КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.846
УДК 004. 72; 004.7

Сиротинський Роман Михайлович
аспірант, асистент
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0002-6280-3290
roman.m.syrotynskyi@lpnu.ua

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

СПЕЦИФІКА ПОБУДОВИ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ В ГІБРИДНИХ ІНФРАСТРУКТУРАХ

Анотація. Популярність використання гібридних інфраструктур стрімко зростає, оскільки вони дозволяють поєднувати переваги локальних обчислювальних ресурсів — контроль, рентабельність, відповідність регуляторним вимогам — з масштабованістю, гнучкістю та високою доступністю хмарних технологій. У таких умовах виникає потреба забезпечити єдиний підхід до інформаційної безпеки, здатний охопити обидва типи середовищ. Архітектура нульової довіри (Zero Trust Architecture, ZTA) розглядається як сучасна та ефективна модель, що дозволяє досягти високого рівня контролю доступу, мінімізувати ризики порушення безпеки та забезпечити захист критичних ресурсів незалежно від їхнього розміщення. Разом із тим, побудова ZTA в гібридних середовищах супроводжується низкою викликів, зумовлених різнорідністю технологій, відсутністю уніфікованих інструментів управління, різним ступенем контролю над компонентами інфраструктури та складністю реалізації єдиних політик автентифікації, авторизації та моніторингу. У статті досліджуються ключові відмінності між традиційною (локальною) та гібридною інфраструктурами, зокрема — з погляду побудови архітектури нульової довіри. Проаналізовано специфіку інтеграції елементів локальних та хмарних середовищ, що часто мають різні механізми ідентифікації користувачів, керування сесіями, журналювання подій та застосування політик доступу. Пропонується низка важливих архітектурних компонентів і технологій, які формують стек компонентів, необхідних для реалізації ZTA у гібридному середовищі. Також описується аналіз викликів впровадження архітектури нульової довіри (Zero Trust) у гібридній мережевій інфраструктурі, зокрема складність гібридних мережевих топологій, складність мікросегментації уніфікація видимості, централізоване керування доступом IAM та інші. З урахуванням виявлених особливостей сформовано поетапний план міграції гібридних інфраструктур до архітектури нульової довіри, що передбачає оцінку та планування, розробку архітектури , вибір рішень та інші важливі кроки.

Ключові слова: архітектура нульової довіри; гібридне середовище; локальна мережа; хмарна інфраструктура; інтеграція; відповідність; мікросегментація; ідентичність.

ВСТУП

У сучасному швидкозмінному цифровому середовищі організації дедалі частіше використовують гібридні середовища, що поєднують локальну інфраструктуру з хмарними ресурсами. Такий підхід забезпечує гнучкість, масштабованість і економічну ефективність, дозволяючи підприємствам оптимізувати робочі навантаження та підвищувати операційну ефективність. Однак взаємопов’язана природа гібридних середовищ створює серйозні

виклики для безпеки, оскільки традиційні моделі безпеки, засновані на периметрі, не здатні ефективно захищати динамічні та розподілені архітектури.

Для вирішення цих викликів з'явилася архітектура нульової довіри (Zero Trust Architecture, ZTA) як революційна концепція кібербезпеки. На відміну від традиційних моделей безпеки, що передбачають довіру в межах мережевого периметра, ZTA працює за принципом «ніколи не довіряй, завжди перевіряй». Це означає, що кожен користувач, пристрій і застосунок повинні проходити постійну автентифікацію та отримувати лише мінімально необхідний рівень доступу для виконання своїх завдань. Основними принципами ZTA є сильна перевірка ідентичності, мікросегментація, безперервний моніторинг та суворий контроль доступу, що дозволяє зменшити ризики, пов'язані з кіберзагрозами, внутрішніми атаками та несанкціонованим доступом.

Інтеграція ZTA у гібридні середовища є необхідною умовою для створення надійної, масштабованої та стійкої мережевої архітектури. Впровадження принципів нульової довіри дає змогу організаціям підвищити рівень безпеки, мінімізувати поверхню атак та застосовувати детальні механізми контролю доступу як у локальних системах, так і в хмарних екосистемах. Оскільки кіберзагрози стають дедалі складнішими, прийняття Zero Trust для гібридних середовищ є не просто опцією, а критичною необхідністю для сучасних підприємств, які прагнуть довгострокової безпеки, відповідності нормативним вимогам та операційної гнучкості.

Постановка проблеми. Впровадження архітектури нульової довіри як моделі безпеки саме по собі є задачею складною та ресурсозатратною. Коли ж справа доходить до гібридних інфраструктур — то це ускладнює ситуацію додатковими новими викликами які не зустрічаються коли інфраструктура побудована на єдиній платформі. Однотипні та різнорідні середовища складно інтегровувати. Виникають такі проблеми як фрагментація ідентичності, збільшена поверхня атаки чи потреба дотримання єдиних регуляторних вимог.

Аналіз останніх досліджень і публікацій. У роботі Тахіра Башира (2024) підкреслюється, що ZTA замінює традиційні периметрові моделі безпеки динамічним підходом, заснованим на принципах мінімально необхідних привілеїв, постійної автентифікації та мікросегментації. У гібридних середовищах він вказує на такі виклики, як складність інтеграції, фінансові витрати та опір організаційним змінам. Водночас дослідження показує, що успішне впровадження ZTA значно зменшує кількість інцидентів безпеки та підвищує ефективність операцій [1].

Скотт Роуз (2021), у рамках стандарту NIST, пропонує фреймворк для планування впровадження ZTA. Він стверджує, що архітектура повинна адаптуватися до конкретних потреб організації, із залученням усіх зацікавлених сторін. Це особливо важливо у гібридних середовищах, де NIST Risk Management Framework допомагає приймати рішення на основі ризиків у хмарних і локальних компонентах [2].

Венката Чімакурті (2020) наголошує на труднощах впровадження ZTA в умовах мультихмарного середовища, зокрема на проблемах узгодження політик та розрізненості ідентичностей. Він рекомендує використання стандартизованих рівнів автентифікації та адаптивного контролю доступу для ефективної взаємодії між хмарними сервісами та локальними ресурсами [3].

Нарешті, О. Б. Придибайло (2024) описує практичні компоненти впровадження ZTA в гібридних середовищах — зокрема центри прийняття політик доступу, системи ідентифікації та логічну мікросегментацію. Він підкреслює необхідність контекстно-орієнтованої авторизації, щоб забезпечити безпечний доступ у розподілених мережах [4].

Узагальнюючи, література підтверджує, що успішне впровадження ZTA у гібридних середовищах вимагає координованого управління ідентичністю, інтелектуального моніторингу та єдиної системи політик доступу. Подальші дослідження можуть зосередитися на застосуванні ШІ, автоматизації та моделюванні загроз для оптимізації Zero Trust у масштабованих гібридних інфраструктурах.

Мета статті. Метою статті є огляд особливостей влаштування гібридних інфраструктур, визначення унікальних викликів при побудові безпекових моделей на кшталт «Архітектура нульової довіри» та висвітлення підходів та кроків впровадження такої безпекової моделі в відповідності до основних принципів нульової довіри та особливостей гібридних інфраструктур.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Розуміння гібридних мережевих архітектур. Гібридне мережеве середовище у корпоративному IT — це інтегрована мережева архітектура, що поєднує локальні дата-центри з хмарною інфраструктурою (AWS, Microsoft Azure, Google Cloud тощо). Така модель дозволяє компаніям зберігати критично важливі додатки та конфіденційні дані у локальних центрах обробки даних, використовуючи при цьому масштабованість, гнучкість і економічність хмарних сервісів [5].

Гібридна мережа забезпечує безперебійний зв'язок між локальними та хмарними додатками, дозволяючи підприємствам оптимізувати продуктивність, безпеку та розподіл ресурсів, а також гарантувати неперервність бізнесу [6].

Прикладом гібридного мережевого середовища в корпоративній інфраструктурі може бути Корпоративний дата-центр + інфраструктура AWS Cloud. Велике підприємство використовує локальний дата-центр для зберігання баз даних, легасі-додатків і критично важливих робочих навантажень, а хмарні ресурси AWS — для масштабованих веб-додатків, AI-аналітики та резервного зберігання. Наприклад фінансова компанія зберігає транзакційні дані клієнтів у локальному центрі для дотримання нормативних вимог, водночас використовуючи AWS для аналітики великих даних та AI-перевірки шахрайства [7].

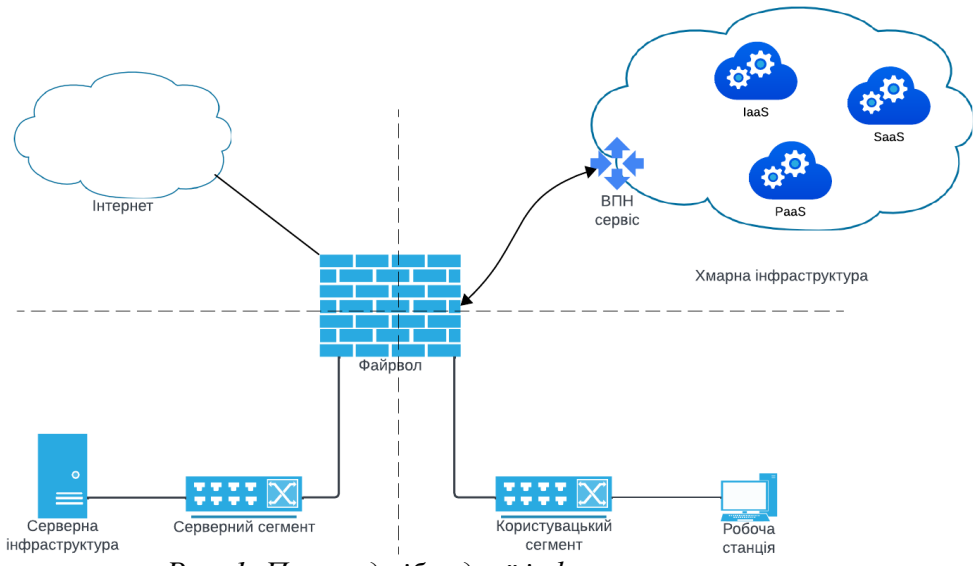

Рис. 1. Приклад гібридної інфраструктури

Іншим варіантом реалізації гібридної інфраструктури є впровадження Microsoft Azure Hybrid Cloud для корпоративного IT. В такому випадку Локальний Active Directory (AD) інтегрується з Azure Active Directory (AAD) для забезпечення єдиного входу (SSO), управління ідентичністю та безпечного доступу до хмарних сервісів. Прикладом може бути міжнародна компанія яка використовує локальний AD для автентифікації співробітників, а також інтегрує Microsoft 365, Azure Virtual Desktop і хмарне сховище для віддаленого доступу працівників [8].

Відмінності між традиційною та гібридною мережевими архітектурами. Гібридні мережеві архітектури поєднують специфіку локальних та хмарних інфраструктур що виливається в певні аспекти, які відрізняються як і від локальних інфраструктур так і від хмарних. Традиційні мережі забезпечують високий рівень контролю та безпеки, але обмежують масштабованість і гнучкість. Гібридна мережева архітектура дає змогу компаніям зменшити витрати, покращити продуктивність і підвищити безпеку, що робить її кращим вибором для сучасних підприємств. В порівняльній таблиці 1 зібрані характеристики монолітних і гібридних архітектур.

Основні принципи архітектури нульової довіри (ZTA). Архітектура нульової довіри (Zero Trust Architecture, ZTA) — це сучасна концепція кібербезпеки, яка усуває поняття довіри за замовчуванням у мережах.

ZTA базується на принципі «ніколи не довіряй, завжди перевіряй», тобто рішення щодо контролю доступу приймаються на основі строгих перевірок ідентичності, оцінки безпеки пристрою та аналізу контекстних ризиків [9]. Такий підхід гарантує динамічну адаптацію політик безпеки до змінних загроз.

Таблиця 1

Аспект	Традиційна мережева архітектура	Гібридна мережева архітектура
Інфраструктура	Повністю локальна інфраструктура з виділеними серверами, мережевим обладнанням та приватними дата-центрами.	Поєднання локальних датацентрів і хмарних сервісів (AWS, Azure, Google Cloud).
Масштабованість	Обмежена фізичними ресурсами; розширення потребує значних інвестицій.	Висока масштабованість; хмарні ресурси можна швидко збільшити або зменшити за потреби.
Гнучкість	Жорстка інфраструктура з фіксованим розподілом ресурсів.	Гнучка та адаптивна; робочі навантаження можна розподіляти між локальними та хмарними ресурсами.
Структура витрат	Високі капітальні витрати (CapEx) на обладнання, обслуговування та IT-персонал.	Знижені CapEx; модель операційних витрат (OpEx) для хмарних сервісів.
Безпека	Периметрова модель безпеки; покладається на брандмауери та VPN для захисту внутрішньої мережі.	Модель нульової довіри (Zero Trust); постійна автентифікація та контроль доступу між локальними та хмарними ресурсами.
Продуктивність і затримка	Низька затримка для локальних додатків, оскільки всі ресурси фізично підключені.	Продуктивність може змінюватися залежно від мережевого з'єднання, але CDN і граничні обчислення у хмарі зменшують затримку.
Надійність та відмовостійкість	Потребує окремих рішень для аварійного відновлення (DR) та резервного копіювання.	Вбудована висока доступність завдяки хмарним DR-рішенням та автоматичному перемиканню у разі збою.

Обслуговування та управління	Вимагає ручних оновлень, патчів і моніторингу з боку внутрішньої IT-команди.	Хмарні провайдери виконують автоматизовані оновлення, моніторинг і технічне обслуговування.
Швидкість розгортання	Повільне розгортання; налаштування нових серверів та мереж займає час.	Швидке розгортання; хмарні ресурси можна підключити за кілька хвилин.
Мережева взаємодія	Використовує традиційні LAN/WAN-архітектури, часто вимагає орендованих каналів зв'язку для віддаленого доступу.	Використовує SD-WAN, VPN, Direct Connect і хмарні пірингові з'єднання для інтеграції локальної та хмарної інфраструктури.
Сфери застосування	Найкращий варіант для компаній, які потребують повного контролю над інфраструктурою (наприклад, банки, урядові установи, легасі-додатки).	Оптимальний варіант для бізнесів, що потребують масштабованості, роботи на віддаленій основі та хмарних обчислень (наприклад, SaaS-компанії, електронна комерція).

Ядро архітектури нульової довіри це її основні принципи, окрім принципу «ніколи не довіряй, завжди перевіряй» до таких відносяться наступні:

Мінімально необхідні привілеї (Least Privilege Access). Принцип мінімально необхідних привілеїв забезпечує надання користувачам, програмам та пристроям мінімального рівня доступу, необхідного для виконання їхніх завдань. Це зменшує поверхню атаки та обмежує потенційні наслідки компрометації [10]. Дотримання принципу повинно здійснюватися в усіх механізмах контролю доступу, йдеться як про надання адміністративного доступу так при керуванні мережевим доступом засобами міжмережевих екранів, тощо. До традиційних засобів таких як конкретизація джерела та призначення мережевого трафіку можна додати використання певних технік та засобів для мінімізації необхідних привілеїв. До таких відносяться наступні:

- Гранульований контроль доступу: ZTA застосовує рольовий (RBAC) та атрибутний (ABAC) контроль доступу, щоб обмежити права користувачів.
- Доступ «just-in-time»: Тимчасові дозволи надаються лише на необхідний час для виконання завдання.
- Обмеження за пристроєм та локацією: Політики доступу враховують безпеку пристрою та фактори ризику, такі як геолокація.

Припущення про компрометацію (Assume Breach). Принцип «припущення про злам» виходить з того, що мережа вже може бути скомпрометована. Тому організація не лише захищається від зовнішніх атак, але й готується до потенційних загроз із середини [11]. Забезпечення стійкості інфраструктури до компрометації якоїсь її частини здійснюється через впровадження архітектурних заходів та інструментів які забезпечують локалізацію, виявлення та реакцію на майбутні інциденти.

- Мікросегментація: Розбиття мережі на ізольовані зони запобігає латеральному переміщенню атакуючих [12].
- Безперервний моніторинг: Використання поведінкової аналітики для виявлення аномальної активності.
- Готовність до інцидентів: Автоматизовані механізми реагування на загрози, такі як Endpoint Detection and Response (EDR), допомагають швидко ліквідувати компрометацію [13].

Чітка верифікація (Explicit Verification). Zero Trust вимагає постійної автентифікації та авторизації кожного запиту на доступ, навіть якщо користувач або пристрій вже були перевірені раніше [14]. Забезпечення верифікації доступу здійснюється файрволами нового покоління з використанням додаткової інформації яка

збирається і передається для прийняття рішення про надання мережевого доступу. Технології які можуть бути використані:

- Багатофакторна автентифікація (MFA): Використовує декілька факторів ідентифікації, таких як біометрія та апаратні токени.
- Перевірка стану пристрою: Перед наданням доступу система перевіряє відповідність пристрою стандартам безпеки.
- Адаптивний доступ: Політики доступу динамічно змінюються на основі поведінкового аналізу та рівня ризику [15].

Значення нульової довіри для захисту гібридних середовищ. Гібридні середовища, що поєднують локальні дата-центри та хмарні сервіси, створюють складні виклики для безпеки, оскільки включають різноманітні точки доступу та мультидоменні системи. ZTA є необхідною для їх захисту, оскільки:

- Зменшує ризики безпеки у хмарі: Гарантує безпеку AWS, Azure та Google Cloud через жорсткі механізми контролю доступу та шифрування [16].
- Забезпечує безпеку при віддаленій роботі: При використанні Bring Your Own Device (BYOD) підключень та гібридних робочих місць ZTA та ZTNA забезпечують контроль доступу та постійне підтвердження автентичності для таких пристроїв.
- Мінімізує ризики від інсайдерських атак: Завдяки припущенню про компрометацію ZTA запобігає несанкціонованому доступу навіть з боку внутрішніх користувачів [17].

Особливості гібридної мережевої архітектури в рамках концепції Zero Trust. Гібридні мережеві архітектури, що працюють у відповідності до принципів Zero Trust, успадковують механізми безпеки як від локальних (on-premises), так і від хмарних середовищ. Їхня суть та спосіб реалізації є схожими до таких які використовуються в не гібридних середовищах. Наприклад мікросегментація. ЇЇ безпекова цінність полягає в в розподілі мережі на ізольовані сегменти, що обмежує поширення атак та зменшує вплив компрометації [18]. Це працює як у хмарних, так і в локальних мережах. Спільними в різних інфраструктурах є потреба проведення безперервного моніторингу та поведінкової аналітики.

Більшість безпекових механізмів які застосовуються в побудові архітектури нульової довіри є спільними в локальних інфраструктурах, хмарних оточеннях а також їх гібридних поєднаннях. Проте в архітектурі нульової довіри зустрічаються унікальні виклики та рішення, які притаманні лише гібридним середовищам, до таких можна віднести наступні:

Інтеграція гібридного управління ідентифікацією та доступом (IAM). Оскільки гібридні середовища повинні автентифікувати користувачів у локальних та хмарних сервісах — це призводить до фрагментації ідентичності. Фрагментована ідентичність породжує потребу вирішення задачі інтеграції та уніфікації інструментів керування ідентичністю. Приклад вирішення — використання Federated Identity Management (FIM) для поєднання локального Active Directory (AD) з Azure AD, AWS IAM чи Google Cloud Identity [19]. Щоб забезпечити вимоги Zero Trust перевірки доцільно використовувати Єдиний вхід (SSO), що поширюється на всі гібридні ресурси.

Організація безпечного з'єднання між локальними та хмарними середовищами (SD-WAN & Direct Cloud Peering) є іншим прикладом унікального для гібридних інфраструктур безпекового механізму.

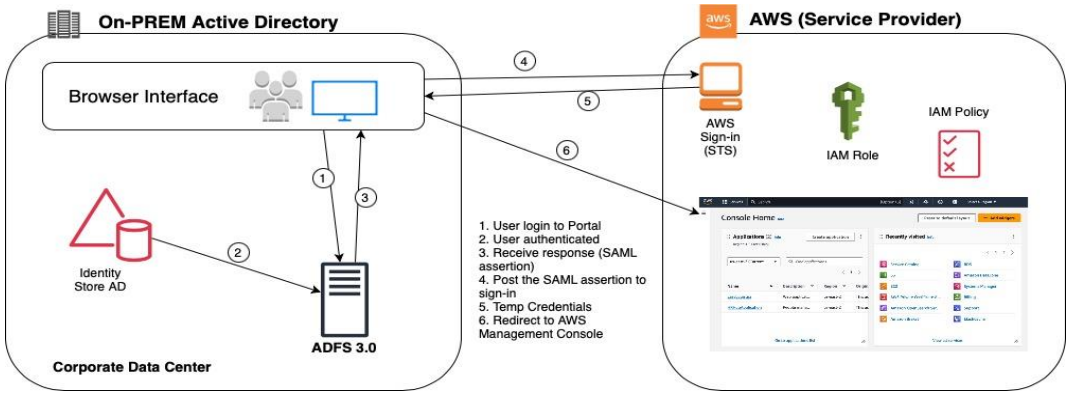

Рис. 2. Процес інтегрованої автентифікації ADFS

Традиційним моделям безпеки на основі VPN важко забезпечити динамічну безпеку в гібридних хмарних з'єднаннях. Недостатня гнучкість, сумісність та продуктивність не дозволяють використовувати їх ефективно між різними платформами. Потенційними рішеннями можуть бути інтеграція Software-Defined WAN (SD-WAN) для створення зашифрованих тунелів між локальною інфраструктурою та хмарними сервісами [20], а також приватні канали зв'язку (AWS Direct Connect, Azure ExpressRoute),які забезпечують низьку затримку та високу безпеку між локальними та хмарними системами.

Управління потоками даних і шифрування в гібридному середовищі. Завдання, яке як і попередні, потребує певних рішень що не зустрічаються за межами гібридних інфраструктур побудованих по архітектурі нульової довіри. Йдеться про гібридні мережі, які потребують уніфікованих стандартів шифрування під час передачі даних між локальною та хмарною інфраструктурою. В сучасних дослідженнях та рекомендаціях пропонується використання кінцевого шифрування (E2EE) за допомогою TLS 1.3 та AES-256 для всіх гібридних потоків даних [21]. Для контролю руху конфіденційних даних між локальним сховищем та хмарними сервісами рекомендується використовувати Cloud Access Security Brokers (CASB).

Виявлення загроз та автоматизоване реагування в гібридній мережі. Складність полягає в тому що гібридні архітектури збільшують атаку поверхню, що ускладнює централізований захист. Багато вже існуючих підходів та інструментів не достатньо гнучкі та не повністю покривають потребу аналітики та реагування в різних середовищах одночасно. Допомогти з вирішенням може оркестровка безпеки на основі штучного інтелекту Zero Trust, яка може виявляти та ізольовувати потенційні загрози в хмарі та локальній інфраструктурі в режимі реального часу [22]. Для інтеграції подій з хмарних та локальних ресурсів використовуються SIEM-системи. На їх базі можна будувати автоматизацію реагування на загрози

Потреба дотримання стандартів безпеки та політик у гібридних середовищах. Згідно регуляторних вимог — гібридні архітектури мають забезпечувати єдине дотримання нормативних вимог для локальних і хмарних середовищ. Таким чином спільних правил повинні дотримуватися різні інфраструктури побудовані на різних платформах. Допомогти з влаштуванням правил які повинні відповідати безпековим стандартам може Zero Trust Policy Automation. Використання Інструменту дозволить управління та підтримку уніфікованих правила для PCI-DSS, NIST, GDPR, HIPAA, та інших стандартів, дотримання яких може бути необхідним.

Аналіз викликів впровадження архітектури нульової довіри (Zero Trust) у гібридній мережевій інфраструктурі. Впровадження та експлуатація архітектури

нульової довіри (ZTA) у гібридних IT-інфраструктурах, які об'єднують хмарні служби та локальні ресурси, створює значні проблеми, пов'язані з архітектурою мережі та керуванням доступом до мережі. Ці проблеми виникають насамперед через складність і різноманітність гібридних середовищ, які вимагають комплексних стратегій для забезпечення ефективної реалізації безпеки.

Однією з основних архітектурних проблем є невід'ємна складність гібридних мережевих топологій. Традиційні локальні інфраструктури часто є жорсткими та статичними, що різко контрастує з динамічною, дуже гнучкою природою хмарних платформ. Ця невідповідність створює суттєві перешкоди для розробки уніфікованих узгоджених проектів мережі та застосування узгоджених політик безпеки в обох середовищах. Крім того, застарілій інфраструктурі часто бракує вбудованої сумісності з сучасними принципами нульової довіри, що вимагає масштабних оновлень або навіть замін для підтримки таких функцій, як мікросегментація та динамічне застосування політики.

Сама по собі мікросегментація, основоположний принцип ZTA, створює ще одну помітну складність. Створення точних мікросегментів у змішаному хмарному та локальному середовищах потребує детального планування та розширених технічних можливостей. Різноманітність і розподілений характер ресурсів ще більше ускладнюють зусилля щодо підтримки чітких меж сегментації та послідовного застосування політики. Ця складність може вплинути на продуктивність, наприклад збільшити затримку, через постійний моніторинг і перевірку потоків мережевого трафіку в реальному часі, що може негативно вплинути на взаємодію з користувачем і швидкість реагування додатків.

Важливою передумовою для успішного ZTA є досягнення уніфікованої видимості всіх мережевих ресурсів. Гібридні середовища зазвичай страждають від фрагментованих систем моніторингу та ізольованих рішень для журналювання, що ускладнює спроби отримати узгоджене розуміння мережевої діяльності та загроз. Без інтегрованої видимості стає значно складніше виявляти потенційні інциденти безпеки або аномальну поведінку та швидко реагувати на них.

Що стосується керування доступом до мережі, централізоване керування ідентифікацією та доступом (IAM) є особливо проблематичним у гібридних налаштуваннях. Підтримка узгоджених уніфікованих політик IAM стає складною, коли ідентифікаційні дані та елементи керування доступом охоплюють локальні служби Active Directory, кілька хмарних постачальників IAM і різні сторонні рішення. Ця складність часто призводить до фрагментації політики, неузгодженості та потенційної вразливості безпеки, оскільки управління автентифікацією, авторизацією та ролями користувачів на різнорідних платформах стає все більш вимогливим.

Безперервна перевірка особи — наріжний камінь підходу Zero Trust — також створює значні операційні проблеми. Впровадження постійної автентифікації та перевірки довіри в режимі реального часу потребує складних технічних інструментів і може спричинити значні витрати ресурсів, особливо коли задіяні застарілі системи. Крім того, постійною проблемою залишається балансування суворих заходів безпеки, таких як постійна автентифікація та детальний контроль доступу, із зручністю та продуктивністю для користувачів.

Ще більше ускладнює питання сумісність між рішеннями постачальників. Організації часто покладаються на продукти від багатьох постачальників, включаючи брандмауери, рішення Zero Trust Network Access (ZTNA), брокери безпеки доступу до хмари (CASB) і програмно-визначені глобальні мережі (SD-WAN). Інтеграція цих різноманітних рішень у послідовну стратегію Zero Trust вимагає ретельного вибору постачальників і значних зусиль щодо інтеграції, щоб уникнути створення прогалин або невідповідностей у політиках безпеки.

Відповідність і нормативні вимоги додають ще один рівень складності. Послідовне дотримання суворих нормативних вимог і стандартів відповідності в хмарних і локальних середовищах потребує прискіпливої уваги до розробки політики, її застосування та готовності до аудиту.

Нарешті, не можна недооцінювати людський фактор. Перехід до нульової довіри від традиційної безпеки на основі периметра означає фундаментальний культурний зсув. Організаційний опір, прогалини в навичках серед IT-персоналу та потреба в інтенсивному навчанні й освіті ще більше ускладнюють успішне впровадження та роботу ZTA у гібридних мережевих середовищах. Таким чином, ефективне впровадження потребує не лише технічних рішень, але й значних інвестицій в організаційне узгодження, комунікацію та постійне навчання.

Вирішення цих взаємопов'язаних проблем потребує продуманого планування, ретельного проектування архітектури, стратегічного вибору постачальників і постійної міжфункціональної співпраці для забезпечення успішного впровадження та стабільної роботи архітектури нульової довіри в гібридних IT-інфраструктурах.

Реалізація архітектури нульової довіри (Zero Trust Architecture, ZTA) у гібридних мережах, що поєднують локальні дата-центри та хмарні сервіси, створює унікальні виклики. Причиною здебільшого є підвищене різноманіття елементів інфраструктур різного походження а також потреба їх інтеграції та спільного керування з дотриманням принципів нульової довіри. Нижче наведено ключові проблеми та ефективні рішення, підтверджені дослідженнями.

Таким чином, впровадження Zero Trust у гібридних середовищах є складним процесом, але правильне управління ідентичностями, шифрування, SD-WAN та AI-контроль допоможуть знизити ризики та покращити безпеку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Архітектурні компоненти та технології. Побудова архітектури нульової довіри (Zero Trust Architecture, ZTA) у гібридних середовищах, які охоплюють локальну та хмарну інфраструктуру, включає низку важливих архітектурних компонентів і технологій, що забезпечують безпеку та ефективність роботи.

Управління ідентичностями та доступом (IAM): IAM є основним компонентом ZTA, який забезпечує перевірку ідентичності та доступ на основі політик. Такі технології, як єдиний вхід (SSO), багатофакторна автентифікація (MFA) та федерація ідентичностей (наприклад, SAML, OAuth, OpenID Connect), гарантують безпечний, орієнтований на ідентичність контроль доступу у гібридних середовищах. Централізовані постачальники ідентичностей (IdP), такі як Azure Active Directory, Okta або Ping Identity, забезпечують послідовне управління ідентичностями та безшовну інтеграцію.

Точка застосування політик (PEP): PEP динамічно застосовують рішення щодо доступу, визначені двигунами політик. Це включає мережеві міжмережеві екрани, шлюзи, рішення програмно-визначеного периметра (SDP) та технології мікросегментації. Рішення, такі як VMware NSX, Cisco ACI, Palo Alto Prisma, AWS Security Groups, Azure Network Security Groups або Cloudflare Access контролюють доступ до ресурсів як у локальному, так і у хмарному середовищах.

Точка прийняття рішень за політиками (PDP**)**: PDP оцінює запити на доступ на основі ідентичності, контексту, чутливості ресурсів та попередньо визначених політик безпеки. До технологій, що реалізують PDP, належать Zero Trust двигуни політик

(наприклад, OPA – Open Policy Agent), централізовані платформи управління політиками та проксі, що враховують ідентичність (IAP), від основних хмарних постачальників.

Мікросегментація та ізоляція мережі: Технології детальної ізоляції мережі, такі як VMware NSX, Cisco ACI або хмарні сервіси сегментації мереж (AWS VPC, Azure VNets, GCP VPC), обмежують горизонтальне переміщення і зменшують площу атак. Мікросегментація доповнює модель ZTA, забезпечуючи тонкий, контекстно-орієнтований контроль комунікацій між ресурсами.

Безперервний моніторинг та видимість: Інструменти безперервного моніторингу та видимості, включаючи системи управління інформацією та подіями безпеки (SIEM), такі як Splunk, Azure Sentinel, Elastic Stack, інструменти управління станом безпеки хмарної інфраструктури (CSPM) і платформи виявлення та реагування на кінцевих точках (EDR/XDR), забезпечують виявлення загроз у режимі реального часу, аналітику та аудит, критичні для підтримки довіри.

Безпечне підключення та шифрування: Безпечні зашифровані комунікації через VPN (IPsec, WireGuard), TLS/SSL та спеціалізовані служби хмарного підключення (AWS Direct Connect, Azure ExpressRoute, Google Cloud Interconnect) гарантують конфіденційність та цілісність обміну даними між локальною та хмарною інфраструктурою.

Автоматизація та оркестрація: Інфраструктура-як-код (IaC) та інструменти автоматизації, такі як Terraform, Ansible, Chef, Puppet або Kubernetes, сприяють послідовному розгортанню, застосуванню та масштабуванню політик Zero Trust у гібридній інфраструктурі.

Разом ці інтегровані компоненти та технології створюють стек, орієнтований на ідентичність та архітектуру безпеки, яка динамічно застосовує принципи Zero Trust у складних гібридних інфраструктурах. Їх ефективність залежить не лише від окремих функціональних можливостей, а й від здатності працювати як єдина система з єдиною політичною логікою, яка базується на ідентичності, контексті доступу та постійному аналізі ризиків.

План міграції до архітектури нульової довіри (Zero Trust) для гібридних мережевих середовищ (локальний ЦОД + хмарний ЦОД). Беручи до уваги досліджені вимоги побудови архітектури нульової довіри та особливості гібридних інфраструктур запропоновано до використання наступний план міграції що покриває необхідні етапи та дозволяє побудувати ефективну безпекову модель.

Рис. 3 План міграції гібридної інфраструктури до АНД

Етап 1: Оцінка та планування

На цьому етапі необхідно провести повну оцінку наявної IT-інфраструктури, зокрема апаратних і програмних ресурсів, ідентичностей, застосунків, а також потоків даних як у локальному, так і в хмарному середовищах. Важливо визначити поточний стан кібербезпеки, виявити наявні прогалини та уточнити вимоги комплаєнсу (відповідності регуляторним стандартам).

Наступним кроком є формулювання чітких цілей щодо безпеки, які відповідають бізнес-завданням і принципам архітектури Zero Trust. Важливо сформувати покрокову дорожню карту, визначивши пріоритетні ресурси та застосунки з найвищими ризиками.

Також необхідно забезпечити підтримку керівництва та узгодити план дій між підрозділами IT, безпеки й комплаєнсу. Це передбачає регулярну комунікацію щодо очікуваних переваг та необхідних змін культури організації.

Етап 2: Розробка архітектури та вибір рішень

На другому етапі слід створити еталонну архітектуру Zero Trust, яка забезпечуватиме єдині підходи до кібербезпеки у гібридному середовищі. Вона має враховувати інтеграцію локальних і хмарних ресурсів, включати централізоване управління ідентичністю (IAM), мікросегментацію та політики мережевого доступу.

Далі необхідно оцінити наявні на ринку рішення, такі як Zero Trust Network Access (ZTNA), брокери захисту доступу до хмарних сервісів (CASB), рішення IAM та інструменти мікросегментації. Важливо протестувати ці рішення у рамках пілотних проєктів (Proof of Concept), перевіряючи їх відповідність вимогам до безпеки, продуктивності та сумісності з інфраструктурою.

Етап 3: Впровадження централізованого управління ідентичностями (IAM)

Цей етап передбачає створення єдиної системи IAM, яка інтегрує локальні сервіси (наприклад, Active Directory) із хмарними рішеннями (Azure AD, Okta, AWS IAM). Важливо запровадити багатофакторну автентифікацію (MFA), єдиний вхід (SSO) та умовний доступ (Conditional Access).

Використання інструментів для безперервної верифікації ідентичностей і адаптивної автентифікації допоможе реалізувати принцип постійного контролю доступу на основі аналізу ризиків поведінки користувачів. Також необхідно регулярно проводити аудит політик доступу, уникаючи фрагментації та забезпечуючи актуальність.

Етап 4: Мікросегментація та контроль доступу на мережевому рівні.

Провести поступову мікросегментацію мережі, починаючи з найкритичніших застосунків та сервісів. Це дозволить створити ізольовані сегменти мережі, керуючи ними за допомогою програмно-визначених мереж (SDN).Традиційні периметрові правила фаєрволів варто поступово замінити політиками доступу на рівні застосунків та сервісів, забезпечуючи динамічний контроль доступу до ресурсів. В той час як управління ідентичністю та моніторинг важливо зробити єдиними, контроль доступу на мережевому рівні пропонується зробити розподіленим, такий підхід дасть декілька переваг, а саме:

- зменшення системного ризику: порушення в одному сегменті чи середовищі з меншою ймовірністю негайно вплине на інші, забезпечуючи стійкість.
- підвищена відмовостійкість і відмовостійкість: розподілені системи можуть ефективніше ізолювати та стримувати загрози, запобігаючи масовим збоям.
- поглиблений захист: розподілена архітектура за своєю суттю відповідає принципам багаторівневої безпеки.
- спрощення та здешевлення впровадження ZTA через відсутність потреби розробки інтеграційних рішень.

Етап 5: Єдина система моніторингу й аналітики безпеки

На цьому етапі створюється централізована система моніторингу, що охоплює і хмарну, і локальну інфраструктури. Слід інтегрувати системи логування, а також рішення класу SIEM (моніторинг подій безпеки), SOAR (автоматизація реагування на інциденти) та аналітики поведінки користувачів (UBA). Крім того, необхідно запровадити та постійно вдосконалювати процедури реагування на інциденти, регулярно проводячи навчальні симуляції для команди.

Етап 6: Повномасштабне розгортання й оптимізація.

Поступово масштабувати впровадження Zero Trust-архітектури на інші ресурси, сервіси та користувачів згідно з початково розробленим планом. Важливо постійно аналізувати ефективність запроваджених політик, вдосконалюючи їх відповідно до змін середовища та загроз. Регулярно переглядати й оновлювати архітектуру, враховуючи нові технології, нормативні вимоги та бізнес-потреби.

Етап 7: Організаційна підтримка й навчання персоналу

Не менш важливим є проведення регулярних тренінгів для IT-персоналу та користувачів, що допоможе створити розуміння принципів Zero Trust, навчить застосовувати їх на практиці.

Потрібно організовувати систематичну інформаційну роботу, спрямовану на зміни корпоративної культури щодо безпеки, а також постійно підтримувати міжфункціональну співпрацю.

Реалізація з використанням запропонованих етапів дозволить організаціям структуровано перейти до моделі Zero Trust, забезпечити послідовне підвищення кібербезпеки та досягти необхідної гнучкості й стійкості своєї гібридної IT-інфраструктури.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Реалізація архітектури нульової довіри (Zero Trust, ZTA) у гібридних мережевих середовищах, що поєднують локальну інфраструктуру та хмарні сервіси, суттєво відрізняється від класичних сценаріїв використання лише локальної або виключно хмарної інфраструктури. Гібридні рішення характеризуються значно вищою складністю мережевої архітектури, яка виникає через необхідність поєднання застарілих, жорстких систем із гнучкими та динамічними хмарними ресурсами. В таких умовах набагато складніше забезпечити єдину видимість, централізоване управління ідентичностями та послідовний контроль доступу. На відміну від класичних архітектур, у гібридних мережах необхідна ретельна стратегія мікросегментації, що забезпечує надійний захист комунікацій між різнорідними середовищами. Крім того, безперервна перевірка доступу і моніторинг у режимі реального часу потребують значно потужніших та інтегрованіших інструментів, ніж при використанні однорідних середовищ. Додаткові складнощі виникають через необхідність забезпечення сумісності рішень різних виробників та дотримання регуляторних вимог, специфічних для різних платформ.

Також для гібридних середовищ характерні більші витрати на експлуатацію, ризики виникнення затримок у роботі застосунків і складніше балансування між високим рівнем безпеки та продуктивністю користувачів. Таким чином, успішне впровадження ZTA у гібридних інфраструктурах значною мірою залежить від ретельного архітектурного планування, стратегічного вибору сумісних між собою технологій та

ефективної організаційної підтримки, що робить його більш ресурсозатратним порівняно з класичними сценаріями.

Перспективами подальших досліджень можуть бути дослідження проблематики контролю мережевого доступу в архітектурі нульової довіри та пошук шляхів до її вирішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies*. https://doi.org/10.32996/jcsts.2024.6.4.8
2. Rose, S. (2021). *Planning for a Zero Trust Architecture*. https://doi.org/10.6028/nist.cswp.08042021-draft
3. Chimakurthi, V. (2020). The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment. *ABC Journal of Advanced Research*. https://doi.org/10.18034/abcjar.v9i2.608
4. Prydybaylo, O. (2024). Zero trust architecture logical components and implementation approaches. *Connectivity*. https://doi.org/10.31673/2412-9070.2024.030711
5. Teykhrib, A. (2016). Data transmission in Hybrid Distributed Environment. *International Journal of Electrical and Computer Engineering, 6*, 2989–2993. https://doi.org/10.11591/ijece.v6i6.12129
6. Liakopoulos, A., Hanemann, A., & Sevasti, A. (2007). Point-to-Point Services in Hybrid Networks: Technologies and Performance Metrics. *International Conference on Networking and Services (ICNS '07)*. https://doi.org/10.1109/ICNS.2007.96
7. Teykhrib, A. (2016). Data transmission in Hybrid Distributed Environment. *International Journal of Electrical and Computer Engineering, 6*, 2989–2993. https://doi.org/10.11591/ijece.v6i6.12129
8. Tchepnda, C., Moustafa, H., & Labiod, H. (2006). Hybrid Wireless Networks: Applications, Architectures and New Perspectives. *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 3*, 848–853. https://doi.org/10.1109/SAHCN.2006.288571
9. Hasan, M. (2024). *Enhancing Enterprise Security with Zero Trust Architecture.* http://dx.doi.org/10.48550/arXiv.2410.18291
10. Singh, J. (2024). Zenith Armor : Advancing Security with Zero Trust Measures. *Interantional journal of scientific research in engineering and management.* https://doi.org/10.55041/ijsrem31326
11. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies.* https://doi.org/10.32996/jcsts.2024.6.4.8
12. Prydybailo, O. (2022). Zero trust architecture: the basics organization principles. *Connectivity.* https://doi.org/10.31673/2412-9070.2022.051620
13. Lund, B., Lee, T., Wang, Z., Wang, T., & Mannuru, N. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia.* https://doi.org/10.3390/encyclopedia4040099
14. Bansal, P. (2024). Zero Trust Security: Is it Optional?. *International Journal of Innovative Science and Research Technology (IJISRT).* https://doi.org/10.38124/ijisrt/ijisrt24sep1521
15. Hussain, M., Pal, S., Jadidi, Z., Foo, E., & Kanhere, S. (2024). Federated Zero Trust Architecture using Artificial Intelligence. *IEEE Wireless Communications, 31,* 30–35. https://doi.org/10.1109/MWC.001.2300405
16. Nutalapati, P. (2023). Zero Trust Architecture in Cloud-Based Fintech Applications. *Journal of Artificial Intelligence & Cloud Computing.* https://doi.org/10.47363/jaicc/2023(2)e152
17. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. *Secur. Commun. Networks, 2021,* 9947347:1–9947347:10. https://doi.org/10.1155/2021/9947347
18. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel, Switzerland), 24.* https://doi.org/10.3390/s24041328
19. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies.* https://doi.org/10.32996/jcsts.2024.6.4.8
20. Sarkar, S., Choudhary, G., Shandilya, S., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability.* https://doi.org/10.3390/su141811213
21. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel, Switzerland), 24.* https://doi.org/10.3390/s24041328

22. Khan, M. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews.* https://doi.org/10.30574/wjarr.2023.19.3.1785

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

Roman Syrotynskyi
Postgraduate student, assistant at the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0002-6280-3290
roman.m.syrotynskyi@lpnu.ua

Ivan Tyshyk
PhD, Associate Professor at the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

SPECIFICITY OF BUILDING A ZERO TRUST ARCHITECTURE IN HYBRID INFRASTRUCTURES

Abstract. The popularity of hybrid infrastructures is growing rapidly, as they allow you to combine the advantages of local computing resources — control, cost-effectiveness, compliance with regulatory requirements — with the scalability, flexibility and high availability of cloud technologies. In such conditions, there is a need to provide a unified approach to information security that can cover both types of environments. Zero Trust Architecture (ZTA) is considered a modern and effective model that allows you to achieve a high level of access control, minimize the risks of security breaches and ensure the protection of critical resources regardless of their location. However, building ZTA in hybrid environments is accompanied by a number of challenges due to the heterogeneity of technologies, the lack of unified management tools, varying degrees of control over infrastructure components and the complexity of implementing unified authentication, authorization and monitoring policies. The article examines the key differences between traditional (local) and hybrid infrastructures, in particular from the point of view of building a zero-trust architecture. The specifics of integrating elements of local and cloud environments, which often have different mechanisms for user identification, session management, event logging, and access policy enforcement, are analyzed. A number of important architectural components and technologies are proposed that form the stack of components necessary for implementing ZTA in a hybrid environment. An analysis of the challenges of implementing a zero-trust architecture in a hybrid network infrastructure is also described, in particular the complexity of hybrid network topologies, the complexity of microsegmentation, visibility unification, centralized access management (IAM), and others. Taking into account the identified features, a phased plan for migrating hybrid infrastructures to a zero-trust architecture has been formed, which involves assessment and planning, architecture development, decision selection, and other important steps.

Keywords: Zero Trust Architecture; hybrid environment; local area network; cloud infrastructure; integration; compliance; microsegmentation; identity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies*. https://doi.org/10.32996/jcsts.2024.6.4.8
2. Rose, S. (2021). *Planning for a Zero Trust Architecture*. https://doi.org/10.6028/nist.cswp.08042021-draft
3. Chimakurthi, V. (2020). The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment. *ABC Journal of Advanced Research*. https://doi.org/10.18034/abcjar.v9i2.608
4. Prydybaylo, O. (2024). Zero trust architecture logical components and implementation approaches. *Connectivity*. https://doi.org/10.31673/2412-9070.2024.030711
5. Teykhrib, A. (2016). Data transmission in Hybrid Distributed Environment. *International Journal of Electrical and Computer Engineering, 6*, 2989–2993. https://doi.org/10.11591/ijece.v6i6.12129
6. Liakopoulos, A., Hanemann, A., & Sevasti, A. (2007). Point-to-Point Services in Hybrid Networks: Technologies and Performance Metrics. *International Conference on Networking and Services (ICNS '07)*. https://doi.org/10.1109/ICNS.2007.96

7. Teykhrib, A. (2016). Data transmission in Hybrid Distributed Environment. *International Journal of Electrical and Computer Engineering, 6*, 2989–2993. https://doi.org/10.11591/ijece.v6i6.12129
8. Tchepnda, C., Moustafa, H., & Labiod, H. (2006). Hybrid Wireless Networks: Applications, Architectures and New Perspectives. *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 3*, 848–853. https://doi.org/10.1109/SAHCN.2006.288571
9. Hasan, M. (2024). *Enhancing Enterprise Security with Zero Trust Architecture.* http://dx.doi.org/10.48550/arXiv.2410.18291
10. Singh, J. (2024). Zenith Armor : Advancing Security with Zero Trust Measures. *Interantional journal of scientific research in engineering and management.* https://doi.org/10.55041/ijsrem31326
11. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies.* https://doi.org/10.32996/jcsts.2024.6.4.8
12. Prydybailo, O. (2022). Zero trust architecture: the basics organization principles. *Connectivity.* https://doi.org/10.31673/2412-9070.2022.051620
13. Lund, B., Lee, T., Wang, Z., Wang, T., & Mannuru, N. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia.* https://doi.org/10.3390/encyclopedia4040099
14. Bansal, P. (2024). Zero Trust Security: Is it Optional?. *International Journal of Innovative Science and Research Technology (IJISRT).* https://doi.org/10.38124/ijisrt/ijisrt24sep1521
15. Hussain, M., Pal, S., Jadidi, Z., Foo, E., & Kanhere, S. (2024). Federated Zero Trust Architecture using Artificial Intelligence. *IEEE Wireless Communications, 31,* 30–35. https://doi.org/10.1109/MWC.001.2300405
16. Nutalapati, P. (2023). Zero Trust Architecture in Cloud-Based Fintech Applications. *Journal of Artificial Intelligence & Cloud Computing.* https://doi.org/10.47363/jaicc/2023(2)e152
17. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. *Secur. Commun. Networks, 2021,* 9947347:1–9947347:10. https://doi.org/10.1155/2021/9947347
18. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel, Switzerland), 24.* https://doi.org/10.3390/s24041328
19. Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. *Journal of Computer Science and Technology Studies.* https://doi.org/10.32996/jcsts.2024.6.4.8
20. Sarkar, S., Choudhary, G., Shandilya, S., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. *Sustainability.* https://doi.org/10.3390/su141811213
21. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel, Switzerland), 24.* https://doi.org/10.3390/s24041328
22. Khan, M. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews.* https://doi.org/10.30574/wjarr.2023.19.3.1785