

УДК 004.7

*Жеребцов Д.В., здобувач,
Кухар А.А., здобувач,
Сергійко В.М., здобувач,
Рудюк Б.М., асистент*

Державний університет «Житомирська політехніка»

МІГРАЦІЯ З IPv4 НА IPv6: ПРОБЛЕМИ, РИЗИКИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ

Глобальне зростання Інтернету поставило під сумнів подальшу придатність протоколу IPv4 з його 32-бітним адресним простором (приблизно 4,3 млрд адрес). Вже у 2011 році Міжнародне агентство з присвоєння адрес IANA, вичерпало запас IPv4-адрес, що спричинило використовувати необхідність впровадження проміжних механізмів, зокрема NAT для продовження життєвого циклу IPv4. Ці обхідні рішення збільшили складність мереж та створили вузькі місця в продуктивності. Натомість розроблений ще у 1990-х роках протокол IPv6 має 128-бітний адресний простір (близько $3,4 \times 10^{38}$ адрес), фактично необмежений для потреб теперішнього і майбутнього Інтернету. Перехід на IPv6 став нагальною необхідністю для підтримки масштабування мережі, появи нових технологій, таких як IoT, 5G, тощо, та усунення обмежень IPv4.

Головною причиною міграції є вичерпання адресного простору IPv4. Регіональні Інтернет-реєстри у різних частинах світу поступово повідомили про відсутність вільних IPv4-адрес протягом 2011–2015 років. Це призвело до різкого зростання вартості IPv4-адрес на вторинному ринку та залежності від NAT-технологій, що створюють затримки і проблеми з продуктивністю. IPv6 повністю розв'язує проблему нестачі адрес завдяки колосальному адресному простору, достатньому для потреб людства на непередбачуване майбутнє.

Окрім адрес, IPv6 пропонує переваги в продуктивності та маршрутизації. Зокрема, спрощений заголовок пакетів і ієрархічна адресація дають змогу зменшити таблиці маршрутизації та прискорити передачу даних, що в реальних впровадженнях дозволило знизити затримки завантаження веб-сторінок на 15–30%. Автоматична конфігурація адрес у IPv6 полегшує управління мережею, усуваючи ручне налаштування для кожного вузла. Покращення безпеки є ще одним аргументом на користь IPv6: протокол спроектовано з урахуванням безпеки, з обов'язковою підтримкою шифрування IPsec для кожного вузла, що підвищує конфіденційність і цілісність даних та зменшує ризики кібератак. Відмова від масового використання NAT

також усуває низку проблем фрагментації мережі і спрощує встановлення прямого кінцевого з'єднання між вузлами.

Перехід на IPv6 є складним багатоетапним процесом, що стикається з технічними та організаційними перешкодами. Перш за все, несумісність протоколів: IPv4 і IPv6 суттєво відрізняються, тому безпосередньо не взаємодіють між собою. Це означає, що пристрої або додатки, що підтримують лише IPv4, не можуть спілкуватися з вузлами IPv6 без спеціальних механізмів переходу. Багато застарілих мережевих пристроїв і програмного забезпечення не підтримують IPv6 або підтримують його частково. Отже, для впровадження нового протоколу часто потрібне оновлення прошивки чи заміна обладнання, що особливо складно в галузях з довгим життєвим циклом пристроїв.

Інфраструктурні виклики включають необхідність модернізації мереж: провайдерам і підприємствам доводиться налаштовувати мережеві пристрої на підтримку двох протоколів одночасно або впроваджувати шлюзи та тунелі. Це ускладнює архітектуру мережі та висуває підвищені вимоги до ІТ-персоналу. Важливим фактором є економічні витрати.

Окрім того, людський фактор теж грає роль: існує брак фахівців, добре обізнаних з IPv6, і необхідність навчати персонал новим протоколам, що потребує часу і ресурсів. У багатьох організаціях спостерігається опір змінам: поки IPv4 працює, керівники не завжди бачать негайну вигоду від впровадження IPv6. Така інерція та побоювання з приводу потенційних збоїв або проблем під час міграції уповільнюють процес переходу.

Процес впровадження IPv6 супроводжується низкою ризиків та загроз, які потребують уваги. Безпека мережі під час переходу є подвійною проблемою.

З одного боку, IPv6 покращує безпеку за рахунок вбудованого IPsec та усунення потреби в NAT. З іншого боку, поява нового протоколу відкриває нові вектори атак. Наприклад, протокол сусіднього виявлення NDP у IPv6 може бути об'єктом специфічних атак, як-то підробка оголошень сусідів або переповнення таблиць сусідства, що раніше не загрожували IPv4. Під час одночасної роботи двох протоколів зловмисники можуть шукати вразливості як в IPv4-, так і в IPv6-стеках.

Якщо ІТ-персонал менш досвідчений з налаштуваннями безпеки IPv6, існує ризик помилкової конфігурації брандмауерів або пропуску фільтрації IPv6-трафіку, що відкриває шлюзи для атак.

Операційні ризики включають можливі збої в роботі сервісів під час переходу. Некоректно налаштовані тунелі або шлюзи можуть призвести до перебоїв у зв'язку, втрати пакетів чи збільшення затримок.

Фінансові ризики пов'язані зі значними первинними інвестиціями: організація може витратити великі кошти на модернізацію, але не отримати негайної віддачі. Це вимагає стратегічного планування бюджету, щоб перехід не вплинув негативно на поточну діяльність.

Ресурсні та кадрові ризики виникають через брак спеціалістів з досвідом IPv6. Потрібно врахувати час на навчання персоналу та можливі помилки через людський фактор.

Таким чином, ефективне управління ризиками в проєктах міграції на IPv6 вимагає комплексного підходу. Він передбачає ретельне планування, тестування в безпечних сегментах, поступове впровадження та постійний моніторинг безпеки і продуктивності.

Перехід від IPv4 до IPv6 – це не просто технічне оновлення, а стратегічний імператив для глобальної мережевої інфраструктури. Сучасний Інтернет вже не може розвиватися на базі обмеженого IPv4, адже вимоги адресації, продуктивності і безпеки зросли багаторазово.

IPv6 пропонує необхідні рішення:

- практично невичерпну адресацію;
- вбудовані засоби безпеки;
- ефективнішу маршрутизацію.

Водночас цей перехід потребує значних зусиль і передбачає подолання згаданих труднощів – від технічних проблем сумісності до економічних витрат і навчання кадрів.

Отже, IPv6 однозначно стає невід'ємною частиною майбутнього Інтернету. Своєчасна та продумана міграція на IPv6 є критичною умовою для забезпечення стійкого функціонування, безпеки та конкурентоспроможного розвитку мережевих ресурсів у світовому масштабі.

Список використаних джерел:

1. Kane A. Challenges and Benefits of Shifting from IPv4 to IPv6 // Scientific Research Publishing. 2025. DOI: <https://doi.org/10.4236/ijids.2025.72002>
2. Gundarwala Y., Deputy M., Patel P. Transitioning from IPv4 to IPv6: Strategies, Challenges, and Adoption Status // International Journal of Engineering Research & Technology. 2024. URL: <https://www.ijert.org/transitioning-from-ipv4-to-ipv6-strategies-challenges-and-adoption-status>