УДК 004.056:004.7
DOI https://doi.org/10.32782/2663-5941/2025.4.2/05

Большакова О.О.
ПЗВО «Міжнародний класичний університет імені Пилипа Орлика»

Кошкін В.К.
ПЗВО «Міжнародний класичний університет імені Пилипа Орлика»

Арамян А.М.
ПЗВО «Міжнародний класичний університет імені Пилипа Орлика»

Бандура В.М.
ПЗВО «Міжнародний класичний університет імені Пилипа Орлика»

Єганов О.Ю.
ПЗВО «Міжнародний класичний університет імені Пилипа Орлика»

СУЧАСНІ ПІДХОДИ ДО ПОБУДОВИ ЕФЕКТИВНИХ ТА БЕЗПЕЧНИХ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

У статті проаналізовано актуальні підходи до проєктування ефективних та безпечних комп'ютерних систем і мереж (КСМ) у контексті цифрової трансформації та зростання кіберзагроз. Показано, що збільшення обсягів даних, розвиток хмарної інфраструктури та підвищення складності IT-середовищ потребують запровадження архітектурних рішень, здатних забезпечити гнучкість, масштабованість та кіберстійкість. Розглянуто мікросервісну та сервісно-орієнтовану архітектуру як основу для побудови адаптивних КСМ, що легко масштабуються й оновлюються відповідно до змін бізнес-вимог.

Хмарні технології визначені як ключовий елемент сучасної IT-інфраструктури, проте підкреслено ризики, які вони породжують: збільшення поверхні атаки, ускладнення захисту даних і потенційна втрата контролю. У зв'язку з цим обґрунтовано доцільність впровадження принципу Security by Design, що передбачає інтеграцію безпеки на всіх етапах розробки, а також застосування Zero Trust Architecture (ZTA), яка забезпечує постійний контроль і перевірку доступу незалежно від джерела запиту.

Детально проаналізовано роль таких механізмів, як багатофакторна автентифікація (MFA) і наскрізне шифрування, як засобів підвищення кіберстійкості систем. Окрема увага приділена використанню штучного інтелекту (ШІ) в управлінні ресурсами, прогнозуванні збоїв і виявленні аномалій у режимі реального часу. ШІ розглянуто як інструмент підвищення динамічності систем захисту, зокрема завдяки адаптивному налаштуванню політик безпеки та аналізу поведінки користувачів. Водночас відзначено виклики, пов'язані із змагальними атаками, що вимагають стійких алгоритмів.

Результатом дослідження є запропонована інтегрована концепція побудови КСМ, яка синтезує можливості COA, принципи ZTA та інтелектуальні засоби на базі ШІ. Такий підхід дозволяє створювати безпечні, адаптивні та ефективні системи для використання в державному, корпоративному й хмарному середовищах.

Ключові слова: *мікросервісна архітектура, сервісно-орієнтована архітектура, кібербезпека, хмарні технології, штучний інтелект, Zero Trust.*

Постановка проблеми. У сучасних умовах цифрової трансформації комп'ютерні системи та мережі (КСМ) є критично важливою інфраструктурою для державних і комерційних структур. Стрімкий розвиток цифрових технологій ускладнив архітектуру КСМ, поставивши перед ними нові вимоги до продуктивності, масштабованості та безпеки, особливо в умовах використання хмарних технологій (AWS, Azure, Google Cloud). Хоча хмарні рішення забезпечують гнуч-

кість і економічність, вони одночасно створюють нові загрози – зростає поверхня атаки, виникають ризики втрати контролю над даними та проблеми з налаштуванням безпеки [1-2].

З огляду на це, інтеграція штучного інтелекту (ШІ) у КСМ набуває стратегічного значення. ШІ дозволяє автоматизувати управління ресурсами, виявляти аномалії у реальному часі, формувати адаптивні системи захисту на основі поведінкового аналізу (наприклад, UEBA), що підвищує рівень кіберзахисту в динамічних середовищах [3]. Водночас поєднання ШІ з хмарною інфраструктурою створює нові виклики, пов'язані з adversarial-атаками, проблемами конфіденційності та потребою у захисті гетерогенних і розподілених середовищ [4].

У відповідь на це виникає потреба у створенні інтегрованих архітектурних рішень, які поєднують хмарні сервіси, ШІ та засоби кіберзахисту в єдину масштабовану і керовану інфраструктуру [5]. Важливу роль у цьому відіграє концепція Zero Trust Architecture (ZTA), яка передбачає перевірку кожної дії незалежно від контексту. Ефективна кібербезпека має охоплювати як технічні (TLS, Post-Quantum Crypto, 2FA, SIEM), так і організаційні заходи [6]. Отже, науково-прикладна проблема полягає не лише у впровадженні окремих технологій, а у розробці цілісних, безпечних та адаптивних підходів до побудови КСМ, здатних відповідати вимогам сучасного цифрового середовища.

Аналіз останніх досліджень і публікацій. Стрімкий розвиток цифрових технологій, зокрема хмарних обчислень, IoT і гібридних мереж, кардинально трансформує архітектуру КСМ, водночас створюючи складні та швидкоплинні кіберзагрози. Це робить традиційні методи захисту застарілими та потребує нових гнучких підходів, серед яких особливу увагу привертає архітектура Zero Trust (ZTA). У поєднанні з технологіями ШІ, такими як машинне навчання та виявлення аномалій, ZTA дозволяє динамічно адаптувати політики безпеки до нових загроз, що особливо актуально в хмарних і розподілених середовищах.

Системи виявлення вторгнень (IDS), інтегровані з алгоритмами ШІ, є ключовими компонентами сучасної кібербезпеки [1]. Наприклад, у роботі Касонго С. (Kasongo S.) [7] описано IDS-платформу на основі рекурентних нейронних мереж (RNN), таких як LSTM і GRU, яка демонструє високу точність виявлення атак. Також застосування алгоритму XGBoost для вибору релевантних ознак дозволяє зменшити обчислювальне навантаження. Інше дослідження Маюранатан М., Сараванан С., Мутусенхіл Б. та Самудураї А. (Mayuranathan M., Saravanan S., Muthusenthil B., Samydurai A.) [8] пропонує гібридний підхід EOS-IDS із використанням глибоких мереж Кронекера (DKNN) для точного виявлення загроз у хмарному середовищі. Робота Луо Х. (Luo X.) [9] презентує адаптивну IDS-модель на основі нечіткої логіки, яка забезпечує гнучке реагування на вторгнення в режимі реального часу.

Серед сучасних підходів особливо ефективним вважається виявлення аномалій на основі мережевих потоків, що дозволяє відстежувати складні загрози, не помітні при аналізі окремих пакетів. У дослідженні Хефзіпах Дж., Валем Р., Шіла М. та Дханалакшмі Дж. (Hephzipah J., Vallem R., Sheela M. & Dhanalakshmi G.) [10] розроблено вдосконалену систему безпеки MMGT-ANN, засновану на штучній нейронній мережі з оптимізацією за теорією мінімаксних ігор, що забезпечує високу точність та швидке реагування на загрози.

Зростає популярність проактивних стратегій захисту, орієнтованих на передбачення загроз і динамічне оновлення політик безпеки. У роботі автора Вонг Й. (Wang Y.) [11] представлено інтелектуальну багаторівневу систему захисту в хмарі, яка об'єднує збір даних, аналіз загроз і адаптивний контроль доступу, що зменшує кількість помилкових спрацювань. Інше дослідження Пейді П. (Paidy P.) [12] досліджує адаптивне тестування безпеки в рамках DevSecOps, де інтеграція ШІ дозволяє автоматизувати тестування у реальному часі, реагуючи на нові вразливості. У роботі Зафера Ф. та Ахтара Ф. (Zafer F., & Akhtar F.) [13] запропоновано хмарне рішення з використанням ШІ для виявлення загроз у реальному часі, що дозволяє значно скоротити тривалість атак та операційні ризики.

Комбінування ZTA з ШІ також розглядається як революційний підхід до побудови сучасної безпеки КСМ. Дослідження Сайрай К. (Sairaj K.) [14] демонструє, що така архітектура перевершує традиційні стратегії за точністю виявлення загроз, швидкістю реакції та загальним рівнем захищеності системи.

Разом із тим, однією з ключових загроз для ШІ-систем залишаються змагальні атаки (adversarial attacks), які використовують майже непомітні зміни у вхідних даних для обману моделі. У роботі Вонг Й., Сан Т., Лі С., Юань Х. Та ін. (Wang Y., Sun T., Li S., Yuan X. Et al.) [15] здійснено комплексний огляд таких атак і методів захисту, зокрема з використанням регуляризації, виявлення аномалій і підвищення стійкості

моделей. Автори класифікують наявні рішення та пропонують ефективні підходи для підвищення надійності ШІ у системах безпеки.

Постановка завдання. Метою статті є комплексне дослідження сучасних підходів до побудови ефективних та безпечних комп'ютерних систем і мереж (КСМ) з урахуванням викликів цифрової трансформації. Зокрема, ставляться такі дослідницькі цілі:

– проаналізувати архітектурні рішення, що забезпечують гнучкість, масштабованість і надійність ІТ-інфраструктури, зокрема мікросервісну архітектуру (МСА) та сервісно-орієнтовану архітектуру (СОА);

– охарактеризувати роль хмарних технологій у забезпеченні масштабованості та економічної ефективності КСМ, а також виявити супутні ризики для кібербезпеки;

– дослідити сучасні підходи до кіберзахисту, зокрема застосування концепції Zero Trust Architecture, засобів шифрування, моніторингу та виявлення загроз;

– виявити переваги використання штучного інтелекту (ШІ) для оптимізації, управління та забезпечення безпеки КСМ, включаючи виявлення аномалій, прогнозування інцидентів і адаптивне управління;

– розробити інтеграційну концепцію побудови КСМ на основі об'єднання принципів СОА, Zero Trust Security та можливостей ШІ.

Виклад основного матеріалу. Побудова ефективних та безпечних КСМ вимагає комплексного підходу, що поєднує в собі технології, практики та постійну адаптацію до нових загроз. Основні напрямки включають архітектурні рішення, кібербезпеку, оптимізацію продуктивності та управління. Розглянемо кожен підхід окремо, де буде охарактеризовано архітектурні підходи, підходи щодо питань з кібербезпеки, підходи з використанням ШІ, що розглядається для оптимізації та управління ефективністю, а також інтелектуального управління КСМ.

1. **Архітектурні підходи.**

Мікросервісна архітектура (МСА). Одним із ключових напрямів у побудові ефективних комп'ютерних систем є використання МСА. Цей підхід передбачає розбиття монолітного додатку на сукупність малих, незалежних сервісів, кожен з яких реалізує окрему бізнес-функцію та взаємодіє з іншими сервісами через стандартизовані API або повідомлення.

Перевагою підходу МСА є можливість незалежної розробки, тестування, розгортання та масштабування окремих компонентів системи. Це значно підвищує гнучкість архітектури, дозволяє командам працювати автономно, сприяє оперативному оновленню сервісів та зменшує час виведення нових функцій на ринок. Крім того, підхід МСА забезпечує високу стійкість до збоїв, наприклад, у разі відмови одного з сервісів система в цілому продовжує функціонувати, обмежуючи область впливу інциденту. Такий підхід є критично важливим для розподілених систем, зокрема у хмарних обчисленнях, де забезпечення безперервності обслуговування користувачів має вирішальне значення.

Хмарні технології. ХТ є однією з важливої складових сучасної ІТ-інфраструктури, що забезпечує високу масштабованість, доступність та економічну ефективність. Залежно від потреб користувача чи організації використовуються а) публічні, б) приватні та в) гібридні хмарні інфраструктури, кожна з яких має свої переваги у контексті безпеки, контролю над даними та витрат.

На рис. 1 показано схему з основними принципи побудови архітектури хмарних обчислень, яка складається з моделей розгортання та основних послуг в залежності від користувацьких потреб. Цей рисунок візуалізує основні аспекти ХТ як фундаментальної складової сучасної ІТ-інфраструктури, що забезпечує високу масштабованість, доступність та економічну ефективність.

В центральній частині схеми відображено глобальний характер ХТ, що підкреслює їхню доступність з будь-якої точки світу. Збільшення та зменшення ресурсів, позначене розширювальними стрілками, ілюструє масштабованість. Елементи, що нагадують гроші, вказують на економічну ефективність, яка досягається завдяки моделі оплати за фактичне використання.

Рисунок розрізняє три основні моделі розгортання хмари, а саме:

– публічна хмара (Public Cloud) представлена хмарою, до якої підключається багато користувачів, символізуючи спільне використання ресурсів, яка є більш гнучкою та економічною, а також доцільною для некритичних додатків, розробки, тестування та швидкого масштабування;

– приватна хмара (Private Cloud) зображена більше як ізольована хмара в межах захищеного параметра, що підкреслює вищий рівень контролю, безпеки та відповідності регуляторним вимогам, оскільки інфраструктура виділена виключно для однієї організації;

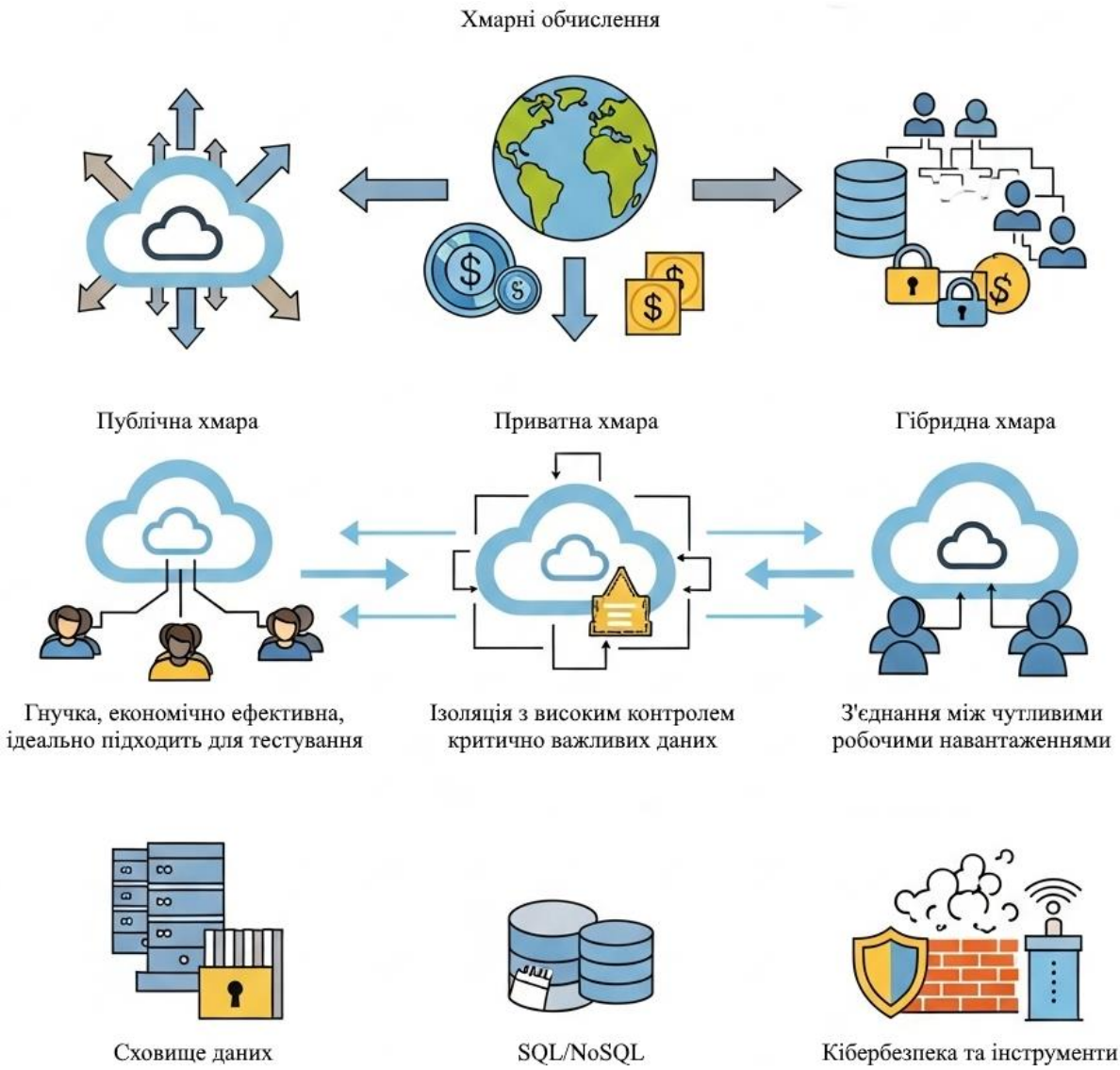

Рис. 1. Основні принципи архітектури хмарних обчислень з моделями розгортання та основними послугами

– гібридна хмара (Hybrid Cloud) представлена зв'язком між публічною та приватною хмарами, з потоками даних між ними, що демонструє її здатність поєднувати переваги обох підходів, дозволяючи розміщувати чутливі дані у приватній частині, а менш критичні навантаження – у публічній.

Сучасні хмарні провайдери надають широкий спектр сервісів, серед яких можна виділити: обчислювальні ресурси (compute) для розгортання і масштабування додатків; сховища даних для зберігання структурованої та неструктурованої інформації; керованої бази даних (SQL, NoSQL) з високою доступністю та надійністю; засоби та інструменти кібербезпеки, що містить шифрування, міжмережеві екрани, системи виявлення загроз, інструменти дотримання нормативів тощо.

Основні послуги провайдерів наведені в нижній частині схеми, які представляють ключові категорії сервісів, які надають хмарні провайдери. До них можна віднести:

– обчислювальні ресурси, які символізують собою іконки серверів, що вказують на віртуальні машини, контейнери та функції без серверів для розгортання та масштабування додатків;

– сховище даних, представлені у вигляді іконок сховищ або дисків, що відображають можливості для зберігання структурованої та неструктурованої інформації;

– керовані бази даних (SQL/NoSQL), позначені як бази даних, підкреслюючи високу доступність та надійність керованих рішень за допомогою SQL та NoSQL;

– засоби та інструменти кібербезпеки, відображені іконками щитів, замків та міжмережевих екранів, що вказує на інтегровані можливості шифрування, моніторинг загроз та інструментів відповідності нормативним вимогам.

На основі рис. 1 можна зазначити, що ХТ є комплексним та гнучким рішенням, оскільки забезпечується необхідна інфраструктура та сервіси для побудови сучасних, ефективних та безпечних КСМ.

Сервісно-орієнтована архітектура (СОА). СОА є архітектурним стилем для розробки програмного забезпечення, який фокусується на створенні додатків з використанням слабко пов'язаних незалежних компонентів, що називаються сервісами. Кожен такий сервіс виконує певну бізнес-функцію і взаємодіє з іншими сервісами за допомогою стандартизованих протоколів.

Основні принципи СОА пов'язані з: сервісами (які є самостійними, незалежними від програмних одиниць, які надають певну бізнес-функціональність, наприклад, сервіс з обробкою платежів); слабкою зв'язаністю (сервіси мінімально залежать один від одного, але зміна одного сервісу не повинна суттєво впливати на інші, що підвищує гнучкість системи); повторне використання (де однією з переваг є можливість повторного використання сервісів без написання коду з нуля); стандартизовані інтерфейси (сервіси спілкуються через чітко визначені, стандартизовані інтерфейси, що дозволяє їм взаємодіяти незалежно від мови програмування чи платформи); абстракція (внутрішня реалізація сервісу прихована від його споживачів). До переваг СОА можна віднести гнучкість та адаптивність, прискорення розробки, спрощення інтеграції та масштабованість.

Важливо розрізняти СОА та МСА, оскільки МСА є більш суворою, специфічною реалізацією принципів СОА. Мікросервіси ще більше «розбивають» додаток на дуже малі, незалежні сервіси, кожен з яких фокусується на одній функції та може розгортатися абсолютно незалежно. SOA ж є ширшою концепцією, яка може включати як великі, так і малі сервіси, і часто передбачає централізовані механізми комунікації. На рис. 2 показано порівняння МСА та СОА.

2. **Підходи щодо питань з кібербезпеки.**

Безпека є невід'ємною складовою проектування, розгортання та експлуатації сучасних комп'ютерних систем і мереж. Ще на етапі розробки має бути реалізований принцип безпеки за замовчуванням (Security by Design), що передбачає інтеграцію захисних механізмів у кожну фазу життєвого циклу системи. Це охоплює проведення аналізу загроз, моделювання ризиків та

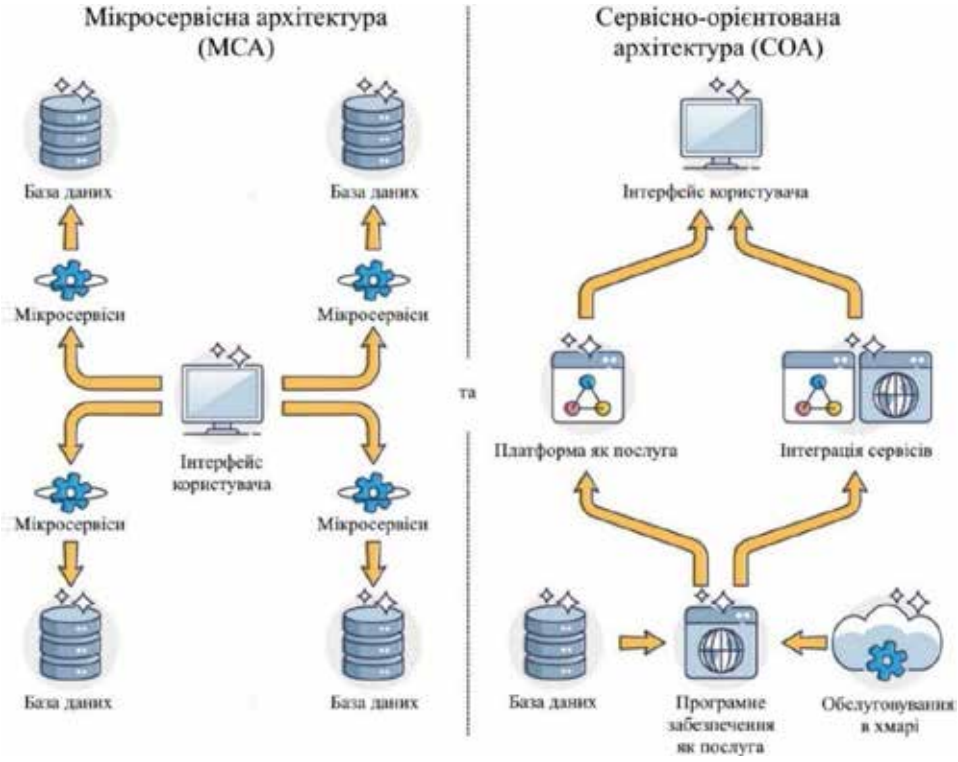

Рис. 2. Порівняння підходів побудови архітектури МСА та СОА для КСМ

проєктування захисту з урахуванням потенційних вразливостей з самого початку, а не як вторинний етап після реалізації функціональності.

Одним із базових підходів до забезпечення надійності є концепція нульової довіри (Zero Trust Architecture), що ґрунтується на принципі «нікому не довіряти, завжди перевіряти». У цій моделі кожен користувач, пристрій або сервіс незалежно від місця розташування повинен пройти сувору автентифікацію та авторизацію перед отриманням доступу до системних ресурсів. Такий підхід мінімізує ризики внутрішніх загроз і несанкціонованого доступу.

Важливе місце в системі кіберзахисту займає наскрізне шифрування даних як під час їх зберігання (на дисках), так і під час передачі мережею. Це дозволяє захистити конфіденційну інформацію навіть у випадку перехоплення чи несанкціонованого доступу до каналів зв'язку. Додатковим рівнем безпеки є багатофакторна автентифікація (БАФ), що передбачає використання кількох способів підтвердження особи (наприклад, поєднання пароля з кодом із SMS або біометричними даними), істотно ускладнюючи можливість злому облікових записів.

На рис. 3 показано архітектуру ZTA, яка на відміну від традиційних моделей, де ідентичність визначається на основі географічного положення або попередньо перевіреної аутентифікації, ZTA базується на припущенні, що порушення будуть, і їх необхідно контролювати.

З моменту первинної концептуалізації ZTA ця модель швидко поширилася в промисловості та урядових організаціях завдяки своїй здатності адаптуватися до ризиків у нових децентралізованих та гібридних схемах обчислювальних систем. Основні елементи ZTA включають контроль ідентичності та доступу, сегментацію та моніторинг, що відображає поточні мінливі та зростаючі вимоги підприємств до роботи з хмарними системами, збільшення кількості віддалених працівників та способи підключення до систем за допомогою Інтернету речей.

3. **Підходи з використанням ШІ.**

ШІ є важливим для побудови як ефективних, так і безпечних КСМ, оскільки його застосування охоплює широкий спектр можливостей. Окрім того, ШІ дозволяє вирішувати складні завдання, оскільки традиційні методи можуть бути надто трудомісткими або неможливими. Підходи використання ШІ охоплюють собою наступне оптимізацію та управління ефективністю, покращення безпеки, а також інтелектуальне управління мережею.

ШІ підвищує ефективність управління IT-ресурсами завдяки автоматизованому прогнозуванню потреб в обчислювальних можливостях (накопичувач, оперативна пам'ять, процесор тощо), що дозволяє динамічно масштабувати системи та оптимізувати використання інфраструктури, особливо в хмарних середовищах, знижуючи при цьому витрати. Крім того, алгоритми ШІ аналізують мережевий трафік у реальному часі, виявляють перевантаження та охоплюють процес маршрутизації даних найоптимальнішими шляхами, що підвищує пропускну здатність та зменшує затримки. Завдяки прогнозному обслуговуванню, яке базується на аналізі телеметрії обладнання та

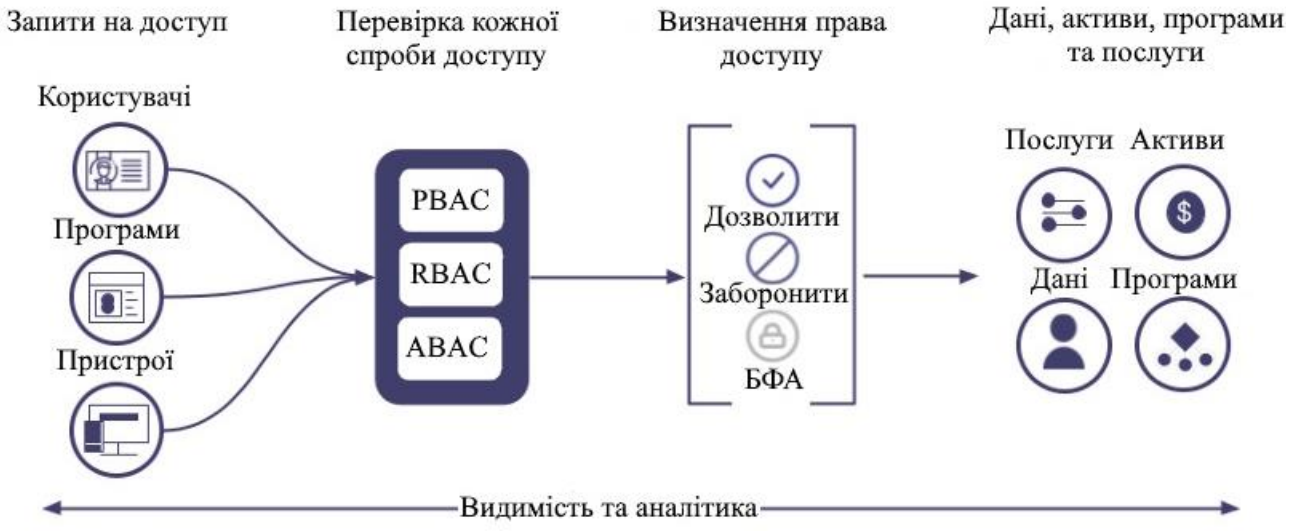

Рис. 3. Загальна архітектура Zero Trust

ПЗ, ШІ може передбачати потенційний збій в системі та проблеми з продуктивністю, що дозволяє здійснювати проактивне технічне обслуговування та мінімізувати час простою систем.

Штучний інтелект істотно покращує кібербезпеку завдяки здатності ефективно виявляти аномалії та нові загрози, виходячи з аналізу нормальної поведінки систем і мереж, що особливо важливо для боротьби з невідомими атаками, зокрема атаками нульового дня. Окрім виявлення, ШІ автоматизує реагування на інциденти, блокуючи шкідливий трафік, ізолюючи заражені пристрої або відкатуючи системи до безпечного стану. Завдяки аналізу великих обсягів журналів та подій безпеки, ШІ швидко корелює дані з різних джерел, виявляючи приховані закономірності та складні атаки, недоступні людині. Крім того, системи ШІ покращують автентифікацію, аналізуючи поведінкові патерни користувачів як додатковий фактор безпеки, та класифікують нові зразки шкідливого програмного забезпечення для швидкого виявлення їхніх характеристик. Важливою є і допомога ШІ в управлінні вразливостями, оскільки ШІ здатний розставити пріоритети та усунути їх, оцінюючи реальний ризик для конкретної інфраструктури.

Інтелектуальне управління мережею включає застосування ШІ для створення самостійно організованих мереж, які самостійно оптимізують та налаштовують свої параметри, значно знижуючи навантаження на адміністраторів, а також для прогнозного аналізу відмов шляхом вивчення історії збоїв і метрик продуктивності мережевого обладнання з метою своєчасного проактивного обслуговування. Таким чином, штучний інтелект виступає не просто додатковим інструментом, а є ключовим елементом сучасних методів побудови ефективних і безпечних комп'ютерних систем і мереж, що відкриває нові можливості для автоматизації, оптимізації та захисту.

4. **Інтеграція COA та ZTS з використанням ШІ для створення загальної концепції побудови ефективних та безпечних КСМ**.

Загальна концепція COA-ZTS на основі ШІ полягає в інтеграції принципів Zero Trust Security безпосередньо у сервісно-орієнтовані системи за допомогою штучного інтелекту, де ШІ забезпечує постійний моніторинг, аналіз поведінки користувачів і сервісів, автоматичне виявлення аномалій та адаптивне управління доступом у режимі реального часу.

Поєднання штучного інтелекту та архітектури Zero Trust може запропонувати новий погляд на вирішення існуючих слабких місць як традиційних, так і інноваційних систем безпеки. В даному випадку інтеграція штучного інтелекту в принципи ZTA може допомогти організаціям створити контекстну безпеку, яка змінюється в режимі реального часу відповідно до нових загроз. Штучний інтелект покращує ZTA шляхом автоматизації функції перевірки, визначення аномалій поведінки та встановлення нових політик на основі змінних ризикових середовищ.

На рис. 4 зображено концептуальну схему, яка ілюструє сучасні підходи до побудови ефективних та безпечних КСМ, який. візуалізує взаємозв'язок між ключовими технологіями та архітектурними принципами, які забезпечують масштабованість, надійність та захищеність ІТ-інфраструктури.

Рисунок складається з двох основних секцій, що відображають архітектурні підходи та аспекти безпеки. Верхня секція з архітектурними підходами (архітектура мікросервісів) відображає схему з представленою мережею взаємопов'язаних, але окремих блоків, які з'єднані лініями й взаємодіють між собою. Такий архітектурний стиль показує, як великий монолітний блок розбивається на малі незалежні сервіси, де кожен сервіс виконує одну конкретну бізнес-функцію і може бути розроблений, розгорнутий або масштабований окремо, що забезпечує високу гнучкість, стійкість до збоїв (де відмова одного сервісу не впливає на всю систему) та швидкість розробки.

Хмарне середовище показує взаємодію та потоки даних, що передбачає використання обчислювальних ресурсів (серверів, сховищ, баз даних) від зовнішніх провайдерів через Інтернет, де забезпечується висока масштабованість, доступність та економічна ефективність, що робить зручним для розгортання мікросервісів.

Контейнеризація в цій концепції висувається в якості технології, яка дозволяє упакувати додаток та всі його залежності (бібліотеки, середовище виконання) в ізольовані, портативні контейнери, що забезпечує уніфіковане середовище виконання для додатка незалежно від базової інфраструктури, що значно спрощує розгортання, масштабування та управління. Варто зауважити, що саме мікросервіси можуть доволі часто розгортатися саме в контейнерах (Docker), а потім керуються за допомогою оркестраторів (Kubernetes).

Нижня секція охоплює питання безпеки, де основна увага буде зосереджена на методах забезпечення безпеки в поєднанні з можливостями ШІ. В даному контексті використовується Zero Trust Security (ZTS), що є одним з сучасних підходів

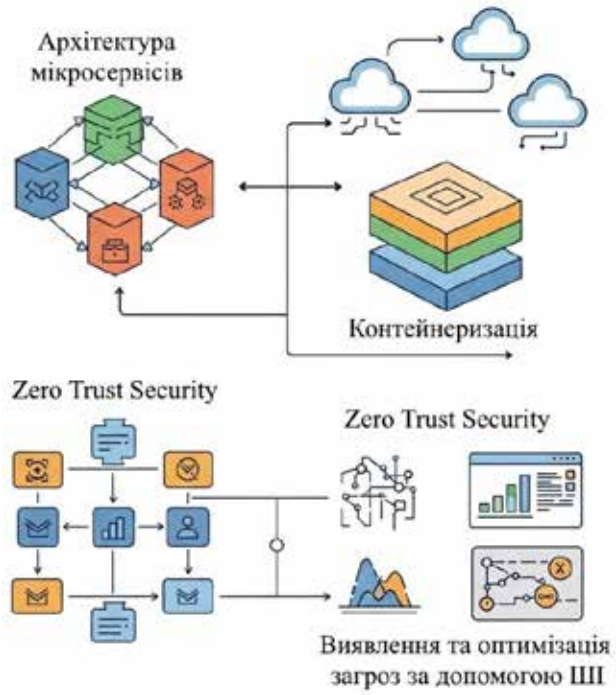

Рис. 4. Концептуальна схема сучасних підходів щодо побудови ефективних та безпечних КСМ

кібербезпеки, де кожен користувач, пристрій та додаток, незалежно від його розташування (навіть всередині мережі), має бути ретельно автентифікований та авторизований перед наданням доступу до будь-яких ресурсів. Діаграма показує складну мережу перевірок і потоків даних між користувачами, пристроями та системами, що ілюструє модель ZTS, де жодному елементу не довіряють за замовчуванням і вимагають постійної аутентифікації та контролю.

ШІ є важливою складовою в сучасній кібербезпеці та оптимізації, оскільки системи на основі ШІ здатні аналізувати величезні обсяги даних у реальному часі, виявляти аномалії та невідомі раніше загрози, прогнозувати потенційні ризики та автоматично реагувати на інциденти безпеки. ШІ також використовується для оптимізації розподілу ресурсів, балансування навантаження та покращення загальної продуктивності системи. Друга частина ілюструє застосування штучного інтелекту (ШІ) для виявлення загроз і оптимізації безпекових рішень.

Далі розглянемо основні переваги та недоліки кожного з підходів до концепції COA-ZTA на основі ШІ в табл. 1.

Висновки. В роботі проаналізовано сучасні підходи до побудови ефективних та безпечних комп'ютерних систем і мереж (КСМ) в умовах стрімкої цифрової трансформації та зростаючих кіберзагроз.

Розглянуто та оцінено ключові архітектурні рішення, такі як мікросервісна архітектура (МСА) та сервісно-орієнтована архітектура (СОА). Виявлено, що вони є критично важливими для забезпечення гнучкості, масштабованості та стійкості сучасних КСМ, дозволяючи системам адаптуватися до мінливих бізнес-вимог та технологічних викликів. Особливу увагу було приділено тому, як ці архітектури сприяють ефективному використанню хмарних технологій, надаючи високу доступність та економічну ефективність, при цьому враховуючи пов'язані з ними кіберризики.

Проведено аналіз сучасних стратегій кібербезпеки, з акцентом на принципах «безпека за замовчуванням» (Security by Design) та архітектури Zero Trust. Визначено, що ZTA є фундаментальним підходом для мінімізації ризиків несанкціонованого доступу та внутрішніх загроз шляхом постійної верифікації кожного користувача та сервісу. Також було вивчено роль таких механізмів, як багатофакторна автентифікація та наскрізне шифрування, у посиленні загального захисту системи.

Систематизовано та визначено ключові переваги використання ШІ для оптимізації функціонування та посилення кібербезпеки КСМ. З'ясовано, що ШІ може значно покращити автоматизацію управління ресурсами, прогнозування продуктивності та ефективне виявлення аномалій та нових кіберзагроз в реальному часі. Одночасно було

Таблиця 1

Характеристика переваг та недоліків концепції СОА-ZTA на основі ШІ

Підхід	Переваги	Недоліки
СОА (Сервісно-орієнтована архітектура)	1) Гнучка структура, яка дозволяє масштабування та повторне використання сервісів. 2) Полегшує інтеграцію між різними платформами. 3) Знижує залежність між компонентами системи.	1) Складність в управлінні великою кількістю сервісів. 2) Висока вартість впровадження та підтримки. 3) Вразливість до міжсервісних загроз без належної безпеки.
ZTA (Zero Trust Architecture)	1) Підвищений рівень безпеки завдяки постійній перевірці доступу. 2) Мінімізація ризиків внутрішніх та зовнішніх загроз. 3) Ефективна модель для хмарних і гібридних середовищ.	1) Висока складність впро-вадження в існуючу ІТ-інфраструктуру. 2) Потреба в постійному моні-торингу та аналізі. 3) Можливе навантаження на продуктивність через багатоетапну перевірку.
Штучний інтелект (ШІ)	1) Автоматизація виявлення загроз і реагування на них. 2) Оптимізація розподілу ресурсів та продуктивності систем. 3) Можливість прогнозування інцидентів у реальному часі.	1) Уразливість до змагальних атак (adversarial attacks). 2) Потреба у великих обсягах якісних даних для навчання моделей. 3) Високі обчислювальні витрати та складність реалізації.

розглянуто виклики, пов'язані з ШІ, такі як змагальні атаки, що підкреслює важливість розробки стійких та адаптивних ШІ-систем.

В якості основних результатів роботи розроблено та представлено інтегровану концепцію, яка поєднує СОА, архітектуру ZTA та принципи ZTS в поєднанні з ШІ. Обґрунтовано, що ця синергія дозволяє створювати високоадаптивні та захищені системи, де ШІ посилює ZTA шляхом автоматизації верифікації, виявлення аномалій поведінки та динамічного налаштування політик безпеки відповідно до контексту та змінних ризиків. Таким чином, досягнуто мети створення комплексного підходу, який забезпечує покращену стійкість та ефективність комп'ютерних систем і мереж у сучасному складному цифровому ландшафті.

Список літератури:

1. Янко А.С. Система захисту комп'ютерної мережі. *Системи управління навігації та зв'язку*. 2022. № 2 (68). С. 91–94. URL: https://doi.org/10.26906/SUNZ.2022.2.091 (дата звернення: 17.07.2025)

2. Кулаковська І. Ризики використання хмарних технологій. *Herald of Khmelnytskyi National University. Technical Sciences*. 2024. № 341(5). С. 45-52. URL: https://doi.org/10.31891/2307-5732-2024-341-5-6 (дата звернення: 17.07.2025)

3. Марченко К. М., Оришака О. В., Марченко А. К., Мельник А. М. Ризики впровадження штучного інтелекту в комп'ютерні системи. *Центральноукраїнський науковий вісник. Технічні науки*. 2022. Вип. 5(36). Ч. 1. С. 119-124. URL: https://doi.org/10.32515/2664-262X.2022.5(36).1.119-124 (дата звернення: 17.07.2025)

4. Jaber T. A. Artificial intelligence in computer networks. *Periodicals of Engineering and Natural Sciences*. 2022. № 10(1). С. 309-322. URL: https://doi.org/10.21533/pen.v10.i1.539 (дата звернення: 17.07.2025)

5. Hu Y., Kuang W., Qin Z., Li K., Zhang J., Gao Y., … & Li K. Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys (CSUR)*. 2024. № *55*(1). С. 1-36. URL: https://doi.org/10.1145/3487890 (дата звернення: 16.07.2025)

6. Ahvanooey M. T., Mazurczyk W., Zhao J., Caviglione L., Choo K. R., Kilger M., … & Misoczki R. Future of cyberspace: A critical review of standard security protocols in the post-quantum era. *Computer Science Review*. 2025. № 57. С. 100738. URL: https://doi.org/10.1016/j.cosrev.2025.100738 (дата звернення: 15.07.2025)

7. Kasongo S. M. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*. 2023. № 199. С. 113-125. URL: https://doi.org/10.1016/j.comcom.2022.12.010 (дата звернення: 16.07.2025)

8. Mayuranathan M., Saravanan S. K., Muthusenthil B., & Samydurai A. An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. *Advances in Engineering Software*. 2022. № 173, С. 103236. URL: https://doi.org/10.1016/j.advengsoft.2022.103236 (дата звернення: 16.07.2025)

9. Luo X. Model design artificial intelligence and research of adaptive network intrusion detection and defense system using fuzzy logic. *Journal of Intelligent & Fuzzy Systems*/ 2021. № 40(4). С. 8227-8235. URL: https://doi.org/10.3233/JIFS-189645 (дата звернення: 16.07.2025)

10. Hephzipah J. J., Vallem R. R., Sheela M. S., & Dhanalakshmi G. An efficient cyber security system based on flow-based anomaly detection using Artificial neural network. *Mesopotamian Journal of Cybersecurity*. 2023. С. 48-56. URL: https://doi.org/10.58496/MJCS/2023/009 (дата звернення: 15.07.2025)

11. Wang Y. Research on Intelligent Cybersecurity Protection System in Cloud Computing Environment. *Innovation in Science and Technology*. 2024. № *3*(4). С. 71-78. URL: https://www.paradigmpress.org/ist/article/view/1198 (дата звернення: 16.07.2025)

12. Paidy P. Adaptive Application Security Testing with AI Automation. *International Journal of AI, BigData, Computational and Management Studies*. 2023. № 4(1). С. 55-63. URL: https://doi.org/10.63282/3050-9416.IJAIBDCMS-V4I1P106 (дата звернення: 16.07.2025)

13. Zafer F., Akhtar F. Enhancing Cyber Resilience with AI-Powered Security: Cloud-Based Real-Time Threat Detection, Autonomous Response, and Multi-Layered Adaptive Defense for Cloud Security. 2025. URL: https://doi.org/10.13140/RG.2.2.14283.09766 (дата звернення: 15.07.2025)

14. Sairaj Kommera. "Enhancing Zero Trust Architecture with AI-Driven Threat Intelligence in Cloud Environments". *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. Vol. 11, no. 1. 2025. Pp. 1524-33. URL: https://doi.org/10.32628/CSEIT251112163 (дата звернення: 17.07.2025)

15. Wang Y., Sun T., Li S., Yuan X., Ni W., Hossain E., Poor H. V. Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey. *IEEE Communications Surveys & Tutorials*. 2023. № *25*(4). С. 2245-2298. URL: https://doi.org/10.1109/COMST.2023.3319492 (дата звернення: 17.07.2025)

Bolshakova O.O., Koshkin V.K., Aramian A.K., Bandura V.M., Yehanov O.Yu. MODERN APPROACHES TO BUILDING EFFICIENT AND SECURE COMPUTER SYSTEMS AND NETWORKS

The article analyzes current approaches to designing effective and secure computer systems and networks (CSN) in the context of digital transformation and the growth of cyber threats. It shows that the increase in data volumes, the development of cloud infrastructure, and the growing complexity of IT environments require the introduction of architectural solutions capable of ensuring flexibility, scalability, and cyber resilience. Microservice and service-oriented architecture are considered as the basis for building adaptive C&N that can be easily scaled and updated in line with changing business requirements. Cloud technologies are identified as a key element of modern IT infrastructure, but the risks they pose are highlighted: increased attack surface, data protection complications, and potential loss of control. In this regard, the feasibility of implementing the Security by Design principle, which provides for the integration of security at all stages of development, as well as the application of Zero Trust Architecture (ZTA), which ensures constant control and verification of access regardless of the source of the request, is justified. The role of mechanisms such as multi-factor authentication (MFA) and end-to-end encryption as means of increasing the cyber resilience of systems is analyzed in detail. Particular attention is paid to the use of artificial intelligence (AI) in resource management, failure prediction, and real-time anomaly detection. AI is considered as a tool for increasing the dynamism of protection systems, in particular through adaptive configuration of security policies and analysis of user behavior. At the same time, challenges related to competitive attacks that require robust algorithms are noted. The result of the study is a proposed integrated concept for building CSPs that synthesizes the capabilities of SOA, ZTA principles, and AI-based intelligent tools. This approach allows the creation of secure, adaptive, and effective systems for use in government, corporate, and cloud environments.

Key words: *microservice architecture, service-oriented architecture, cybersecurity, cloud technologies, artificial intelligence, Zero Trust.*

Дата надходження статті: 17.07.2025
Дата прийняття статті: 25.07.2025
Опубліковано: 27.10.2025