

ВІД PERIMETER SECURITY ДО ZERO TRUST: ПОРІВНЯЛЬНИЙ АНАЛІЗ ТА ПРАКТИЧНІ ПІДХОДИ ДО ПОБУДОВИ ЗАХИЩЕНИХ ІТ-СИСТЕМ

Вінницький національний технічний університет

Анотація

Zero Trust є сучасною моделлю захисту інформації, що базується на принципі "не довіряй, перевіряй". Вона полягає у тому, що доступ до ресурсів повинен контролюватися на кожному етапі взаємодії з мережею. Ця парадигма набуває великої поширеності у сфері корпоративної безпеки та дозволяє захищати дані у контексті хмарних середовищ та гібридних моделей роботи. Розглянуто еволюцію парадигм безпеки, принципи та механізми обох моделей, їхню ефективність у контексті сучасних кіберзагроз, хмарних сервісів та розподілених інфраструктур. Особливу увагу приділено практичним аспектам імплементації Zero Trust, включаючи аудит активів, мікросегментацію, автентифікацію, контроль доступу та моніторинг.

Ключові слова: Zero Trust, perimeter security, кібербезпека, мікросегментація, контроль доступу, автентифікація, хмарні технології, SASE, архітектура безпеки, ідентичність, мережеві загрози.

Abstract

Zero Trust is a modern information security model based on the principle of 'don't trust, verify.' It means that access to resources must be controlled at every stage of interaction with the network. This paradigm is becoming increasingly widespread in the field of corporate security and allows data to be protected in the context of cloud environments and hybrid working models. The evolution of security paradigms, the principles and mechanisms of both models, and their effectiveness in the context of modern cyber threats, cloud services, and distributed infrastructures are considered. Particular attention is paid to the practical aspects of Zero Trust implementation, including asset auditing, micro-segmentation, authentication, access control, and monitoring.

Keywords: Zero Trust, perimeter security, cybersecurity, microsegmentation, access control, authentication, cloud technologies, SASE, security architecture, identity, network threats.

Вступ

Зростання цифровізації та хмарних технологій стало розчиною для старих моделей кібербезпеки. Традиційні техніки периметрової орієнтації вже не спростовуються з моделями гібридної роботи, BYOD та винесенням даних за межі локальної мережі. У цьому контексті появилася потреба у новій парадигмі безпеки, що не покладається на локацію користувача чи рівень довіри до перевіреного об'єкта. Ці засади стали основою для концепції Zero Trust.

Метою роботи є здійснення глибокого порівняльного аналізу perimeter security та Zero Trust, визначення їхніх переваг, недоліків і сфер ефективного застосування, а також розгляд практичних аспектів переходу до Zero Trust у сучасних ІТ-системах. Робота також висвітлює ключові виклики впровадження та перспективи подальшого розвитку архітектур безпеки.

Результати дослідження

Традиційна модель безпеки мережі (perimeter security) базується на ідеї мережевого периметра – своєрідного «замку», за межами якого знаходиться потенційна загроза, а всередині – безпечне «королівство». Центральними компонентами цієї моделі є брандмауери (firewalls), VPN, системи виявлення/запобігання вторгнення (IDS/IPS) та демілітаризовані зони (DMZ). Ці засоби працюють як бар'єри, що контролюють вхідний і вихідний трафік та забезпечують захист від зовнішніх атак.

Проте така модель має суттєві обмеження. По-перше, вона припускає, що всі ресурси всередині мережі є довіреними – після того, як користувач або пристрій пройшов аутентифікацію, йому може бути надано досить широкий доступ. Це створює ризик «горизонтального руху» зловмисника (lateral movement): якщо периметр буде зламаний, атакуючий може вільно пересуватися всередині мережі,

маючи значні привілеї. NIST теж звертає увагу, що периметрові фаєрволи добре захищають від зовнішніх загроз, але «менш корисні для виявлення та блокування атак зсередини» або для захисту віддалених пристроїв [1].

По-друге, традиційний підхід не справляється добре з новими тенденціями – хмарними сервісами, віддаленими працівниками, мобільними пристроями. Як зауважують експерти, традиційна perimeter security стає все менш ефективною, оскільки межі мережі розмиваються, а користувачі підключаються з будь-якого місця. Крім того, обмежена видимість всередині периметра – ще один виклик: системи безпеки, що концентруються на граничному контролі, часто не забезпечують повний журнал активностей та не дають достатньої аналітики внутрішніх дій, що ускладнює виявлення інсайдерських загроз. Підсумовуючи, модель perimeter security залишається корисною, але в сучасних умовах вона має серйозні вади й не відповідає потребам захисту в епоху хмар, мобільності та складних внутрішніх загроз [2].

Поява концепції Zero Trust (нульової довіри) стала реакцією на невідповідність класичної моделі безпеки новим викликам: компрометації периметра, складним хмарним ландшафтам, а також загрозам зсередини організації. Основна ідея Zero Trust полягає в тому, що жодному користувачеві, пристрою чи запиту не можна довіряти за замовчуванням, навіть якщо він вже перебуває «всередині мережі». NIST у своїй спеціальній публікації SP 800-207 чітко формулює цю парадигму: організація має постійно перевіряти довіру (identity, пристрій, контекст), а також застосовувати політики з мінімальними привілеями (least privilege) і припускати, що порушення безпеки можливе (assume breach).

Фішинг та соціальна інженерія залишаються серйозними загрозами в сучасному цифровому світі. Поєднання технічних, освітніх та організаційних заходів є ключем до ефективної протидії цим атакам. Постійне підвищення обізнаності користувачів та впровадження новітніх технологій можуть значно знизити ризики, пов'язані з фішингом та соціальною інженерією.

Важливо розуміти, що кіберзлочинці постійно вдосконалюють свої методи, адаптуючись до нових захисних механізмів. Тому захист від таких загроз має бути динамічним процесом, а не одноразовим заходом. Організації повинні регулярно проводити навчання персоналу, симулювати фішингові атаки для підвищення пильності працівників та впроваджувати багаторівневі системи захисту.

Особливо вразливими до атак соціальної інженерії є нові користувачі цифрових технологій, люди похилого віку та особи, які не мають достатньої обізнаності щодо кібербезпеки. Тому важливо проводити широкомасштабні освітні кампанії, спрямовані на різні верстви населення.

У кінцевому підсумку, людський фактор залишається найслабшою ланкою в системі кібербезпеки. Навіть найдосконаліші технічні засоби захисту можуть виявитися неефективними, якщо користувач добровільно надає свої дані під впливом психологічних маніпуляцій. Саме тому формування культури кібербезпеки та критичного мислення має стати пріоритетом для суспільства в епоху цифрової трансформації [1].

Крім того, для реалізації Zero Trust використовуються різні технології: багатофакторна автентифікація (MFA), системи управління ідентичністю (IAM), програмно-визначені периметри (SDP), мікросегментація, а також рішення для моніторингу й аналізу поведінки. Це не просто новий набір інструментів – це нова архітектурна стратегія. Перехід до Zero Trust – це поступовий процес, а не одноразова технологічна заміна: багато організацій сьогодні перебувають у «гібридному» режимі, де частина мережі все ще захищається периметровими засобами, а частина – за моделлю ZT [3].

Щоб чітко зрозуміти різницю між традиційною perimeter security і Zero Trust, доцільно розглянути їхні ключові характеристики в порівнянні (табл.1).

Таблиця 1 – Порівняльний аналіз perimeter security та Zero Trust

Критерій	Perimeter Security	Zero Trust Architecture (ZTA)
Модель довіри	Імпліцитна довіра після входу в мережу	Жодної довіри за замовчуванням (“never trust, always verify”)
Контроль доступу	Широкий доступ після аутентифікації (наприклад, VPN, внутрішні ресурси)	Гранулярний доступ, заснований на ідентичності, контексті та політиках “least privilege”

Продовження табл. 1

Сегментація мережі	Зазвичай велика мережа з обмеженою сегментацією	Мікросегментація: поділ на дрібні зони з окремими політиками доступу
Моніторинг і логування	Обмежене внутрішнє спостереження, реагування в основному реактивне	Безперервний моніторинг, поведінковий аналіз, контекстна оцінка доступу, реакція в реальному часі
Припущення про загрози	Припускається, що загрози переважно зовнішні	Припускається, що порушення можуть бути в будь-якому місці
Гнучкість для хмари/мобільності	Обмежена – периметр стає розмитим	Висока: підтримка хмар, віддаленої роботи, IoT, мікросервісів

У традиційній моделі *once-in, trusted*; у ZTA – перевірка при кожному запиті. Zero Trust мінімізує права, даючи лише те, що справді потрібно (*least privilege*), тоді як у *perimeter security* доступ може бути надто широким. Мікросегментація ZTA значно обмежує рух всередині мережі навіть після входу користувача, що знижує ризик при компрометації [4]. У Zero Trust системи постійно збирають телеметрію, аналізують поведінкові патерни та приймають рішення на основі контексту. ZTA оптимально підходить для сучасних ІТ-систем, де кордони мережі не мають чітких меж [2].

Такий порівняльний аналіз демонструє, що Zero Trust – це не просто “оновлення *firewall*”, а фундаментальна переорієнтація безпеки.

Однією зі стрижнів Zero Trust є ідентичність користувача або пристрою. Впровадження багатофакторної автентифікації (MFA), централізованих систем ідентифікації (IdP), а також політик, що визначають, який рівень доступу має бути наданий за певного контексту (наприклад, час, місцезнаходження, стан пристрою) – це критичні кроки. За допомогою IAM можна реалізувати принцип «*least privilege*», тобто надати користувачам мінімальні привілеї, які їм насправді потрібні для їхніх задач [5]. Крім того, організація повинна мати можливість оцінювати стан пристрою перед наданням доступу. Наприклад, перевіряти, чи встановлені оновлення, чи пристрій відповідає політикам безпеки, перш ніж надати привілеї.

Ще один дуже важливий підхід – поділ мережі на дрібні сегменти (мікросегментація). Це означає, що внутрішня мережа не є єдиним великим довіреним простором: навіть після аутентифікації доступ до ресурсів обмежується відповідними зоною та політиками. Такий підхід суттєво обмежує потенціал зломисника рухатися латерально (*lateral movement*). Для реалізації мікросегментації організації можуть використовувати різні інструменти – від програмних елементів (агенти) на кінцевих пристроях до програмно-визначених рішень, які керують мережевим трафіком і контролюють політики безпеки. Наприклад, платформа Tufin забезпечує візуалізацію мережі, автоматизацію політик безпеки й підтримку мікросегментації [6].

Zero Trust передбачає постійне спостереження: не лише логування, а й аналітику поведінки. Організації встановлюють системи SIEM (Security Information and Event Management), UEBA (User and Entity Behavior Analytics), щоб відстежувати аномалії, що можуть вказувати на підозрілу активність. Цей моніторинг дозволяє приймати рішення в реальному часі – наприклад, якщо поведінка пристрою або користувача раптово змінюється (геолокація, новий пристрій, незвичний час доступу), система може підвищити ступінь перевірки або навіть обмежити доступ [5].

Оскільки Zero Trust включає великі й детальні політики доступу, їхнє ручне управління може стати важким і помилковим. Тому багато організацій використовують автоматизацію – *policy-as-code*, контролери прийняття рішень, точки примусового виконання, які автоматично застосовують політики на основі поточного контексту. Наприклад, платформи, як Tufin, допомагають автоматизувати й адаптувати політики безпеки в мережах, знижуючи ручну працю та ризик помилок [6].

Більшість компаній не переходить на Zero Trust відразу “все й одразу”. Замість цього використовують поетапну стратегію: спочатку впроваджують ключові компоненти (наприклад, IAM та мікросегментацію критичних сервісів), потім розширюють модель на інші частини системи. Також важливо створити програму змін (*change management*): потрібен міжфункціональний офіс Zero Trust, підтримка з боку керівництва, чітка комунікація, щоб працівники розуміли, чому новий підхід впроваджують, як він вплине на їхню роботу, і що дасть бізнесу [7].

У разі, якщо частина або вся інфраструктура розміщена в хмарі, або у співробітників є віддалений доступ, Zero Trust-архітектура має охоплювати *workload* (робочі навантаження), API, дані. Наприклад,

використовуються рішення для сегментації між сервісами в хмарі, перевірки ідентичності при доступі до хмарних ресурсів, шифрування даних у польоті та в стані спокою [5].

Незважаючи на численні переваги, багато організацій стикаються з серйозними перешкодами при переході на Zero Trust. Ось найпоширеніші бар'єри [8-10]:

- Легасі-системи (Legacy infrastructure). Багато компаній мають старі додатки й інфраструктуру, які не підтримують сучасні засоби контролю доступу, автентифікацію або мікросегментацію. Інтегрувати ці системи в Zero Trust-архітектуру часто складно, дорого або навіть технічно неможливо без серйозного оновлення або рефакторингу.

- Культурні та організаційні зміни. Перехід на Zero Trust – це не просто технічний проект, а зміна мислення: співробітники звикли до “всередині мережі – безпечного” підходу. Нові вимоги (часті перевірки, більше автентифікацій, строгі політики) можуть зустріти опір. Організаційні команди (безпека, мережі, IAM) повинні працювати дуже тісно, що не завжди просто [8].

- Вартість. Zero Trust рішення можуть вимагати значних початкових інвестицій: ліцензії для IAM, інструменти мікросегментації, агентські рішення, аналітичні системи (SIEM, UEBA), а також ресурси для проектування і впровадження. Для багатьох організацій це велике фінансове навантаження, особливо якщо бюджет обмежений.

- Недостатність кваліфікованих кадрів. Впровадження Zero Trust вимагає висококваліфікованих фахівців: архітектори безпеки, експерти IAM, аналітики поведінки, інженери автоматизації політик. Не всі організації мають такі ресурси або можуть їх швидко найняти.

- Складність з користувацьким досвідом (UX). З одного боку, Zero Trust підвищує безпеку, але може ускладнити роботу для користувачів: часті перевірки, MFA, додаткові кроки автентифікації – все це може знизити зручність або продуктивність. Баланс безпеки й зручності – це часта проблема, яку потрібно враховувати під час проектування політик.

Перспективи розвитку Zero Trust сьогодні – це не просто черговий тренд у кібербезпеці, а справжній фундамент для майбутніх архітектур систем, який відповідає на нові виклики світу, що стрімко змінюється. Далі – ключові напрямки, які, ймовірно, визначать майбутнє ZT.

Один із найпомітніших трендів – це глибока інтеграція AI/ML до Zero Trust. Алгоритми машинного навчання дозволяють здійснювати динамічну оцінку ризику, аналіз поведінки користувачів і пристроїв, автоматизоване прийняття політик доступу на основі поточного контексту. За прогнозами експертів, ZT-архітектури стануть ще «розумнішими» – AI відповідатиме за формування оцінок ризику в режимі реального часу, коригування прав доступу та адаптацію політик без втручання людини [11].

Розвиток бездротових мереж (5G, а далі – 6G) і масштабне поширення пристроїв IoT означають, що число «ідентичностей» у системі значно зросте. Для захисту таких систем потрібно переосмислювати ZT-модель. Дослідники пропонують архітектури, в яких принципи Zero Trust вбудовані безпосередньо у життєвий цикл AI-моделей, що працюють на граничних пристроях (edge). У контексті IoT це означає: перевірка кожного повідомлення, верифікація пристрою, використання мікросегментації, а також захист даних на рівні моделювання (наприклад, через федеративне навчання або блокчейн-ідентичність). У статті з arXiv описано концепцію Zero-Trust Foundation Models (ZTFM), яка поєднає поведінкову аналітику, мікросегментацію та перевірку даних, щоб забезпечити безпечну AI-інфраструктуру для IoT [12].

У міру розвитку квантових обчислень традиційна криптографія може опинитися під загрозою. У відповідь на це вже з'являються ідеї квантово-стійкої Zero Trust-архітектури, яка підтримує нові криптографічні підходи (наприклад, lattice-based алгоритми) для обміну ключами та мікросегментації безпечним чином. Це дає змогу підготуватися до майбутнього, коли квантові атаки стають реальністю [12].

Із зростанням складності Zero Trust-імплементацій компанії все більше співпрацюють із зовнішніми системними інтеграторами і консультантами. За даними аналітиків, багато організацій вже включають у свої ZT-плани спеціальних партнерів, які допомагають з проектуванням, впровадженням та адаптацією під індустріальні стандарти. Ця тенденція не лише підсилює можливості впровадження, а й прискорює масштабування ZT як стратегії [3].

У майбутньому автоматизація стане ще важливішою. Політики доступу будуть формалізовані як код (policy-as-code), рішення прийняття рішень (PDP) та їх виконання (PEP) – автоматично керуватимуть доступом на основі аналітики та контексту. Такі підходи підвищують швидкість реагування, знижують помилки, пов'язані з ручним адмініструванням, і дозволяють масштабувати Zero Trust [11].

Висновки

Перехід від традиційної моделі perimeter security до архітектури Zero Trust є закономірним етапом розвитку кібербезпеки в умовах хмарної трансформації, розподілених інфраструктур і підвищеної мобільності користувачів. Периметровий підхід більше не відповідає сучасним викликам, оскільки ґрунтується на застарілому припущенні про безпеку внутрішньої мережі. Натомість Zero Trust відмовляється від довіри за замовчуванням та покладається на постійну перевірку, принцип мінімальних привілеїв, оцінку контексту, мікросегментацію й детальний контроль доступу.

Практична реалізація Zero Trust показує, що найбільш ефективно працюють комплексні підходи, які включають якісне управління ідентичністю, контроль стану пристроїв, сегментацію середовища, поведінкову аналітику, постійний моніторинг активності та автоматизацію політик. Поступова імплементація, підтримана змінами в організаційній культурі, дозволяє знизити ризики, мінімізувати збої та адаптувати модель до потреб бізнесу.

Водночас впровадження Zero Trust супроводжується низкою бар'єрів – технічних, організаційних та економічних. Старі системи часто несумісні з новими підходами, компаніям бракує кваліфікованих фахівців, а зміни у звичному процесі роботи можуть викликати опір персоналу. Незважаючи на це, світові тенденції демонструють, що Zero Trust дедалі активніше інтегрується в державні стандарти, корпоративні політики та хмарні сервіси.

Перспективи розвитку Zero Trust пов'язані з автоматизацією, інтеграцією зі штучним інтелектом, масштабуванням у сферу IoT та формуванням архітектур «Zero Trust by default». У майбутньому Zero Trust, імовірно, стане основою безпекових стандартів, на яких будуть будуватися як корпоративні, так і державні IT-системи. Це дозволить створити більш стійкі, адаптивні та захищені інформаційні середовища в умовах зростаючого рівня кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rose S., Borchert O. Zero Trust Architecture. *NIST Special Publication 800-207*. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf> (date of access: 10.11.2025).
2. What Is Zero Trust Architecture? Key Elements and Use Cases. *Palo Alto Networks*. URL: <https://www.paloaltonetworks.in/cyberpedia/what-is-a-zero-trust-architecture> (date of access: 10.11.2025).
3. Ichiriu M. A Guide to the NIST Zero Trust Architecture. *Zero Trust Security Solutions for Critical Asset Defense & Enterprise Resilience*. URL: <https://www.zentera.net/blog/nist-zero-trust-architecture> (date of access: 10.11.2025).
4. Ezebuike M. Understanding NIST 800-207: The Blueprint for Zero Trust Architecture. *LinkedIn: Log In or Sign Up*. URL: <https://www.linkedin.com/pulse/understanding-nist-800-207-blueprint-zero-trust-ezebuike-michael-5sape/> (date of access: 10.11.2025).
5. Zero Trust архітектура: Впровадження і майбутнє корпоративної безпеки – IT ORAKUL. *IT Orakul*. URL: <https://itorakul.com.ua/zero-trust-arhitektura/> (дата звернення: 11.11.2025).
6. Zero Trust з Tufin: Мікросегментація та Безпека. *Провідний IT-дистриб'ютор України | Мережеві рішення безпеки*. URL: <https://nwu.ua/blog/tufin/vprovadzhennya-zero-trust-z-tufin-povnij-posibnik-dlya-tehnichnih-fahivtsiv/> (date of access: 11.11.2025).
7. Zero Trust без потрясінь: як перейти на нову модель кіберзахисту без ризику для бізнесу. *Бізнес новини України | Бізнес UA*. URL: <https://businessua.com/telekom/107090zero-trust-bez-potryasin-yak-pereiti-na-novu-model-kiberzahistu-bez-riziku-dlya-biznesu.html> (date of access: 12.11.2025).
8. timesofexplore. Zero Trust Cybersecurity Guide 2025: Implementation & ROI. *Times of explore*. URL: <https://www.timesofexplore.com/2025/09/zero-trust-cybersecurity-guide-2025.html> (date of access: 12.11.2025).
9. Zero Trust Architecture: The Ultimate Guide to Modern Security (2025). *Liquidity Feed*. URL: https://liquidityfeed.com/article/what-is-the-zero-trust-network-security-model/?utm_source=chatgpt.com (date of access: 14.11.2025).
10. Carter E. Zero Trust Architecture 2025: Adoption Guide. *Online Hash Crack*. URL: <https://www.onlinehashcrack.com/guides/cybersecurity-trends/zero-trust-architecture-2025-adoption-guide.php> (date of access: 14.11.2025).

11. K N. 17 Zero Trust Key Trends to Watch in 2025. *LinkedIn: Log In or Sign Up*. URL: <https://www.linkedin.com/pulse/17-zero-trust-key-trends-watch-2025-neha-kulkarni-myjyf/> (date of access: 15.11.2025).

12. Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *arXiv.org*. URL: <https://arxiv.org/abs/2505.23792> (date of access: 15.11.2025).

Пінчук Дар'я Олександрівна – студентка групи ІКІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: **Бондаренко Ірина Олексіївна** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Pinchuk Daria O. – student of group IKITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor: **Bondarenko Iryna O.** – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua