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

Актуальність теми дисертації.

Дисертаційна робота Зубка В.Ю. присвячена проблемі підвищення захищеності топологічного простору глобальної комп'ютерної мережі Інтернет від кібернетичних атак, вектором яких є система глобальної маршрутизації.

Глобальна комп'ютерна мережа Інтернет була створена і розвивається як об'єднання комп'ютерних мереж. Вона є фактично найбільшою комп'ютерною системою завдяки системі глобальної маршрутизації, але ця система є вразливою до кібернетичних атак. 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.

Система глобальної маршрутизації мережі Інтернет складається з мережевих префіксів – ідентифікаторів окремих комп'ютерних мереж, автономних систем – груп з одного чи більше мережевих префіксів під загальним керуванням, та протоколу маршрутизації BGP-4, який забезпечує обмін між автономними системами інформацією про досяжність мережевих префіксів відповідно до закладеного алгоритму та додаткових адміністративно встановлених правил, що також мають назву «політика маршрутизації». Фундаментальна основа системи глобальної маршрутизації - протокол маршрутизації BGP-4 - має вади інформаційної безпеки, які призводять до

несанкціонованої зміни шляхів пересилання пакетів. Механізми атак спрямовані на утворення хибних маршрутів до певних підмереж з метою порушення доступу до інформаційних ресурсів, перехоплення інформації, несанкціонованого використання чужого адресного простору для проведення інших кібернетичних атак тощо.

Всі методи захисту від атак, вектором яких є система глобальної маршрутизації, поділяють на два напрями. Перший напрям – реагування на інциденти, тобто виявлення та інформування про несанкціоновані зміни в глобальній маршрутизації. Він забезпечується використанням власних чи сторонніх служб моніторингу глобальної маршрутизації Другий напрям – запобігання інцидентам, тобто унеможливлення чи ускладнення перехоплення маршруту. Другий напрям здебільшого представлений методами криптографічного захисту цілісності певних атрибутів маршруту.

Всі відомі засоби та методи запобігання перехопленню маршрутів для досягнення максимально надійного захисту потребують максимально широкого впровадження, фактично на ста відсотках вузлів мережі. Але на даний момент лишається невирішеним питання достатності методів захисту, яке конфліктує з проблемою обчислювальной складності. Крім того, в історії комерційного використання комп’ютерної мережі Інтернет відсутні вдалі приклади глобального впровадження нових засобів, що зачіпляють основи її функціонування. Отже, в осяжній перспективі загрози інформаційній безпеці в наслідок атак на глобальну маршрутизацію залишаються невідворотними.

Таким чином, тема підвищення захищеності системи глобальної маршрутизації комп'ютерної мережі Інтернет, якій присвячена дисертаційна робота Зубка В.Ю., є актуальною науково-прикладною проблемою.

Науковий рівень дисертації. В дисертації відображено результати аналізу 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 було визначено вимоги до захисту системи глобальної маршрутизації. продемонстровано розроблені та вдосконалені методи, моделі, методики підвищення захищеності топології. Глобальну комп'ютерну мережу представлено як топологічний простір, що утворений системою глобальної маршрутизації. Надано обґрунтування того, що кібернетичні атаки на систему глобальної маршрутизації є атаками на топологію комп'ютерної мережі.

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.

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 нову 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. В основу моделі покладено *запропонований* в роботі формальний опис елементів системи глобальної маршрутизації та відношень між ними.

Розроблено *ризик-орієнтовану модель зв'язків 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.

Отримала подальший розвиток методика формування ефективних міжвузлових зв'язків комп'ютерної мережі Інтернет завдяки запровадженню оцінки ризику кібератак на систему глобальної маршрутизації в якості додаткового критерію ефективності топології.

Обґрунтованість і достовірність наукових результатів. Наукові положення, висновки і рекомендації, викладені в дисертаційній роботі, є достатньо обґрунтованими за рахунок коректного використання відомих принципів організації комп'ютерних мереж, методів і моделей теорії графів, теорії складних мереж, захисту інформації, елементів теорії множин та комбінаторики. Достовірність основних наукових результатів дисертаційної роботи підтверджується наведеною в розд. 2-6 системою визначень, тверджень та формальних методик, яка не містить логічних протиріч, а також збіжністю результатів авторських обчислювальних експериментів з даними, наведеними в відомих публікаціях.

Повнота викладу основних результатів дисертації в опублікованих працях. 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.

Практичне значення отриманих результатів. 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 та підвищення захищеності топології зв’язків інтернет-вузла, що є суб’єктом глобальної маршрутизації, застосування якої для аналізу фактичних зв'язків Інтернет-провайдерів дає можливість виявити найбільш ефективні рішення, які не є очевидними без її застосування;
- 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;
- наведені практичні результати дисертаційної роботи впроваджено в комерційних та державних установах, що підтверджено представленими в дисертації документами.

Практичну цінність роботи підтверджують документи про чотири впровадження результатів дисертації, три з яких виконано в організаціях відповідної галузі та спеціалізації.

Недоліки та зауваження до змісту та оформлення дисертаційної роботи. В результаті вивчення рукопису дисертації варто, на думку опонента, привернути увагу до таких недоліків та зауважень.

1) В розділі 2 автор недостатньо уваги приділив аргументації вибору бази топології, на якій утворюється топологічний простір глобальної комп’ютетрної мережі Інтернет, що його досліджує автор.
2) Авторові не вдалось остаточно перейти від застосування нечіткого визначення топології комп’ютерних мереж до чіткого визначення математичної топології. Про це свідчить словосполучення «модель топології», яке неодноразово зустрічається в тексті дисертації, зокрема на сторінках 182, 212, 285. Очевидно, що тут йдеться про

модель комп'ютерної мережі Інтернет, що описує відносини між вузлами мережі на рівні логічної структури, в той час як математична топологія є структурою, яка сама може слугувати такою моделлю.

3) Не зовсім вдало введено поняття «топологічний простір мережевого префікса», оскільки при формуванні мети та завдань дослідження йшлось про захист системи глобальної маршрутизації, а у висновках йдеться про ризик перехоплення маршруту в топологічному просторі окремого мережевого префіксу, що ускладнює розуміння зв'язку між поставленим завданням та отриманим результатом.
4) В розділі 2 при формуванні бази топології Інтернет не враховується пропускна здатність з'єднань, відсоток помилок та інші характеристики, які властиві мережам передачі даних. Аргументація такого рішення не наведена.
5) В розділі 4 серед характеристик Інтернет-вузла, які автор запропонував використовувати для формування метрики значущості *S*, відсутні типові для розподілених комп'ютерних систем кількісні характеристики вузлів, такі як продуктивність, пропускна спроможність, навантаження. Це також потребує окремого пояснення, якого бракує.
6) В тексти дисертації присутні незрозумілі посилання, зокрема: на ст. 52: «буде детально розібрано в гл.3»; на ст.151: «як описано гл.2 та гл.4»; на ст.251: «за методикою, викладеною в гл.5». Навіть якщо припустити, що йдеться про відповідні номери *розділів* дисертації, деякі посилання надані з порушенням логіки викладення матеріалу, зокрема, в третьому розділі на ст.151.

Зроблені зауваження суттєво не впливають на представлення виконаних автором наукових досліджень та отриманих результатів.

Загальний висновок. За результатами вивчення дисертації та публікацій за темою дисертації, вважаю, що дисертаційна робота Зубка В. Ю. «Розвиток теорії захищеності топології глобальних комп'ютерних мереж від кібератак на систему глобальної маршртутизації» є завершеною науковою працею, виконаною в цілому на високому науковому рівні, в якій вирішено актуальну науково-прикладну проблему підвищення захищеності топології глобальної комп'ютерної мережі Інтернет від атак на систему глобальної маршрутизації.

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
заступник директора з наукової роботи
Інституту проблем реєстрації інформації
д.т.н., проф. О.Г.Додонов