РОЛЬ КЛАСИЧНИХ МЕРЕЖЕВИХ ACL У СУЧАСНІЙ АРХІТЕКТУРІ ZERO TRUST

Рой Є.О., Доленко О.Д., Поддубний В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток інформаційно-комунікаційних технологій, масовий перехід до хмарних обчислень, гібридних моделей роботи та концепції Bring Your Own Device (BYOD) повністю розмив традиційні межі корпоративних мереж [1]. Класична парадигма мережевої безпеки, яка спиралася на концепцію периметрового захисту, більше не здатна забезпечити ефективний захист від несанкціонованого доступу та внутрішніх інцидентів [2]. Відповіддю на ці виклики стала розробка концепції архітектури нульової довіри (Zero Trust Architecture, ZTA), формалізованої у стандарті NIST SP 800-207 [2, 3]. Фундаментальним принципом ZTA є абсолютна відсутність неявної (апріорної) довіри до будь-якого суб'єкта, пристрою чи мережевого з'єднання, незалежно від його фізичного чи логічного розташування стосовно периметра організації [2]. У цьому зв'язку виникає важлива науково-практична задача оцінки місця, функціональних можливостей та перспектив використання класичних мережевих списків контролю доступу (Access Control Lists, ACL) у сучасних високоефективних екосистемах захисту.

Метою доповіді є систематичний аналіз трансформаційної ролі класичних мережевих ACL при переході від периметрової моделі безпеки до ZTA, визначення їхніх технічних обмежень у динамічних середовищах та обґрунтування оптимальної моделі їхньої інтеграції у складі точок виконання політик (Policy Enforcement Points, PEP).

Класичні ACL функціонують на мережевому та транспортному рівнях моделі OSI (L3/L4), виконуючи пакетну фільтрацію на основі заголовків пакетів: IP-адрес джерела та призначення, номерів портів і типів протоколів [4]. Головною архітектурною перевагою ACL є їхня апаратна реалізація безпосередньо у спеціалізованих мікросхемах (ASIC) мережевого обладнання – маршрутизаторів, комутаторів та базових брандмауерів [4]. Це забезпечує високу швидкість обробки трафіку, мінімальну затримку та відсутність значного навантаження на обчислювальні ресурси [4]. На рівні мережевої інфраструктури ACL виконують критичну функцію первинного рубежу оборони: відсікають нелегітимний трафік, запобігають поширенню несанкціонованих запитів та забезпечують мікросегментацію мережевих зон [4]. Водночас, статичні ACL мають низку системних обмежень, які унеможливлюють їхнє використання як єдиного або основного інструменту розмежування доступу в концепції Zero Trust [2, 4]. По-перше, ACL не володіють контекстною обізнаністю – вони не спроможні аналізувати ідентичність користувача, рівень його привілеїв, атрибути контексту сесії, стан безпеки кінцевого пристрою та поведінкові ризики [4]. По-друге, у динамічних хмарних і мобільних середовищах ручне адміністрування статичних правил призводить до їхнього непропорційного розростання, виникнення конфліктів, дублювання та затінення правил [4].

Складність супроводження сотень локальних ACL на різнорідному обладнанні створює ризики помилок конфігурації [2, 4]. Відповідно до базової моделі NIST SP 800-207, ZTA чітко розділяє площину управління та площину даних [2]. Центральними елементами площини управління є двигун політик (Policy Engine, PE) та адміністратор політик, які разом утворюють точку прийняття рішень [2]. У такій архітектурі класичні мережеві ACL трансформуються зі статичних автономних конфігурацій у гнучкий виконуючий механізм нижнього рівня у складі точок виконання політик (PEP) [2, 5]. Сучасні дослідження демонструють високу ефективність синергії ACL із системами моніторингу та алгоритмами штучного інтелекту (ШІ) й машинного навчання [6]. На основі безперервного моніторингу аномалій ШІ-модуль автоматично формує та реконфігурує правила ACL в режимі реального часу, забезпечуючи динамічну адаптацію політик до поточних умов [5]. Практична реалізація Zero Trust у корпоративних інфраструктурах вимагає гібридного підходу до розмежування доступу [2]. Інструменти ZTNA (Zero Trust Network Access) забезпечують гранульований, ідентифікаційно-орієнтований доступ безпосередньо до окремих застосунків на рівні L7 [2]. Натомість класичні ACL зберігають своє фундаментальне значення для забезпечення базової мережевої гігієни: захисту інфраструктурних інтерфейсів управління, ізоляції технологічних мереж та пристроїв без можливості встановлення агентів за допомогою спеціалізованих апаратних шлюзів ізоляції [2].

Отже, класичні мережеві ACL не втрачають своєї актуальності в епоху Zero Trust, проте змінюють своє функціональне призначення. З автономного інструменту розмежування доступу вони перетворюються на високошвидкісний підпорядкований елемент PEP. Гібридна інтеграція апаратного потенціалу ACL із динамічними ZTNA-платформами та ШІ-керованим моніторингом дозволяє досягти оптимального балансу між високою продуктивністю мережі та надійною безпекою за принципами Zero Trust.

Список літератури

1. Нечволод К. В., Сєвєрінов О. В., Власов А. В. Аналіз безпеки даних в EMM системах. Системи управління, навігації та зв'язку. Збірник наукових праць. 2019. Т. 3, № 55. С. 131–134. DOI: https://doi.org/10.26906/SUNZ.2019.3.131.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020. 59 p. DOI: https://doi.org/10.6028/NIST.SP.800-207 (date of access: 24.10.2026).

3. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems. Computer and Information Systems and Technologies: Proceedings of the Seventh International Scientific and Technical Conference. Kharkiv: KNURE, 2024. P. 54–55.

4. Kannan Y. Access control list (ACL) Compliance Verification and Alarm Systems: Strengthening Network Security. Authorea Preprints. 2024. DOI: https://doi.org/10.22541/au.171011477.72357180/v1 (date of access: 24.10.2026).

5. AI-Driven Analysis for Network Systems: Enhancing IDS Alerts and ACL Integration. International Journal on Advances in Security, 2024. pp. 1–10. URL: https://www.thinkmind.org/articles/sec_v17_n34_2024_1.pdf (date of access: 24.10.2026).