Лекція 7. Хмарні технології в корпоративних інформаційних системах

Поняття та моделі хмарних обчислень: SaaS, PaaS, IaaS. Переваги та ризики використання хмарних корпоративних систем. Безпека даних у хмарі. Браузерний доступ до корпоративних платформ як елемент сучасної IT-інфраструктури підприємства

Хмарні обчислення в корпоративних інформаційних системах (КІС) — це парадигма надання IT-ресурсів (обчислювальних потужностей, сховищ даних, додатків) як послуг через мережу Інтернет або локальну мережу. Замість утримання власної фізичної інфраструктури, бізнес орендує ресурси у провайдерів, що дозволяє гнучко масштабувати систему та оптимізувати витрати.

У КІС зазвичай виділяють три базові рівні надання хмарних послуг: SaaS, PaaS, IaaS.

https://onbiz.biz/cloud-computing-models/
https://www.sim-networks.com/ukr/blog/cloud-computing-service-models
https://www.youtube.com/watch?v=6_pLtA9OTNs

Слайд 1. Основні моделі обслуговування (Cloud Service Models)

IaaS (Infrastructure as a Service) – інфраструктура як послуга. Надає віртуалізовані обчислювальні ресурси: сервери, мережі та системи зберігання даних. Клієнт самостійно встановлює операційні системи та додатки.
Приклади: AWS, Microsoft Azure, Google Cloud Platform.

PaaS (Platform as a Service) – платформа як послуга. Надає готове середовище для розробки, тестування та розгортання власних корпоративних додатків без необхідності керувати базовою інфраструктурою.
Приклади: Google App Engine, Heroku.

SaaS (Software as a Service) – програмне забезпечення як послуга. Модель, за якої користувачі отримують доступ до готових корпоративних систем через браузер або API за передплатою.
Приклади: Microsoft 365, Salesforce, SAP ERP Cloud.

Популярні типи хмарних рішень:
ERP-системи: Управління виробництвом, фінансами, ресурсами (наприклад, SAP, Microsoft Dynamics NAV, BAS).

CRM-системи: Взаємодія з клієнтами та відстеження лідів (наприклад, HubSpot, Salesforce, Zoho).
https://shelfy.com.ua/categories/crm-systems/cloud/

Хмарні сховища: Google Drive, Dropbox, Microsoft OneDrive.

Віртуальні офіси: Windows 365, Google Workspace.

Хмарні провайдери та сервіси:
В Україні та за кордоном популярні як глобальні (AWS, Microsoft Azure, IBM), так і локальні провайдери (Tucha, GigaCloud, UCloud, Датагруп), які пропонують віртуальні сервери, сховища та спеціалізовані сервіси.

Слайд 2. Моделі розгортання (Cloud Deployment Models)

Вибір моделі залежить від вимог до безпеки та контролю над даними в компанії:
Приватна хмара (Private Cloud): Інфраструктура призначена виключно для однієї організації. Вона може перебувати у власному дата-центрі або у провайдера, але доступ до неї суворо обмежений. Забезпечує найвищий рівень безпеки.
Публічна хмара (Public Cloud): Хмарні ресурси належать сторонньому постачальнику і доступні для багатьох компаній одночасно. Це найбільш економний варіант з оплатою за фактичне споживання.
Гібридна хмара (Hybrid Cloud): Поєднання приватної та публічної хмар. Наприклад, критично важливі дані зберігаються в приватній хмарі, а обчислювальні піки обробляються ресурсами публічної.
Спільнотна хмара (Community Cloud): Інфраструктура, що спільно використовується кількома організаціями зі спільними інтересами (наприклад, державні органи або наукові установи).

tinyurl.com/vwunb45v

Слайд 3. Переваги та ризики для корпорацій

Переваги	Виклики та ризики
Економія (OPEX замість CAPEX): Відмова від купівлі дорогого обладнання.	**Залежність від інтернету:** Бе до КІС неможливий.
Масштабованість: Швидке додавання ресурсів під час пікових навантажень.	**Безпека та конфіденційність** даних на боці провайдера.
Мобільність: Доступ до корпоративних даних	**Складність міграції:** Перене

Слайд 4. Переваги та ризики використання хмарних корпоративних систем

Використання хмарних рішень у корпоративному секторі – це завжди баланс між швидкістю розвитку та контролем над даними. Нижче наведено детальний розбір плюсів та потенційних загроз.

Переваги (Pros)

Економічна ефективність (Зміна моделі витрат): Замість великих капітальних інвестицій у залізо (CAPEX), компанія переходить на щомісячні операційні платежі (OPEX). Ви платите лише за ті потужності, які реально використовуєте.

Масштабованість та гнучкість: Якщо бізнес різко зростає (наприклад, у сезон розпродажів), хмара дозволяє за лічені хвилини додати сервери чи пам'ять. Коли потреба зникає — ресурси так само легко вимикаються.

Мобільність та віддалена робота: Співробітники мають доступ до корпоративної системи з будь-якої точки світу та з будь-якого пристрою. Це критично для сучасних гібридних форматів роботи.

Швидке впровадження (Time-to-Market): Розгортання нової ERP чи CRM-системи в хмарі займає дні або тижні, тоді як закупівля та налаштування власних серверів може тривати місяцями.

Відмовостійкість (DR): Провайдери (як-от AWS чи Azure) мають систему резервного копіювання в різних географічних зонах. Якщо один дата-центр вийде з ладу, система автоматично переключиться на інший.

Слайд 5. Переваги та ризики використання хмарних корпоративних систем

Ризики (Cons)

Залежність від провайдера (Vendor Lock-in): перенесення величезної бази даних з однієї хмари в іншу — це складний і дорогий процес. Компанія стає «заручником» тарифів та технічних рішень конкретного постачальника.

Безпека та конфіденційність: зберігання даних на чужому обладнанні завжди несе ризик несанкціонованого доступу. Хоча провайдери мають потужний захист, людський фактор або вразливості в API залишаються загрозою.

Якість інтернет-з'єднання: робота хмарної КІС повністю залежить від стабільності мережі. Будь-які перебої у провайдера зв'язку паралізують роботу всього офісу.

Складність контролю витрат: без чіткого моніторингу легко «накрутити» рахунок за хмару (наприклад, забувши вимкнути тестові сервери), що може виявитися дорожчим за власне обладнання.

Юридичні та комплаєнс-ризики: законодавство деяких країн вимагає зберігати персональні дані громадян виключно на серверах усередині країни. Використання закордонних хмар може призвести до штрафів.

Слайд 6. Безпека даних у хмарі для корпоративних інформаційних систем

Безпека даних у хмарі — це не лише відповідальність провайдера, а й спільна стратегія захисту. Для корпоративних систем (КІС) діє модель **розподіленої відповідальності**: провайдер відповідає за безпеку самої хмари (залізо, мережі), а компанія — за безпеку даних усередині неї.

Ключові аспекти безпеки КІС у хмарі

1. Шифрування даних (Encryption)

Це фундамент захисту. Дані мають бути зашифровані на двох етапах:

Під час передачі (In-transit): захист каналів зв'язку між офісом та хмарою за допомогою протоколів TLS/SSL.

Під час зберігання (At-rest): шифрування баз даних та файлових сховищ на дисках провайдера.

2. Керування ідентифікацією та доступом (IAM)

У хмарних КІС діє принцип мінімальних привілеїв:

MFA (Мультифакторна автентифікація): обов'язкове підтвердження входу через додаток або SMS.

Рольова модель (RBAC): кожен співробітник має доступ лише до тих модулів системи, які потрібні для роботи.

Слайд 7. Безпека даних у хмарі для корпоративних інформаційних систем

3. Ізоляція ресурсів
У публічних хмарах використовується *мультиоренда* (декілька компаній на одному сервері). Для КІС критично важливо забезпечити логічну ізоляцію через віртуальні приватні мережі (**VPC**) та фаєрволи, щоб дані інших клієнтів провайдера не перетиналися з вашими.

4. Резервне копіювання та відновлення (Backup & DR)
Хмарні системи дозволяють автоматизувати створення бекапів. Важливо мати план **Disaster Recovery** — стратегію швидкого відновлення роботи КІС у разі кібератаки (наприклад, вірусу-шифрувальника) або технічного збою.

5. Комплаєнс та юридична безпека
Корпоративні дані часто підпадають під регулювання:
GDPR: захист персональних даних європейських користувачів.
PCI DSS: якщо КІС обробляє платежі картками.
Локальні закони: вимоги щодо фізичного розміщення серверів у певній країні.

Слайд 8. Основні загрози для хмарних КІС

Помилки в налаштуваннях: Найчастіша причина витоків (наприклад, відкритий доступ до сховища S3 для всіх в інтернеті).

Внутрішні загрози: Крадіжка даних власними співробітниками, які мають легітимний доступ.

Злам облікових записів: Якщо адміністратор не використовує MFA, вся КІС опиняється під загрозою.

Порада: Для максимальної безпеки корпорації часто обирають **гібридну модель** — найчутливіші дані залишаються на власних серверах, а загальні процеси виносяться в хмару.

Слайд 9. Браузерний доступ до корпоративних платформ як елемент сучасної IT-інфраструктури підприємства

Браузерний доступ (Web-based access) перетворив корпоративні інформаційні системи (КІС) з важких стаціонарних програм на гнучкі сервіси. Це ключовий елемент моделі **SaaS**, де браузер виступає універсальним клієнтом для ERP, CRM чи HRM-систем.

Слайд 10. Переваги браузерного доступу (Web-based access)

Кросплатформність та уніфікація
Адміністраторам не потрібно встановлювати окреме ПЗ на кожен комп'ютер. Система однаково працює на Windows, macOS, Linux або планшетах. Це знімає проблему сумісності версій.
Централізоване оновлення
Будь-які зміни, виправлення помилок або нові модулі впроваджуються на сервері. Користувач отримує оновлену версію просто після оновлення сторінки в браузері.
Зниження вимог до заліза (Thin Client)
Основні обчислення відбуваються в хмарі. Робоче місце співробітника може бути недорогим ноутбуком або «тонким клієнтом», оскільки браузер не потребує великих потужностей.
Zero Trust та безпека доступу
Сучасні системи використовують технології SSO (Single Sign-On). Співробітник один раз входить у корпоративний профіль і отримує доступ до всіх веб-ресурсів компанії без повторного введення паролів.

Слайд 11. Архітектурні особливості

Frontend (Клієнтська частина): Використовує сучасні фреймворки (React, Angular, Vue) для створення інтерфейсу, що не поступається за швидкістю десктопним програмам.

Backend (Серверна частина): Опрацьовує запити через API. Це дозволяє легко інтегрувати браузерну КІС з іншими сервісами (наприклад, поштою чи месенджерами).

Протоколи захисту: Весь трафік обов'язково шифрується через HTTPS, а сесії користувачів мають обмежений час життя для запобігання крадіжці даних.

Слайд 12. Виклики браузерного підходу

Кешування та витоки: Браузери можуть зберігати фрагменти конфіденційних даних у кеші або історії. Це вимагає налаштування спеціальних політик безпеки (наприклад, заборона збереження паролів).

Обмеження функціоналу: Деякі складні операції (наприклад, пряма робота зі специфічним периферійним обладнанням — сканерами, промисловими верстатами) складніше реалізувати через браузер, ніж через нативне ПЗ.

Підсумок: Браузерний доступ робить IT-інфраструктуру «невидимою» для користувача, дозволяючи зосередитися на бізнес-процесах, а не на технічних нюансах софту.

https://molodyivchenyi.ua/index.php/journal/article/view/6208
https://hub.kyivstar.ua/articles/hmarni-servisi-dlya-biznesu-oglyad-p-yati-rishen

Хмарні технології та сервіси - лекція 2. Типи хмар, IaaS, PaaS, SaaS
https://www.youtube.com/watch?v=MNrLXXQWBoc