https://doi.org/10.31891/2219-9365-2025-84-46
УДК 004.056.5:004.4’242:005.52

ЧОРНЕНЬКИЙ Микола
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0009-0008-9321-4599
СКЛЯРЕНКО Олена
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0000-0001-6555-1223

ХМАРНІ ТА ЛОКАЛЬНІ ERP-РІШЕННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ

У статті досліджуються сучасні тенденції використання ERP-рішень щодо процедур вибору архітектур, які задовольняють вимогам безпеки і поєднують можливість модернізації з адаптивністю до змін у бізнесі. Метою дослідження було проаналізувати та порівняти хмарні та локальні ERP-архітектури в аспекті бізнес-вимог і вимог державних органів, адаптивності, збереження та захисту конфіденційних даних, а також підходів до оновлення програмного забезпечення. Для забезпечення цілісної картини критерії аналізу було розподілено на сім груп, надано короткий аналіз кожного з них. За результатами проведеного порівняльного аналізу хмарних і локальних архітектур ERP було створено загальний набір критеріїв відбору, який може слугувати практичною основою для прийняття рішень на підприємствах різних типів.

Встановлено, що профіль основних ризиків в обох архітектурах є в основному схожим, тоді як розподіл відповідальності за експлуатацію відрізняється, тому рішення щодо вибору архітектури слід приймати з урахуванням типових ситуацій у компанії. Аналіз та порівняння типових загроз і вразливих місць у хмарних і локальних моделях дозволив створити профілі для типових сценаріїв вибору архітектури.

На основі проведеного аналізу сформовано практичні рекомендації для підприємств щодо придатності хмарного або локального розгортання для типових корпоративних сценаріїв.

Ключові слова: ERP, хмарні сервіси, хмарна архітектура, локальна архітектура, безпека, адаптивність, механізми захисту, типові сценарії, технічні засоби контролю.

CHORNENKYI Mykola, SKLIARENKO Olena
Private Higher Educational Establishment «European University»

CLOUD AND ON-PREMISES ERP SOLUTIONS IN THE CONDITIONS OF DIGITAL BUSINESS TRANSFORMATION

The article examines current trends in the use of Enterprise Resource Planning (ERP) systems with a focus on architectural selection procedures that meet modern security requirements while ensuring flexibility, scalability, and long-term adaptability to dynamic business environments. Particular attention is paid to the balance between the need for continuous modernization of ERP solutions and the necessity to maintain control over critical business processes and sensitive data.

The purpose of the study is to analyze and compare cloud-based and on-premises ERP architectures in the context of business and public-sector requirements, operational adaptability, data preservation, confidentiality, regulatory compliance, and approaches to software maintenance and updates. To ensure a comprehensive and structured analysis, the evaluation criteria were grouped into seven key categories, including security and data protection, cost of ownership, scalability, flexibility of customization, regulatory compliance, system availability, and responsibility distribution between stakeholders. Each group of criteria is briefly analyzed, highlighting its impact on the overall effectiveness of ERP deployment.

The comparative analysis demonstrates that cloud and on-premises ERP architectures share a largely similar risk profile in terms of cyber threats and vulnerabilities; however, they differ significantly in the allocation of operational and security responsibilities between the service provider and the organization. As a result, the choice of architecture should be based not only on technological considerations but also on the organization’s internal competencies, risk tolerance, regulatory constraints, and typical operational scenarios.

The analysis and comparison of common threats and vulnerabilities inherent in both deployment models made it possible to develop risk profiles for typical ERP architecture selection scenarios. Based on these findings, practical recommendations were formulated regarding the appropriateness of cloud or on-premises ERP solutions for various types of enterprises. The proposed set of unified selection criteria can serve as a practical decision-making framework for organizations seeking to implement or modernize ERP systems in a secure and sustainable manner.

Keywords: ERP, cloud services, cloud architecture, on-premises architecture, security, adaptability, protection mechanisms, typical scenarios, technical controls.

Стаття надійшла до редакції / Received 28.10.2025
Прийнята до друку / Accepted 19.11.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ’ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному цифровому світі ERP-системи стали основним інструментом управління бізнес-процесами, даними та ресурсами підприємства. З огляду на зростання обсягів даних, збільшення складності операційних процесів і появу нових моделей взаємодії, як-от дистанційна робота, глобальні ланцюги

постачання, автоматизація тощо, необхідно вибрати архітектуру ERP-рішення, яка забезпечує безпечне зберігання інформації, стабільність, масштабованість і технологічну гнучкість.

З точки зору кібербезпеки, можливостей оновлення, експлуатаційних витрат, дотримання законодавчих вимог [1, 2] та інтеграції з іншими цифровими інструментами, хмарні сервіси, локальні впровадження та гібридні моделі суттєво відрізняються один від одного. У процесі цифрової трансформації підприємствам необхідно не тільки автоматизувати свої процеси, а й забезпечити стійкість до кібератак, зберегти власну технологічну актуальність та зменшити операційні ризики.

Проблема полягає в тому, що вибір між хмарними та локальними ERP-рішеннями не може базуватися виключно на фінансових або технічних аспектах. Він вимагає оцінки загроз для інформаційної безпеки, врахування регуляторних обмежень; крім того, необхідно брати до уваги швидкість пристосування до змін на ринку, а також доступ до інновацій, таких як штучний інтелект (ШІ), аналітика, автоматизація та інтеграційні платформи. Відсутність системного підходу до оцінки архітектури ERP-рішень може збільшити ризики витоку даних, технологічного старіння, перевитрати ресурсів і втрати конкурентних переваг.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Сучасна наукова та прикладна література демонструє постійну тенденцію до переходу ERP-рішень у хмару [3]. При цьому зростають вимоги до інформаційної безпеки, можливості постійного оновлення та інтеграції з аналітичними сервісами. Дослідження показують, що вибір певної архітектури (хмарної, локальної, гібридної) має безпосередній вплив на профіль ризику та оперативну стійкість [4]. Хмарні моделі характеризуються оновленнями, які контролюються постачальниками, та інтегрованими механізмами захисту, натомість локальні інсталяції забезпечують більший контроль, але пов’язані з вищими витратами та навантаженням на внутрішні команди.

Значна частина публікацій присвячена нормативним і процедурним основам безпеки, зокрема рамкам GDPR [1] та ISO/IEC 27001 [2], вимогам до управління даними, контролю доступу, аудитів, а також вбудованому захисту даних та налаштуванням, що сприяють захисту даних. Водночас підкреслюються їхні обмеження: оскільки норми оновлюються повільно, а стандарти мають рекомендаційний характер, необхідним є доповнення їх організаційними директивами та технічними засобами, які швидко розвиваються.

Публікації зосереджуються на багаторівневих механізмах захисту, серед яких шифрування «в русі» та «в стані спокою», токенізація чутливих областей, багатофакторна автентифікація, а також використання DLP/IDS/IPS та SIEM для раннього виявлення аномалій і реагування на інциденти. Окремо виділено використання алгоритмів штучного інтелекту для виявлення нетипової поведінки користувачів і нетипових транзакцій, а також методи забезпечення незмінності протоколів доступу (передусім за допомогою механізмів блокчейну) в рамках аудитів [4].

Галузеві дослідження вказують на розбіжність між вимогами: у сферах із суворими нормами (державна влада, оборона, охорона здоров’я, фінанси) основна увага приділяється суверенітету даних, прозорій перевірці та контрольованості змін; натомість у виробничих та орієнтованих на продукцію підприємствах – інтеграції функцій аналізу, прогнозування, масштабованості та взаємодії із зовнішніми платформами. Це створює більшу потребу в процедурах вибору архітектур, які поєднують вимоги безпеки, можливість модернізації та адаптивність до змін у бізнесі.

Підсумовуючи, можна сказати, що наявні літературні джерела одностайні в тому, що вибір між хмарними та локальними ERP-моделями повинен базуватися на поєднанні технічних заходів, як-от шифрування, токенізація, MFA, а також DLP/IDS/IPS/SIEM, організаційних політик і дотримання стандартів, таких як GDPR та ISO/IEC 27001. Як показує практика, хмарні рішення полегшують оновлення та доступ до інтегрованих механізмів безпеки. Локальні рішення, навпаки, забезпечують більший прямий контроль, але спричиняють вищі експлуатаційні витрати та несуть ризик помилок конфігурації. Водночас у літературі бракує публікацій, де б ці підходи порівнювалися з урахуванням таких аспектів, як кібербезпека, частота оновлень та адаптивність до вимог бізнесу.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою дослідження є аналіз та порівняння хмарних і локальних ERP-архітектур в аспекті бізнес-вимог і вимог державних органів, адаптивності, збереження та захисту конфіденційних даних, а також підходів до оновлення програмного забезпечення. Ще одним завданням у рамках дослідження є підготувати основі проведеного аналізу практичні рекомендації для підприємств щодо вибору відповідної архітектури.

У рамках поставленої мети були визначені такі основні завдання дослідження:

– аналіз основних відмінностей архітектури ERP;

– аналіз та порівняння типових загроз та вразливих місць в хмарних і локальних моделях;

– створення профілів для типових сценаріїв вибору архітектури;

– формування практичних порад щодо придатності хмарного або локального розгортання для типових корпоративних сценаріїв.

Отже, мета цієї статті полягає в тому, щоб узагальнити критеріальні підходи та практичні міркування щодо вибору між хмарними та локальними архітектурами ERP, а також надати практичні рекомендації для підприємств у різних регуляторних та операційних контекстах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Вибір між хмарним і локальним розгортанням має прямий вплив на кіберстійкість, витрати, частоту оновлень і здатність швидко впроваджувати зміни. Щоб уникнути фрагментованих рішень, критерії було розподілено на сім груп і надано короткий аналіз кожного з них, після чого висновки було узагальнено у вигляді наочної таблиці.

Відповідальність за інфраструктуру визначає, хто забезпечує доступність, надмірність, моніторинг та виправлення, а отже, вона впливає на ризики простою та необхідність додаткових посад у штаті компанії. У хмарній архітектурі більшість обов'язків щодо інфраструктури (обчислення, зберігання, резервне копіювання, відновлення після аварій, моніторинг) покладається на постачальника; організація зосереджується на конфігурації, тестуванні та використанні. Локальна інфраструктура перекладає повний цикл підтримки (апаратне/віртуальне середовище, база даних, резервне копіювання та відновлення, ведення журналів, цілодобова підтримка) на IT-команду.

Порушення безпеки та недотримання нормативних вимог мають фінансові та репутаційні наслідки; базові засоби контролю та політики є обов'язковими в будь-якій моделі [3]. Хмара отримує оновлення безпеки, що управляються провайдером, постійний моніторинг, вбудовану відповідність загальним стандартам (ISO/SOC/GDPR). Своєю чергою, локальна інфраструктура потребує власних процесів: управління вразливостями, аудит, DLP/IDS/IPS/SIEM, навчання персоналу, підтримка «приватність за замовчуванням» і задокументовані політики.

Ритм та керованість оновлень безпосередньо впливають на вразливість, стабільність і загальну вартість підтримки. У випадку хмари провайдер регулярно випускає оновлення та патчі; клієнт тестує власні налаштування та інтеграції перед етапом виробництва. Натомість локальна інфраструктура перекладає відповідальність на IT-команду за планування, оновлення, міграцію даних, регресійні тести та розгортання.

Необхідність низькорівневого доступу (ОС/БД/мережа) диктує вибір між максимальною гнучкістю та стандартизованими межами. Хмарна інфраструктура обмежена стандартами постачальника послуг системної платформи, тоді як локальна інфраструктура забезпечує більшу гнучкість і ширші можливості.

Експлуатаційні витрати, резервне копіювання та відновлення після аварій є одними з ключових умов безперебійної роботи бізнесу. У хмарі вся відповідальність лежить на провайдерові, з яким укладено чіткі угоди щодо реалізації таких заходів та їхньої загальної вартості. З іншого боку, локальна інфраструктура працює за внутрішніми політиками, і її вартість зазвичай є передбачуваною, але не точною через пов'язані із цим ризики.

Можливість швидко масштабувати ресурси та оперувати новими інструментами (аналітика, автоматизація, машинне навчання) скорочує час отримання практичної цінності. Хмарне розгортання має еластичний набір ресурсів і швидкий доступ до інновацій екосистеми з мінімальним «тертям» під час впровадження. Локальна інфраструктура вимагає додаткових закупівель обладнання, технічних робіт, проєктів тощо, що негативно впливає на терміни та кінцевий бюджет.

Результати вищевиконаного аналізу наведено в порівняльний таблиці 1.

Під час вибору архітектури доцільно окреслити спектр типових загроз і вразливостей для ERP-систем, оскільки вони визначають вимоги до технічних засобів контролю та організаційних політик. Наявні дослідження свідчать, що, незалежно від моделі надання послуг, основні загрози становлять соціальна інженерія (з використанням скомпрометованих облікових даних), помилки в конфігураціях доступу та сегментації, вразливі місця у вебінтерфейсах та інтерфейсах інтеграції API, а також недосконаліть реєстрації подій та моніторингу безпеки [5]. Ці елементи становлять основну «поверхню атаки» і пояснюють необхідність моніторингу системи та прозорих перевірок доступу.

Дослідження Panorama Consulting (2024) [3] показує, що 78,6% нововпроваджених ERP-систем є хмарними, натомість 21,4% впроваджуються локально. Це дозволяє зробити висновок, що компанії надають високий пріоритет оптимізації рівня безпеки та зменшенню експлуатаційних витрат. Звіти IDC (2024) [7], засновані на міграції до SAP Cloud ERP Private, показують, що завдяки автоматизованим механізмам моніторингу та патчингу хмарні інструменти прискорюють оновлення безпеки на 58%, виявляють кіберзагрози на 89% швидше та зменшують операційні ризики бізнесу на 42%.

Проте профіль ризику варіюється залежно від архітектурної моделі. У разі локального розгортання зазвичай виникають такі проблеми, як застарілі версії операційної системи та бази даних, обмеженість інструментів патч-менеджменту, фрагментований моніторинг журналів, а також ризики фізичного доступу до апаратного забезпечення. У хмарних середовищах одними з найбільших ризиків є неправильна конфігурація політик доступу (IAM/ACL) та багатокористувацька архітектура у разі невірно застосованих налаштувань [5].

Таблиця 1

Порівняльна таблиця прямих відмінностей хмарної та локальної архітектур

Аспект аналізу	Змістовна характеристика	Хмарна архітектура	Локальна архітектура
Модель управління інфраструктурою та експлуатацією	Розподіл відповідальності за побудову, підтримку, моніторинг, резервне копіювання та відновлення інфраструктурних компонентів	Провайдер забезпечує ресурси, моніторинг і відновлення; організація зосереджується на конфігурації прикладних модулів, тестуванні та експлуатації	Повний цикл робіт (апаратні/віртуальні середовища, ОС/СКБД, мережа, резервування, DR, моніторинг) забезпечує IT-підрозділ підприємства
Безпека та відповідність нормативним вимогам	Реалізація засобів контролю (шифрування, IAM/MFA, DLP/IDS/IPS/ SIEM), аудитів і політик, необхідних для відповідності регуляторним вимогам	Частина контролів та оновлень безпеки керується провайдером; доступні сертифікації (ISO/SOC), централізований моніторинг; замовник керує доступами на прикладному рівні	Упровадження контролів, аудитів, навчання персоналу та процедури керування вразливостями реалізуються внутрішньо; вищий ризик конфігураційних помилок
Політика оновлення та супроводу програмного забезпечення	Принципи, частота та відповідальність за впровадження оновлень, патчів, міграцій і регресійного тестування	Регулярні релізи й безпекові патчі керовані провайдером; організація тестує власні конфігурації та інтеграції перед промисловим використанням	Усі процедури оновлення, тестування, міграцій і розгортання виконує внутрішня IT-команда; вищі часові та операційні витрати
Рівень технічного контролю	Глибина доступу до низькорівневих параметрів ОС/СКБД/мережі та можливостей оптимізації	Обмежений низькорівневий контроль; акцент на конфігурації сервісів і стандартних засобах інтеграції	Повний низькорівневий контроль за системними компонентами, можливість спеціалізованого тюнінгу, драйверів і специфічних інтеграцій
Експлуатаційні витрати, резервне копіювання та відновлення після збоїв	Структура витрат, обсяг гарантійних зобов'язань, організація резервування та перевірки процедур відновлення	Вартість і DR-процедури визначені договором; резервування типово автоматизоване й регламентоване сервісною пропозицією провайдера	Витрати та ризики визначаються внутрішніми політиками й компетенціями персоналу; резервування/DR потребують окремих технічних рішень і бюджетів
Масштабованість	Здатність системи оперативно збільшувати доступні ресурси відповідно до навантаження	Еластичне масштабування ресурсів із мінімальними затримками та без необхідності придбання додаткового обладнання	Масштабування вимагає закупівель, модернізації інфраструктури та технічних робіт, що збільшує тривалість і вартість впровадження
Доступ до інновацій	Можливість інтеграції нових функціональних можливостей, сервісів і технологічних компонентів	Швидкий доступ до екосистемних сервісів і нових функцій постачальника; інновації впроваджуються з мінімальним операційним опором	Використання нових можливостей потребує окремих проєктів, інвестицій та інтеграцій; технологічне оновлення є повільнішим

Рекомендований мінімальний набір технічних засобів контролю для обох моделей включає шифрування «в русі» та «у стані спокою», багатофакторну автентифікацію, токенізацію чутливих полів, використання систем DLP/IDS/IPS, платформи SIEM з кореляцією подій, а також регулярне управління вразливостями. Як повідомляє Nucleus Research (2024) [7], перехід на хмарну ERP дозволяє знизити початкові витрати на персонал на 50% і витрати на оперативну підтримку в 5,5 разів. Це має непрямий вплив на здатність підприємств впроваджувати регулярні оновлення безпеки без затримок через бюджетні обмеження.

Ефективність цих заходів контролю залежить від організаційної структури. Це включає встановлення офіційних правил класифікації даних та доступу до них (включно з термінами зберігання та процедурами видалення), інтеграцію стратегій «захисту за замовчуванням / за замовленням» у бізнес-процеси та інтеграції, регулярне навчання співробітників методам захисту від соціального інжинірингу, політики реагування на інциденти та забезпечення безперервності роботи (з визначеними ролями та ескалаціями), а також аудити відповідності вимогам таких стандартів, як GDPR та ISO/IEC 27001, з аудитами доступу та регулярними аналізами ризиків. Узагальнені кількісні показники наведено у таблиці 2.

Підсумовуючи, можна сказати, що основні ризики для хмарних і локальних моделей в основному однакові. Однак оперативна відповідальність за підтримку контролю та процесів розподіляється по-різному: у хмарній моделі багато функцій виконує постачальник, тоді як локальна модель вимагає добре розроблених внутрішніх процедур і ресурсів. Незалежно від обраної архітектури, для забезпечення конфіденційності та

цілісності даних необхідно впровадити основні технічні засоби контролю разом з організаційними політиками.

Таблиця 2

Узагальнені характеристики для безпекового порівняння хмарної та локальної архітектур

Аспект аналізу	Хмарна архітектура	Локальна архітектура
Встановлення оновлень безпеки	Суттєво швидше (орієнтовно +58%)	Залежить від ресурсів IT-підрозділу; часто повільніше
Виявлення кіберінцидентів	Прискорене (орієнтовно +89%)	Триваліший час до виявлення
Сукупний операційний ризик	Зниження (приблизно на 42%)	Вищий у разі відкладених оновлень/патчів

Подальші рішення щодо архітектури слід приймати з урахуванням типових ситуацій у компанії. З огляду на галузеву практику можна виокремити низку найхарактерніших сценаріїв:

- Суворе регулювання / суверенітет даних. У компаніях, діяльність яких пов’язана з високими вимогами до контролю (наприклад, уряд, оборона, фінанси, охорона здоров’я), пріоритетними є прозорість аудиту, контроль змін і локальне зберігання даних.
- Висока швидкість інновацій / обмежені IT-ресурси. У середовищах, де бізнес-вимоги часто змінюються, існує потреба в доступі до нових послуг, а внутрішня експертиза є недостатньою.
- Складні інтеграції / прямий доступ до бази даних. Є вибором для сценаріїв, за яких низькорівневе управління, специфічні драйвери, налаштування або інтеграція в застарілі системи мають вирішальне значення.
- Нерівномірне завантаження/масштабування. Для компаній зі сценарями сезонних пікових навантажень і непередбачуваних потреб велике значення мають гнучкість і швидке розширення ресурсів.

Базуючись на цих типових сценаріях та аналітичних даних, наведених вище, можна створити дерево рішень щодо вибору архітектури ERP (рисунок 1).

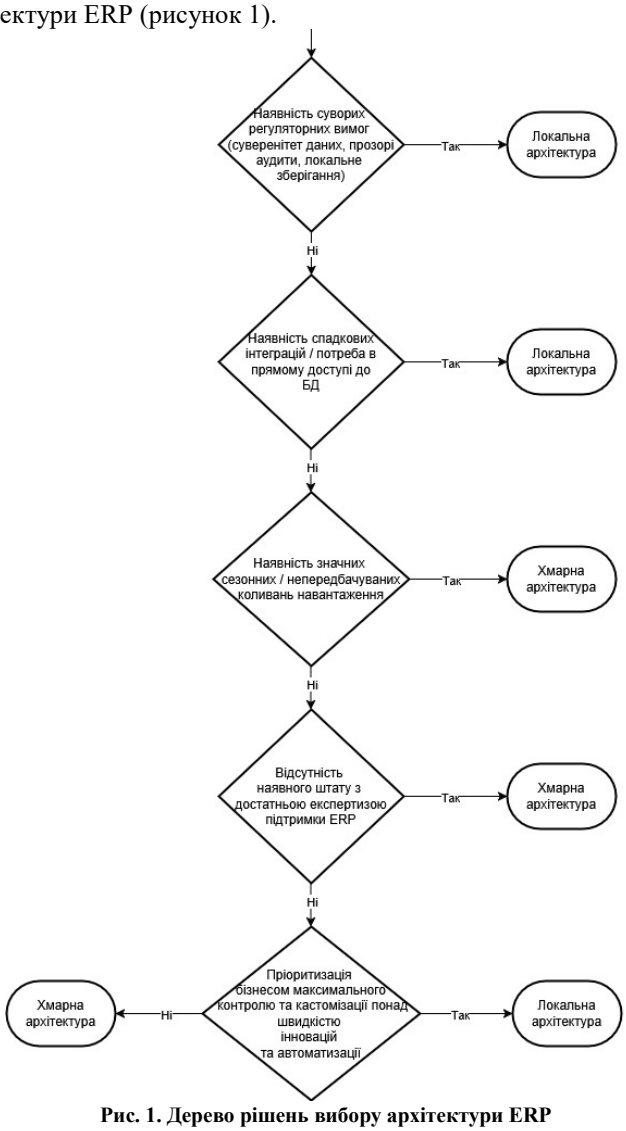

Рис. 1. Дерево рішень вибору архітектури ERP

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У рамках дослідження було проведено порівняльний аналіз хмарних та локальних архітектур ERP з точки зору безпеки, можливості оновлення та адаптації системи до бізнес-вимог та регуляторних вимог. Було створено загальний набір критеріїв відбору (відповідальність за інфраструктуру; безпека та відповідність вимогам; модель оновлення; рівень технічного контролю; експлуатаційні витрати та резервне копіювання/відновлення; масштабованість і доступ до інновацій), який може слугувати практичною основою для прийняття рішень для різних типів підприємств.

Визначено, що профіль основних ризиків в обох архітектурах є в основному схожим, тоді як розподіл відповідальності за експлуатацію відрізняється: у хмарній моделі постачальник бере на себе значну частину контролю та оновлень, натомість у локальній моделі ці завдання покладаються на внутрішню IT-службу.

Практичні поради базуються на узагальнених типових ситуаціях застосування. Хмарне розгортання підходить для вимог швидкої інновації, регулярних керованих оновлень і гнучкого масштабування при обмежених IT-ресурсах. Використання локального розгортання є виправданим, якщо існують суворі вимоги до суверенітету даних і прозорого аудиту, а також необхідний технічний контроль на низькому рівні або прямий доступ до баз даних та конкретних інтеграцій. У цій статті ми свідомо не розглядали гібридні комбінації, щоб зосередитися на чіткій дихотомії «хмара чи локальне розміщення» та надати чіткі рекомендації щодо прийняття рішень.

Запропонований підхід дозволяє нам провести систематичне порівняння переваг і недоліків хмарних та локальних архітектур ERP, зіставити вимоги до безпеки, можливості оновлення та адаптивності з реальними умовами експлуатації та запропонувати підприємствам практичні рекомендації для прийняття обґрунтованого рішення.

Література

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. URL: https://gdpr.eu (дата звернення: 27.10.2025).
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022. URL: https://www.iso.org/standard/27001 (дата звернення: 27.10.2025).
3. Panorama Consulting. The 2024 ERP Report. URL: https://4439340.fs1.hubspotusercontent-na1.net/hubfs/4439340/Reports/ERP%20Report/2024-erp-report-panorama-consulting-group.pdf (дата звернення: 27.10.2025).
4. Чорненький М.В., Скляренко О.В. Аналіз технологій зберігання конфіденційних даних у CRM/ERP-системах управління бізнес-процесами підприємства. *Таврійський науковий вісник*. Серія: Технічні науки, 29 травня 2025 р. С. 225–232.
5. ENISA. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 27.10.2025).
6. Nucleus Research. Cloud ERP gets faster payback and lower support costs (industry note), 2024. URL: https://www.dsdinc.com/wp-content/uploads/2020/03/Nucleus-Research-Cloud-ERP-Gets-43-Percent-Faster-Payback-1.pdf?utm_source=chatgpt.com (дата звернення: 27.10.2025).
7. DC. Business Value of Enhancing Security and Resiliency with SAP Cloud ERP Private (SAP-sponsored case study), 2024. URL: https://www.sap.com/research/idc-findings-on-sap-cloud-erp-private (дата звернення: 27.10.2025).

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Retrieved from: https://gdpr.eu
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022. Retrieved from: https://www.iso.org/standard/27001
3. Panorama Consulting. The 2024 ERP Report. Retrieved from: https://4439340.fs1.hubspotusercontent-na1.net/hubfs/4439340/Reports/ERP%20Report/2024-erp-report-panorama-consulting-group.pdf
4. Chornenkyi M.V., Skliarenko O. V. Analysis of confidential data storage technologies in CRM/ERP business process management systems of an enterprise. Tavria Scientific Bulletin. Series: Technical Sciences, May 29, 2025, p. 225–232.
5. ENISA. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
6. Nucleus Research. Cloud ERP gets faster payback and lower support costs (industry note), 2024. Retrieved from: https://www.dsdinc.com/wp-content/uploads/2020/03/Nucleus-Research-Cloud-ERP-Gets-43-Percent-Faster-Payback-1.pdf?utm_source=chatgpt.com
7. DC. Business Value of Enhancing Security and Resiliency with SAP Cloud ERP Private (SAP-sponsored case study), 2024. Retrieved from: https://www.sap.com/research/idc-findings-on-sap-cloud-erp-private