроблені та впроваджені надійні засоби запобігання атакам на систему глобальної маршрутизації. Однак запропоновані наразі засоби ефективні лише при стовідсотковому впровадженні на всіх вузлах мережі. Натомість, для глобальних мереж є типовим широкий територіальний розподіл вузлів, розташування в різних країнах та різне підпорядкування, і це є основною причиною неможливості розробки та впровадження уніфікованих систем захисту інформації, що реалізували б єдину політику безпеки для всієї

мережі. Комплексний підхід до захисту системи глобальної маршрутизації полягає в розробці та впровадженні нового протоколу глобальної маршрутизації BGPSec, що обговорюється 20 років, і досі дискутується достатність запропонованих в ньому засобів захисту маршрутів, а також можливість глобального впровадження.

З викладених причин актуальною науково-прикладною проблемою є підвищення захищеності системи глобальної маршрутизації Інтернет від кібернетичних атак на систему глобальної маршрутизації. 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.

2. Науковий рівень дисертації

Новизна наукових положень та результатів, отриманих особисто здобувачем, полягає в наступному:

- 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;
- запропоновано вдосконалену модель оцінювання ризику інформаційної безпеки на базі відомої моделі DREAD, яка, завдяки додатковій деталізації загроз та критеріїв ризику, забезпечує підвищення якості рішень, що приймаються з питань захисту інформації в комп'ютерній мережі Інтернет;
- 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 вцілому. Це дозволило, в свою чергу, синтезувати такі метричні характеристики мережевих вузлів, які, на відміну від відомих характеристик, відображають складові ризику перехоплення маршруту;

- вперше запропоновано метричні характеристики вузлів, які дозволяють оцінювати складові ризику перехоплення маршруту до певного мережевого префікса, що дає можливість порівняння топологій за рівнем захищеності шляхом оцінки ризиків інформаційної безпеки;
- 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.

3. Обґрунтованість і достовірність наукових результатів

Обґрунтованість і достовірність наукових результатів і висновків дисертаційної роботи забезпечуються виконаними теоретичними та експериментальними дослідженнями запропонованої ризик-орієнтованої моделі топології мережі Інтернет і методу оцінювання ефективності топології відповідно до ризику кібератак на систему глобальної маршрутизації з коректним використанням методів системного аналізу, дискретної математики, комбінаторики, теорії графів, теорії складних мереж, теорії множин, а також методи управління інформаційною безпекою. Отримані результати досліджень узгоджуються з відомими експериментальними даними та адекватно відображують досліджувані процеси, а їх достовірність підтверджується практичним використанням результатів роботи.

4. Повнота викладу основних результатів дисертації в друкованих працях

Матеріалами дисертаційної роботи достатньо повно викладено в 39 публікацій, з яких 18 публікацій у журналах, що входять до затвердженого МОН України переліку фахових видань, 4 публікації статей в закордонних виданнях, проіндексованих в міжнародній наукометричній базі Scopus, 15 публікації у працях і матеріалах міжнародних українських та закордонних конференцій, 1 позитивне ріщення на видачу деклараційного патенту України на корисну модель, та 1 авторське свідоцтво на програмний твір. 32 публікації підготовано одноособно. 5 публікацій видано англійською мовою.

5. Практичне значення отриманих результатів

Наряду з науковими, в роботі продемонстровано такі практичні результати:

- отримано характеристики кібернетичних атак на систему глобальної маршрутизації, які сприяють складанню моделі порушника та моделі загроз, що є важливим етапом проєктування системи управління інформаційною безпекою інформаційно-комп'ютерної системи, функціонування якої пов'язане з Інтернет;
- запропоновано методику оцінювання захищеності топології зв'язків інтернет-вузла, що є суб'єктом глобальної маршрутизації, яка доповнює існуючі методи протидії атакам на систему глобальної маршрутизації та спирається на сучасні методи управління інформаційною безпекою;
- 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.

В дисертації представлено документи, що підтверджують практичне впровадження результатів дисертаційної роботи в галузевих організаціях.

6. Зауваження до змісту та оформлення дисертаційної роботи

1) В результаті огляду існуючих та перспективних напрямків протидії кібератакам на систему глобальної маршрутизації, та узагальнення факторів, які перешкоджають впровадженню захисту системи глобальної маршрутизації, автором сформульовано власні вимоги до розроблюваних засад захисту системи глобальної маршрутизації, проте незрозуміло, чи вважає автор цей перелік вимог достатнім або вичерпним, та чи можуть вони слугувати критеріями оцінювання методів захисту відповідно до ДСТУ ISO/IEC 15408-2:2017.
2) Серед вразливостей системи глобальної маршрутизації виділено архітектурні вразливості протоколу BGP-4 та досліджено загрози, що з них витікають. Відсутній аналіз інших вразливостей системи глобальної маршрутизації, або аргументованого виснову їхньої несуттєвості в даному дослідженні.
3) В підрозділі 2.1 є помилки в нумерації рисунків на посилань на них.
4) Для оцінювання ризику за факторами загроз запропонована вдосконалена моделі оцінки ризику, але нема пояснення, яким чином з'являються початкові оцінки.
5) У викладеній у розділі 5 методиці оцінювання захищеності топології бракує деталізації способу застосування запропонованої в 3 розділі вдосконаленої моделі оцінки ризику, а в шостому розділі також бракує прикладу її застосування в представленні експериментів.
6) Ефективність запропонованого методу зниження ризику перехоплення маршруту мала б бути наведена у порівнянні із існуючими методами, опис яких було наведено в першому розділі (зокрема, авторизація джерела маршруту, авторизація шляху), або продемонстрована його ефективність при одночасному використанні разом із згаданими методами.
7) В матеріалах розділу 5 бракує демонстрації, як саме запропоновані моделі та методики задовольняють сформульованим в першому розділі вимогам універсальності, безмасштабності, автономності та непротирічності.

Зазначені зауваження не впливають суттєво на загальну оцінку роботи.

7. Загальний висновок

Дисертаційна робота Зубка В. Ю. «Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршртутизації» є завершеною науковою працею, в якій вирішено важливу науково-практичну задачу підвищення захищеності топології глобальної комп'ютерної мережі Інтернет від атак на систему глобальної маршрутизації шляхом вдосконалення міжмережевих зв'язків на основі ризик-орієнтованого підходу. 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 спеціальної кафедри СК-31
Навчально-наукового інституту інформаційної безпеки
Національної академії СБ України
доктор технічних наук, професор Олександр ЮДІН
«12» 04 2021 року

ПІДПИС ЗАСВІДЧУЮ
Перший проректор
Національної академії СБ України
доктор педагогічних наук, доцент Володимир АРТЕМОВ
«14» 04 2021 року