http://www.moderntechno.de/index.php/meit/article/view/meit42-02-074
DOI: 10.30890/2567-5273.2025-42-02-074

УДК: 004.056.5:004.78 + 004.8

STRATEGIES FOR PROTECTING HYBRID AND MULTI-CLOUD ENVIRONMENTS FOR INTELLIGENT DATA PROCESSING

СТРАТЕГІЇ ЗАХИСТУ ГІБРИДНИХ І МУЛЬТИХМАРНИХ СЕРЕДОВИЩ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ДАНИХ

Protsenko N.M. / Проценко Н.М.
Ph. D. (Econ.), Assoc. Prof. / к.е.н., доц.
ORCID: 0000-0002-7467-0491
Butenko T.A. / Бутенко Т.А.
Ph. D. (Econ.), Assoc. Prof. / к.е.н., доц.
ORCID: 0000-0002-7723-0790
Synyavina Y.V. / Синявіна Ю.В.
Ph. D. (Econ.), Assoc. Prof. / к.е.н., доц.
ORCID: 0000-0002-2015-810X
Syry V.M. / Сирий В.М.
senior lecturer/старший викладач
ORCID: 0000-0002-1060-1710
State Biotechnological University, Kharkiv, Alchevskikh, 44, 61002
Державний біотехнологічний університет, Харків, Алчевських, 44, 61002

Анотація. *Метою дослідження є стратегії захисту гібридних і мультихмарних середовищ для інтелектуальної обробки даних. Особливості таких архітектур потребують уніфікованого управління безпекою та комплексного підходу, що поєднує технічні, організаційні та правові заходи. Стратегії захисту повинні охоплювати всі елементи архітектури, передбачати автоматизацію управління безпекою, безперервний моніторинг та адаптацію до нових загроз, підтримувати баланс між безпекою та продуктивністю аналізу даних.*

Ключові слова: *інформаційні технології, захист інформації, хмарні обчислення, штучний інтелект, інтелектуальна обробка даних.*

Вступ

Всеосяжна цифровізація призвела до стрімкого зростання обсягів споживання даних. За даними статистичного порталу Statista у 2025 році глобальний обсяг створених, зібраних, скопійованих та спожитих даних сягне 181 ЗБ. Дослідження IDC показують, що приблизно 90 % світових даних було згенеровано протягом останніх двох років. Щодня генерується приблизно 402,74 млн ТБ даних [1].

На сьогодні обсяг, швидкість та різноманітність даних перевищують можливості традиційних систем їх обробки. Це вимагає більш потужних, гнучких і масштабованих технологій інтелектуальної обробки даних (Intelligent Data Processing – IDP).

Сучасний бізнес потребує аналітики в режимі реального часу, ефективного зберігання та надійних систем управління великими даними (Big Data). Майже 80 % організацій у всьому світі використовують інтелектуальний аналіз великих обсягів даних (Data Minning) для виявлення прихованих закономірностей, трендів, кореляцій та інсайтів. Це дозволяє приймати обґрунтовані рішення та оптимізувати бізнес-процеси [2-4].

Хмарні рішення відіграють центральну роль в інтелектуальній обробці даних, надаючи масштабовану, економічну інфраструктуру для зберігання, керування та аналізу величезних обсягів даних, що дозволяє швидко розгортати складні AI/ML моделі, забезпечує високу доступність, відмовостійкість та гнучкість, перетворюючи IT-інфраструктуру з капітальних витрат на керований сервіс (IaaS, PaaS, SaaS). Це дозволяє компаніям зосередитися на інноваціях, а не на обслуговуванні серверів.

Специфіка таких рішень, а саме розподілені зберігання та обробка даних, потребує розробки відповідних стратегій захисту та їх подальшої конкретизації у вигляді політик безпеки.

Основна частина

Стандартом сучасної інтелектуальної обробки даних є гібридні та мультихмарні середовища, оскільки вони дозволяють поєднувати безпеку локальних серверів із масштабованістю публічних хмар [5].

Гібридна хмара (Hybrid Cloud) дозволяє поєднати приватну інфраструктуру (on-premises) з однією публічною хмарою (наприклад, AWS або Azure). Це надає можливість зберігати чутливі дані локально, а обчислювальні потужності для навчання моделей орендувати в хмарі.

Мультихмара (Multi-cloud) передбачає використання послуг кількох хмарних провайдерів одночасно. Це виключає залежність від одного постачальника та забезпечує вибір найкращих інструментів для конкретних завдань (наприклад, Google Vertex AI – для ML, а Azure – для аналітики).

Такі архітектури дозволяють розподілене навчання моделей через можливість тренувати великі мовні моделі (LLM) на GPU-кластерах у хмарі,

використовуючи анонімізовані дані з локальних сховищ.

Особливістю гібридної інфраструктури є так звана «обробка на межі» (Edge Computing), коли попередня обробка даних виконується локально і лише найважливіша інформація передається в хмару для глибокого аналізу.

Гібридні та мультихмарні обчислення здатні забезпечити «суверенітет даних» (Data Sovereignty) шляхом локалізації зберігання даних у певній країні, тоді як аналітичні алгоритми можуть працювати глобально.

Для ефективної роботи в таких середовищах використовують оркестратори, які роблять інфраструктуру «невидимою» для розробника: Kubernetes – стандарт для розгортання контейнеризованих AI-застосунків у будь-якому середовищі; Google Anthos – платформа для управління застосунками в гібридних та мультихмарних сценаріях; Azure Arc, що дозволяє запускати сервіси Azure (наприклад, SQL чи ML) на будь-якій інфраструктурі; AWS Outposts, що надає нативні сервіси AWS для роботи безпосередньо у дата-центрі.

На сьогодні гібридні та мультихмарні обчислення надають такі переваги для бізнесу як: оптимізація витрат (використання Spot Instances провайдерів замість ресурсів на вимогу); відмовостійкість (якщо хмарний провайдер має технічні збої, інтелектуальні сервіси автоматично перемикаються на інші); швидкість інновацій (доступ до найсучасніших AI-чіпів через хмару без необхідності їх купівлі). Галузеві аналітичні звіти свідчать, що компанії, які впроваджують такі рішення досягають скорочення операційних витрат майже на 40 % [3].

Вкрай важливими є питання своєчасності та еластичності надання ресурсів. Оскільки хмарні обчислення дозволяють надавати ресурси на вимогу, підприємства можуть масштабувати свої задачі у відповідності до коливання робочого навантаження. Ця гнучкість необхідна для управління різним ступенем вимог до обробки даних у реальному часі. Організації можуть узгоджувати свою інфраструктуру з фактичним попитом, уникаючи надмірного виділення ресурсів та мінімізуючи витрати під час низької активності.

Проте, важливо враховувати і проблеми, які пов’язані з впровадженням IDP у хмарі, управлінням даними та їх безпекою. Це критично важливо для галузей,

що працюють з конфіденційною інформацією та зобов'язані забезпечувати відповідність процесів аналізу даних нормативним вимогам з кібербезпеки. Ці проблеми вимагають вибору надійних систем захисту, безперервного моніторингу й автоматизації прийняття рішень та значних інвестицій з боку провайдерів хмарних послуг [5].

На сьогодні актуальними трендами є: безпека хмарних додатків (Cloud-Native Security), де інструменти та практики безпеки інтегруються в процес розробки DevSecOps та забезпечують захист додатків із самого початку їх життєвого циклу; mesh-архітектури кібербезпеки (CSMA), які дозволяють інтегрувати різні хмарні та локальні рішення безпеки в єдину систему, забезпечувати централізоване управління та взаємодію; розширення концепції «нульової довіри» Zero Trust, що поширюється на ланцюги постачання хмарних сервісів та захист даних у гібридних і мультихмарних середовищах [6, 7].

Ключовими характеристиками гібридних чи мультихмарних середовищ є: можливість динамічно виділяти ресурси для Data Mining; розподілене зберігання даних, коли останні можуть знаходитися в різних локаціях та хмарних сервісах; інтеграція спеціалізованих технологій для машинного навчання, обробки великих даних та аналітики; складність управління, що потребує координування безпеки в різних середовищах з різноманітними інструментами.

Така розподілена архітектура створює унікальні виклики безпеці даних. Тут загрози конфіденційності зумовлені несанкціонованим доступом до чутливих даних під час передачі між хмарами, витоком даних через неправильно налаштовані сервіси та спільним використанням інфраструктури (multi-tenancy) у публічних хмарах. Загрози цілісності можуть витікати з модифікації даних під час передачі між компонентами системи та несумісністю форматів даних при інтеграції різних систем. Загрози доступності пов'язані з атаками типу «відмова в обслуговуванні» та залежністю від мережевого з'єднання між компонентами.

Стратегії захисту гібридних і мультихмарних середовищ можуть бути реалізовані за наступним планом.

1. Шифрування даних з використанням стандарту AES-256 для захисту

даних у сховищах, TLS/SSL для захисту передачі даних між компонентами системи, конфіденційних обчислень (confidential computing) для аналізу зашифрованих даних у процесі використання.

2. Керування ключами шифрування із застосуванням хмарних сервісів управління ключами (KMS), реалізацією власних рішень для повного контролю над ключами, розділенням ключів для різних середовищ та типів даних.

3. Контроль доступу та автентифікація через централізоване управління ідентичністю (Identity and Access Management), багатофакторну автентифікацію для критичних операцій, рольовий контроль доступу (RBAC) з мінімальними привілеями та аудит усіх операцій з даними.

4. Захист периметру та сегментація мережі за рахунок віртуальних приватних хмар (VPC) та підмереж для ізоляції компонентів, брандмауерів на рівні програм та мереж, VPN та приватних каналів для зв'язку між хмарами.

5. Захист даних при інтелектуальному аналізі через анонімізацію та псевдонімізація даних перед обробкою, диференційний захист приватності (Differential Privacy) для результатів аналізу та контроль використання даних у ML-моделях.

6. Безпечна розробка та інтеграція шляхом застосування DevSecOps підходу для вбудовування безпеки на ранніх етапах, сканування вразливостей у контейнерах та віртуальних машинах, безпечної інтеграції API між різними хмарними сервісами.

Для реалізації такого плану можна застосувати наступні технології та інструменти:

– *хмарні сервіси безпеки*: AWS Security Hub, Azure Security Center, Google Cloud Security Command Center, спеціалізовані сервіси для Data Loss Prevention (DLP);

– *контейнерна безпека*: захист Kubernetes-середовищ (Pod Security Policies, Network Policies) та сканування образів контейнерів;

– *інфраструктура як код (IaC)* зі статичним аналізом шаблонів Terraform, CloudFormation та політикою безпеки за замовчанням;

– *SIEM-системи* для гібридних середовищ з централізованим моніторингом подій безпеки з різних джерел та аналітикою поведінки для виявлення аномалій.

Правові та регуляторні аспекти стратегій безпеки гібридних і мультихмарних архітектур можуть базуватися на наступних засадах.

– Відповідність вимогам загального регламенту GDPR про захист даних громадян Європейського Союзу; федеральному закону США 1996 року HIPAA, що встановлює стандарти захисту конфіденційної медичної інформації пацієнтів; міжнародному стандарту безпеки PCI DSS від провідних платіжних систем (Visa, Mastercard, American Express та ін.), що встановлює обов'язкові вимоги для всіх організацій, які обробляють, зберігають або передають дані власників платіжних карток, з метою захисту їхньої конфіденційної інформації від шахрайства та кіберзагроз.

– Дані повинні задовольняти вимогам щодо їх зберігання у конкретних географічних регіонах, а політики безпеки узгоджуватися між різними юрисдикціями.

– Слід укладати чіткі угоди з постачальниками хмарних послуг та визначати відповідальність зацікавлених сторін за усі аспекти безпеки.

Майбутніми напрямами розвитку стратегій безпеки гібридних і мультихмарних середовищ для інтелектуальної обробки даних можуть бути:

- конфіденційні обчислення на апаратному забезпеченні для обробки зашифрованих даних (наприклад, Intel SGX, AMD SEV);
- безпека на основі машинного навчання з автоматичним виявленням загроз та аномалій;
- Zero Trust архітектури з постійною перевіркою довіри для всіх компонентів системи;
- захист усього життєвого циклу даних з інтеграцією захисту на всіх етапах – від збору до видалення.

Висновки

Інтелектуальна обробка даних та хмарні обчислення разом пропонують проривну синергію, яка має величезні перспективи для бізнесу. Гібридні та мультихмарні середовища у поєднанні зі штучним інтелектом і машинним навчанням здатні суттєво збільшити продуктивність аналізу великих обсягів інформації, забезпечити високу гнучкість і масштабованість інформаційних процесів.

Використання гібридних і мультихмарних інфраструктур для інтелектуальної обробки даних потребує уніфікованого управління безпекою, єдиної стратегії, яка вимагає комплексного підходу, що поєднує технічні, організаційні та правові заходи, охоплює всі компоненти архітектури, передбачає автоматизацію управління безпекою, безперервний моніторинг та адаптацію до нових загроз, підтримує баланс між безпекою та швидкістю аналізу даних.

Організації, які реалізують продуману стратегію захисту можуть безпечно використовувати переваги цих архітектур для інтелектуального аналізу із забезпеченням конфіденційності, цілісності та доступності даних.

Впровадження таких технологій стає каталізатором інновацій та започатковує новий рівень економічної ефективності та конкурентоспроможності сучасного бізнесу.

Література:

1. Bartley K. Big data statistics: How much data is there in the world? [Електронний ресурс]. URL: https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/.

2. Джулій В.М., Горбатюк О.М. Структура, функції системи інтелектуальної обробки даних. [Електронний ресурс]. URL: https://elar.khmnu.edu.ua/server/api/core/bitstreams/7625433e-0cfc-484d-b416-57fb0347a057/content.

3. Top 9 Data and Analytics Trends to Watch in 2026. [Електронний ресурс].

URL: https://intellias.com/data-analytics-trends/.

4. Mounica Achanta, «The Impact of Real-Time Data Processing on Business Decision – making.» International Journal of Scientific Research, vol. 13, no. 7, July. 2024. [Електронний ресурс]. URL: https://www.ijsr.net/archive/v13i7/SR24708033511.pdf.

5. The Best Cloud Trends for 2025 & the 5 Best Practices To Keep Up With Them. [Електронний ресурс]. URL: https://www.liquidweb.com/blog/cloud-trends/.

6. П’ять основних принципів безпеки гібридної хмари. [Електронний ресурс]. URL: https://corewin.ua/ceo-blog/hybrid-cloud-security/.

7. Безпека хмарних сховищ і технологій. [Електронний ресурс]. URL: https://datami.ee/ua/blog/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/.

Abstract. *The purpose of the study is to develop strategies for protecting hybrid and multi-cloud environments for intelligent data processing. The features of such architectures require unified security management and a comprehensive approach that combines technical, organizational, and legal measures. Protection strategies should cover all elements of the architecture, provide for automation of security management, continuous monitoring and adaptation to new threats, and maintain a balance between security and data analysis performance.*

Keywords: *information technology, information protection, cloud computing, artificial intelligence, intelligent data processing.*

Статтю відправлено: 26.12.2025