УДК 004.056.5:004.75

https://doi.org/10.52058/2786-6025-2025-11(52)-1844-1863

Батаєв Сергій Вікторович аспірант Ворицького університету, керівник технологічного відділу, компанія ЕЛЕКС, м. Львів, https://orcid.org/0009-0009-9564-9403

Федорчук Анна Леонідівна кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук та інформаційних технологій, Житомирський державний університет імені Івана Франка, м. Житомир, https://orcid.org/0000-0001-8227-3210

Багнюк Ольга Миколаївна старший викладач кафедри обчислювальної техніки, Національний університет водного господарства та природокористування, м. Рівне, https://orcid.org/0000-0002-7898-2337

ZERO TRUST У ВЕБАРХІТЕКТУРІ: НОВІ ПІДХОДИ ДО БЕЗПЕКИ В УМОВАХ РОЗПОДІЛЕНИХ СИСТЕМ

Анотація. У роботі проведено комплексне дослідження проблеми забезпечення безпеки веб-архітектур у розподілених системах та обґрунтовано доцільність переходу до моделі з архітектурою нульової довіри (АНД).

Авторами з'ясовано, що традиційні моделі захисту втрачають ефективність у динамічному середовищі, де користувачі, сервіси та дані розподілені між різними доменами й хмарними платформами. Проаналізовано сучасні загрози для вебархітектур, серед яких домінують компрометація облікових даних, уразливості API, бічна рухливість атак і внутрішні загрози, що зумовлюють потребу у новій парадигмі довіри.

У ході дослідження проведено порівняльний аналіз традиційних і Zero Trust (ZT) моделей безпеки за критеріями масштабованості, контролю доступу, рівня адаптивності, вразливості до внутрішніх атак і здатності до проактивного моніторингу. Встановлено, що концепція ZT забезпечує динамічний контекстний контроль доступу, мінімізацію привілеїв і підвищену стійкість до інцидентів безпеки. Детально розглянуто структурні компоненти АНД та наведено узагальнений алгоритм функціонування АНД, що відображає повний цикл оцінювання довіри: автентифікацію запиту, контекстну оцінку ризику, формування політик доступу та безперервний моніторинг. Проведено аналіз особливостей реалізації ZT у хмарних, мікросервісних і контейнеризованих середовищах, де доведено ефективність мікросегментації, поведінкової

аналітики (UEBA) та багатофакторної автентифікації для зниження ризику горизонтального поширення атак.

Отримані результати підтверджують, що впровадження ZTA дозволяє створити адаптивну, гнучку й масштабовану модель безпеки, у якій довіра визначається динамічно, а кожна взаємодія в системі контролюється у режимі реального часу. Практична значущість роботи полягає у формуванні методичних засад проектування безпечних вебархітектур, здатних відповідати вимогам міжнародних стандартів кібербезпеки (NIST SP 800-207, ISO/IEC 27001) і забезпечувати надійний захист розподілених середовищ нового покоління.

Ключові слова: архітектура нульової довіри, веб-архітектура, розподілені системи, мікросегментація, кібербезпека, політики доступу, підходи безпеки.

Bataiev Sergii Postgraduate Student of The University of Warwick, Head of Technology Department, ELEKS inc., Lviv, https://orcid.org/0009-0009-9564-9403

Fedorchuk Anna Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Computer Science and Information Technology, Zhytomyr Ivan Franko State University, Zhytomyr, https://orcid.org/0000-0001-8227-3210

Bagnyuk Olga Senior Lecturer at the Department of Computer Engineering, National University of Water Management and Nature Resources Use, Rivne, https://orcid.org/0000-0002-7898-2337

ZERO TRUST IN WEB ARCHITECTURE: NEW APPROACHES TO SECURITY IN DISTRIBUTED SYSTEMS

Abstract. The paper presents a comprehensive study of the problem of ensuring the security of web architectures in distributed systems and justifies the feasibility of transitioning to a Zero Trust Architecture (ZTA) model. The authors have found that traditional security models are losing their effectiveness in a dynamic environment where users, services, and data are distributed across different domains and cloud platforms. It analyzes current threats to web architectures, among which account compromise, API vulnerabilities, lateral movement attacks, and internal threats dominate, necessitating a new trust paradigm.

The study conducted a comparative analysis of traditional and Zero Trust (ZT) security models based on criteria such as scalability, access control, adaptability, vulnerability to internal attacks, and proactive monitoring capabilities. It was found that the ZT concept provides dynamic contextual access control, privilege

minimization, and increased resilience to security incidents. The structural components of the ZTA are examined in detail, and a generalized algorithm for the functioning of the ZTA is presented, reflecting the full cycle of trust assessment: request authentication, contextual risk assessment, access policy formation, and continuous monitoring. An analysis of the features of ZT implementation in cloud, microservice, and containerized environments is conducted, proving the effectiveness of microsegmentation, behavioral analytics (UEBA), and multi-factor authentication in reducing the risk of horizontal attack propagation.

The results confirm that the implementation of ZTA allows the creation of an adaptive, flexible, and scalable security model in which trust is determined dynamically and each interaction in the system is controlled in real time. The practical significance of the work lies in the formation of methodological principles for designing secure web architectures that are capable of meeting the requirements of international cybersecurity standards (NIST SP 800-207, ISO/IEC 27001) and providing reliable protection for next-generation distributed environments.

Keywords: zero trust architecture, web architecture, distributed systems, microsegmentation, cybersecurity, access policies, security approaches.

Постановка проблеми. Сучасні веб-системи дедалі частіше функціонують у розподіленому середовищі, де дані, сервіси та користувачі розміщені в різних географічних точках і взаємодіють через глобальні мережеві інфраструктури. Така модель характерна для хмарних і мікросервісних архітектур, контейнеризованих застосунків та корпоративних екосистем, шо інтегрують численні API, бази даних і модулі. Розподілений характер цих систем суттєво підвищує ефективність і масштабованість, однак водночас створює новий спектр ризиків для кібербезпеки. Класичні моделі довіри, які побудовані на фіксованих мережевих периметрах («внутрішнє – безпечне, зовнішнє – небезпечне») втрачають актуальність у динамічному середовищі, де користувачі, сервіси та дані постійно переміщуються між різними доменами і платформами [1-2].

У таких умовах суттєво зростає кількість атак через API, компрометації облікових даних, зловживань правами доступу та внутрішніх загроз. Особливо небезпечною є так звана «бічна рухливість», коли зловмисник отримавши доступ до одного сервісу або контейнера може безперешкодно переміщуватися між іншими компонентами системи. Традиційні засоби кіберзахисту (фаєрволи, антивірусні системи, багатофакторна автентифікація) не забезпечують належного рівня контролю в умовах постійних змін архітектури, появи нових вузлів і сервісів.

Відповіддю на ці виклики стала концепція Zero Trust Architecture або архітектура «нульової довіри» (АНД) – модель безпеки, що ґрунтується на

принципі «ніколи не довіряй, завжди перевіряй». На відміну від традиційного підходу, АНД передбачає, що жоден користувач, пристрій або сервіс не може вважатися надійним за замовчуванням, оскільки кожен запит підлягає автентифікації, авторизації і перевірці у контексті поточного ризику.

Для веб-архітектури це означає необхідність постійного контролю взаємодій між усіма компонентами системи, незалежно від їхнього розташування у мережі [3].

Впровадження принципів АНД у веб-архітектурі розподілених систем потребує глибокого переосмислення традиційних моделей доступу, моніторингу, управління та обміну даними. Основними складниками стають управління ідентифікацією та доступом – Identity and Access Management (IAM), мікросегментація, контекстна авторизація, багатофакторна автентифікація – Multi-Factor Authentication (MFA), постійний моніторинг активності користувачів і сервісів, а також наскрізне шифрування на всіх рівнях взаємодії. Однак практична реалізація цих принципів супроводжується низкою проблем, зокрема, підвищеним навантаженням на систему, можливими затримками у відповіді, а також складністю інтеграції в існуючі веб-платформи, які проєктувалися за класичною моделлю безпеки [3-4].

Тому сутність проблеми полягає в необхідності розроблення нових архітектурних рішень і підходів до побудови веб-архітектур, що дозволять ефективно інтегрувати принципи Zero Trust (ZT) без втрати продуктивності, зручності використання та гнучкості системи. Це вимагає формування узгоджених політик доступу, оптимізації процесів автентифікації й авторизації, а також створення адаптивних механізмів контролю безпеки, здатних протидіяти як зовнішнім, так і внутрішнім загрозам у сучасних розподілених середовищах.

Аналіз останніх досліджень та публікацій. Проблематика забезпечення безпеки веб-архітектури набуває особливої актуальності в умовах динамічного розвитку хмарних технологій, мікросервісних систем та розподілених середовищ, шо привертає значну увагу сучасних дослідників. У наукових працях останніх років спостерігається зростання інтересу до концепції АНД, що передбачає відмову від традиційних моделей захисту (які базуються на концепції «периметра») до переходу архітектури з принципом «ніколи не довіряй, завжди перевіряй» з динамічним контролем доступу, автентифікацією на основі контексту та постійним моніторингом користувацької активності. Такий підхід розглядається як основа для побудови стійких веб-систем, здатних протидіяти сучасним кіберзагрозам.

У дослідженнях [5-6] акцентується увага на теоретичних засадах моделі АНД. Авторами визначено ключові принципи (мікросегментацію, багаторівневу автентифікацію, безперервний моніторинг і контекстно-залежний

контроль доступу) та доведено, що впровадження цих принципів знижує ризики як внутрішніх, так і зовнішніх атак. Водночас з цим не до кінця вирішеним залишається питання масштабування АНД у великих розподілених архітектурах, де кількість вузлів і запитів ускладнює централізоване управління політиками доступу.

У наукових працях [7-8] представлено архітектурні рішення щодо реалізації АНД у розподілених середовищах, де авторами запропоновано моделі управління ідентичностями та мікросегментації, які дають змогу мінімізувати ризики компрометації компонентів системи.

Проте недостатньо досліджене питання ефективності запропонованих моделей у реальному веб-середовищі, оскільки відсутні узагальнені методи їхньої адаптації до динамічно масштабованих веб-платформ.

На противагу цьому у роботах [1, 9] розглядаються практичні аспекти реалізації АНД за допомогою LAM, MFA та поведінкової аналітики. Авторами запропоновані алгоритми динамічного управління довірою, які забезпечують підвищений рівень безпеки користувачів у хмарних середовищах. Разом із тим зазначається, що залишаються проблеми інтеграції АНД з CI/CD-процесами та мікросервісними архітектурами, де важливо не знижувати продуктивність системи.

Використання АНД набуло широкого значення у середовищах Інтернет речей та гібридних мережах в дослідженні [10], де автори доводять ефективність легких протоколів автентифікації та контекстного контролю доступу. Попри це, відкритими залишаються питання забезпечення масштабованості, низької затримки обробки запитів і сумісності таких підходів з веб-архітектурами.

Зрештою, впровадження АНД супроводжується правовими та організаційними аспектами, що є важливим у критично-інформаційній інфраструктурі. Авторами в роботі [11] вказують на потребу узгодження технічних рішень з національними стандартами безпеки та політиками конфіденційності, оскільки при впровадженні АНД може бракувати комплексних підходів, які поєднують технічні, правові та архітектурні вимоги у єдину модель управління довірою.

Тому аналіз останніх досліджень свідчить про **сутність проблеми** полягає у тому, що в умовах розподілених систем і зростання складності вебінфраструктури традиційні моделі безпеки стають неефективними. Виникає необхідність у розробці **нових архітектурних рішень**, що дозволять впровадити **принципи Zero Trust** без суттєвого зниження продуктивності та без порушення логіки взаємодії між компонентами вебсистеми. Це визначає актуальність дослідження **нових підходів до побудови безпечних веб-архітектур** на основі Zero Trust, здатних протидіяти як зовнішнім, так і внутрішнім загрозам у сучасних розподілених середовищах.

Постановка мети та завдання дослідження. Метою дослідження є обґрунтування теоретичних засад і розроблення архітектурних підходів до впровадження принципів Zero Trust у вебархітектурах розподілених систем з метою підвищення їхньої безпеки, стійкості до внутрішніх та зовнішніх загроз і забезпечення динамічного контролю довіри між усіма компонентами системи. Для досягнення поставленої мети необхідно вирішити наступні завдання:

- проаналізувати сучасні виклики інформаційної безпеки у розподілених веб-архітектурах та обмеження традиційних моделей захисту;
- дослідити принципи, структурні елементи та механізми функціонування АНД у контексті веб-систем;
- провести порівняльний аналіз традиційних та ZT моделей безпеки за критеріями ефективності, масштабованості, рівня контролю доступу та захисту від внутрішніх атак.
- визначити роль і взаємодію ключових компонентів ZT у веб-архітектурі;
- обґрунтувати практичні підходи до інтеграції ZT у хмарні, мікросервісні та контейнеризовані середовища розподілених систем.

Виклад основного матеріалу. ***Доцільність використання архітектури Zero Trust та порівняння з традиційними моделями безпеки.*** Розвиток сучасних веб-архітектур, орієнтованих на розподіл, масштабованість та інтеграцію хмарних сервісів кардинально змінив уявлення про безпеку. У таких системах користувачі, сервіси та дані постійно переміщуються між різними доменами, середовищами виконання та географічними зонами. У результаті традиційна модель безпеки, яка базується на принципі мережевого периметру втратила свою ефективність [4].

Традиційна парадигма забезпечення безпеки веб-систем базується на побудові чітко окресленого мережевого периметра, всередині якого всі суб’єкти вважаються довіреними.

Основними засобами такої моделі виступають [2, 12]:

- міжмережеві екрани (Firewall), які контролюють трафік між внутрішнім і зовнішнім середовищем;
- VPN-тунелі, що створюють захищені канали зв’язку для авторизованих користувачів;
- антивірусні рішення та системи виявлення й запобігання вторгненням (IDS/IPS), орієнтовані на розпізнавання відомих шаблонів атак;
- рольова авторизація (RBAC), у межах якої права доступу визначаються наперед відповідно до посадових ролей.

Попри свою ефективність у централізованих інформаційних системах, ці підходи демонструють низку суттєвих обмежень у контексті сучасних розподілених веб-архітектур [5, 9].

1) Передусім їм властива відсутність динамічності, оскільки політики доступу залишаються статичними й не враховують контекст виконання запиту (час, геолокацію, тип пристрою, рівень ризику).

2) Єдиний периметр безпеки створює ризик каскадного компрометування: у разі злому одного вузла зловмисник отримує доступ до всієї внутрішньої інфраструктури.

3) Надмірна довіра до "внутрішніх" користувачів також становить критичну вразливість, адже більшість атак сьогодні здійснюються шляхом зловживання або викрадення облікових даних.

4) Традиційні засоби контролю доступу виявляються малопридатними для масштабування, оскільки централізовані системи управління безпекою не адаптовані до мікросервісних і контейнеризованих архітектур, де взаємодія між компонентами є динамічною, а мережеві межі — розмитими.

Головна проблема полягає в тому, що традиційні системи безпеки оперують поняттям «довіреного доступу». Якщо користувач або сервіс один раз пройшов процес автентифікації – йому часто надається широкий набір прав у межах мережі, що власне створює передумови для внутрішніх атак для швидкого поширення шкідливого впливу всередині веб-інфраструктури [3].

У відповідь на такі виклики сформувалася концепція ZT – підхід, який повністю переглядає логіку побудови безпеки веб-архітектури. В умовах розподілених веб-систем така модель є ефективною, оскільки вона забезпечує контроль довіри на всіх рівнях – від автентифікації користувача до взаємодії між мікросервісами. Кожен запит перевіряється з урахуванням контексту (час, місце, пристрій, роль, рівень ризику тощо), а рівень доступу визначається відповідно до поточної безпекової ситуації [4].

Перевага ZT полягає у можливості мінімізувати наслідки потенційного проникнення навіть у разі компрометації одного вузла або користувацького акаунта зловмисник не зможе отримати доступ до інших компонентів системи. Для цього використовуються механізми мікросегментації, мінімізації привілеїв та поведінкової аналітики (UEBA), які постійно аналізують дії користувачів і виявляють аномалії в реальному часі [3].

Таблиця 1

Порівняльний аналіз традиційних моделей та Zero Trust у веб-архітектурі

Критерій	Традиційна модель безпеки	ZT у веб-архітектурі
Принцип захисту	Безпека по мережевому периметру (довіра всередині мережі)	Безперервна перевірка кожного запит
Контроль доступу	Статичні політики (ролі, групи)	Динамічні політики на основі контексту й ризику

Критерій	Традиційна модель безпеки	ZT у веб-архітектурі
Захист внутрішніх ресурсів	Мінімальний або відсутній	Повна ізоляція та мікросегментація сервісів
Масштабованість	Обмежена в розподілених системах	Висока, через розподілену логіку контролю
Аналіз активності	Переважно реактивний (журнали подій)	Проактивний, через поведінкову аналітику (UEBA)
Вразливість до внутрішніх атак	Висока	Значно знижена завдяки принципу мінімальних привілеїв
Вимоги до ресурсів	Менші, але обмежена ефективність	Вищі, але забезпечують адаптивний рівень захисту

Джерело: сформовано авторами

Отже, традиційні підходи до безпеки веб-архітектур не відповідають вимогам сучасних розподілених систем, де межі між «внутрішнім» і «зовнішнім» середовищем стираються. Концепція ZT забезпечує більш гнучку, адаптивну та масштабовану модель захисту, орієнтовану на контекст взаємодії та рівень ризику.

Практичні результати впровадження свідчать про значне зниження рівня кіберінцидентів, покращення виявлення аномалій та підвищення контролю над кожним елементом системи.

Саме тому ZT стає ключовим напрямом розвитку безпеки веб-архітектур у розподілених середовищах, поєднуючи технологічну ефективність із концептуально новим баченням довіри.

Архітектури «нульової довіри». Концепція АНД є сучасною парадигмою безпеки, яка замість створення фіксованого периметра безпеки передбачає постійний контроль, перевірку та динамічну оцінку довіри для кожного запиту до ресурсу. Основна мета АНД полягає у мінімізації наслідків потенційного компрометування шляхом ізоляції компонентів, застосування принципу найменших привілеїв (Least Privilege) та постійної валідації кожної взаємодії у системі [5, 13]. Розглянемо структурні складові АНД в табл. 2.

Таблиця 2

Структурні складові та компоненти архітектури «нульової довіри»

Складові та компоненти	Пояснення
Policy Engine (механізм прийняття рішень щодо довіри)	Аналізує кожен запит на основі контекстних атрибутів: ідентичність користувача, тип пристрою, місце розташування, рівень ризику, історія поведінки, час доступу тощо. Використовує алгоритми машинного навчання для оцінки ризиків у реальному часі.
Policy Administration (адміністратор політик)	Реалізує рішення Policy Engine, формує відповідні правила для пристроїв або сервісів, керує сертифікатами, токенами та ключами доступу.
Policy Enforcement Point (точка застосування політик)	Безпосередньо виконує перевірку та дозволяє або блокує запити доступу відповідно до рішень, прийнятих PE. Зазвичай реалізується у вигляді проксі-серверів, шлюзів або сервісних mesh-агентів.
Identity and Access Management (керування ідентичностями та доступом.)	Забезпечує багатофакторну автентифікацію (MFA), атрибутивну авторизацію (ABAC) та контроль життєвого циклу облікових записів. Всі дії користувачів логуються для подальшого аудиту.
Microsegmentation Layer (шар мікросегментації)	Розділяє інфраструктуру на дрібні ізольовані зони, унеможливлюючи горизонтальне переміщення зловмисника в межах системи. Кожен сегмент має власні політики доступу та моніторингу.
Continuous Monitoring and Analytics (безперервний моніторинг і поведінкова аналітика)	Відстежує активність користувачів, процесів і мережевих потоків для виявлення аномалій у режимі реального часу. Використовує UEBA-технології (User and Entity Behavior Analytics).
Data Protection Layer (рівень захисту даних)	Включає наскрізне шифрування даних “у русі” та “у спокої”, захист метаданих, цифрові підписи, контроль версій і верифікацію цілісності інформації.
Security Orchestration, Automation and Response (автоматизація рішень безпеки)	Забезпечує узгоджену реакцію на інциденти, інтеграцію з CI/CD-процесами та автоматичне оновлення політик у динамічних розподілених середовищах.

Джерело: сформовано авторами

На основі описаних структурних складових АНД розглянемо реалізацію та взаємодію такої архітектури, що відбувається за наступним алгоритмом [13]:

1. Користувач або сервіс надсилає запит до ресурсу
↓
2. Складова *Policy Enforcement Point* перехоплює запит і передає метадані до *Policy Engine*
↓
3. *Policy Engine*, використовуючи *Identity and Access Management*, бази ризиків і контекстну інформацію приймає рішення щодо довіри
↓
4. Складова *Policy Administration* формує правила, які *Policy Enforcement Point* застосовує для дозволу або блокування доступу
↓
5. Усі події записуються в систему моніторингу, що постійно оновлює рівень довіри до кожного суб′єкта

Наведений алгоритм показує функціонування АНД та пояснюється наступним чином.

1. Ініціація запиту. Користувач, пристрій або сервіс формує запит на доступ до ресурсу (API, веб-сервісу, бази даних чи хмарного застосунку). Разом із запитом передаються атрибути автентифікації (токен, сертифікат, ключ, сесійні дані тощо) та метадані про контекст (час, IP-адреса, геологічна локація, тип пристрою, середовище виконання);

2. Перехоплення та ініціальна перевірка. Компонент *Policy Enforcement Point* перехоплює запит і проводить попередню валідацію, перевірку цифрового підпису, відповідність базовим політикам доступу, відповідність TLS-шифруванню тощо.

Після чого метадані запиту передаються до *Policy Engine* для подальшої оцінки ризику.

3. Контекстна оцінка ризику та прийняття рішення. Складові модуля *Policy Engine*, взаємодіючи з підсистемою *Identity and Access Management*, базами ризиків і поведінкової аналітики (UEBA) проводить динамічну оцінку запиту. На основі атрибутів користувача, типу пристрою, місця розташування, історії поведінки, часу доступу та рівня довіри формується контекстне рішення – «дозволити», «відхилити» або «запросити додаткову автентифікацію», наприклад, (MFA).

4. Формування та застосування політик, де компонент *Policy Administrator* реалізує рішення *Policy Engine*, формує відповідні правила доступу (policy tokens, ACL-списки, динамічні політики) і передає їх до компонента *Policy*

Enforcement Point, який застосовує політику в реальному часі – надає, обмежує або блокує доступ до запитуваного ресурсу.

5. Моніторинг, логування та зворотний зв'язок. Усі дії користувача, зокрема запити, дозволи, відмови, спроби несанкціонованого доступу фіксуються за допомогою *Continuous Monitoring and Analytics*. Отримані дані надходять у поведінкові моделі UEBA, які оновлюють рівень довіри суб'єкта. Це дозволяє адаптивно змінювати політики доступу, формувати нові правила безпеки та автоматизувати реагування на інциденти через SOAR-платформу.

Такий алгоритм забезпечує циклічну модель Zero Trust, де кожен запит є об'єктом оцінки незалежно від походження. Це створює замкнену петлю довіри, у якій моніторинг та аналітика безперервно вдосконалюють політики, підвищуючи рівень кіберстійкості розподіленої системи.

Характеристика розподілених систем та необхідність переходу до Zero Trust у контексті розподілених веб-архітектур. В контексті веб-архітектури розподілені системи є однією з базових парадигм сучасної обчислювальної інфраструктури, що визначає архітектуру більшості веб-платформ, хмарних сервісів, мікросервісних застосунків і корпоративних екосистем. Розподілена система – це сукупність територіально роз'єднаних та незалежних комп'ютерів, що працюють разом як єдине ціле, надаючи користувачам або іншим системам уявлення про роботу єдиної, зв'язної системи, де взаємодія компонентів відбувається через мережу із застосування спільних протоколів і правил обміну даними. Вони можуть мати різні характеристики, наприклад, розподілена файлова система (що дозволяє спільно використовувати файли через мережу), розподілені обчислення (де завдання розділяється між кількома комп'ютерами для прискорення обробки) тощо.

З іншого боку розподілену систему можна описати як множину вузлів (host, node), які виконують частини єдиного обчислювального процесу, координуючи свої дії через мережеві протоколи. Така система забезпечує ілюзію цілісності, приховуючи від користувача фізичний розподіл завдань, що досягається завдяки механізмам синхронізації, узгодженості даних і транзакційного контролю.

До основних архітектурних принципів та властивостей розподілених систем можна віднести:

- прозорість, де користувач взаємодіє з системою як із цілісною сутністю, не усвідомлюючи розподілу процесів і даних між вузлами;
- масштабованість, оскільки система зберігає працездатність і продуктивність при збільшення кількості вузлів, користувачів чи обсягів даних;
- відмовостійкість, що обумовлюється здатністю системи зберігати функціональність у разі відмови окремих компонентів завдяки реплікації та резервуванню;

- гетерогенність, що є можливим завдяки інтеграції різнорідних апаратних, програмних та мережевих платформ у єдину інфраструктуру;
- асинхронність, коли компоненти функціонують незалежно та взаємодіють між собою за допомогою асинхронних викликів або черг повідомлень;
- децентралізоване управління з відсутністю єдиного центру контролю або точки відмови, що підвищує стійкість до атак і технічних збоїв.

Характеристики архітектурних принципів та властивостей зумовлюють як високу ефективність розподілених систем, так і складність їх захисту, оскільки множинність вузлів, різнорідність середовищ і відсутність фіксованого периметра роблять їх особливо вразливими до кібератак.

Прикладами реалізації розподілених архітектур в веб-середовищі можуть бути:

- хмарні обчислення (платформи, які реалізують розподілені центри обробки даних, що забезпечують динамічне масштабування, балансування навантаження та геореплікацію даних);
- мікросервісна архітектура (де кожен модуль виконує окрему бізнес-функцію, спілкуючись з іншими за допомогою API);
- системи доставки контенту (мережі, які можуть зберігати копії веб-ресурсів на вузлах у різних країнах, скорочуючи затримку доступу до даних);
- Інтернет речей (сенсорні мережі та підходи периферійних обчислень створюють мільйони точок збору й обробки даних у розподіленому середовищі);
- блокчейн-системи (децентралізована система, де довіра забезпечується математичними та криптографічними методами, а не централізованим адміністратором).

В табл. 3 показано приклади реалізації розподілених архітектур у веб-середовищі, де буде описано тип архітектури, приклад реалізації, ключові характеристики, переваги та потенційні ризики для кожного прикладу.

Таблиця 3

Приклади реалізації розподілених архітектур у веб-середовищі

Тип архітектури	Приклад реалізації	Ключові характеристики	Переваги	Потенційні ризики
Хмарні обчислення	AWS, Microsoft Azure, Google Cloud Platform	Розподілені центри обробки даних, геореплікація, балансування навантаження	Масштабованість, гнучкість, висока доступність	Залежність від постачальника, ризики витоку даних

Тип архітектури	Приклад реалізації	Ключові характеристики	Переваги	Потенційні ризики
Мікросервісна архітектура	Netflix, Uber, Spotify	Незалежні сервіси, що взаємодіють через API або черги повідомлень	Висока гнучкість, простота оновлення, ізоляція збоїв	Ускладнене управління, потреба у DevOps-підході
Системи доставки контенту	Cloudflare, Akamai, Fastly	Географічно розподілені вузли кешування даних	Зменшення затримки, підвищення швидкодії сайтів	Можливі проблеми синхронізації контенту
Інтернет речей	Smart City платформи, AWS IoT Core	Сенсорні мережі, децентралізована обробка даних «на межі»	Реальний час, автономність, ефективність	Уразливість кінцевих пристроїв, складність управління
Блокчейн-системи	Bitcoin, Ethereum, Hyperledger	Повністю децентралізована мережа з криптографічною довірою	Прозорість, незмінність даних, відсутність єдиного центру	Високе енергоспоживання, обмежена масштабованість

Джерело: сформовано авторами

Проблематика безпеки розподілених систем полягає у тому, що розподіл створює низку загроз безпеці, які характерні для централізованих моделей, зокрема:

1) відсутність єдиного периметра безпеки, оскільки традиційні засоби захисту (фаєрволи, VPN) не забезпечують комплексного контролю при взаємодії компонентів між хмарами, дата-центрами та користувацькими пристроями;

2) бічна рухливість зловмисників в тих випадках, коли компрометація одного сервісу часто відкриває шлях до решти системи;

3) ускладнення управління ідентичністю та політикою доступу, оскільки у багатодоменному середовищі стає важко централізовано відстежувати автентичність усіх користувачів і вузлів;

4) проблеми конфіденційності та захисту даних під час синхронізації, оскільки реплікація між різними вузлами може створювати вікна уразливості;

5) вразливості API та сервісної взаємодії, коли більшість атак у мікросервісних архітектурах здійснюються саме через слабо захищені точки взаємодії API.

Таким чином існує необхідність переходу до Zero Trust у контексті розподілених веб-архітектур. У класичних централізованих архітектурах безпеки основою захисту виступав фіксований мережевий периметр, усередині якого усі суб'єкти вважалися довіреними. Проте в умовах розподілених систем та хмарних обчислень такий підхід втратив ефективність. Межі між "внутрішнім" і "зовнішнім" середовищем більше не існують, оскільки користувачі, сервіси, пристрої та дані постійно переміщуються між різними доменами.

АНД передбачає постійну автентифікацію, авторизацію та оцінку ризиків кожного запиту незалежно від його походження чи розташування у мережі. На рис. 1 показано узагальнену схему АНД у веб-архітектурі розподілених систем. АНД в умовах розподіленого середовища забезпечує:

- мікросегментацію ресурсів для запобігання горизонтальному поширенню атак;
- централізоване управління ідентичностями (Identity and Access Management, IAM);
- поведінкову аналітику користувачів і сервісів (User and Entity Behavior Analytics, UEBA);
- наскрізне шифрування даних у русі та спокої;
- адаптивні політики доступу, що динамічно враховують контекст, пристрій, місце, час і рівень довіри.

Розглянемо на рис. 1 узагальнену схему АНД у веб-архітектурі розподілених систем.

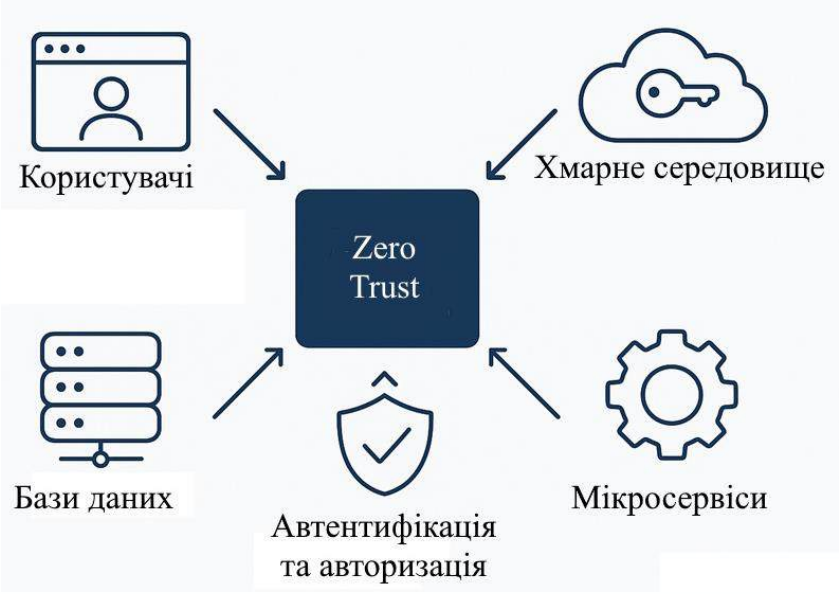

Рисунок 1 - Узагальнення схема АНД у веб-архітектурі розподілених систем

Джерело: сформовано авторами

Узагальнюючи можна зробити висновок, що розподілені системи становлять ядро сучасних веб-архітектур, забезпечуючи масштабованість, надійність і гнучкість у глобальних обчислювальних середовищах. Водночас їхня складність і динамічність створюють нові виклики для кібербезпеки, подолати які можливо лише шляхом переходу до АНД. Використання АНД формує методологічну основу для створення безпечних веб-систем у децентралізованих середовищах, поєднуючи контроль довіри, контекстну автентифікацію, поведінкову аналітику та політики мінімальних привілеїв у єдину динамічну модель безпеки.

Підходи щодо безпеки за допомогою ZT в умовах розподілених систем. Розвиток розподілених веб-архітектур, орієнтованих на мікросервісні моделі, контейнеризацію, децентралізовані обчислення та інтеграцію хмарних сервісів, зумовлює потребу у нових підходах до безпеки, які враховують постійну змінність середовища, відсутність єдиного мережевого периметра та динамічний характер взаємодій між компонентами системи. У цьому контексті ZT стає не лише моделлю захисту, а концептуальною основою побудови безпечних розподілених систем, у яких кожна взаємодія проходить перевірку незалежно від місця розташування або статусу користувача.

Нова архітектура безпеки у розподілених середовищах спирається на низку ключових принципів, які відрізняють її від традиційних моделей.

1. Явна перевірка доступу, де кожен запит до ресурсів проходить ретельну автентифікацію та авторизацію. Це включає багатофакторну автентифікацію (MFA), аналіз ризику сесії та оцінку контексту запиту (наприклад, часу доби, місцезнаходження користувача, тип пристрою або наявність сертифікатів). Наприклад, якщо співробітник намагається отримати доступ до корпоративної бази даних з особистого ноутбука вдома, система може вимагати одноразовий код, а також перевірити, чи пристрій відповідає політикам безпеки.

2. Принцип мінімальних привілеї**,** коли користувачі та пристрої отримують лише той рівень доступу, який необхідний для виконання конкретної задачі. Це зменшує ризик ненавмисного або зловмисного доступу до критичних ресурсів. Реалізація можлива через рольові моделі доступу (RBAC), атрибутивні політики (ABAC), а також механізми Just-In-Time (JIT) або Just-Enough Access (JEA), які дозволяють надати тимчасові права для виконання конкретної операції. Наприклад, інженер може отримати доступ до серверного середовища лише на час проведення технічного обслуговування, після чого привілеї автоматично відкликаються.

3. Мікросегментація передбачає собою інфраструктуру, яка ділиться на дрібні логічні зони (сервіси, середовища або кластерні групи), кожна з яких має власні політ. доступу. Це обмежує поширення загроз і локалізує можливі атаки. На рис. 2 показ. прикл. мікросегментації та її впливу на структ. веб-середовища.

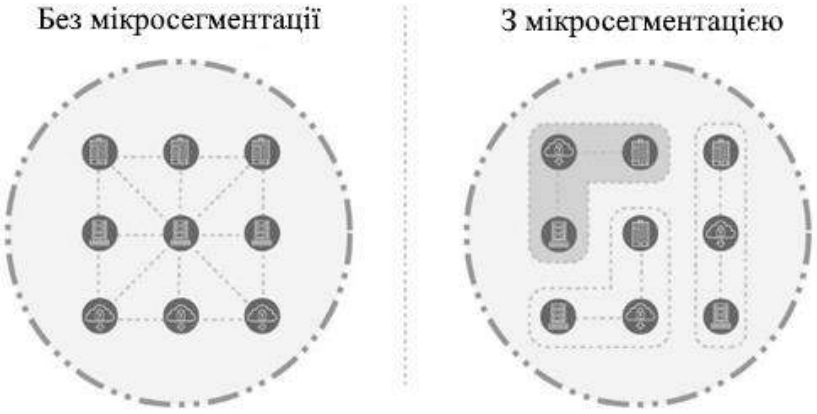

Рисунок 2 - Порівняння веб-архітектури ZT
з мікросегментацією та її відсутністю
Джерело: сформовано авторами на основі [10]

Мікросегментацію реалізують за допомогою програмно-визначених мереж (SDN), віртуальних приватних мереж (VPC) та контейнерів з ізольованим мережевим стеком. Наприклад, компрометація одного сервісу не дозволить зловмиснику автоматично отримати доступ до інших частин системи.

4. Контекстно-залежний контроль доступу відповідає за надання доступу до ресурсів, що надається з урахуванням поточного контексту: стану пристрою, геолокації користувача, часу доби або попередньої активності. Адаптивні політики можуть вимагати додаткової перевірки у разі підозрілих дій. Наприклад, запит на доступ із незвичайного географічного розташування може потребувати повторної автентифікації або підтвердження через мобільний додаток.

5. Безперервний моніторинг та оцінка ризиків на основі ZT передбачає постійне спостереження за поведінкою користувачів та станом систем. Дані збираються через системи SIEM, аналізуються за допомогою UEBA та у разі аномалій можуть автоматично запускати сценарії реагування через SOAR (Security Orchestration, Automation and Response). Наприклад, спроба доступу до бази даних у неробочий час може спровокувати автоматичне блокування сесії та сповіщення адміністратора.

6. Захист даних та управління ключами (End-to-End Encryption and Key Management), де всі дані у ZT шифруються як під час зберігання, так і під час передачі. Використовуються сучасні протоколи TLS 1.3 та AES-256, апаратне шифрування, ізольована обробка даних (наприклад, Intel SGX) і централізоване керування ключами через KMS. Це забезпечує захист від несанкціонованого доступу навіть у разі компрометації окремих вузлів мережі.

7. Перевірка довіри пристроїв (Device Trust), де доступ до ресурсів налається лише з пристроїв, що відповідають корпоративним політикам безпеки. Оцінюється наявність антивірусного ПЗ, шифрування диска, актуальність

операційної системи та апаратної підтримки безпеки (TPM). Системи MDM, такі як Microsoft Intune або VMware Workspace ONE, дозволяють централізовано здійснювати перевірку та управління пристроями.

Застосування цих підходів у розподілених системах створює багаторівневий захист, дозволяє обмежити наслідки потенційних атак і забезпечує безпечну роботу користувачів і пристроїв навіть поза традиційним корпоративним периметром. Результатом впровадження таких підходів АНД на практиці у розподілених веб-системах забезпечує: зниження ризику внутрішніх атак та компрометації облікових даних; підвищення прозорості взаємодії між сервісами через єдині журнали подій; скорочення часу виявлення та реагування на інциденти безпеки; підвищення рівня відповідності міжнародним стандартам (ISO/IEC 27001, NIST SP 800-207); формування адаптивного середовища, у якому безпека масштабується разом із зростанням системи.

Висновки. У результаті проведеного дослідження встановлено, що традиційні моделі безпеки веб-архітектур, засновані на принципі мережевого периметра, втрачають ефективність в умовах динамічного розвитку розподілених систем, хмарних технологій і мікросервісних середовищ. Основною причиною цього є розмиття меж між «внутрішнім» і «зовнішнім» середовищем, а також поява численних точок взаємодії між сервісами, пристроями та користувачами. Проведений порівняльний аналіз традиційних моделей і АНД показав, що остання забезпечує значно вищий рівень контролю доступу, захисту внутрішніх ресурсів і масштабованості, а також дозволяє мінімізувати ризики компрометації облікових даних, реалізувати проактивне виявлення аномалій і скоротити час реагування на кіберінциденти.

Доведено, що модель АНД є сучасною концепцією безпеки, яка забезпечує постійний контроль довіри на всіх рівнях взаємодії системи. На відміну від класичних підходів, ZT не передбачає довіри до жодного елемента мережі за замовчуванням, що унеможливлює бічну рухливість атак і знижує ризик внутрішніх загроз. Встановлено, що ключовими структурними компонентами архітектури ZT у веб-середовищі є Policy Engine, Policy Enforcement Point, Identity and Access Management (IAM), Microsegmentation Layer, Continuous Monitoring and Analytics, Data Protection та Security Orchestration. Їхня взаємодія формує замкнений цикл управління довірою, який забезпечує адаптивне прийняття рішень щодо доступу в режимі реального часу.

Обґрунтовано, що ефективне впровадження принципів ZT у розподілених веб-архітектурах можливе лише за умов інтеграції таких технологій, як багатофакторна автентифікація (MFA), атрибутивний контроль доступу (ABAC), поведінкова аналітика (UEBA), мікросегментація та наскрізне шифрування. Сукупне застосування цих механізмів забезпечує комплексний, багаторівневий і динамічний захист інформаційних ресурсів.

Показано, що впровадження ZT у хмарних, мікросервісних і контейнеризованих середовищах сприяє підвищенню прозорості взаємодії між компонентами системи, поліпшенню управління ідентичностями та зниженню ризику внутрішніх атак. Це формує передумови для створення гнучких і масштабованих архітектур, здатних адаптуватися до зміни середовища без втрати рівня безпеки.

Визначено, що концепція ZT не є лише технічним рішенням, а методологічною основою побудови сучасних політик кібербезпеки, яка поєднує технологічні, організаційні та аналітичні підходи. Її впровадження сприяє підвищенню кіберстійкості підприємств, забезпеченню відповідності міжнародним стандартам (NIST SP 800-207, ISO/IEC 27001) та розвитку практики адаптивного управління ризиками у веб-архітектурах.

Подальші наукові дослідження доцільно спрямувати на розроблення та вдосконалення механізмів інтелектуального управління довірою в межах АНД для веб-систем із розподіленою структурою. Актуальним напрямом є створення адаптивних моделей оцінювання ризиків на основі машинного навчання та поведінкової аналітики (UEBA), які забезпечуватимуть автоматичне коригування політик доступу в реальному часі.

Література:

1. Umakor M. F. Architectural innovations in cybersecurity: designing resilient zero-trust networks for distributed systems in financial enterprises. *International Journal of Engineering Technology Research & Management (IJETRM).* 2024. Т. 8. №. 02. С. 147-63. DOI: https://doi.org/10.5281/zenodo.16923731

2. Сиротинський Р., Тишик І. Специфіка побудови архітектури нульової довіри в гібридних інфраструктурах. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2025. Т. 4. №. 28. С. 272-287. DOI: https://doi.org/10.28925/2663-4023.2025.28.846

3. Edo O. C. et al. Zero trust architecture: Trend and Impacton information security. *International Journal of Emerging Technology and Advanced Engineering.* 2022. Т. 12. №. 7. С. 140-147. DOI: https://doi.org/10.46338/ijetae0722_15

4. Kumar P. Next-generation secure authentication and access control architectures: advanced techniques for securing distributed systems in modern enterprises. *International Journal of Computational and Experimental Science and Engineering.* 2025. № 11(3). P. 4966-4995. DOI: https://doi.org/10.22399/ijcesen.3294

5. Khan M. J. Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*. 2023. Т. 19. №. 3. P. 105-116. DOI: https://doi.org/10.30574/wjarr.2023.19.3.1785

6. Єсін В. І., Вілігура В. В., Сватовський І. І. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти. *Radiotekhnika.* 2023. №. 214. P. 32-64. DOI: https://doi.org/10.30837/rt.2023.3.214.04

7. Golovko G., Taranenko I., Kushch O. ZERO TRUST: WHY TRADITIONAL SECURITY MODELS NO LONGER WORK. *Системи управління, навігації та зв'язку.*

Збірник наукових праць. 2025. Т. 2. №. 80. С. 97-101. DOI: https://doi.org/10.26906/SUNZ.2025.2.097

8. Куперштейн Л., Кренцін М. Модель нульової довіри для гібридної піринговой мережі. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*. 2024. №. 3. С. 236-242. DOI: https://doi.org/10.31891/2219-9365-2024-79-31

9. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Бороденко Д. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. Т. 30. С. 67-77. DOI: https://doi.org/10.32447/20784643.30.2024.07

10. Маньковський Б., Довбняк В., Опірський І. ДОСЛІДЖЕННЯ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ZERO TRUST В IOT-СИСТЕМАХ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Т. 1. №. 29. С. 73-91. DOI: https://doi.org/10.28925/2663-4023.2025.29.864

11. Dalal A. Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks. *International Journal of Management, Technology and Engineering*. 2021. № 11(9). P. 142-164. DOI: http://dx.doi.org/10.2139/ssrn.5268092

12. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2023. Т. 1. №. 21. С. 223-233. DOI: https://doi.org/10.28925/2663-4023.2023.21.223233

13. Mensah F. Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity. *International Journal of Academic and Industrial Research Innovations (IJAIRI)*. 2024. Т. 10. С. 339-346.

References:

1. Umakor, M. F. (2024). Architectural innovations in cybersecurity: designing resilient zero-trust networks for distributed systems in financial enterprises. *International Journal of Engineering Technology Research & Management (IJETRM)*, *8*(02), 147-63. Retrieved from: https://doi.org/10.5281/zenodo.16923731 [In English]

2. Syrotynskyi R., Tyshyk I. (2025). Spetsyfika pobudovy arkhitektury nulovoi doviry v hibrydnykh infrastrukturakh [The specifics of building zero trust architecture in hybrid infrastructures]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnik*a», *4*(28), 272-287. Retrieved from: https://doi.org/10.28925/2663-4023.2025.28.846 [In Ukrainian]

3. Edo, O. C., Tenebe, T., Etu, E. E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero trust architecture: Trend and Impacton information security. *International Journal of Emerging Technology and Advanced Engineering*, *12*(7), 140-147. Retrieved from: https://doi.org/10.46338/ijetae0722_15 [In English]

4. Kumar P. (2025). Next-generation secure authentication and access control architectures: advanced techniques for securing distributed systems in modern enterprises. *International Journal of Computational and Experimental Science and Engineering,* 11(3), 4966-4995. Retrieved from: https://doi.org/10.22399/ijcesen.3294 [In English]

5. Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116. DOI: https://doi.org/10.30574/wjarr.2023.19.3.1785

6. Yesin, V. I., Vilihura, V. V., & Svatowsky, I. I. (2023). Zabezpechennia bezpeky u rozpodilenykh informatsiinykh systemakh: osnovni aspekty [Ensuring security in distributed

information systems: key aspects]. *Radiotekhnika*, (214), 32-64. Retrieved from: https://doi.org/10.30837/rt.2023.3.214.04 [In Ukrainian]

7. Golovko, G., Taranenko, I., & Kushch, O. (2025). ZERO TRUST: WHY TRADITIONAL SECURITY MODELS NO LONGER WORK. *Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats, 2*(80), 97-101. Retrieved from: https://doi.org/10.26906/SUNZ.2025.2.097 [In English]

8. Kupershtein L., & Krentsin M. (2024). Model nulovoi doviry dlia hibrydnoi pirynhovoi merezhi [Zero-trust model for hybrid peer-to-peer network]. *MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES*, (3), 236-242. Retrieved from: https://doi.org/10.31891/2219-9365-2024-79-31 [In Ukrainian]

9. Korobeinikova, T. I., Zhuravel, I. M., Bodak, A. O., & Borodenko, D. V. (2024). Kontseptsiia nulovoi doviry: suchasni metody zabezpechennia kiberbezpeky v korporatyvnykh merezhakh. [Zero Trust Concept: Modern Methods of Ensuring Cybersecurity in Corporate Networks]. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti,* 30, 67-77. Retrieved from: https://doi.org/10.32447/20784643.30.2024.07 [In Ukrainian]

10. Mankovskyi, B., Dovbniak, V., & Opirskyi, I. (2025). DOSLIDZhENNIa MOZhLYVOSTI REALIZATsII KONTsEPTsII ZERO TRUST V IOT-SYSTEMAKh [RESEARCH ON THE FEASIBILITY OF IMPLEMENTING THE ZERO TRUST CONCEPT IN IOT SYSTEMS]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»,* 1(29), 73-91. Retrieved from: https://doi.org/10.28925/2663-4023.2025.29.864 [In Ukrainian]

11. Dalal A. (2021). Designing Zero Trust Security Models to Protect Distributed Networks and Minimize Cyber Risks. *International Journal of Management, Technology and Engineering,* 11(9),142-164. Retrieved from: http://dx.doi.org/10.2139/ssrn.5268092 [In English]

12. Vorokhob, M., Kyrychok, R., Yaskevych, V., Dobryshyn, Yu., & Sydorenko, S. (2023). SUChASNI PERSPEKTYVY ZASTOSUVANNIa KONTsEPTsII ZERO TRUST PRY POBUDOVI POLITYKY INFORMATsIINOI BEZPEKY PIDPRYIeMSTVA [CURRENT PROSPECTS FOR APPLYING THE ZERO TRUST CONCEPT IN DEVELOPING AN ENTERPRISE INFORMATION SECURITY POLICY]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»,* 1(21), 223–233. Retrieved from: https://doi.org/10.28925/2663-4023.2023.21.223233 [In Ukrainian]

13. Mensah, F. (2024). Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity. *International Journal of Academic and Industrial Research Innovations (IJAIRI)*, *10*, 339-346.