КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.864
УДК 004.056.5

Маньковський Богдан Олегович
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0009-0001-3857-9842
bohdan.mankovskyi.kb.2023@lpnu.ua

Довбняк Владислав Олегович
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0009-0005-5494-3877
vladyslav.dovbniak.kb.2023@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ZERO TRUST В IOT-СИСТЕМАХ

Анотація. У статті розглядається можливість застосування концепції Zero Trust у сфері Інтернету речей (IoT), що в умовах зростання кіберзагроз і критичності даних стає одним із ключових напрямів підвищення безпеки інформаційних систем. З традиційною парадигмою периметрової безпеки, яка передбачає довіру до внутрішніх компонентів мережі, вже не можливо ефективно протидіяти сучасним загрозам, особливо в контексті IoT-середовищ, де пристрої часто мають обмежені ресурси, відсутні механізми постійного моніторингу та складну структуру з'єднань між модулями. Zero Trust, як архітектурна концепція безпеки, базується на принципі «нікому не довіряй, завжди перевіряй» і передбачає обов'язкову верифікацію всіх користувачів, пристроїв та служб незалежно від їхнього розташування у мережі. У статті виконано детальний аналіз теоретичних засад Zero Trust, включаючи принципи ідентифікації, багатофакторної автентифікації, мікросегментації, мінімальних привілеїв, постійного моніторингу та динамічного контролю доступу. Проведено порівняльну характеристику традиційних та Zero Trust-підходів у контексті безпеки IoT, а також окреслено технічні виклики, пов'язані з їхньою інтеграцією. На основі огляду сучасних наукових джерел та практичних прикладів визначено, що імплементація Zero Trust в IoT-середовищі потребує спеціалізованих рішень, зокрема на рівні легковагих протоколів безпеки, використання довірених обчислювальних модулів, динамічного управління ключами, а також централізованих систем управління доступом. У роботі запропоновано концептуальну модель Zero Trust-архітектури для IoT-інфраструктури, що враховує обмеження пристроїв і особливості їхньої взаємодії, а також визначено алгоритм адаптивного контролю доступу на основі поведінкових характеристик. Дослідження показує, що впровадження Zero Trust у сфері IoT є не лише можливим, а й доцільним з точки зору зниження ризиків несанкціонованого доступу, зменшення площі атаки та покращення загального рівня безпеки цифрової екосистеми. Результати можуть бути використані як основа для розробки політик безпеки IoT-систем, зокрема в критичній інфраструктурі, промислових мережах і смарт-середовищах, де загрози конфіденційності, цілісності та доступності набувають особливого значення.

Ключові слова: Zero Trust; IoT; інформаційна безпека; мікросегментація; багатофакторна автентифікація; Forrester TEI; Microsoft; Google BeyondCorp; AWS; Cisco; поведінковий аналіз; економічна ефективність; SIEM; UEBA; регуляторна відповідність.

ВСТУП

У сучасному цифровому середовищі стрімке поширення хмарних технологій, віддаленого доступу, мобільних додатків та особливо пристроїв Інтернету речей (IoT) призводить до розмиття периметру корпоративної мережі. Усе більше компаній відмовляються від традиційної централізованої моделі інфраструктури на користь гібридних та розподілених рішень, що включають хмарні сервіси, edge-компоненти, віддалені офіси та мобільні робочі станції. Водночас, інтеграція тисяч автономних пристроїв IoT у критичні бізнес-процеси створює новий рівень уразливості, оскільки такі пристрої часто не мають вбудованих засобів захисту, працюють на спрощених ОС і використовують нестандартні або слабкозахищені протоколи обміну даними.

Ці трансформації ускладнюють використання класичних моделей кібербезпеки, які базуються на понятті довіри до внутрішнього середовища організації. Традиційна perimeter-based модель, що передбачає фільтрацію трафіку лише на межі мережі та умовне поділення середовища на «довірене» і «недовірене», виявляється неефективною в умовах постійної мобільності користувачів, наявності віддалених робочих місць і активного використання сторонніх додатків та хмарних сервісів. У середовищі, де фізичний периметр або повністю зникає, або змінюється щогодини, виникає потреба в новій парадигмі управління доступом і захистом.

У відповідь на ці виклики сформувалась концепція Zero Trust (ZT) — модель безпеки, що базується на принципі «нікому не довіряй за замовчуванням» і передбачає перевірку кожного доступу незалежно від розташування користувача або пристрою. Zero Trust передбачає ідентифікацію та автентифікацію кожного суб’єкта доступу, безперервний моніторинг, контроль стану пристрою (device posture), застосування динамічних політик доступу на основі контексту (рівень ризику, геолокація, час доби, тип запиту), а також використання механізмів поведінкової аналітики для виявлення аномалій.

У поєднанні з принципами least privilege, microsegmentation та криптографічного захисту, архітектура Zero Trust забезпечує високий рівень адаптивності до змінного середовища загроз. Особливої актуальності вона набуває в умовах розширеного використання IoT, оскільки дозволяє ізолювати пристрої один від одного, контролювати кожен трафік та мінімізувати наслідки компрометації. У зв’язку з цим, вивчення можливостей, обмежень та економічної доцільності впровадження Zero Trust у корпоративні середовища, включно з IoT, є важливим завданням для сучасної кібербезпеки.

Актуальність теми. Застосування концепції Zero Trust у корпоративних IT-інфраструктурах уже підтвердило свою ефективність як з погляду підвищення рівня кіберзахисту, так і з позиції економічної доцільності. Згідно зі звітом аналітичного агентства Forrester, впровадження архітектури Zero Trust дозволяє суттєво знизити ймовірність витоку даних [2], мінімізувати інциденти безпеки та скоротити витрати на IT-підтримку, забезпечуючи при цьому швидку окупність інвестицій [2]. Багато компаній, що використовують хмарні рішення, вже перейшли на цю модель або активно впроваджують її в гібридному форматі, інтегруючи багаторівневу автентифікацію, контроль доступу та поведінкову аналітику у свої щоденні операції.

Однак, попри успішне використання Zero Trust у класичних IT-середовищах, її застосування в галузі Інтернету речей (IoT) досі залишається обмеженим. Переважна більшість IoT-пристроїв розробляються без належного врахування принципів безпеки,

мають обмежені ресурси, нестандартні протоколи та значну розподіленість, що ускладнює централізоване управління доступом і моніторинг. Крім того, відсутність єдиних стандартів у сфері IoT-безпеки створює бар'єри для впровадження єдиної архітектури Zero Trust у мультипротокольних середовищах.

Водночас загроза з боку уразливих IoT-компонентів зростає. Атаки на інфраструктуру дедалі частіше починаються з компрометації слабкозахищених сенсорів, камер спостереження або контролерів, що виступають початковим вектором проникнення. Це підтверджує критичну необхідність розробки та впровадження адаптивних моделей Zero Trust, які враховують специфіку IoT: обмежену потужність, відсутність постійного оновлення, географічну розподіленість і варіативність сценаріїв використання.

Таким чином, дослідження питань реалізації Zero Trust у контексті IoT має не лише теоретичну, а й практичну вагу. Воно дозволяє окреслити шляхи подолання існуючих бар'єрів, сприяє розвитку безпекових стандартів і допомагає сформувати ефективну, масштабовану архітектуру захисту для сучасних цифрових систем з підвищеним рівнем динаміки й розгалуженості.

Аналіз останніх досліджень і публікацій. Концепція Zero Trust (ZT) посіла центральне місце у стратегіях кібербезпеки підприємств у відповідь на розмиття традиційного мережевого периметру, хмарну міграцію та зростання атак з боку внутрішніх користувачів. В основі підходу лежить відмова від будь-якої апріорної довіри та сувора перевірка доступу до ресурсів на основі атрибутів пристрою, користувача та контексту запиту. Визначальні принципи моделі викладені у документі NIST SP 800-207, де представлено референсну архітектуру Zero Trust, логіку контролю доступу та механізми перевірки ідентичності [3].

Габріс і Чапман наголошують, що впровадження ZT не має єдиного шаблону — кожна організація повинна адаптувати архітектуру під власні цілі, структуру ресурсів і рівень ризику [4]. У корпоративних середовищах реалізація ZT базується на мікросегментації, багаторівневій автентифікації, інтеграції з UEBA (User and Entity Behavior Analytics) та динамічному контролі доступу [5].

У сфері Інтернету речей (IoT) застосування Zero Trust розглядається у поодиноких працях Х'юбера і Кандаха, які пропонують модель Zero Trust+, що демонструє зростання продуктивності у 20% в умовах масштабованих IoT-середовищ за рахунок оптимізації механізмів довіри [6]. Шахад Аль-Тамімі зазначає, що стандартні підходи ZT не пристосовані до енергообмежених вбудованих пристроїв, і пропонують інтеграцію мікросегментації, динамічного контролю доступу та identity-verification в IoT-фреймворках [7].

Абухасель [8] у своїй роботі пропонує Zero-Trust Network-Based Access Control Scheme (ZTN-ACS) для промислових середовищ Industry 5.0, що поєднує принципи Zero Trust із механізмами глибокого навчання для забезпечення стійкого й адаптивного управління доступом до IoT-пристроїв. Модель передбачає врахування телеметричних даних пристрою, стану мережі та сценарного контексту, що забезпечує високий рівень точності прийняття рішень щодо авторизації.

У свою чергу, Liu та співавтори [9] здійснили систематичний аналіз досліджень у сфері Zero Trust з фокусом на його реалізацію в IoT. Автори підкреслюють необхідність динамічної оцінки довіри, підтримки міжплатформної взаємодії та інтеграції локальних ML-модулів для виявлення аномалій у поведінці пристроїв. Їхня робота є важливим внеском у формування методологічної бази для впровадження Zero Trust у гетерогенних розподілених системах з обмеженими ресурсами.

Незважаючи на наявність окремих прикладних реалізацій, академічна спільнота поки що не виробила уніфікованої моделі впровадження Zero Trust у сфері IoT. Це ставить під сумнів можливість масштабованого й ефективного захисту розподілених мереж з великою кількістю пристроїв, що мають різні характеристики, обмежену продуктивність і використовують несумісні протоколи зв'язку.

Постановка проблеми. Застосування концепції Zero Trust у сфері Інтернету речей супроводжується низкою викликів, які суттєво обмежують її повноцінне впровадження в практичних середовищах. Серед них — технічна неспроможність IoT-пристроїв забезпечити складні криптографічні обчислення, обмежена підтримка політик доступу на рівні прошивки, а також відсутність стандартів, які б дозволили адаптивне управління контекстом підключення. На сьогодні переважна більшість ZT-фреймворків створена з урахуванням хмарних або корпоративних середовищ і не враховує специфіки ресурсно-обмежених мереж.

Наявні підходи залишаються фрагментарними, а емпіричні докази ефективності ZT в реальних IoT-сценаріях — поодинокими. Це унеможливлює їх широке впровадження без суттєвого переосмислення архітектури, адаптації логіки перевірки довіри, а також побудови нових моделей взаємодії між пристроями, користувачами та сервісами.

Проблема полягає в тому, що на сьогодні не існує комплексної, гнучкої та масштабованої моделі реалізації Zero Trust у середовищах IoT, яка б враховувала обмеження пристроїв, складність політик управління доступом і необхідність динамічного реагування на загрози в реальному часі. Саме ця проблема потребує системного дослідження.

Метою дослідження є виявлення, обґрунтування та оцінка можливостей реалізації концепції Zero Trust у середовищах IoT шляхом аналізу архітектурних принципів ZT, технічної сумісності з IoT-платформами, прикладів реалізацій провідних провайдерів та економічної ефективності впровадження.

Завдання дослідження.

1. Провести всебічний аналіз можливостей адаптації архітектури Zero Trust до середовищ Інтернету речей (IoT), з урахуванням їхньої гетерогенності, обмежених обчислювальних ресурсів і нестандартних протоколів.
2. Систематизувати ключові принципи моделі Zero Trust відповідно до рекомендацій національного інституту стандартів і технологій США (NIST SP 800-207).
3. Дослідити технічну реалізацію Zero Trust-архітектури провідними постачальниками рішень у сфері інформаційної безпеки (Microsoft, Google, AWS, Cisco).
4. Оцінити застосовність зазначених рішень до IoT-інфраструктур із точки зору сумісності, ефективності та безпечного масштабування.
5. Проаналізувати економічну ефективність впровадження моделей Zero Trust у корпоративному середовищі, зокрема на основі методології Total Economic Impact (TEI) від Forrester.
6. Визначити основні технічні, організаційні та регуляторні перешкоди для впровадження Zero Trust.
7. Сформувати практичні рекомендації щодо поетапної імплементації архітектури Zero Trust у реальних IoT-середовищах з урахуванням динаміки кіберзагроз, необхідності масштабованості та дотримання галузевих нормативних вимог.

ZERO TRUST: КОНЦЕПЦІЯ ТА ПРИНЦИПИ

Zero Trust (ZT) — це сучасна модель інформаційної безпеки, що базується на принципі «нікому не довіряй за замовчуванням». Вона передбачає, що жоден користувач, пристрій або процес не може вважатися безпечним лише на підставі належності до внутрішньої мережі, геолокації чи автентифікації на одному рівні. Натомість, кожен запит до ресурсів проходить перевірку — незалежно від джерела походження, що забезпечує гнучкий і динамічний контроль безперервного доступу.

У практичному сенсі ZT — це не один продукт чи рішення, а набір архітектурних принципів та технологічних підходів, які реалізуються в залежності від специфіки середовища. На рисунку 1 подано логіку обробки запиту в системі Zero Trust — від перевірки ідентичності до адміністрування доступу на основі політик.

Рис. 1. Цикл перевірки запиту в системі Zero Trust

Концепція Zero Trust реалізується через набір взаємопов'язаних принципів, кожен з яких спрямований на усунення «довіри за замовчуванням» і побудову багаторівневої, динамічної безпеки:

- Явна перевірка (Explicit Verification). Кожен запит до системи, навіть якщо він походить із внутрішньої мережі, повинен проходити автентифікацію, авторизацію та перевірку політик доступу. Це передбачає багатофакторну автентифікацію (MFA), оцінку ризиків сесії, аналіз контексту (час, місце, пристрій) і наявність сертифікатів.
- Мінімізація привілеїв (Least Privilege Access). Користувачі та пристрої отримують лише той рівень доступу, який потрібен для виконання конкретного завдання. Це реалізується через рольову модель (RBAC), атрибутивний доступ (ABAC), політики Just-In-Time (JIT) та Just-Enough-Access (JEA). Привілеї мають бути тимчасовими та контрольованими.
- Мікросегментація (Microsegmentation). Інфраструктура розбивається на окремі логічні зони (зазвичай — сервіси, кластерні групи, середовища), кожна з яких має власні політики доступу. Це дозволяє локалізувати загрози та мінімізувати вплив можливого вторгнення. Мікросегментація реалізується через програмно-визначену мережу (SDN), віртуальні мережі (VPC) та контейнери з ізольованим мережевим стеком. На рис. 2 візуалізовано вплив мікросегментації на архітектуру корпоративної мережі.

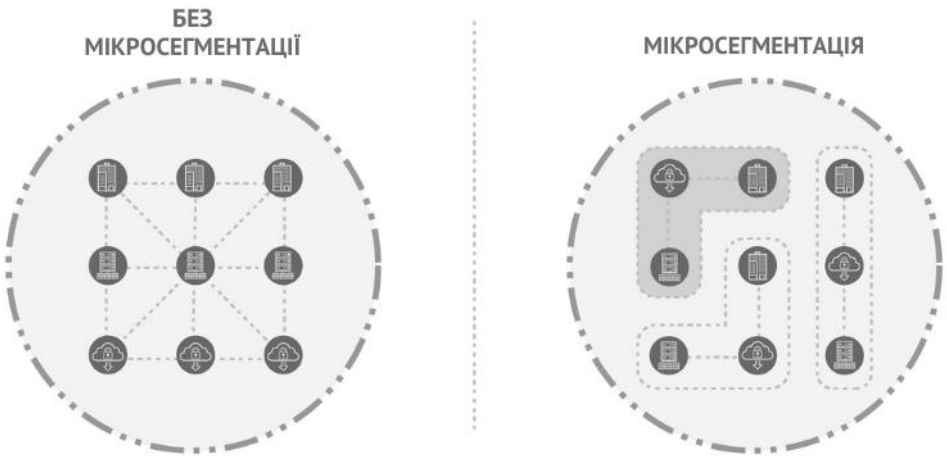

Рис. 2. Порівняння архітектури без мікросегментації та її присутністю

- Динамічна політика доступу (Context-Aware Access Control). Доступ до ресурсів ґрунтується на оцінці контексту: тип пристрою, статус антивірусу, геолокація, час доби, попередня активність користувача. Політика може бути адаптивною: наприклад, запити у неробочий час або з невідомої локації можуть вимагати додаткової автентифікації.
- Постійний моніторинг та аналітика (Continuous Monitoring and Risk Assessment). Zero Trust передбачає безперервне спостереження за подіями безпеки, поведінкою користувачів та станом систем. Дані збираються через SIEM (Security Information and Event Management), аналізуються у режимі реального часу з використанням UEBA та можуть автоматично запускати сценарії реагування за допомогою SOAR (Security Orchestration, Automation and Response).
- Інтегрований захист даних (End-to-End Encryption and Key Management). Усі дані повинні бути захищені як у стані спокою, так і при передачі. Використовуються сучасні криптографічні протоколи (TLS 1.3, AES-256), апаратне шифрування, механізми ізольованої обробки даних (наприклад, Intel SGX), а також централізоване керування ключами через KMS (Key Management Services).
- Перевірка пристроїв (Device Trust). Доступ до корпоративних ресурсів можливий лише з перевірених пристроїв. Це означає оцінку відповідності пристрою політикам безпеки: наявність антивірусу, шифрування диска, актуальність ОС, включений TPM (Trusted Platform Module). Інструменти MDM (Mobile Device Management) — такі як Microsoft Intune або VMware Workspace ONE — дозволяють централізовано управляти цими перевірками.

У практиці реалізація Zero Trust базується на моделі доступу за принципом «запит–оцінка–рішення–реакція». У запиті беруть участь такі логічні компоненти:

- Policy Engine (PE): оцінює запит на доступ, ґрунтуючись на політиках та зовнішніх сигналах (ризик, поведінка).
- Policy Administrator (PA): формує правила доступу та передає команди контролю.
- Policy Enforcement Point (PEP): технічно застосовує дозволи/заборони — на шлюзах, proxy, серверах.

ISSN 2663 - 4023

На рис. 3 представлено архітектуру ZT згідно з моделлю NIST SP 800-207 [10]. Вона відображає поділ на «Площину даних» і «Площину політик», наявність авторизованих/неавторизованих суб'єктів та необхідність зовнішніх даних (SIEM, ID, CDM) для прийняття рішень.

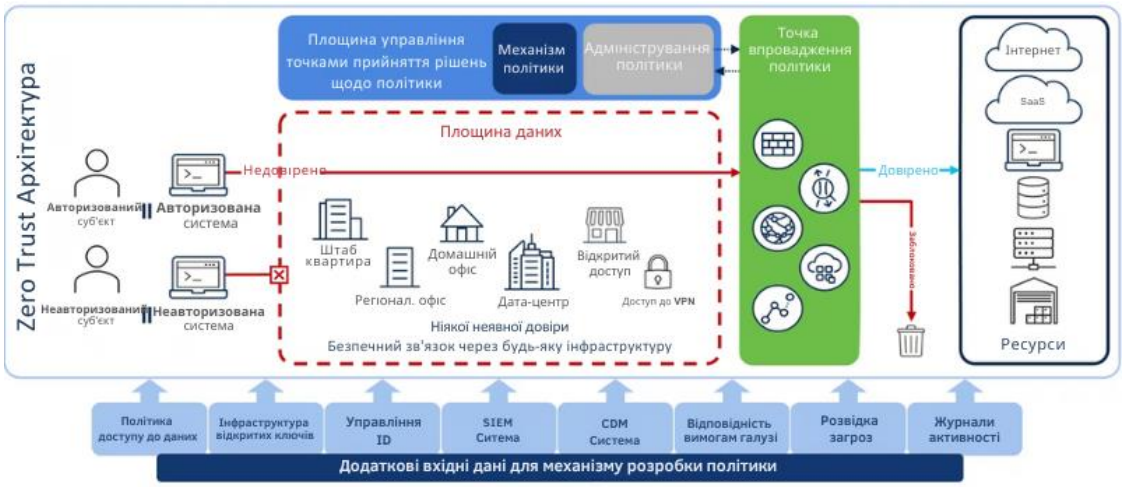

Рис. 3. Архітектура Zero Trust згідно з NIST SP 800-207

Усі компоненти взаємодіють через API і можуть бути реалізовані в хмарі або гібридному середовищі. Постачальники (Microsoft, Google, AWS, Cisco) мають власні реалізації цих блоків, вбудовані у свої платформи.

Сучасна реалізація Zero Trust дедалі більше інтегрується з системами на базі AI/ML — для прогнозування ризиків, адаптації політик в реальному часі, побудови поведінкових профілів та автоматизованого реагування. У майбутньому це відкриває шлях до самонавчальних безпекових систем, де політики формуються не вручну, а на основі статистичних та поведенкових патернів.

Технічна частина впровадження Zero Trust.

Zero Trust (ZT) починається з явної автентифікації — кожен запит, навіть з внутрішньої мережі, перевіряється через MFA (Multi-Factor Authentication, багатофакторна автентифікація). Наприклад, у Azure AD (Azure Active Directory) користувач, який намагається увійти з нової геолокації, отримує вимогу підтвердити ідентифікацію через додаток Microsoft Authenticator. Технології на кшталт Okta або Google Workspace Identity дозволяють інтегрувати MFA з різними додатками, включаючи кастомні SaaS-сервіси (Software-as-a-Service). Після автентифікації запускається контекстно-залежний контроль доступу: система оцінює ризик на основі атрибутів, як-от час доби (доступ до фінансових систем може блокуватися вночі), тип пристрою (мобільний телефон vs. корпоративний ноутбук) або наявність оновлень ОС. Google BeyondCorp, наприклад, використовує проксі-сервер, який аналізує сотні параметрів, включаючи стан пристрою (Device Posture) через агенти, що перевіряють антивірус, шифрування диска та версію ПО.

Для обмеження горизонтального пересування в мережі застосовується мікросегментація. У AWS (Amazon Web Services) кожен сервіс ізолюється в окремій VPC (Virtual Private Cloud), а комунікація між ними регулюється через Security Groups — правила, що дозволяють лише конкретні порти (наприклад, 3306 для MySQL). Платформи типу Illumio PCE (Policy Compute Engine) автоматизують цей процес: якщо в хмарному кластері Kubernetes створюється новий под (Pod), Illumio автоматично

застосовує політики, що забороняють йому зв'язок із іншими сервісами, доки адміністратор явно не дозволить доступ. Cisco пропонує схоже рішення — Tetration, яке аналізує потоки даних між серверами та створює правила мікросегментації на основі шаблонів трафіку [11].

Принцип мінімальних привілеїв (Least Privilege) реалізується через інструменти типу CyberArk для керування привілейованими акаунтами або Microsoft PIM (Privileged Identity Management), де права адміністраторів активуються лише після схвалення керівником та автоматично відключаються через заданий час. У хмарних середовищах, як AWS, це досягається за допомогою IAM (Identity and Access Management): роль для EC2-інстансу може дозволяти лише читання з S3-бакета, а не запис або видалення. Для тимчасового доступу використовується JIT (Just-In-Time Access) — наприклад, у Cisco Duo інженер може отримати права на 30 хвилин для виправлення конфігурації мережевого обладнання, після чого доступ анулюється.

Постійний моніторинг забезпечується через SIEM-системи (Security Information and Event Management), такі як Splunk або Microsoft Sentinel, які агрегують логи з усіх джерел: фаєрволів, серверів, кінцевих пристроїв. Для аналізу поведінки застосовується UEBA (User and Entity Behavior Analytics) — наприклад, якщо обліковий запис бухгалтера раптом починає масово експортувати файли з CRM (Customer Relationship Management), система маркує це як аномалію та запускає автоматичне розслідування через SOAR (Security Orchestration, Automation, and Response). У Microsoft Defender такі сценарії можна налаштувати через Playbooks: блокування акаунта, відправка повідомлення в Slack або створення тікета в ServiceNow.

Контроль пристроїв — ключовий елемент ZT. Microsoft Intune або VMware Workspace ONE перевіряють, чи має пристрій оновлену ОС, активний антивірус (наприклад, Bitdefender або CrowdStrike), чи включений TPM (Trusted Platform Module) для зберігання ключів. У Google BeyondCorp агент Endpoint Verification сканує пристрій перед доступом до корпоративного Gmail: якщо виявлено джейлбрейк або відсутність шифрування, доступ блокується. Для IoT-пристроїв (Internet of Things) використовуються спеціалізовані рішення, як Azure Sphere, які генерують унікальні ідентифікатори та автоматично патчать вразливості.

Шифрування реалізується на всіх рівнях: дані в стані спокою (наприклад, через AES-256 у AWS S3), під час передачі (TLS 1.3 для веб-трафіку) та у пам'яті (Intel SGX для захисту обробки даних). Azure Key Vault або AWS KMS (Key Management Service) централізують управління ключами: автоматична ротація, аудит доступів, інтеграція з хмарними сервісами. Наприклад, якщо додаток потребує доступу до зашифрованої бази даних, він отримує ключ через API KMS лише після перевірки TLS-сертифіката та IP-адреси.

Економічна ефективність впровадження Zero Trust (на основі звітів Forrester для Microsoft та Illumio).

Впровадження моделі Zero Trust не лише підвищує рівень безпеки, а й має чіткі економічні наслідки, що можуть бути кількісно оцінені. Аналітичні агентства, зокрема Forrester, провели незалежні дослідження Total Economic Impact (TEI) для рішень Microsoft та Illumio, які надають змогу проаналізувати вартість впровадження, очікувану вигоду та терміни окупності.

Таблиця 1

Порівняльний аналіз економічної ефективності Zero Trust для Microsoft та Illumio

Параметр	Microsoft Zero Trust	Illumio Zero Trust Segmentation
ROI (3 роки)	92%	111%
Загальна вигода (3 роки)	$13,3 млн	$10,2 млн
Період окупності	< 6 місяців	6 місяців
Зменшення ризиків	– Зменшення ймовірності витоку даних на 50% – Зниження інцидентів безпеки	– Скорочення «радіусу ураження» на 66% – Уникнення збоїв: $3,8 млн
Оптимізація витрат	– Скорочення витрат на підтримку IT: $1,7 млн – Зниження звернень у help desk на 50%	– Зменшення навантаження на команди безпеки: $2,1 млн – Економія на інструментах: $3 млн
Ключові переваги	– Інтеграція з хмарною екосистемою (Microsoft 365, Azure) – Автоматизація доступів (SSO, MFA)	– Мікросегментація для ізоляції атак – Інфраструктурна агностичність (хмара, on-premises)
Вартість впровадження	Не вказано (акцент на вигодах)	$4,8 млн (загальні витрати за 3 роки)
Методологія	Total Economic Impact (TEI) з акцентом на масштабованість та інтеграцію	Total Economic Impact (TEI) з фокусом на зменшення наслідків інцидентів

Як демонструє аналіз, обидва рішення — Microsoft і Illumio — забезпечують значну економічну ефективність, що підтверджується незалежними дослідженнями Total Economic Impact, проведеними агентством Forrester. Зокрема, у випадку Microsoft Zero Trust сукупна вигода за три роки перевищує $13 млн, а рентабельність інвестицій (ROI) становить 92%, при цьому термін окупності не перевищує шести місяців [2]. Такий ефект досягається завдяки глибокій інтеграції з екосистемою Azure, автоматизації контролю доступу, зниженню навантаження на службу підтримки та оптимізації витрат на інфраструктуру (Forrester, 2021) [1].

Рішення Illumio демонструє ще вищий ROI — 111% протягом того ж періоду, з економічним ефектом у понад $10 млн [1]. Основною відмінністю є акцент на мікросегментацію, що дозволяє значно зменшити радіус ураження при атаках, уникнути критичних збоїв і зменшити навантаження на команди безпеки. Згідно з результатами дослідження, впровадження Illumio дозволяє скоротити наслідки інцидентів та забезпечити більш ефективний контроль над East-West трафіком у складних мережевих середовищах (Forrester, 2022) [2].

Таким чином, стратегія Zero Trust не лише підвищує рівень інформаційної безпеки, але й дозволяє організаціям досягти значної економії ресурсів. Вибір постачальника залежить від існуючої IT-архітектури, пріоритетів безпеки та здатності організації масштабувати обрану модель. Microsoft орієнтована на глибоку екосистемну інтеграцію, тоді як Illumio забезпечує точковий підхід до ізоляції загроз.

Порівняльний аналіз провайдерів рішень Zero Trust (Microsoft, Google, AWS, Cisco).

На сучасному ринку інформаційної безпеки провідні гравці пропонують власні реалізації Zero Trust-архітектури. Хоча базові принципи (мінімальні привілеї, явна автентифікація, сегментація, моніторинг) залишаються незмінними, реалізація відрізняється залежно від технічних підходів, фокусу платформи та інфраструктурної спадщини компанії.

Нижче наведено порівняння чотирьох основних провайдерів: Microsoft, Google, Amazon Web Services (AWS) та Cisco.

Таблиця 2

Порівняльний аналіз основних провайдерів Zero Trust

Характеристика	Microsoft	Google	AWS	Cisco
Архітектура	Інтегрована Zero Trust модель з Azure AD, Defender, Intune, Conditional Access	BeyondCorp Enterprise — ZT без VPN, фокус на атрибутивному контролі доступу	Модульна ZT-архітектура з Verified Access, IAM, GuardDuty	Комплексна модель: ZTNA, SecureX, Duo, Tetration
Сильні сторони	Інтеграція з Microsoft 365, повна автоматизація, глибока аналітика (Sentinel)	Контекстно-залежний доступ, оцінка стану пристрою (Device Trust), проксі-рівень контролю	Потужна IAM-структура, fine-grained policies, інтеграція з VPC	Підтримка IoT/OT, глибока мережна аналітика, microsegmentation
Інфраструктурна орієнтація	Хмара + гібрид (Azure, on-premises)	Хмара (Google Cloud)	Хмара (AWS)	Гібрид + традиційні мережі (Cisco Meraki, Catalyst)
Управління пристроями	Intune, Defender for Endpoint	Endpoint Verification	Systems Manager, AWS IoT Device Defender	ISE, Duo Trust Monitor
Аналітика та моніторинг	Microsoft Sentinel, Defender	Chronicle, BeyondCorp Threat Intelligence	CloudTrail, GuardDuty, Macie	SecureX, Umbrella, Tetration
Автентифікація / SSO / MFA	Azure AD, Conditional Access, SSO + MFA (Microsoft Authenticator)	Cloud Identity, Context-Aware Access, MFA	AWS IAM + MFA + STS	Duo Security, Adaptive MFA, SSO
Ціноутворення (орієнтовне)	EMS + Defender ~$8.80/користувач/ місяць	У складі Google Workspace Enterprise (~$20/користувач/ місяць)	Покомпонентно (IAM безкоштовно, GuardDuty — від обсягу логів)	Duo: від $6/користувач/ місяць; SecureX — в складі Cisco Secure
Відповідність стандартам	ISO/IEC 27001, NIST 800-207, GDPR	FedRAMP, NIST 800-207	PCI-DSS, ISO 27017, NIST, HIPAA	NIST, ISO/IEC, SOC 2

Microsoft пропонує універсальне рішення для компаній, які вже використовують екосистему Microsoft 365 та Azure. Його перевагою є централізованість, висока ступінь автоматизації та відповідність очікуванням enterprise-сегменту, що спрощує адаптацію та розгортання.

Google фокусується на хмарно-орієнтованих середовищах із пріоритетом мобільності. Його модель контекстно-залежного доступу й оцінка стану пристрою дозволяють реалізувати Zero Trust без необхідності VPN. Хоча вартість рішень Google є вищою, вона виправдана функціональною повнотою та безшовною інтеграцією у Google Workspace.

AWS орієнтований на DevOps-інфраструктури з високим рівнем деталізації політик і гнучкою системою керування доступом, однак відсутність єдиної централізованої консолі ускладнює інтеграцію та адміністрування.

Cisco, своєю чергою, пропонує гібридне рішення, яке найбільше підходить організаціям із розгалуженою традиційною інфраструктурою, значною присутністю IoT/OT-пристроїв та вже існуючою мережевою архітектурою Cisco. Вибір постачальника Zero Trust-рішень значною мірою залежить від наявної цифрової екосистеми, рівня зрілості безпекових процесів і пріоритетів організації — як технічних, так і організаційних.

Інтеграція архітектури Zero Trust у контексті IoT: стратегічні, технічні та регуляторні виміри.

Сучасна інтенсивна експансія IoT-технологій у корпоративні екосистеми — від індустріальних сенсорних платформ і медичних телеметричних пристроїв до багатофункціональних контролерів промислової автоматизації — суттєво модифікує уявлення про межі мережевої безпеки. Мережевий периметр, як категорія, дедалі більше втрачає актуальність унаслідок дифузного розташування кінцевих пристроїв, які не лише генерують, а й обробляють критично важливу інформацію. У цьому світлі архітектура Zero Trust (ZT), побудована на відмові від апріорної довіри, становить домінантну парадигму безпеки постпериметрального етапу цифровізації.

Особливу увагу слід приділити динаміці змін у цифрових екосистемах, де IoT стає фундаментальним компонентом не лише як транспортна технологія для даних, а як інтегральний елемент прийняття рішень в умовах кіберфізичних систем. У зв’язку з цим безпека таких середовищ не може обмежуватися класичним захистом периметра або реактивним підходом. Необхідна проактивна архітектура довіри, що функціонує на основі постійної верифікації, багатофакторної аутентифікації, глибокої поведінкової аналітики [12] та енд-то-енд шифрування.

IoT-пристрої за своєю природою — гетерогенні, ресурсно обмежені та часто функціонально автономні. Вони працюють на основі закритих прошивок, мають нестандартні стекові інтерфейси [12] та відсутність прямої підтримки критичних безпекових протоколів. Ці фактори унеможливлюють пряме імплементування традиційних засобів інформаційного захисту, зокрема мережевих екранувальних засобів, повнофункціональних SIEM або IAM-рішень. Ефективне впровадження Zero Trust у таких середовищах вимагає застосування концептуально адаптованих моделей оцінки довіри, що передбачають глибоку аналітику, мікросегментацію, атрибутивну авторизацію, контроль контексту доступу, а також включення елементів самонавчальних систем для підвищення гнучкості реагування.

До базових технічних вимог до IoT-компонентів, що підлягають включенню в Zero Trust-інфраструктуру, належать:

1) Наявність апаратних засобів довіри (TPM 2.0, Secure Element);
2) Підтримка актуальних криптографічних протоколів (TLS 1.3, DTLS, AES-GCM);
3) OTA-механізми для регулярного оновлення прошивок і системного забезпечення;
4) Використання цифрових сертифікатів X.509 для ідентифікації;
5) Вбудовані агенти телеметрії, які генерують лог-файли і підтримують взаємодію з централізованими SIEM;
6) Відповідність стандартам взаємодії з керуючими платформами (MQTT, OPC-UA, SNMP).

Процес інтеграції включає кілька послідовних фаз: детальна інвентаризація пристроїв, класифікація за критичністю, побудова логічної мікросегментації, налаштування атрибутивних правил доступу, верифікація поведінки через UEBA-модулі, а також впровадження адаптивної політики контролю доступу з урахуванням змін контексту.

Таблиця 3

Класифікація IoT-пристроїв за параметрами сумісності з принципами архітектури Zero Trust

Категорія	Приклад	Функціональні можливості для ZT	Платформа керування	Сфера застосування
Промислові IoT-пристрої	Siemens SIMATIC S7-1500	TPM, мікросегментація, глибока ізоляція	Siemens TIA Portal	Високоточне виробництво
Медичні системи	Philips HealthSuite IoT	Шифрування медичних даних, відповідність HIPAA	HealthSuite Platform	Цифрова медицина
Відеоспостереження	Axis + Azure Sphere	TLS/OTA, політики доступу, централізоване керування	Azure IoT Hub	Інфраструктурна безпека
Сенсори в логістиці	AWS IoT-сумісні пристрої	KMS, контроль зон покриття, аналіз аномалій	AWS IoT Core	Управління ланцюгами постачання
Критичне обладнання	Schneider Electric EcoStruxure	IEC 62443 сумісність, повна сегментація	EcoStruxure Platform	Інфраструктура енергетики
Інтелектуальні шлюзи	Cisco IR1101, Advantech UNO	SDN-профілювання, MPLS-тунелювання	Cisco DNA Center	Розподілені об’єкти
Побутові системи	Google Nest, SmartThings	Локальний контроль, хмарна інтеграція	Google Home	Розумний дім

Інфраструктурна імплементація Zero Trust передбачає побудову системи багаторівневого захисту, де кожен елемент IoT-середовища проходить контекстну оцінку у режимі реального часу. Це реалізується через системи динамічного управління політиками, що базуються на поведінковій аналітиці (AI/ML), з інтеграцією у SIEM, SOAR і KMS. Модель повинна враховувати зміни стану пристрою, його геолокації, історії транзакцій та поведінкових патернів, а також бути здатною автоматично коригувати рівень довіри та доступу на основі нових даних.

Не менш важливою є регуляторна інтеграція. Зокрема, імплементація ZT у середовищі IoT має бути скоординована з положеннями NIST SP 800-213, ISO/IEC 27001, IEC 62443 та галузевими специфікаціями. Аудит політик, реєстри контролю доступу, системи інцидентного реагування мають бути сумісні з вимогами комплаєнсу для забезпечення юридичної захищеності оператора системи.

Культурна трансформація організації, орієнтована на безпеку IoT, включає формування нових політик і процедур, підвищення кіберграмотності персоналу, створення команд цифрової безпеки, які працюють на перетині DevSecOps, OT та управління ризиками. Це передбачає створення міждисциплінарної моделі прийняття рішень у режимі реального часу на основі єдиного інформаційного простору аналітики ризиків.

Попри теоретичну привабливість концепції Zero Trust та її стратегічну доцільність у контексті IoT, на практиці впровадження цієї архітектури супроводжується низкою технічних, організаційних та регуляторних викликів. З іншого боку, успішна реалізація принципів ZT відкриває значні переваги як для безпеки інфраструктури, так і для управління ризиками. Ключові складнощі впровадження Zero Trust у середовищах з IoT-компонентами та потенційні переваги реалізації цієї моделі наведено в табл. 4.

Таблиця 4

Складнощі впровадження та переваги реалізації архітектури Zero Trust в умовах IoT-інфраструктур

Складнощі впровадження	Переваги реалізації
Застаріле обладнання (legacy), яке не підтримує сучасні механізми безпеки	Ізоляція атак через мікросегментацію та політики мінімального доступу
Обмежені обчислювальні ресурси IoT-пристроїв	Гнучке керування політиками доступу в реальному часі
Складність масштабованої мікросегментації великих середовищ	Покращене виявлення загроз завдяки телеметрії, UEBA та SIEM
Брак кваліфікованих спеціалістів у сфері IoT/OT-безпеки	Відповідність міжнародним стандартам (ISO, NIST, IEC)
Відсутність єдиного підходу до ZT у сфері IoT	Підвищення кіберстійкості, адаптивність до змін середовища

Застосування високоспеціалізованих платформ — Azure Sphere, Cisco Cyber Vision, AWS IoT Defender, Palo Alto XIoT — є каталізатором ефективної реалізації політик ZT, адже забезпечує масштабованість, інтероперабельність, уніфікацію телеметрії та автоматизоване реагування. Середовище має підтримувати мультипротокольну взаємодію, включати засоби криптографічної ізоляції, підтримувати перевірку цілісності компонентів та забезпечувати контроль життєвого циклу пристрою на кожному етапі.

З огляду на результати проведеного аналізу, для ефективного впровадження архітектури Zero Trust у корпоративних середовищах доцільно реалізовувати поступову, поетапну стратегію, орієнтовану на ризик-орієнтований підхід. Особливу увагу слід приділити сегментам із високою критичністю — такими як привілейовані акаунти, зовнішній доступ, фінансові дані та середовища розробки. Передумовою формування ефективної політики доступу є повна інвентаризація цифрових активів, включно з користувачами, пристроями, службами та взаємозв'язками між ними.

Інтеграція інструментів поведінкової аналітики (UEBA), систем централізованого моніторингу (SIEM) та засобів автоматизованого реагування (SOAR) дає змогу підвищити адаптивність безпекової інфраструктури та зменшити час реакції на інциденти. З огляду на складність архітектури Zero Trust, особливо у середовищах із великою кількістю IoT-пристроїв, важливим є навчання персоналу, формування нової культури управління ризиками та розбудова міжфункціональної взаємодії між IT, безпекою та бізнес-структурами.

Також критичним є дотримання регуляторних вимог — як міжнародних (ISO/IEC 27001, NIST SP 800-207), так і галузевих (GDPR, NIS2), особливо для організацій, що працюють у регульованих секторах або мають справу з персональними даними. Для забезпечення технічної життєздатності підходу доцільно розпочинати з пілотних проєктів у контрольованих середовищах, поступово масштабуючи політики ZT на інші домени. У випадку IoT-компонентів особливої уваги потребує сегментація, шифрування, перевірка відповідності пристроїв, а також використання edge-рішень та шлюзів безпеки.

Перспективи впровадження Zero Trust у «розумному місті».

Концепція Zero Trust може стати ключовим елементом цифрової трансформації муніципальних IT-систем, зокрема в контексті реалізації ініціатив «розумного міста». Для Львова, де активно впроваджуються елементи Smart City — системи відеоспостереження, моніторингу трафіку, екології, освітлення, енергоспоживання та управління транспортом — архітектура Zero Trust пропонує новий рівень контролю,

видимості та безпеки. Водночас її реалізація має бути адаптована до специфіки наявної інфраструктури, яка часто є неоднорідною, технологічно застарілою або слабо інтегрованою між собою.

Ініціативи з цифровізації у Львові вже охоплюють десятки підсистем — від екологічних сенсорів до систем диспетчеризації транспорту. Це створює унікальну можливість для впровадження Zero Trust не лише як безпекової парадигми, а як підходу до уніфікації та оркестрації цифрової взаємодії між об'єктами міського середовища. Застосування сучасних IoT-шлюзів типу Cisco IR1101 або Advantech UNO дозволяє реалізувати механізми тунелювання, контекстної авторизації та мікросегментації між логічними зонами IoT. Це дає змогу ізолювати трафік між окремими сегментами (наприклад, відеокамерами та контролерами освітлення), що значно підвищує рівень захищеності інфраструктури. Хмарні платформи типу Microsoft Azure Sphere, AWS IoT Core або Google Cloud IoT підтримують ідентифікацію пристроїв, OTA-оновлення, керування сертифікатами та шифрування, що дозволяє покрити критичні IoT-сервіси (відеоспостереження, енергетика, транспорт). Зокрема, застосування Azure IoT Defender забезпечує постійну перевірку цілісності прошивки та оцінку ризику поведінки пристроїв. Розгортання систем SIEM/UEBA у структурі міських IT-служб (наприклад, у Львівському комунальному центрі IT) дозволяє виявляти аномалії, створювати профілі поведінки пристроїв та оперативно реагувати на загрози у реальному часі. Вбудовані сценарії реагування (playbooks) можуть автоматично блокувати компрометовані вузли або перенаправляти трафік до зон ізоляції. При забудові нових мікрорайонів, як-от у районі Рясне-2, можна з самого початку застосовувати ZT-принципи: передбачати мікросегментовану інфраструктуру, розгортати шлюзи довіри, застосовувати атрибутивний контроль доступу та взаємодії між компонентами на рівні edge-комп'ютингу.

Проте більшість IoT-рішень, встановлених у Львові до 2020 року, не підтримують апаратну довіру або захищені канали зв'язку, що унеможливлює їх інтеграцію у Zero Trust без модифікації. Часто вони не мають навіть елементарної автентифікації на рівні API або використовують застарілі протоколи (наприклад, HTTP замість HTTPS). Міські сервіси використовують різні платформи керування пристроями, що ускладнює централізоване впровадження політик доступу. Крім того, деякі відомства не мають інтегрованих систем обліку обладнання, що унеможливлює верифікацію довіри до пристрою при запиті доступу. Для підтримки Zero Trust необхідна постійна аналітика, кореляція подій, оновлення політик — чого складно досягти без кваліфікованих фахівців. Навчання персоналу, створення центрів компетенцій та формування багатопрофільних команд DevSecOps — критично важливі умови для успішної реалізації. Масштабне оновлення інфраструктури, закупівля нових шлюзів, розгортання SIEM та SOAR-систем потребують значних інвестицій, які не завжди можливі в умовах обмеженого бюджету міста.

Найперше слід оновити обладнання в системах відеоспостереження, зокрема камери, що не підтримують шифрування або мають відкриті порти керування; контролери освітлення, що працюють по незахищених протоколах (наприклад, Modbus без TLS); мережеві комутатори, які не мають можливості аутентифікації пристроїв через 802.1X; шлюзи, які не підтримують мікросегментацію або централізоване керування політиками доступу. У транспортній інфраструктурі варто замінити GPS-трекери, які не мають можливості OTA-оновлень, а також оновити маршрутизатори в автобусах, які не підтримують сучасні протоколи VPN або не мають вбудованих засобів фільтрації трафіку. В енергетичному секторі необхідно переоснастити лічильники та сенсори, що використовують застарілий зв'язок без шифрування даних (наприклад, RS-485 без

захисту). Це дозволить сформувати централізовану базу даних пристроїв, що критично необхідно для побудови довірчої моделі Zero Trust. Це дозволить сформувати централізовану базу даних пристроїв, що критично необхідно для побудови довірчої моделі Zero Trust. Наприклад, реалізувати ZT-архітектуру в одному мікрорайоні або в комунальному підприємстві «Львівелектротранс» — як полігон для обкатки рішень. Формування CSIRT або аналогічного центру компетенцій дозволить постійно оновлювати політики безпеки та реагувати на інциденти.

Починати імплементацію слід з найбільш критичних сегментів (відеоспостереження, транспорт, енергомережі) з поступовим масштабуванням у менш критичні сфери (освітлення, паркування, інформаційні табло). Здійснити повну інвентаризацію IoT-інфраструктури із класифікацією за критичністю, версією прошивки, підтримкою TPM та відповідністю протоколам безпеки. Встановити пілотний проєкт з впровадження Zero Trust на базі одного з мікрорайонів або комунального підприємства, інтегруючи SIEM/SOAR, шлюзи безпеки та агентське програмне забезпечення на IoT-пристроях. Запровадити міжвідомчу програму з кібербезпеки муніципального рівня з навчанням персоналу, створенням локального центру кіберінцидентів (CSIRT) та побудовою єдиного інформаційного простору для аналізу ризиків.

У підсумку, Львів має потенціал стати зразковим прикладом реалізації адаптивної архітектури Zero Trust у межах українського урбаністичного середовища. Враховуючи темпи цифровізації, зростання кіберзагроз, підтримку відкритих стандартів та активну позицію місцевої влади щодо інновацій, реалізація ZT у Львові — це не лише виклик, а й стратегічна можливість для зміцнення міської кіберстійкості. Поєднання технологічних рішень, нормативного забезпечення та організаційної зрілості дозволить створити модель кіберзахисту, яку можуть наслідувати інші міста України та регіону.

ВИСНОВОКИ

Концепція Zero Trust дедалі більше утверджується як базова модель побудови інформаційної безпеки в умовах складних, гібридних і розподілених цифрових середовищ. У межах виконаного дослідження виконано комплексний аналіз можливостей інтеграції архітектури **Zero Trust** у середовище IoT-пристроїв. На основі огляду актуальних стандартів, зокрема NIST SP 800-207, доведено технічну сумісність концепції за умови повної інвентаризації активів, застосування апаратних коренів довіри та сучасних криптопротоколів. Систематизація шести базових принципів Zero Trust — явної перевірки, найменших привілеїв, мікросегментації, безперервного моніторингу, контекстно-залежного доступу та наскрізного шифрування – дозволила сформувати уніфіковану матрицю вимог і контрольних показників, що слугує практичним фреймворком для оцінки готовності IoT-компонентів.

Практичний блок охоплює порівняльний розгляд реалізацій Zero Trust у Microsoft, Google, AWS і Cisco. Найвищу готовність до IoT-сценаріїв демонструють Microsoft(Defender /Entra ID) та AWS (IAM/IoT Core) завдяки нативній інтеграції з хмарними шлюзами й підтримці Device PostureAssessment, тоді як Google BeyondCorp та рішення Cisco потребують додаткових вузлів телеметрії й глибшого налаштування OT-протоколів. Жодне з розглянутих рішень не є «plug & play»; критичними факторами успіху залишаються наявність агентів, OTA-оновлень, підтримка X.509-сертифікатів і повноцінні API для SIEM/SOAR-систем.

Економічна оцінка, виконана за методологією Forrester Total Economic Impact, засвідчила, що впровадження Zero Trust забезпечує середню рентабельність інвестицій близько 92 % для стеку Microsoft та до 111 % для спеціалізованих рішень Illumio зі строком окупності 6–9 місяців. Найбільшу частку економії формують скорочення часу виявлення й ліквідації інцидентів, зниження простоїв сервісів і консолідація інструментів захисту.

Одночасно ідентифіковано шість ключових бар'єрів: поширеність legacy-обладнання без TPM, енергоресурсні обмеження пристроїв, складність мікросегментації великих OT-мереж, дефіцит фахівців з IoT/OT-безпеки, фрагментарність стандартів і жорсткі регуляторні вимоги (NIST SP 800-213, IEC 62443, ISO 27001), що потребують додаткової сертифікації та аудиту.

Виходячи з отриманих результатів сформовано поетапну дорожню карту впровадження Zero Trust у міських та промислових IoT-мережах: від створення єдиного реєстру активів і запуску пілотної мікросегментації у критичних сегментах, через розгортання SIEM / UEBA / SOAR з автоматизованим реагуванням, до масштабування архітектури та формування культури безпеки і власного CSIRT. Таким чином, дослідження підтверджує, що Zero Trust є технічно здійсненою та економічно доцільною стратегією захисту IoT-інфраструктур, здатною суттєво обмежити радіус ураження й підвищити кіберстійкість організацій за умови поетапного впровадження, підтримки менеджменту та системного навчання персоналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Whisper2Shout – Unhooking technique: [Електронний ресурс] - Режим доступу: Forrester. The Total Economic Impact™ Of Illumio Zero Trust Segmentation (ZTS) [Електронний ресурс]. – Forrester Research, 2023. – Режим доступу: https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/6435d3cbc91af0d3133fc068_Total-Economic-Impact-Illumio-Zero-Trust-Segmentation.pdf.
2. Forrester. The Total Economic Impact™ Of Zero Trust Solutions From Microsoft [Електронний ресурс]. – Forrester Research, 2022. – Режим доступу: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Zero-Trust-TEI-Study.pdf.
3. Rose S. Planning for a Zero Trust Architecture [Електронний ресурс]. – NIST Cybersecurity White Paper (Draft), 2021. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf.
4. Garbis J., Chapman J. Zero Trust Architectures [Електронний ресурс] // In: Zero Trust Security. – Springer, 2021. – С. 31–54. – Режим доступу: https://link.springer.com/chapter/10.1007/978-1-4842-6702-8_3.
5. Swetha M. J., Asha S. N., Raghavendra M. Zero Trust Architecture in Modern Computer Networks [Електронний ресурс] // World Journal of Advanced Research and Reviews. – 2020. – Режим доступу: https://wjarr.com/content/zero-trust-architecture-modern-computer-networks.
6. Brennan H., Farah K. Zero Trust+: A Trusted-based Zero Trust Architecture for IoT at Scale [Електронний ресурс] // 2024 IEEE International Conference on Consumer Electronics (ICCE). – 2024. – Режим доступу: https://ieeexplore.ieee.org/document/10444321.
7. Al-Tamimi S. Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review [Електронний ресурс] // 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). – 2024. – Режим доступу: https://ieeexplore.ieee.org/document/10811176.
8. Abuhasel K. A. A Zero-trust Network-based Access Control Scheme for Sustainable and Resilient Industry 5.0 [Електронний ресурс] // ResearchGate. – 2023. – Режим доступу: https://www.researchgate.net/publication/374865665

9. Liu C., Tan R., Wu Y., Feng Y., Jin Z., Zhang F., Liu Y., Liu Q. Zero Trust Architecture for Cyber Security in Industry 4.0 and 5.0 [Електронний ресурс] // Cybersecurity. – 2024. Режим доступу: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0
10. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture [Електронний ресурс] // NIST Special Publication 800-207. – Gaithersburg : National Institute of Standards and Technology, 2020. – 59 с. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
11. Cisco Systems. Zero Trust Architecture Guide [Електронний ресурс]. – Cisco, 2022. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-ag.html
12. Ghasemshirazi S., Shirvani G., Alipour M. A. Towards Effective Zero Trust in Internet of Things (IoT): Challenges and Future Directions [Електронний ресурс] // arXiv. – 2023. – Режим доступу: https://arxiv.org/pdf/2309.03582.
13. Li S., Iqbal M., Saxena N. Future Industry Internet of Things with Zero-trust Security [Електронний ресурс] // ResearchGate. – 2022. – Режим доступу: https://www.researchgate.net/publication/359147843.
14. Bicer C., Murturi I., Donta P. K., Dustdar S. A Novel Zero Trust Model for Access Control in IoT Networks [Електронний ресурс] // arXiv. – 2023. – Режим доступу: https://arxiv.org/pdf/2311.16744.
15. Mohseni-Ejiyeh A. Enhancing IoT Security Through Adaptive Zero Trust Architecture [Електронний ресурс] // arXiv. – 2023. – Режим доступу: https://arxiv.org/pdf/2309.01293.
16. Ma X., Fang F., Wang X. Towards AI-enabled Zero Trust Security for the Industrial Internet of Things [Електронний ресурс] // arXiv. – 2025. – Режим доступу: https://arxiv.org/pdf/2501.03601.
17. Ghasemshirazi S., Shirvani G., Alipour M. A. Zero Trust: Applications, Challenges, and Opportunities [Електронний ресурс] // ResearchGate. – 2023. – Режим доступу: https://www.researchgate.net/publication/373753509.
18. Ismail M., Abd El-Gawad A. F. Revisiting Zero-Trust Security for Internet of Things [Електронний ресурс] // ResearchGate. – 2023. – Режим доступу: https://www.researchgate.net/publication/377021858.
19. Li S. Editorial: Zero Trust based Internet of Things [Електронний ресурс] // ResearchGate. – 2020. – Режим доступу: https://www.researchgate.net/publication/341958873.
20. Simpson W. R. Toward a Zero Trust Metric [Електронний ресурс] // Procedia Computer Science. – 2022. – Vol. 201. – С. 1222–1230. https://www.sciencedirect.com/science/article/pii/S1877050922007530.
21. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
22. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
23. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Bohdan Mankovskyi
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0001-3857-9842
bohdan.mankovskyi.kb.2023@lpnu.ua

Vladyslav Dovbniak
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0005-5494-3877
vladyslav.dovbniak.kb.2023@lpnu.ua

Ivan Opirskyy
Doctor of Technical Sciences, Professor, Head of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

RESEARCH ON THE FEASIBILITY OF IMPLEMENTING THE ZERO TRUST CONCEPT IN IOT SYSTEMS

Abstract. This article explores the feasibility of applying the Zero Trust concept in the field of the Internet of Things (IoT), which, in the context of increasing cyber threats and data sensitivity, has become a key direction for enhancing information system security. Traditional perimeter-based security paradigms, which assume trust in internal network components, are no longer effective in countering modern threats—particularly within IoT environments where devices often have limited resources, lack continuous monitoring mechanisms, and involve complex interconnections. Zero Trust, as a security architecture concept, is based on the principle of "never trust, always verify" and requires mandatory verification of all users, devices, and services, regardless of their location within the network. The article provides a detailed analysis of the theoretical foundations of Zero Trust, including principles of identification, multi-factor authentication, microsegmentation, least privilege access, continuous monitoring, and dynamic access control. A comparative overview of traditional and Zero Trust approaches in the context of IoT security is presented, along with an outline of the technical challenges associated with their integration. Based on a review of current scientific literature and practical examples, it is established that implementing Zero Trust in IoT environments requires specialized solutions, particularly lightweight security protocols, trusted computing modules, dynamic key management, and centralized access control systems. The paper proposes a conceptual model of Zero Trust architecture for IoT infrastructures that accounts for device limitations and communication patterns, and defines an adaptive access control algorithm based on behavioral characteristics. The findings demonstrate that implementing Zero Trust in the IoT domain is not only feasible but also advisable from the standpoint of reducing unauthorized access risks, minimizing the attack surface, and enhancing the overall security posture of digital ecosystems. The results may serve as a foundation for developing IoT security policies, especially in critical infrastructure, industrial networks, and smart environments, where threats to confidentiality, integrity, and availability are particularly significant.

Keywords: Zero Trust; IoT; information security; microsegmentation; multi-factor authentication; Forrester TEI; Microsoft; Google BeyondCorp; AWS; Cisco; behavioral analysis; cost-effectiveness; SIEM; UEBA; regulatory compliance.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Forrester. *The Total Economic Impact™ of Illumio Zero Trust Segmentation (ZTS)*. Forrester Research, 2023. https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/6435d3cbc91af0d3133fc068_Total-Economic-Impact-Illumio-Zero-Trust-Segmentation.pdf
2. Forrester. *The Total Economic Impact™ of Zero Trust Solutions from Microsoft*.– Forrester Research, 2022. – Available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Zero-Trust-TEI-Study.pdf

3. Rose S. *Planning for a Zero Trust Architecture* [Electronic resource]. – NIST Cybersecurity White Paper (Draft), 2021. – Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf
4. Garbis J., Chapman J. *Zero Trust Architectures*. In: *Zero Trust Security* [Electronic resource]. – Springer, 2021. – pp. 31–54. – Available at: https://link.springer.com/chapter/10.1007/978-1-4842-6702-8_3
5. Swetha M. J., Asha S. N., Raghavendra M. *Zero Trust Architecture in Modern Computer Networks* [Electronic resource]. – *World Journal of Advanced Research and Reviews*, 2020. – Available at: https://wjarr.com/content/zero-trust-architecture-modern-computer-networks
6. Brennan H., Farah K. *Zero Trust+: A Trusted-based Zero Trust Architecture for IoT at Scale* [Electronic resource]. – *2024 IEEE International Conference on Consumer Electronics (ICCE)*, 2024. – Available at: https://ieeexplore.ieee.org/document/10444321
7. Al-Tamimi S. *Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review* [Electronic resource]. – *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, 2024. – Available at: https://ieeexplore.ieee.org/document/10811176
8. Abuhasel K. A. *A Zero-trust Network-based Access Control Scheme for Sustainable and Resilient Industry 5.0* [Electronic resource]. – *ResearchGate*, 2023. – Available at: https://www.researchgate.net/publication/374865665
9. Liu C., Tan R., Wu Y., Feng Y., Jin Z., Zhang F., Liu Y., Liu Q. *Zero Trust Architecture for Cyber Security in Industry 4.0 and 5.0* [Electronic resource]. – *Cybersecurity*, 2024. – Available at: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0
10. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture* [Electronic resource]. – *NIST Special Publication 800-207*. Gaithersburg: National Institute of Standards and Technology, 2020. – 59 p. – Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
11. Cisco Systems. *Zero Trust Architecture Guide* [Electronic resource]. – Cisco, 2022. – Available at: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-ag.html
12. Ghasemshirazi S., Shirvani G., Alipour M. A. *Towards Effective Zero Trust in Internet of Things (IoT): Challenges and Future Directions* [Electronic resource]. – *arXiv*, 2023. – Available at: https://arxiv.org/pdf/2309.03582
13. Li S., Iqbal M., Saxena N. *Future Industry Internet of Things with Zero-trust Security* [Electronic resource]. – *ResearchGate*, 2022. – Available at: https://www.researchgate.net/publication/359147843
14. Bicer C., Murturi I., Donta P. K., Dustdar S. *A Novel Zero Trust Model for Access Control in IoT Networks* [Electronic resource]. – *arXiv*, 2023. – Available at: https://arxiv.org/pdf/2311.16744
15. Mohseni-Ejiyeh A. *Enhancing IoT Security Through Adaptive Zero Trust Architecture* [Electronic resource]. – *arXiv*, 2023. – Available at: https://arxiv.org/pdf/2309.01293
16. Ma X., Fang F., Wang X. *Towards AI-enabled Zero Trust Security for the Industrial Internet of Things* [Electronic resource]. – *arXiv*, 2025. – Available at: https://arxiv.org/pdf/2501.03601
17. Ghasemshirazi S., Shirvani G., Alipour M. A. *Zero Trust: Applications, Challenges, and Opportunities* [Electronic resource]. – *ResearchGate*, 2023. – Available at: https://www.researchgate.net/publication/373753509
18. Ismail M., Abd El-Gawad A. F. *Revisiting Zero-Trust Security for Internet of Things* [Electronic resource]. – *ResearchGate*, 2023. – Available at: https://www.researchgate.net/publication/377021858
19. Li S. *Editorial: Zero Trust based Internet of Things* [Electronic resource]. – *ResearchGate*, 2020. – Available at: https://www.researchgate.net/publication/341958873
20. Simpson W. R. *Toward a Zero Trust Metric* [Electronic resource]. – *Procedia Computer Science*, 2022, Vol. 201, pp. 1222–1230. – Available at: https://www.sciencedirect.com/science/article/pii/S1877050922007530
21. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security*. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
22. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
23. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security.* [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.