International Science Journal of Engineering & Agriculture
2026; 5(1): 66-79
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20260501.07
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Проєктний аналіз впровадження системи кібербезпеки zero trust

Олена Доля
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-0364-988X

Анотація: У роботі виконано проєктний аналіз впровадження підходу *Zero Trust* у корпоративній IT-інфраструктурі в умовах розмивання мережевого периметра, розвитку хмарних сервісів, SaaS та віддаленої/гібридної роботи. Метою є обґрунтування доцільності та формування практичного плану поетапного впровадження Zero Trust із визначенням обсягу робіт, залежностей, ресурсів, ризиків і вимірюваних критеріїв успіху.

Запропоновано цільову архітектуру (TO-BE), що поєднує керування ідентичностями та доступом (IAM/SSO/MFA), принцип найменших привілеїв, сегментацію/мікросегментацію, Zero Trust Network Access (ZTNA), контроль стану кінцевих точок (MDM/EDR), захист даних (класифікація, DLP) та безперервний моніторинг і реагування (SIEM/SOAR). Для проєктування й пріоритизації ініціатив застосовано комбіновану методику: архітектурну декомпозицію за доменами контролів, gap-аналіз AS-IS/TO-BE, моделювання загроз і ризик-орієнтоване ранжування контролів.

Практичну перевірку ефективності продемонстровано експериментом у форматі «до/після» для критичного сервісу: у періоді B увімкнено MFA, впроваджено ZTNA-політику доступу до застосунку, використано сигнал *device posture* та забезпечено централізоване журналювання в SIEM. Отримано ілюстративні результати, що показують зниження частки успішних фішингових входів, скорочення кількості інцидентів, а також суттєве покращення операційних метрик реагування (MTTD/MTTR). Результатом роботи є структурований план впровадження, набір KPI та підхід до контролю якості політик, що забезпечують керованість трансформації та підстави для масштабування Zero Trust на інші домени.

Ключові слова: Zero Trust, кібербезпеки, IAM, MFA, SSO, мікросегментація, EDR, SIEM, DLP, MTTD, MTTR.

1. Вступ

Проблематика кібербезпеки в галузі IT упродовж останніх років суттєво загострилася через цифровізацію бізнес-процесів, активне використання хмарних сервісів і SaaS, розвиток віддаленої/гібридної роботи та зростання кількості кінцевих точок (мобільні пристрої, BYOD, IoT/IIoT). За цих умов традиційна «периметрова» модель захисту втрачає ефективність: компрометація облікових даних, фішинг, атаки через підрядників або уразливості кінцевих точок дають змогу зловмиснику отримувати доступ до ресурсів незалежно від фізичного розташування в мережі.

Підхід *Zero Trust* розглядається як відповідь на зазначені виклики, оскільки базується на постійній перевірці кожного запиту до ресурсу, принципі мінімальних привілеїв та обліку контексту доступу (ідентичність, стан пристрою, місце та інші сигнали). Однак практичне впровадження Zero Trust є складним комплексним проєктом, що зачіпає IAM (SSO/MFA), мережеві політики та сегментацію, контроль пристроїв, захист даних і процеси моніторингу/реагування.

Актуальність проєктного аналізу впровадження Zero Trust полягає в необхідності визначити оптимальну послідовність робіт, залежності та ризики, оцінити витрати й ресурси, а також сформувати вимірювані критерії успіху (KPI). Саме така постановка дозволяє перейти від декларативної концепції до керованої програми змін, яка забезпечує практичний безпековий ефект без критичного погіршення доступності та зручності для користувачів.

2. Аналіз літератури

Сучасна література щодо Zero Trust концентрується навколо таких напрямів: (1) базові архітектурні принципи та референсні моделі; (2) практичні впровадження у великих організаціях; (3) конкретні технічні механізми (IAM, мікросегментація, контроль пристроїв, захист даних, моніторинг); (4) оцінювання ефективності та метрики.

2.1. Архітектурні основи Zero Trust. NIST SP 800-207 формалізує поняття компонентів Zero Trust (policy engine/policy administrator, точки виконання політик, телеметрія) та підкреслює, що ключовою одиницею захисту є *ресурс*, а не мережевий сегмент [1]. Подальший розвиток підходів у NIST SP 800-207A деталізує приклади «еталонних» сценаріїв і технік реалізації (зокрема для хмарних/гібридних середовищ) [2].

2.2. Практичні кейси та еволюція від периметра до контекстного доступу. Серія публікацій BeyondCorp описує перехід до моделі доступу «на основі ідентичності й пристрою» та демонструє, що Zero Trust може бути масштабованим у великих екосистемах, якщо організація має розвинені процеси управління ідентичностями, інвентаризацію пристроїв та стабільні канали телеметрії [3–5].

2.3. Огляди та систематизація досліджень. Оглядові роботи останніх років узагальнюють таксономію Zero Trust, типові контролі та проблеми впровадження.

Зокрема, Syed та ін. пропонують узагальнену картину Zero Trust (мережа, ідентичність, пристрої, дані) та підкреслюють роль безперервної оцінки ризику доступу [6]. Систематичний огляд Mushtaq та ін. (2025) підкреслює тенденцію до інтеграції Zero Trust із хмарними сервісами та автоматизацією політик, а також наголошує на проблемах вимірюваності ефекту й дефіциті відтворюваних експериментів [7].

2.4. Zero Trust у хмарі, edge та IoT/IIoT. Зростає кількість робіт, що адаптують Zero Trust до середовищ IoT/edge, де характерними є обмежені ресурси, висока гетерогенність пристроїв та складність централізованого керування. Liu та ін. виконують систематичний огляд застосування принципів Zero Trust в IoT і показують, що ключовими проблемами є управління ідентичностями для пристроїв, довіра до телеметрії та практична реалізація безперервної оцінки контексту [8]. Для промислових сценаріїв розглядаються архітектури захищеного віддаленого доступу та контроль сесій у IIoT, зокрема з поєднанням мережевих політик і endpoint-контролів [9]. У ширшому контексті цифрової трансформації промисловості підкреслюється, що Zero Trust у IIoT потребує узгодження з вимогами надійності, латентності та безперервності виробничих процесів [10].

2.5. Сегментація та мікросегментація. У частині мережевих контролів важливим елементом Zero Trust залишається сегментація/мікросегментація для обмеження lateral movement. Дослідження в цій області фокусуються на тому, як формалізувати правила доступу між сервісами/компонентами та як оцінювати якість політик (повнота покриття, мінімальність, ризик помилок). Basta та ін. пропонують підхід до оцінювання стратегій сегментації як частини Zero Trust, наголошуючи на потребі формалізованих вимог і перевірки політик на великих топологіях [11].

2.6. Захист даних, конфіденційність і довіра до виконання. Окремий пласт досліджень присвячено захисту даних і довірі до середовищ виконання. Han, Kim, Lee та Shin пропонують модель контролю доступу в парадигмі Zero Trust із використанням TEE/SGX як механізму

підсилення довіри до виконання політик у хмарі [12]. Такі підходи важливі для сценаріїв, де критичною є довіра не лише до користувача/пристрою, а й до середовища, у якому обробляються дані.

2.7. Безперервна перевірка, Zero Trust Network Access (ZTNA) та контроль сесій. Ідентичність та автентифікація в Zero Trust виходять за межі «одноразового входу»: актуальними є безперервна верифікація та адаптивні політики доступу. Xiao та ін. пропонують підхід Age of Trust (AoT) як frame-work безперервної перевірки на основі телеметрії та поведінкових сигналів [13]. У проєктному контексті ZTNA розглядають як практичний клас рішень для контролю доступу до застосунків у гібридних середовищах; огляд Attar Bashi та Senan узагальнює підходи до ZTNA, зокрема питання інтеграції з IAM і мережевими політиками [14].

2.8. Моніторинг, реагування та метрики ефективності. Критично важливими для проєктного аналізу є метрики, які дозволяють виміряти результат: покриття MFA, частка керованих пристроїв, кількість інцидентів, MTTD/MTTR, частка доступів за принципом least privilege тощо. Водночас література підкреслює, що прямий зв'язок між впровадженням Zero Trust і зниженням збитків від інцидентів часто складно формалізувати через багатофакторність безпекових програм та нестачу відкритих даних [6,7]. З технологічного боку підкреслюється важливість якісної телеметрії та швидкого реагування; огляд Alioto показує, що сучасні платформи моніторингу спираються на апаратні та системні механізми для збору даних і підтримки security analytics у реальному часі [15].

2.9. Додаткові сучасні напрями. Окремі сучасні роботи торкаються спеціалізованих сценаріїв Zero Trust. Наприклад, Bandara та ін. розглядають поєднання Zero Trust із мережевими механізмами 5G (network slicing) для підвищення безпеки взаємодії сервісів [16]. У 2025 році з'являються оновлені огляди та узагальнення процедур упровадження Zero Trust і кібербезпекових практик у ширшому контексті організаційної готовності та керування змінами [17,18].

2.10. Висновки з аналізу літератури та research gaps. На основі аналізу джерел можна виділити аспекти, що розкриті достатньо добре:

- архітектурні принципи Zero Trust і типові компоненти (NIST) [1,2];
- практичні патерни доступу «на основі ідентичності й пристрою» (BeyondCorp) [3–5];
- узагальнення напрямів (IAM, сегментація, endpoint, data, monitoring) у вигляді оглядів [6,7].

Водночас недостатньо розкритими (актуальними для подальших досліджень) залишаються такі напрями:

1. Відтворювані методики оцінювання ефекту Zero Trust. Бракує універсальних протоколів «до/після», які б пов'язували технічні KPI (MFA coverage, MTTD/MTTR) із бізнес-збитками та ризиками [6,7].
2. Кількісні моделі ризику для policy engine. У багатьох роботах декларується «безперервна оцінка», але на практиці мало формалізується, як саме ризик агрегується з телеметрії та перетворюється на політики доступу [6,12].
3. Масштабована мікросегментація в гетерогенних/ середовищах. Існують підходи до проєктування політик, але бракує досліджень про їх підтримку при еволюції сервісів, а також про валідацію політик на реальних топологіях [9].
4. Zero Trust для IoT/edge з урахуванням обмежень ресурсів та операційних вимог.

Потрібні узгоджені підходи до керування ідентичностями пристроїв, надійної телеметрії та безперервної оцінки контексту в умовах обмежених ресурсів, а також узгодження з вимогами IIoT до латентності/безп

5. Відтворювані «процедури впровадження» та організаційна готовність. Багато робіт описують принципи та архітектуру, але меншою мірою формалізують послідовність кроків,

критерії готовності та типові компроміси безпеки/зручності для користувачів у реальних організаціях [15,16].

Таким чином, література підтверджує стратегічну доцільність Zero Trust, але для практичного впровадження в організаціях критичною є саме проєктна складова: поетапність, вимірюваність, управління ризиками та інтеграція з процесами IT і безпеки.

3. Мета та задачі дослідження.

Мета дослідження — обґрунтувати доцільність і розробити проєктний план впровадження підходу *Zero Trust* (обсяг, етапи, бюджет, ризики, KPI) для корпоративної IT-інфраструктури.

Об'єкт дослідження — корпоративна IT-інфраструктура та процеси забезпечення доступу до ресурсів (onpremise/хмара/гібрид) в умовах розмивання мережевого периметра.

Предмет дослідження — методи та інструменти впровадження *Zero Trust*: IAM (SSO/MFA), сегментація/мікр контроль стану пристроїв (MDM/EDR), ZTNA, захист даних (класифікація/DLP), моніторинг і реагування (SIEM/SOAR).

Задачі дослідження:

1. описати поточний стан (AS-IS): мережа, доступи, кінцеві точки, дані, процеси реагування;
2. сформувати цільовий стан (TO-BE) та вимоги до контролів Zero Trust;
3. запропонувати дорожню карту впровадження

(пілот → масштабування → операціоналізація);

4. виконати оцінку витрат, ресурсів і термінів (WBS/план-графік);
5. скласти реєстр ризиків та заходи з їх мінімізації;
6. визначити KPI/метрики ефективності та методику їх вимірювання.

4. Огляд методів сучасної науки й практики щодо розв'язання поставлених задач.

У цьому розділі узагальнено методи, що найчастіше застосовуються в сучасній науці й практиці для проєктування та оцінювання впроваджень *Zero Trust*. Методи підібрано так, щоб вони покривали задачі формування TO-BE, пріоритизації контролів, планування впровадження та вимірювання ефекту [1,2,6,7].

4.1. Архітектурна декомпозиція та мапування доменів контролів. Метод базується на референсних моделях Zero Trust (компоненти policy engine/administrator, policy enforcement point, телеметрія) та декомпозиції архітектури на домени контролів (Identity, Device, Network, Data, Visibility) [1,2]. Для кількісної оцінки прогресу (підхід до вимірювання «покриття контролів») [1,2] застосовується показник покриття [1,2]:

$$C = \frac{N_{impl}}{N_{req}} \cdot 100\backslash\%, \quad (1)$$

де:

- C — покриття реалізації контролів, %;
- N_{impl} — кількість реалізованих (впроваджених) контролів у заданому домені/профілі;
- N_{req} — кількість контролів, що визначені як обов'язкові у цільовому профілі (TO-BE).

Оцінку покриття за доменами подано на рис. 1.

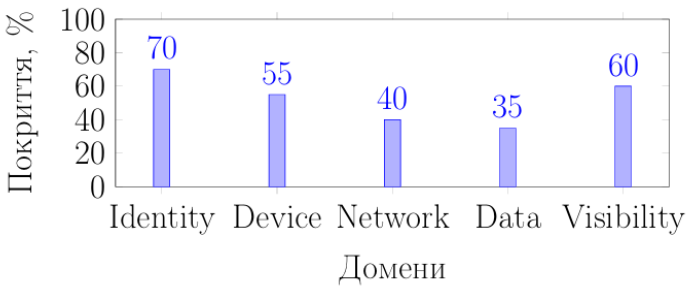

Рис. 1. Приклад мапування поточного покриття контролів Zero Trust за доменами.

На рис. 1 показано приклад порівняння покриття доменів контролів (Identity, Device, Network, Data, Visibility) у відсотках. Діаграма демонструє, які напрямки вже відносно зрілі (вищі стовпчики), а які залишаються «вузькими місцями» програми впровадження (нижчі стовпчики). Водночас слід враховувати, що значення є агрегованими: однакове покриття може означати різну якість налаштувань і різний фактичний рівень зниження ризику, тому інтерпретація потребує підтвердження аудитом конфігурацій і телеметрією.

Сильні сторони: забезпечує спільну «мову» для стейкхолдерів, дозволяє структурувати дорожню карту й залежності між контролями [1,2]. Слабкі сторони: саме по собі покриття не гарантує зниження ризику; важлива якість конфігурацій і контекст впровадження [6,7].

4.2. Gap-аналіз AS-IS/TOBE. Gap-аналіз дозволяє формалізувати розрив між поточним станом A та цільовим станом T для набору критеріїв/контролі У практиці оцінювання зрілості/готовності ZTA та планування трансформацій такий розрив часто описують нормалізованими шкалами [7]. Розрив можна подати у вигляді (2) вектора [7]:

$$\mathbf{g} = \mathbf{T} - \mathbf{A},\ g_i \in [0,1], \tag{2}$$

де:

- $\mathbf{A} = (A_1,\ldots,A_n)$ — вектор оцінок поточного стану (AS-IS) за n критеріями/контролями; • $\mathbf{T} = (T_1,\ldots,T_n)$ — вектор оцінок цільового стану (TO-BE) за тими ж критеріями;
- $\mathbf{g} = (g_1,\ldots,g_n)$ — вектор розривів;
- g_i — нормалізований дефіцит за i-м критерієм (0 — розриву немає, 1 — максимальний розрив у вибраній шкалі).

Приклад візуалізації розривів g_i наведено на рис. 2.

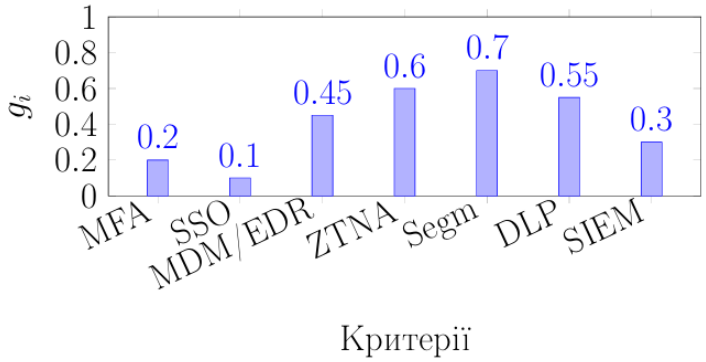

Рис 2. Приклад результатів gap-аналізу: нормалізовані розриви g_i між AS-IS і TO-BE.

Рис. 2 відображає нормалізовані розриви $g_i \in [0,1]$ між AS-IS і TOBE за вибраними контролями. Вищі значення g_i означають більший дефіцит (тобто більший обсяг робіт/інвестицій), тому графік зручний для первинного формування беклогу ініціатив. Обмеженням є те, що нормалізація та самі оцінки часто експертні: без узгодженої шкали й джерел даних такий рисунок може створювати ілюзію точності та вимагати додаткової валідації через інвентаризацію активів і вимірювану телеметрію.

Сильні сторони: дає прозору базу для обґрунтування пріоритетів і плану робіт; добре поєднується з проєктним плануванням. Слабкі сторони: оцінки часто експертні й можуть бути упередженими; потрібна валідація телеметрією та аудитами [6].

4.3. Моделювання загроз і сценаріїв атак (threat modeling). Threat modeling застосовується для виділення критичних ресурсів/сервісів та сценаріїв компрометації, що визначають вимоги до політик доступу й контекстних сигналів [1,6]. Для пріоритизації загроз у практиці

управління ризиками (зокрема при плануванні контролів ZTA) часто застосовується (3) базова ризик-оцінка [6]:

$$R_k = P_k \cdot I_k \tag{3}$$

де:

- R_k — оцінка ризику для k-ї загрози; • P_k — ймовірність реалізації k-ї загрози (напр., за експертною шкалою [0;1] або 1–5);
- I_k — вплив/збиток від реалізації k-ї загрози (напр., фінансовий, операційний або за бальною шкалою);
- k — індекс загрози/сценарію атаки.

Приклад побудови дерева сценаріїв подано на рис. 3.

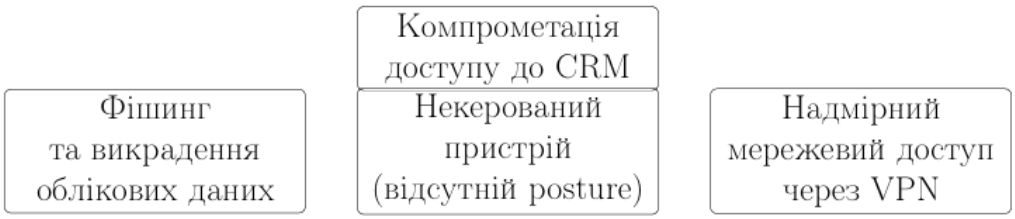

Рис 3. Спрощене дерево сценаріїв для threat modeling критичного сервісу.

На рис. 3 наведено спрощене дерево сценаріїв компрометації доступу до CRM через три типові вектори: фішинг, некерований пристрій та надмірний VPN-доступ. Така схема допомагає «приземлити» абстрактні вимоги Zero Trust на конкретні управлінські рішення (MFA, device posture, ZTNA, звуження мережевих прав). Недоліком є спрощення: дерево не показує повного ланцюга атак (наприклад, ескалацію привілеїв, зловживання токенами, помилки конфігурації), тому для виробничого використання потрібне деталювання вузлів, прив'язка до активів та перевірка припущень на даних SOC.

Сильні сторони: фокусується на реальних шляхах атаки та «больових точках» (облікові дані, пристрої, lateral movement), підсилює обґрунтованість вибору контролів [6,14]. Слабкі сторони: якість залежить від повноти знань про активи/загрози; складно формалізувати для великих гетерогенних середовищ без автоматизації та інвентаризації.

4.4. Оцінювання ризиків і пріоритизація контролів (зважена модель). Для проєктного планування потрібне ранжування ініціатив за очікуваним ефектом і складністю. Практичний підхід — зважена сума (multi-criteria scoring), де кожен контроль оцінюється за критеріями (зниження ризику, вартість, складність інтеграції, вплив на UX, комплаєнс) [6,7]. Формалізація через зважену суму застосовується в оглядових роботах як простий механізм пріоритизації в умовах неповних даних [7]. Інтегральний бал (7):

$$S_j = \sum_{i=1}^{m} w_i r_{ij}\,, \quad \sum_{i=1}^{m} w_i = 1, \tag{4}$$

де:

- S_j — інтегральний бал пріоритетності j-го контролю/ініц
- m — кількість критеріїв оцінювання;
- w_i — вага i-го критерію (частка важливості),

Pmi=1 wi = 1;

- r_{ij} — оцінка j-го контролю за i-м критерієм (нормалізована або у бальній шкалі);
- i — індекс критерію, j — індекс контролю.

Приклад ранжування контролів за балом S_j наведено на рис. 4.

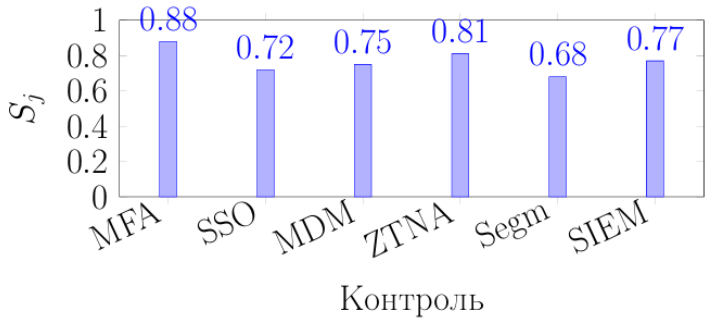

Рис 4. Приклад пріоритизації контролів за інтегральним балом S_j.

Рис. 4 ілюструє результат пріоритизації контролів за інтегральним балом S_j (чим вищий стовпчик, тим вищий пріоритет). Така візуалізація корисна для комунікації з менеджментом і формування послідовності впровадження. Водночас слід критично оцінювати джерело балів: значення S_j сильно залежать від ваг w_i та шкал r_{ij}, а також можуть не враховувати залежності між контролями (наприклад, MFA як передумова для адаптивних політик), тому результати потрібно доповнювати аналізом залежностей і ризиків впровадження.

Сильні сторони: прозора логіка вибору пріоритетів; легко інтегрується в WBS/план-графік і бюджетування.

Слабкі сторони: залежність від експертних ваг; ризик «псевдоточності», якщо шкали не узгоджені та немає історичних даних [7].

4.5. Формалізована оцінка. політик сегментації/мікросегментації. Сегментація є ключовим механізмом зменшення lateral movement. У наукових роботах пропонуються метрики оцінювання стратегій мікросегментації та перевірки політик на великих топологіях [11]. Як базову кількісну характеристику «жорсткості» політики можна використовувати відношення дозволених взаємодій до всіх потенційних взаємодій [11]:

$$D = \frac{|E_{allow}|}{|E_{possible}|}, \tag{5}$$

де:

- D — щільність дозволів (чим менше D, тим менше дозволених взаємодій);
- E_{allow} — множина дозволених з’єднань/взаємодій між компонентами;
- $E_{possible}$ — множина всіх потенційно можливих з’єднань (за заданою моделлю компонентів);
- $|\cdot|$ — потужність множини (кількість елементів).

Динаміку зменшення щільності дозволів D ілюструє рис. 5.

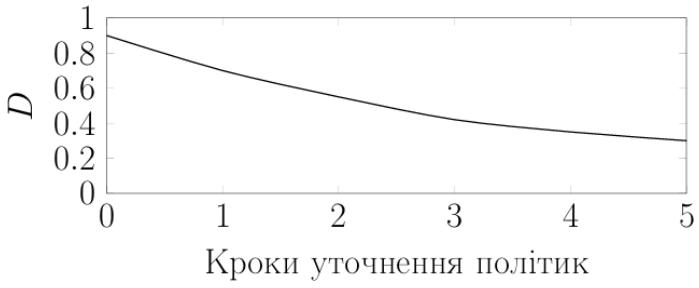

Рис 5. Ілюстрація: зниження щільності дозволів D у міру уточнення правил мікросегментації.

На рис. 5 показано ілюстративну залежність щільності дозволів *D* від кроків уточнення політик: зі зростанням числа ітерацій *D* зменшується, що означає звуження множини дозволених взаємодій і потенційне обмеження lateral movement. Сильна сторона такого графіка — наочне відображення «tightening» політик. Проте він не демонструє, чи не було порушено бізнес-функціональність: падіння *D* може супроводжуватись збоєм легітимних потоків трафіку, тому на практиці потрібне паралельне відстеження показників доступності/помилок застосунків і контроль змін.

Сильні сторони: дає формальний критерій «зменшення поверхні взаємодій»; придатний для валідації політик і контрольованого tightening. Слабкі сторони: у legacy-середовищах важко отримати повну картину залежностей; існує ризик порушення працездатності через надмірне звуження [11].

4.6. Експериментальний підхід «до/після» для KPI. Для перевірки практичного ефекту впроваджених контролів застосовується експеримент «до/після» (A/B у часі) з вимірюванням KPI (MFA coverage, MTTD/MTTR, інциденти, результати фішинг-тестів) [6,7]. Для кількісного порівняння періодів використовується стандартна формула відносної зміни показника [6,7]:

$$\Delta x = \frac{x_B - x_A}{x_A} \cdot 100\backslash\%. \quad . \tag{6}$$

де:

- Δx — відносна зміна показника x між періодами, %;
- x_A — значення показника у періоді A (“до”);
- x_B — значення показника у періоді B (“після”).

Порівняння MTTD та MTTR у періодах A і B показано на рис. 6.

Рис 6. Приклад порівняння MTTD та MTTR для періодів A (до) і B (після).

Рис. 6 порівнює MTTD та MTTR у двох періодах (A — до, B — після), що дозволяє наочно оцінити вплив змін у моніторингу та доступі на швидкість виявлення й реагування. Зменшення стовпчиків у періоді B інтерпретується як покращення операційної керованості. Водночас без контексту експерименту можливі хибні висновки: метрики можуть змінюватися через зовнішні фактори (інший профіль атак, зміни в SOC, різна кількість інцидентів), тому для коректної інтерпретації потрібні контрольні припущення, однакова тривалість періодів і пояснення джерел даних.

Сильні сторони: забезпечує вимірюваність і демонструє прикладну цінність для бізнесу (через KPI); добре підтримує рішення про масштабування.

Слабкі сторони: потрібні якісні журнали/телеметрія; можливі впливи сторонніх факторів (сезонність атак, зміни в процесах SOC), тому потрібні контрольні припущення.

4.7. Аналіз методів. Методи 1–2 задають структуру та «карту» робіт, але без методів 3–4 можуть не відобразити реальні ризики. Метод 5 дає формальні метрики для мережевого домену, однак потребує інвентаризації залежностей. Метод 6 переводить проєкт у вимірювану площину, але залежить від зрілості моніторингу та якості даних.

4.8. Обґрунтування вибору методики для виконання задач дослідження. Для розв'язання поставлених задач у роботі обрано комбіновану методику, що поєднує:

- архітектурну декомпозицію за NIST (метод 1) як основу TO-BE та вимог [1,2];
- gap-аналіз (метод 2) для формування переліку робіт і залежностей;
- threat modeling (метод 3) та зважене ранжування

(метод 4) для пріоритизації контролів із найбільшим ризик-ефектом [6,7,14];

- формальну перевірку сегментації (метод 5) у частині мережевих політик [11];
- експеримент «до/після» (метод 6) як інструмент валідації ефекту на пілоті та підставу для масштабування.

Такий вибір аргументований тим, що він одночасно забезпечує (а) архітектурну узгодженість, (б) керованість проєкту та (в) вимірюваний результат у KPI, що прямо відповідає задачам дослідження.

5. Планування й проведення експерименту

5.1. Мета та дизайн експерименту. Метою експерименту є кількісно оцінити ефект від пілотного впровадження контролів Zero Trust для одного критичного сервісу (умовно: корпоративний портал/CRM) за підходом *«до/після»*. Дизайн експерименту включає два періоди спостереження однакової тривалості:

- Період A (до впровадження): поточні механізми доступу (пароль/VPN за потреби), базовий журнал доступів.
- Період B (після впровадження): ввімкнено MFA для доступу до сервісу, застосовано ZTNAполітику доступу за принципом найменших привілеїв, увімкнено контроль стану пристрою (керований/некерований) та централізоване журналювання в SIEM.

5.2. Об'єкт експерименту та контрольні впливи. У пілоті використовуються такі керовані зміни (interventions):

1. MFA для всіх користувачів сервісу.
2. ZTNA замість широкого мережевого доступу: доступ надається лише до конкретного застосунку.
3. Device posture (умовно): доступ дозволяється лише з керованих пристроїв (зареєстрованих у MDM/EDR) або знижується рівень доступу для некерованих.
4. Централізований моніторинг: події автентифікації/а та алерти EDR передаються до SIEM.

5.3. Метрики та методика вимірювання. Для оцінювання ефекту визначено набір метрик кібербезпеки та операційної керованості:

- MFA_cov — покриття MFA, % користувачів із MFA.
- Managed_dev — частка керованих пристроїв, %.
- Phish_SR — частка успішних фішингових входів (за результатами симульованих фішинг-тестів), %.
- Inc — кількість підтверджених інцидентів доступу до сервісу за період.
- MTTD — середній час виявлення інциденту.
- MTTR — середній час реагування/локалізації.

Оцінювання виконується на основі журналів IAM/SSO, SIEM-алертів та реєстру інцидентів SOC. Для метрик часу використовуються стандартні визначення (7,8) (узгоджені з практикою вимірювання операційної ефективності реагування) [6,7]:

$$\mathrm{MTTD} = \frac{1}{N}\sum_{i=1}^{N}\left(t_{\mathrm{detect}}^{(i)} - t_{\mathrm{start}}^{(i)}\right), \qquad (7)$$

де:

- MTTD — середній час виявлення інциденту;
- N — кількість інцидентів у вибірці;
- $t_{start}^{(i)}$ — момент початку *i*-го інциденту (або оцінка моменту компрометації/першої події);
- $t_{detect}^{(i)}$ — момент виявлення *i*-го інциденту.

$$\text{MTTR} = \frac{1}{N}\sum_{i=1}^{N}\left(t_{resolve}^{(i)} - t_{detect}^{(i)}\right) \quad (8)$$

де:

- MTTR — середній час реагування/відновлення (локалізації) після виявлення;
- $t_{resolve}^{(i)}$— момент завершення реагування (локалізація/ус для *i*-го інциденту;
- $t_{detect}^{(i)}$ — момент виявлення *i*-го інциденту.

5.4. Ілюстративні результати «до/після». Результати нижче наведено як приклад оформлення експерименту у табл.1 (структура відтворювана на реальних даних організації).

Таблиця 1. Порівняння метрик у пілоті Zero Trust (приклад «до/після»)

Показник	Період A (до)	Період B (після)
MFA_cov, %	0	98
Managed_dev, %	35	80
Phish_SR, %	12.0	3.0
Inc, к-сть	6	2
MTTD, год	18.0	4.5
MTTR, год	36.0	10.0

5.5. Обробка результатів експерименту. Для кількісного порівняння періодів A і B використано відносну зміну показників [6,7]:

$$\Delta x = \frac{x_B - x_A}{x_A} \cdot 100\backslash\%. \quad (9)$$

На основі даних табл. 1 отримано такі оцінки ефекту:

- покриття MFA зросло на +98 п.п. (з 0% до 98%);
- частка керованих пристроїв збільшилась на +45 п.п. (з 35% до 80%);
- частка успішних фішингових входів зменшилась на 75% (з 12% до 3%);
- кількість інцидентів доступу зменшилась на 66.7% (з 6 до 2);
- MTTD зменшився на 75% (з 18 год до 4.5 год);
- MTTR зменшився на 72.2% (з 36 год до 10 год).

5.6. Висновки по розділу.

Пілотний експеримент показує, що навіть обмежене за охопленням впровадження Zero Trust (MFA + ZTNA + контроль пристрою + SIEM) може дати вимірюваний ефект: зменшення частки успішних фішингових входів, скорочення кількості інцидентів доступу та суттєве покращення операційної керованості через зниження MTTD і MTTR. Отримані результати підтверджують доцільність масштабування підходу на інші сервіси за умови поетапного впровадження та контролю впливу на зручність користувачів.

6. Обговорення результатів

Узагальнення результатів показує, що поєднання IAM (SSO/MFA), контекстних сигналів (керованість пристрою), ZTNA та централізованого моніторингу (SIEM) дозволяє перейти від «периметрової» логіки доступу до керованих політик, орієнтованих на ризик. Результати пілоту у форматі «до/після» (зміни MTTD/MTTR частки успішних фішингових входів та кількості інцидентів) підтверджують практичний ефект навіть при обмеженому охопленні.

6.1. SWOT-аналіз запропонованого підходу впровадження Zero Trust:

- Strengths (Сильні сторони): вимірюваність ефекту через KPI; зменшення ризику компрометації облікових даних завдяки MFA; зниження lateral movement через сегментацію/обмеження доступу; підвищення керованості через телеметрію та SIEM.
- Weaknesses (Слабкі сторони): залежність від якості інвентаризації активів і телеметрії; значні інтеграційні витрати; ризик погіршення UX при надмірно жорстких політиках; складність підтримки політик у гетерогенних/legacy середовищах.
- Opportunities (Можливості): автоматизація політик через risk-based access; масштабування на хмарні сервіси та SaaS; підвищення відповідності комплаєнсу; використання SOAR для скорочення MTTR.
- Threats (Загрози): помилки конфігурації

IAM/політик доступу; vendor lock-in; обхід контролів через компрометацію токенів/сесій; зростання складності керування при швидкій зміні застосунків і топологій.

6.2. Наукова новизна.

Наукова новизна роботи полягає у запропонуванні інтегрованої, проєктно-орієнтованої методики впровадження Zero Trust, яка поєднує: (1) архітектурну декомпозицію доменів контролів; (2) gap-аналіз ASIS/TO-BE; (3) threat modeling і ризик-орієнтовану пріоритизацію; (4) формалізовані метрики для мікросегментації експериментальний протокол «до/після» для перевірки KPI на пілоті. Додатковою новизною є формалізація набору показників, що напряму зв’язують технічні зміни доступу та моніторингу з операційними метриками реагування (MTTD/MTTR) у межах одного проєктного циклу.

6.3. Перспективи подальших досліджень.

Перспективними напрямами подальших досліджень є: (1) побудова кількісних моделей ризику для policy engine (агрегація сигналів контексту, динамічні пороги доступу); (2) методи валідації політик мікросегментації на реальних топологіях із мінімізацією ризику збоїв; (3) порівняння ефективності ZTNA-рішень у різних архітектурах (on-premise/хмара/гібрид); (4) розширення експериментального дизайну (контрольні групи, аналіз конфаундерів, довші періоди спостереження) для підвищення відтворюваності результатів.

7. Висновки

У роботі виконано проєктний аналіз впровадження моделі *Zero Trust* та сформовано практичні результати, що дозволяють перейти від концепції до керованого плану трансформації.

1. Сформовано цільовий стан (TO-BE) Zero Trust,який інтегрує IAM/SSO/MFA, least privilege, ZTNA, контроль стану пристрою (MDM/EDR), сегментацію/мікросегментацію, захист даних (класифікація/DLP) та моніторинг/реагування (SIEM/SOAR).

2. Запропоновано комбіновану методику та поетапний підхід впровадження (архітектурна декомпозиція, gap-аналіз AS-IS/TO-BE, threat modeling, ризикорієнтована пріоритизація, пілот → масштабування → операціоналізація), що зменшує ризики збоїв і дає змогу керувати змінами.

3. Продемонстровано експериментальну валідацію KPI у форматі «до/після»: поєднання MFA+ZTNA+dev posture+SIEM може знижувати кількість інцидентів і покращувати операційні метрики реагування (MTTD/MTTR), що створює підстави для масштабуванн та подальшого вдосконалення системи метрик.

References:

1) Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST SP 800-207). National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-207

2) Chandramouli, R., & Butcher, Z. (2023). *Zero Trust Architecture* (NIST SP 800-207A). National Institute of Standards and Technology. doi:10.6028/NIST.S 207A

3) Ward, A., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login: The USENIX Magazine, 39*(6).

4) Osborn, M., McWilliams, B., Beyer, B., & Saltonstall, M. (2016). BeyondCorp Part II: Design to deployment at Google. *;login: The USENIX Magazine, 41*(1), 28–34.

5) Cittadini, L., Spear, K., Beyer, B., & Saltonstall, M. (2016). BeyondCorp Part III: The access proxy. *;login: The USENIX Magazine, 41*(4).

6) Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10*, 57143–57179. doi:10.1109/ACCESS.2022.3174679

7) Mushtaq, M. F., Mohsin, M., & Mushtaq, M. (2025). Zero trust architecture: A systematic literature review. *Sensors, 25*(19), 6118. doi:10.3390/s25196118

8) Liu, Y., Zhou, Y., Li, X., & Sun, J. (2024). Dissecting zero trust: A systematic review of its principles, applications, and challenges in IoT. *Cyber- security, 7*, 20. doi:10.1186/s42400-024-00212-0

9) Federici, M., Martintoni, A., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics, 12*(3), 566. doi:10.3390/electronics12030566

10) Li, S., Iqbal, M. U., & Saxena, N. (2022). Enabling future industry 4.0-based secure IIoT: A survey on IIoT and the use of the digital twin. *Information Systems Frontiers, 24*, 1–26. doi:10.1007/s10796021-10199-5

11) Basta, A., Ikram, M., Kaafar, M. A., & Walker, D. (2022). Evaluating zero-trust micro-segmentation strategies in enterprise networks. In *2022 IEEE/IFIP Network Operations and Management Symposium (NOMS)*. doi:10.1109/NOMS54207.2022.9789888

12) Han, M., Kim, J., Lee, S., & Shin, J. (2024). S-ZAC: SGX-enabled zero-trust access control in cloud computing. *Electronics, 13*(16), 3213. doi:10.3390/electronics13163213

13) Xiao, Y., Du, Q., Cheng, W., Diamantoulakis, P. D., & Karagiannidis, G. K. (2024). Age of Trust (AoT): A continuous verification framework for wireless networks. *arXiv*. arXiv:2406.02190

14) Attar Bashi, A., & Senan, E. M. (2025). Overview of zero trust network access (ZTNA): Security, challenges and future directions. *International Journal of Professional Computer Science & Communications, 11*(1). doi:10.31436/ijpcc.v11i1.494

15) Alioto, M. (2022). Hardware-supported security analytics for edge and cloud: A review. *IEEE Open Journal of the Solid-State Circuits Society, 2*, 127–146. doi:10.1109/OJSSCS.2022.3223274

16) Bandara, E., Liang, X., Shetty, S., Mukkamala, R., Rahman, A., & Keong, N. W. (2022). Skunk: A blockchain and zero trust security enabled federated learning platform for 5G/6G network slicing. In *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 109–117). doi:10.1109/SECON55815.2022.9

17) Lund, B. D., Berryman, B., & Haar, M. (2025). Cybersecurity procedures in the zero trust era. *arXiv*. arXiv:2505.18872

18) Gambo, A., & Almulhem, A. (2025). A systematic literature review of zero trust. *arXiv*. arXiv:2503.11659

Project analysis of the implementation of a zero trust cybersecurity system

Olena Dolia
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-0364-988X

Abstract: This paper provides a projectoriented analysis of implementing the *Zero Trust* security model in a corporate IT environment. The topic is motivated by the increasing cyber risk landscape, hybrid work, and the erosion of the traditional network perimeter due to cloud services, mobile endpoints, and third-party access. The goal is to justify the implementation feasibility and to propose an actionable delivery roadmap, including scope definition, phased rollout, resource planning, risk management, cost estimation, and measurable success criteria.

The proposed target architecture combines identity and access management (IAM, SSO, MFA), least-privilege access, network segmentation (including micro-segmentation), endpoint security and device posture controls (MDM/EDR), data protection (classification and DLP), and continuous monitoring and incident response (SIEM/SOAR). A phased implementation approach is outlined: AS-IS assessment, TO-BE design, pilot deployment for a critical service, enterprise-wide scaling, and operationalization via policies, staff training, and security KPIs.

Key words: Zero Trust, cybersecurity, IAM, MFA, SSO, micro-segmentation, EDR, SIEM, DLP, MTTD, MTTR.