

**Онищук Оксана Олександрівна**

кандидат технічних наук, доцент

Волинський національний університет, Луцьк, Україна

ORCID: 0000-0002-8342-3011

oksanaoo2024@gmail.com

ЗАСТОСУВАННЯ ZERO TRUST ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. У статті досліджено сучасні підходи до програмно-технічної реалізації концепції Zero Trust як одного з найбільш перспективних напрямів забезпечення інформаційної безпеки корпоративних інформаційних систем. Актуальність дослідження зумовлена стрімким розвитком цифрових технологій, широким використанням хмарних сервісів, мобільних пристроїв, віддаленої роботи та зростанням кількості кіберзагроз, що суттєво знижує ефективність традиційної моделі захисту, побудованої на мережевому периметрі. На основі аналізу міжнародних стандартів та наукових досліджень розглянуто принципи архітектури Zero Trust, визначені у рекомендаціях NIST SP 800-207, серед яких безперервна перевірка кожного запиту, принцип мінімальних привілеїв (Least Privilege), автоматична заборона доступу за замовчуванням (Default Deny), централізоване керування цифровими ідентичностями та постійний моніторинг подій безпеки. Запропоновано програмно-технічну реалізацію системи захисту корпоративних ресурсів із використанням сервера керування ідентифікацією Keycloak, вебсервера Nginx, що виконує функції точки виконання політик доступу (Policy Enforcement Point), та контейнерної платформи Docker, яка забезпечує автоматизоване розгортання й ізоляцію компонентів системи. Для реалізації централізованого контролю доступу застосовано рольову модель RBAC, що дозволяє ефективно керувати правами користувачів без модифікації прикладного програмного забезпечення. Практичну перевірку працездатності запропонованої архітектури виконано за допомогою інструмента Policy Evaluation Tool системи Keycloak. Проведено експериментальне моделювання сценаріїв авторизації користувачів із різними рівнями привілеїв. Результати тестування підтвердили ефективність реалізації політик безпеки, відповідність принципам Zero Trust та можливість автоматичного блокування несанкціонованих запитів. Встановлено, що запропоноване рішення забезпечує централізоване керування доступом, скорочує час реагування на інциденти інформаційної безпеки, мінімізує ризики компрометації корпоративних ресурсів і може бути інтегроване до існуючої IT-інфраструктури без внесення змін до прикладних систем. Отримані результати підтверджують доцільність використання архітектури Zero Trust як ефективної основи побудови сучасних корпоративних систем інформаційної безпеки.

Ключові слова: Zero Trust, інформаційна безпека, Keycloak, Nginx, RBAC, IAM, Docker, кібербезпека, корпоративні системи.

ВСТУП

Стрімкий розвиток цифрових технологій, широке використання хмарних сервісів, мобільних пристроїв та віддаленої роботи суттєво змінили характер сучасних кіберзагроз. Класична модель захисту інформаційних систем, що базується на побудові мережевого периметра, дедалі частіше виявляється недостатньо ефективною, оскільки після проходження первинної автентифікації користувач автоматично отримує високий рівень довіри всередині корпоративної мережі. Необхідність удосконалення систем управління інформаційною безпекою визначається також міжнародними стандартами ISO/IEC 27001 та ДСТУ ISO/IEC 27001, які наголошують на ризик-орієнтованому підході до захисту інформаційних активів [1, 2].

Концепція Zero Trust пропонує принципово інший підхід до побудови систем інформаційної безпеки, який базується на безперервній перевірці кожного користувача, пристрою та запиту незалежно від їхнього місцезнаходження. Основним принципом архітектури є правило «Never Trust, Always Verify»,



що забезпечує мінімізацію ризиків внутрішніх та зовнішніх атак. Теоретичні засади цієї концепції детально викладені у стандарті NIST SP 800-207 та працях Джона Кіндер Вага [3–5].

Впровадження політики Нульової довіри набуває особливої актуальності для корпоративних інформаційних систем, які обробляють конфіденційні дані та забезпечують доступ великої кількості користувачів до критично важливих ресурсів. Використання сучасних засобів централізованої автентифікації, рольового керування доступом та постійного моніторингу дозволяє суттєво підвищити рівень захищеності корпоративної інфраструктури [3, 8, 11].

Постановка проблеми

Більшість корпоративних інформаційних систем досі використовує класичну модель захисту, побудовану навколо мережевого периметра. У такій архітектурі компрометація одного облікового запису або одного вузла може призвести до поширення атаки всередині мережі, що створює значні ризики для конфіденційності, цілісності та доступності інформаційних ресурсів [1, 3].

Додатковими факторами ризику стали широке використання хмарних сервісів, мобільних пристроїв, віддаленої роботи та концепції Bring Your Own Device (BYOD). За таких умов виникає необхідність переходу до архітектури, яка забезпечує безперервний контроль кожного запиту, мінімальні привілеї користувачів та централізоване керування політиками доступу. Реалізація таких вимог можлива шляхом використання архітектури Zero Trust, яка сьогодні вважається одним із найбільш перспективних напрямів розвитку корпоративної кібербезпеки [3, 5, 13, 15].

Аналіз останніх досліджень і публікацій

Концепція Zero Trust була запропонована Джоном Кіндервагом (John Kindervag) як відповідь на недоліки традиційної моделі мережевої безпеки, що базувалася на довірі до внутрішнього периметра мережі. Подальший розвиток ця концепція отримала після публікації стандарту NIST SP 800-207, який визначив базові принципи побудови архітектури Нульової довіри та сформував сучасний підхід до організації безпечного доступу до корпоративних ресурсів [3–5].

Питання реалізації архітектури Zero Trust досліджували S. Rose, O. Borchert, S. Mitchell та S. Connelly, які запропонували модель взаємодії компонентів Policy Decision Point (PDP) та Policy Enforcement Point (PEP), а також визначили принципи безперервної автентифікації, авторизації та контролю доступу [3, 4].

Вагомий внесок у розвиток моделей керування доступом зробили D. Ferraiolo, D. Kuhn, R. Chandramouli, а також R. Sandhu, які розробили концепцію Role-Based Access Control (RBAC), що сьогодні є одним із найбільш поширених механізмів реалізації авторизації в корпоративних інформаційних системах [11, 12].

Практичні аспекти реалізації сучасних систем централізованої автентифікації та керування цифровими ідентичностями висвітлено у документації Keycloak, тоді як питання побудови захищених шлюзів доступу розглянуто в офіційній документації Nginx. Контейнеризація програмних компонентів із використанням Docker забезпечує масштабованість, ізоляцію сервісів та спрощує процеси розгортання інформаційних систем [8–10].

Попри значну кількість наукових праць, питання комплексної інтеграції серверів керування ідентифікацією, засобів централізованої авторизації, рольових моделей доступу та принципів Zero Trust у корпоративних інформаційних системах залишаються актуальними. Особливої уваги потребує практична реалізація таких рішень із використанням програмного забезпечення з відкритим вихідним кодом, що забезпечує економічну доцільність їх впровадження та можливість адаптації до вимог конкретних організацій [3, 8–13].

Метою роботи є розроблення та дослідження програмно-технічної реалізації політики Zero Trust у корпоративній інформаційній системі шляхом інтеграції сервера автентифікації Keycloak, веб-сервера Nginx та рольової моделі доступу RBAC. Для досягнення поставленої мети було визначено такі завдання: дослідити принципи концепції Zero Trust; проаналізувати можливості Keycloak як системи IAM; реалізувати захищений шлюз доступу на базі Nginx; провадити рольову модель RBAC; провести тестування реалізованої системи; оцінити ефективність запропонованої архітектури.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Концепція Zero Trust (нульової довіри) є одним із найсучасніших підходів до побудови систем інформаційної безпеки, що ґрунтується на принципі повної відсутності апіорної довіри до будь-якого користувача, пристрою чи програмного компонента незалежно від їх фізичного або мережевого розташування. На відміну від традиційної моделі периметрового захисту, де користувач після проходження автентифікації автоматично вважається довіреним, архітектура Zero Trust передбачає постійну перевірку автентичності, авторизації та контексту кожного запиту до інформаційних ресурсів.



Основні положення цієї концепції визначено у стандарті NIST Special Publication 800-207 «Zero Trust Architecture», який сьогодні є міжнародним орієнтиром щодо побудови сучасних систем кібербезпеки [3, 4].

Ідея Zero Trust була запропонована американським дослідником Джоном Кіндервагом (John Kindervag) у компанії Forrester Research. Він сформулював принцип «Never Trust, Always Verify» («Ніколи не довіряй — завжди перевіряй»), який став основою нової архітектури захисту корпоративних інформаційних систем. Згідно з цією концепцією, жоден користувач, незалежно від місця підключення, не повинен автоматично отримувати доступ до ресурсів без проходження процедур перевірки особи, оцінювання ризику та відповідності встановленим політикам безпеки [5].

Відповідно до рекомендацій NIST SP 800-207, архітектура Zero Trust складається з декількох взаємопов'язаних компонентів, центральне місце серед яких займають Policy Decision Point (PDP) та Policy Enforcement Point (PEP). Компонент PDP (Policy Decision Point) здійснює аналіз усіх параметрів запиту, перевіряє політики безпеки, атрибути користувача, рівень довіри до пристрою та приймає рішення щодо надання або відмови у доступі. PEP (Policy Enforcement Point) виконує рішення, отримане від PDP, забезпечуючи фактичне надання або блокування доступу до корпоративних ресурсів [3].

У запропонованій роботі функції Policy Decision Point реалізовано за допомогою системи Keycloak, яка є сучасною платформою керування цифровими ідентичностями (Identity and Access Management, IAM). Keycloak підтримує централізовану автентифікацію користувачів, реалізує механізми Single Sign-On (SSO), багатофакторної автентифікації (MFA), федерації користувачів, а також підтримує сучасні протоколи безпеки OAuth 2.0, OpenID Connect та SAML 2.0. Завдяки цьому сервер може здійснювати перевірку особи користувача, аналізувати його ролі, права доступу та приймати рішення відповідно до визначених політик безпеки [8].

Функції Policy Enforcement Point у розробленій системі виконує веб сервер Nginx, який працює як захищений шлюз між користувачем і корпоративними інформаційними ресурсами. Після отримання рішення від сервера Keycloak вебсервер або дозволяє доступ до захищеного ресурсу, або блокує його. Такий підхід забезпечує централізований контроль усіх запитів без необхідності внесення змін до прикладного програмного забезпечення та значно підвищує рівень захищеності корпоративної мережі [9].

Важливим елементом реалізації політики Zero Trust є використання контейнерної технології Docker, яка забезпечує ізольоване виконання всіх компонентів системи, спрощує процес розгортання програмного забезпечення та забезпечує однаковість середовищ розроблення, тестування і промислової експлуатації. Контейнеризація також сприяє масштабуванню інформаційної системи та підвищує її стійкість до відмов [10].

Одним із ключових принципів Zero Trust є Least Privilege Access (принцип мінімальних привілеїв). Його суть полягає у наданні користувачеві лише тих повноважень, які необхідні для виконання службових обов'язків. Обмеження надлишкових прав значно знижує ризик несанкціонованого доступу та мінімізує наслідки можливого компрометування облікового запису [3, 13].

Іншим фундаментальним принципом є Default Deny, відповідно до якого будь-який доступ до інформаційних ресурсів забороняється за замовчуванням і надається лише після успішного проходження всіх процедур аутентифікації, авторизації та перевірки відповідності політикам безпеки. Реалізація цього принципу дозволяє значно скоротити площу потенційної атаки та виключає можливість випадкового надання надлишкових прав користувачам [3].

Особливе значення у сучасних корпоративних системах має принцип Continuous Monitoring (безперервний моніторинг). Він передбачає постійне відстеження поведінки користувачів, аналіз журналів подій, контроль активності пристроїв та оперативне реагування на будь-які аномалії. Постійний моніторинг дозволяє своєчасно виявляти спроби несанкціонованого доступу, внутрішні загрози та атаки, що можуть виникати навіть після успішної автентифікації користувача [1, 2, 15].

Одним із базових механізмів реалізації авторизації в інформаційних системах є рольова модель керування доступом RBAC (Role-Based Access Control). На відміну від класичних дискреційних моделей, RBAC передбачає призначення прав доступу не окремим користувачам, а ролям, які відповідають посадовим або функціональним обов'язкам співробітників. Користувач отримує необхідні дозволи автоматично після призначення відповідної ролі. Такий підхід значно спрощує адміністрування корпоративної системи, забезпечує централізоване управління політиками безпеки та мінімізує кількість помилок під час керування правами доступу [11, 12].

Крім контролю доступу, сучасні стандарти інформаційної безпеки рекомендують використовувати комплексний підхід до управління ризиками. Відповідно до вимог міжнародного стандарту ISO/IEC 27001:2022 та його українського аналога ДСТУ ISO/IEC 27001:2023, система управління інформаційною безпекою повинна забезпечувати оцінювання ризиків, безперервне вдосконалення процесів захисту інформації, аудит подій безпеки та постійне оновлення політик відповідно до нових кіберзагроз [1, 2].



Таким чином, поєднання принципів Zero Trust, сучасних засобів централізованої автентифікації й авторизації (Keycloak), захищеного шлюзу доступу (Nginx), контейнерної платформи Docker та рольової моделі RBAC забезпечує створення багаторівневої системи захисту корпоративної інформаційної інфраструктури. Запропонований підхід відповідає сучасним міжнародним вимогам у сфері кібербезпеки та створює основу для побудови масштабованих і стійких до сучасних загроз корпоративних інформаційних систем.

МЕТОДИКА ДОСЛІДЖЕННЯ

Практична реалізація виконувалася із застосуванням контейнерної технології Docker Compose, що забезпечила ізольоване середовище функціонування компонентів системи. До складу програмного комплексу входили: сервер автентифікації Keycloak; веб-сервер Nginx; проксі-сервер Gatekeeper; Docker Compose для автоматизації розгортання. Після створення окремого середовища (Realm) було виконано реєстрацію клієнта, налаштовано політики авторизації, рольову модель доступу та режим примусового виконання політик (Enforcing). Для оцінювання ефективності системи використовувався інструмент Policy Evaluation Tool, який дозволяє моделювати сценарії доступу користувачів із різними рівнями привілеїв. Додатково аналізувались журнали подій Keycloak для контролю процесів автентифікації та авторизації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Практична реалізація запропонованої архітектури Zero Trust виконувалася із застосуванням технології контейнеризації Docker, що, спрощує процес розгортання та гарантує однаковість середовищ розроблення й експлуатації. Перед початком розгортання було перевірено працездатність підсистеми Windows Subsystem for Linux (WSL), а також коректність встановлення Docker Engine. Результати перевірки підтвердили готовність програмного середовища до подальшого розгортання компонентів інформаційної системи (рис. 1).

```
provisioning the new WSL instance Ubuntu
This might take a while...
Create a default Unix user account: user
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password: |
```

Рисунок 1. Перевірка готовності середовища Docker та стану підсистеми WSL.

Подальше розгортання інфраструктури було автоматизовано за допомогою Docker Compose. Конфігурація системи реалізована у файлі docker-compose.yml, який визначає взаємодію трьох основних сервісів: сервера автентифікації Keycloak, вебсервера Nginx, що імітує захищений корпоративний ресурс, та проксі-сервера Gatekeeper, який здійснює перевірку токенів доступу перед передаванням запиту до вебсервера. Фрагмент конфігураційного файлу наведено на рисунку 2.

Після створення конфігурації запуск усієї інфраструктури здійснювався командою `docker-compose up -d`

У результаті всі сервіси були успішно ініціалізовані, що підтверджується статусом `Started` у консолі Docker. Використання контейнеризації дозволило автоматизувати процес розгортання, забезпечити ізоляцію компонентів та значно спростити масштабування системи.

Після запуску інфраструктури було виконано конфігурацію сервера Keycloak відповідно до принципів архітектури Zero Trust. Насамперед створено окремий Realm `ZeroTrust-Lab`, який використовується як ізольоване середовище для керування користувачами, ролями та політиками безпеки. Використання окремого Realm дозволяє відокремити прикладні політики доступу від глобальних параметрів сервера, що спрощує адміністрування та підвищує безпеку системи. Наступним етапом стало створення клієнта `my-secure-app`, який представляє корпоративний веб ресурс у системі керування

ідентифікацією. Для клієнта встановлено тип Confidential, що передбачає використання секретного ключа під час взаємодії між проксі-сервером та Keycloak. Крім того, налаштовано параметр Redirect URI, який обмежує можливість перенаправлення користувачів лише до довіреного шлюзу доступу.

```

1 services:
2   keycloak:
3     image: quay.io/keycloak/keycloak:latest
4     command: start-dev
5     environment:
6       - KEYCLOAK_ADMIN=admin
7       - KEYCLOAK_ADMIN_PASSWORD=admin
8     ports:
9       - "8080:8080"
10
11 # Це наш "Охоронець" (Proху)
12 gatekeeper:
13   image: keycloak/keycloak-gatekeeper:latest
14   ports:
15     - "3000:3000"
16   command:
17     - --discovery-url=http://keycloak:8080/realms/ZeroTrust-Lab
18     - --client-id=my-secure-app
19     - --listen=0.0.0.0:3000
20     - --upstream-url=http://protected-app:80
21     - --skip-openid-provider-tls-verify=true
22
23 # Це наш сайт, тепер він захищений всередині мережі Docker
24 protected-app:
25   image: nginx:latest
26   expose:
27     - "80"
  
```

Рисунок 2. Конфігураційний файл docker-compose.yml для розгортання компонентів системи.

З метою реалізації одного з основних принципів Zero Trust — Default Deny — у налаштуваннях клієнта було активовано режим Policy Enforcement Mode – Enforcing. За такого режиму будь-який запит до захищеного ресурсу автоматично блокується, якщо він не відповідає визначеним політикам авторизації. Даний інструмент дозволяє моделювати різні сценарії авторизації та перевіряти правильність роботи політик доступу без впливу кешування браузера або сторонніх факторів.

Перший експеримент передбачав перевірку доступу користувача user, якому призначено лише стандартні ролі системи. Після виконання процедури оцінювання політик система сформувала рішення Deny, тобто доступ до корпоративного ресурсу було заборонено. Отриманий результат свідчить, що система успішно реалізує принцип Never Trust, Always Verify та правило Default Deny. Незважаючи на успішну автентифікацію користувача, відсутність ролі trusted_worker унеможливило доступ до захищеного вебресурсу.

Другий експеримент моделював роботу співробітника ivan_worker, якому попередньо було призначено роль trusted_worker. Після запуску процедури перевірки політик система сформувала рішення Permit, що підтвердило відповідність користувача встановленим вимогам безпеки (рис. 3).

У даному випадку сервер Keycloak успішно виконав автентифікацію користувача, перевіряв його ролі та дозволив доступ до корпоративного ресурсу через проксі-сервер.

Events

Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events Admin events

Search events Refresh 1-6

Time	User ID	Event saved type	IP address	Client
> April 13, 2026 at 4:08 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN_ERROR	172.18.0.1	my-secure-app
> April 13, 2026 at 4:08 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN_ERROR	172.18.0.1	my-secure-app
> April 13, 2026 at 4:08 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN_ERROR	172.18.0.1	my-secure-app
> April 13, 2026 at 4:08 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN_ERROR	172.18.0.1	my-secure-app
> April 13, 2026 at 4:07 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN	172.18.0.1	my-secure-app
> April 13, 2026 at 4:06 PM	c73f3f8a-49e3-42de-89a2-e6bc603dc764	LOGIN	172.18.0.1	my-secure-app

1-6

Рисунок 3. Результат перевірки політик для користувача ivan_worker (Permit).



Рисунок 4. Фіксація успішних спроб автентифікації користувача `ivan_worker` для клієнта `my-secure-app`.

Порівняльний аналіз результатів двох експериментів підтвердив ефективність реалізованої архітектури Zero Trust. Система не обмежується перевіркою факту автентифікації користувача, а здійснює аналіз його ролей, політик доступу та відповідності встановленим правилам безпеки в режимі реального часу. Для користувача без необхідних повноважень доступ до ресурсу автоматично блокується, тоді як легітимний співробітник із відповідною роллю отримує дозвіл на роботу із захищеним сервісом (рис.4). Отримані результати підтверджують працездатність запропонованої програмно-технічної реалізації політики Zero Trust та демонструють можливість її використання для захисту корпоративних інформаційних систем. Застосування серверів Keycloak, Nginx, Gatekeeper і контейнерної платформи Docker забезпечує централізоване керування доступом, реалізацію принципу мінімальних привілеїв, автоматичне блокування несанкціонованих запитів та підвищення загального рівня інформаційної безпеки. Отримані результати підтвердили ефективність реалізації принципів Zero Trust: забезпечено централізоване керування доступом; реалізовано принцип мінімальних привілеїв; виключено можливість доступу користувачів без необхідних ролей; забезпечено безперервний моніторинг усіх подій автентифікації; підвищено рівень захищеності корпоративної інфраструктури. Порівняння результатів показало, що запропонована система істотно знижує ризики компрометації корпоративних ресурсів навіть у випадку викрадення облікових даних користувача без відповідних повноважень.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі досліджено сучасні підходи до реалізації політики Zero Trust у корпоративних інформаційних системах та виконано практичну реалізацію відповідної архітектури. На основі аналізу міжнародних стандартів і сучасних технологій кібербезпеки розроблено програмно-технічне рішення, яке забезпечує централізоване керування ідентифікацією користувачів, реалізує принципи мінімальних привілеїв, безперервної перевірки доступу та автоматичного блокування несанкціонованих запитів. Використання Keycloak як сервера прийняття рішень (Policy Decision Point) і Nginx як точки виконання політик (Policy Enforcement Point) дозволило створити гнучку систему контролю доступу без внесення змін до прикладного програмного забезпечення.

Практичне тестування підтвердило ефективність запропонованої архітектури та її відповідність сучасним вимогам кібербезпеки. Запровадження принципу Default Deny, використання рольової моделі RBAC, централізованої автентифікації та журналювання подій забезпечують високий рівень захисту корпоративних інформаційних ресурсів і мінімізують ризик несанкціонованого доступу.

Практична реалізація запропонованого рішення чітко продемонструвала переваги впровадження концепції Zero Trust у корпоративному середовищі порівняно з традиційними моделями захисту мережевого периметра.

Однією з ключових переваг є незалежність механізмів захисту від прикладного програмного забезпечення (Decoupling). Реалізація політик безпеки здійснюється на рівні інфраструктури, а не у вихідному коді прикладних систем. Завдяки цьому для впровадження політики Zero Trust не потрібно модифікувати програмний код веб застосунків або корпоративних сервісів. Веб Сервер Nginx, виконуючи функції Policy Enforcement Point, лише контролює мережевий трафік і передає запити на перевірку серверу Keycloak, який приймає рішення щодо надання доступу. Такий підхід забезпечує високу масштабованість рішення та дозволяє швидко інтегрувати механізми Zero Trust у будь-які корпоративні сервіси, зокрема вебпортали, API, бази даних та хмарні платформи.

Важливою перевагою запропонованої архітектури є централізоване керування правами доступу та можливість їх миттєвого відкликання. На відміну від традиційних систем, де зміна прав користувача часто потребує оновлення конфігурацій або очищення кешу на декількох серверах, у запропонованій системі всі



рішення щодо доступу приймаються централізовано сервером Keycloak. Будь-яка зміна ролей або атрибутів користувача миттєво впливає на процес авторизації, а нові запити автоматично перевіряють відповідно до актуальної політики безпеки. Це суттєво скорочує час реагування на інциденти інформаційної безпеки та мінімізує так зване «вікно атаки», коли скомпрометований обліковий запис ще може використовуватися зловмисником.

Результати дослідження також підтвердили справедливості сучасної концепції «Identity is the New Perimeter» («Ідентичність — це новий периметр»). На відміну від класичних моделей, де рівень довіри визначався фізичним розташуванням користувача всередині корпоративної мережі, запропонована система базується виключно на перевірці цифрової ідентичності. Кожен запит супроводжується криптографічно захищеним токеном доступу, який підтверджує особу користувача, його ролі та права. Таким чином, навіть підключення з довіреної мережі або локального сегмента не є достатньою підставою для отримання доступу до інформаційних ресурсів. Це дозволяє безпечно використовувати корпоративні сервіси через мережу Інтернет без повної залежності від традиційних VPN-рішень.

Проведене експериментальне дослідження підтвердило, що запропонована архітектура ефективно реалізує основні принципи Zero Trust — Never Trust, Always Verify, Least Privilege Access, Default Deny та Continuous Verification. Система здійснює оцінювання кожного запиту в режимі реального часу, що значно підвищує стійкість корпоративної інформаційної інфраструктури до сучасних кіберзагроз, включаючи компрометацію облікових записів, внутрішні загрози та несанкціоноване використання привілеїв.

Практична цінність отриманих результатів полягає в тому, що запропоноване рішення побудоване на основі програмного забезпечення з відкритим вихідним кодом (Keycloak, Nginx, Docker), не потребує модифікації існуючих корпоративних застосунків та може бути інтегроване у вже функціонуючу IT-інфраструктуру з мінімальними витратами часу й ресурсів. Це робить запропоновану архітектуру придатною для використання як у великих корпоративних мережах, так і в інформаційних системах державних установ, навчальних закладів та підприємств різних галузей.

Перспективами подальших досліджень є інтеграція механізмів багатофакторної автентифікації (MFA), використання атрибутної моделі керування доступом (ABAC), застосування методів машинного навчання для виявлення аномальної поведінки користувачів, інтеграція із системами SIEM для автоматизованого реагування на інциденти кібербезпеки, а також дослідження можливостей використання технологій безперервної оцінки ризиків (Continuous Risk Assessment) та адаптивного контролю доступу в корпоративних інформаційних системах. Це дозволить ще більше підвищити рівень захисту інформаційних ресурсів та забезпечити відповідність сучасним міжнародним вимогам у сфері інформаційної та кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022). <https://www.iso.org/standard/82875.html>
2. Ukrainian Scientific Research and Training Center for Standardization, Certification and Quality. (2023). *Informatsiina bezpeka, kiberbezpeka ta zakhyst pryvatnosti. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy* (ISO/IEC 27001:2022, IDT) [Information security, cybersecurity and privacy protection—Information security management systems—Requirements] (DSTU ISO/IEC 27001:2023). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=105446
3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
5. Kindervag, J. (2010). *Build security into your network's DNA: The Zero Trust network architecture*. Forrester Research. <https://www.forrester.com/report/build-security-into-your-networks-dna-the-zero-trust-network-architecture/RES56682>
6. Humble, J., & Farley, D. (2011). *Continuous delivery: Reliable software releases through build, test, and deployment automation*. Addison-Wesley.
7. Kim, G., Humble, J., Debois, P., & Willis, J. (2021). *The DevOps handbook: How to create world-class agility, reliability, & security in technology organizations* (2nd ed.). IT Revolution Press.
8. Keycloak. (2024). *Keycloak documentation*. <https://www.keycloak.org/documentation>
9. NGINX, Inc. (n.d.). *NGINX documentation*. <https://nginx.org/en/docs/>



10. Merkel, D. (2014). Docker: Lightweight Linux containers for consistent development and deployment. *Linux Journal*, 2014(239). <https://www.linuxjournal.com/content/docker-lightweight-linux-containers-consistent-development-and-deployment>
11. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38–47. <https://doi.org/10.1109/2.485845>
12. Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control* (2nd ed.). Artech House.
13. Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson.
14. Yurchenko, O. M. (2001). *Zakhyst informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu* [Protection of information in computer systems against unauthorized access]. European University Publishing House.
15. National Institute of Standards and Technology. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B). <https://pages.nist.gov/800-63-4/sp800-63b.html>

**Onyshchuk Oksana /**

candidate of technical sciences, associate professor

Volyn National University, Lutsk, Ukraine

ORCID: 0000-0002-8342-3011

oksanaoo2024@gmail.com

APPLICATION OF THE ZERO TRUST ARCHITECTURE TO ENHANCE CYBERSECURITY OF CORPORATE INFORMATION SYSTEMS

Abstract. The article investigates modern approaches to the software and technical implementation of the Zero Trust concept as one of the most promising approaches to ensuring the security of corporate information systems. The relevance of the study is determined by the rapid development of digital technologies, widespread adoption of cloud services, mobile devices, remote work, and the growing number of cyber threats, all of which significantly reduce the effectiveness of traditional perimeter-based security models. Based on the analysis of international standards and recent scientific research, the paper examines the fundamental principles of the Zero Trust architecture defined in NIST Special Publication 800-207, including continuous verification of every access request, the Least Privilege principle, Default Deny policy enforcement, centralized identity management, and continuous security monitoring. A software and technical solution for protecting corporate resources is proposed using the Keycloak identity and access management platform, the NGINX web server acting as a Policy Enforcement Point (PEP), and the Docker container platform, which provides automated deployment, service isolation, portability, and scalability of the developed infrastructure. The implementation employs the Role-Based Access Control (RBAC) model to provide centralized authorization and efficient management of user permissions without modifying the source code of enterprise applications. The proposed architecture was experimentally validated using the Policy Evaluation Tool integrated into Keycloak. Several authorization scenarios involving users with different privilege levels were simulated to evaluate the effectiveness of the implemented security policies. The obtained results confirmed the correct operation of the Zero Trust mechanisms by automatically denying unauthorized requests and allowing access only to users possessing the required roles and permissions. The implementation demonstrated effective centralized access management, immediate policy enforcement, rapid privilege revocation, and reduced risks of unauthorized access to corporate resources. The research findings indicate that the proposed solution significantly improves the security of enterprise information systems, supports scalable deployment, and can be integrated into existing corporate infrastructures without modifying application software. The developed architecture confirms the practical applicability of the Zero Trust model and may serve as a basis for further research on adaptive access control, multi-factor authentication, behavioral analytics, and Security Information and Event Management (SIEM) integration.

Keywords: Zero Trust, information security, corporate information systems, Keycloak, NGINX, Docker, RBAC, identity and access management, authentication, authorization, cybersecurity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022). <https://www.iso.org/standard/82875.html>
2. Ukrainian Scientific Research and Training Center for Standardization, Certification and Quality. (2023). *Informatsiina bezpeka, kiberbezpeka ta zakhyst pryvatnosti. Systemy upravlinnia informatsiinoiu bezpekoiu. Vymohy* (ISO/IEC 27001:2022, IDT) [Information security, cybersecurity and privacy protection—Information security management systems—Requirements] (DSTU ISO/IEC 27001:2023). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=105446
3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>



5. Kindervag, J. (2010). *Build security into your network's DNA: The Zero Trust network architecture*. Forrester Research. <https://www.forrester.com/report/build-security-into-your-networks-dna-the-zero-trust-network-architecture/RES56682>
6. Humble, J., & Farley, D. (2011). *Continuous delivery: Reliable software releases through build, test, and deployment automation*. Addison-Wesley.
7. Kim, G., Humble, J., Debois, P., & Willis, J. (2021). *The DevOps handbook: How to create world-class agility, reliability, & security in technology organizations* (2nd ed.). IT Revolution Press.
8. Keycloak. (2024). *Keycloak documentation*. <https://www.keycloak.org/documentation>
9. NGINX, Inc. (n.d.). *NGINX documentation*. <https://nginx.org/en/docs/>
10. Merkel, D. (2014). Docker: Lightweight Linux containers for consistent development and deployment. *Linux Journal*, 2014(239). <https://www.linuxjournal.com/content/docker-lightweight-linux-containers-consistent-development-and-deployment>
11. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2), 38–47. <https://doi.org/10.1109/2.485845>
12. Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control* (2nd ed.). Artech House.
13. Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson.
14. Yurchenko, O. M. (2001). *Zakhyst informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu* [Protection of information in computer systems against unauthorized access]. European University Publishing House.
15. National Institute of Standards and Technology. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B). <https://pages.nist.gov/800-63-4/sp800-63b.html>

Отримано редакцією журналу / Received: 12.06.26

Прорецензовано / Revised: 20.06.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.