Дячук О.Ю., ст. викладач
Окунькова О.О., ст. викладач
Млинський Б.М., здобувач
Державний університет «Житомирська політехніка»

ЕВОЛЮЦІЯ ТА ПЕРСПЕКТИВИ ЗАГРОЗ BGP-HIJACKING У КВАНТОВУ ЕПОХУ

Розвиток Інтернету привів до ускладнення його інфраструктури, що зробило безпеку маршрутизації одним із пріоритетних завдань. Протокол BGP (Border Gateway Protocol) залишається основою маршрутизації глобального трафіку, однак він не передбачає вбудованих механізмів аутентифікації та перевірки достовірності маршрутних оголошень. Це створює передумови для атак на маршрутизацію, серед яких найсерйознішою є BGP-hijacking. Останні дослідження вказують на те, що поява квантових комп'ютерів може як посилити загрози, так і надати нові можливості для захисту.

Історично атаки на BGP розпочалися з локальних маніпуляцій маршрутами, але згодом отримали глобальний масштаб, що підтверджують випадки зловживання в міжнародних телекомунікаційних мережах. З розвитком штучного інтелекту автоматизація таких атак стала ще більш витонченою, а з появою квантових обчислень можливості для маніпуляції маршрутами можуть зрости експоненційно.

BGP-hijacking передбачає зловмисне внесення змін до маршрутних таблиць, що дозволяє перенаправляти трафік через неконтрольовані вузли. Основними видами таких атак є:

1. Перехоплення трафіку – перенаправлення даних через вузли, які можуть аналізувати або змінювати інформацію.
2. Дестабілізація мережі – створення конфліктів у маршрутах, що може призвести до порушення доступності певних ресурсів.
3. Фальсифікація маршрутних оголошень – видавання автономної системи за власника IP-префіксу з метою маніпуляції трафіком.

Відсутність централізованої аутентифікації у BGP призводить до того, що будь-який оператор мережі може зробити оголошення про доступність певного маршруту, навіть якщо це не відповідає дійсності. Це дозволяє зловмисникам експлуатувати вразливості маршрутизації та завдавати значної шкоди інформаційному обміну.

Основний вплив квантових технологій на безпеку BGP полягає в тому, що квантові комп'ютери мають потенціал значно вплинути на традиційні методи захисту. З одного боку, вони можуть прискорити процес зламу класичних криптографічних алгоритмів, що використовуються для захисту BGP. З іншого боку, квантова криптографія відкриває можливості для створення нових механізмів автентифікації, які будуть стійкими до атак квантових комп'ютерів.

Серед основних загроз, які може створити квантова епоха для BGP, можна виділити:

1. Злам криптографічних методів – квантові алгоритми, зокрема алгоритм Шора, здатні розшифровувати існуючі криптографічні протоколи, що робить нинішні методи аутентифікації вразливими.
2. Автоматизація атак – завдяки квантовим обчисленням можливим стає швидке тестування слабких місць у маршрутизації та прогнозування змін у мережі для її компрометації.

Попри нові загрози, квантова криптографія відкриває перспективи у створенні нових методів безпеки, які можуть підвищити захищеність BGP. Одним із найбільш перспективних напрямів є квантове розподілення ключів (QKD – Quantum Key Distribution), яке дозволяє обмінюватися криптографічними ключами так, що будь-яка спроба перехоплення буде виявлена.

Квантові комп'ютери можуть використовуватися не лише для атак, а й для їх виявлення. Завдяки здатності швидко обробляти величезні масиви даних, вони можуть аналізувати мережевий трафік у реальному часі, ідентифікуючи підозрілі маршрути.

У найближчі десятиліття, в міру того як квантові обчислення ставатимуть доступнішими, методи атак BGP-hijacking можуть кардинально змінитися. З одного боку, це підвищує загрози компрометації маршрутизації на глобальному рівні, а з іншого – змушує операторів мережевої інфраструктури адаптуватися до нових викликів. Майбутні розробки у сфері постквантової криптографії та автоматизованих систем моніторингу маршрутизації визначать стійкість Інтернету перед загрозами квантової епохи.

З огляду на майбутні виклики, необхідно розробляти адаптивні підходи до безпеки BGP, поєднуючи криптографічні, аналітичні та інтелектуальні методи захисту. Це дозволить не лише знизити ризики атак, а й забезпечити стабільність глобальних мереж у майбутньому.

Список використаних джерел:

1. Ekparinya P., Gramoli V., Jourjon G. Double-Spending Risk Quantification in Private, Consortium and Public Ethereum Blockchains. Cryptography and Security. 2018. URL: https://arxiv.org/abs/1805.05004?utm_source=chatgpt.com (дата звернення: 15.03.2025).
2. Estimating the Impact of BGP Prefix Hijacking / P. Sermpezis та ін. Networking and Internet Architecture. 2021. URL: https://arxiv.org/abs/2105.02346v1 (дата звернення: 15.03.2025).