Оцінка ризиків та політика інформаційної безпеки

1. Ідентифікація активів

Ключові активи компанії CloudTech Solutions

На основі описаної IT-інфраструктури, ключові активи можна визначити як наступні компоненти, які є критичними для надання хмарних послуг малому та середньому бізнесу:

Хмарні сервери – хостинг веб-застосунків, баз даних, CRM-систем та інших бізнес-застосунків для клієнтів.

Мережева інфраструктура – маршрутизатори, комутатори, файєрволи, системи IDS/IPS, VPN-доступ.

Системи зберігання даних – SAN та NAS для централізованого зберігання, резервного копіювання та відновлення даних.

Клієнтські застосунки – веб- та мобільні інтерфейси (Android, iOS) для доступу користувачів до сервісів.

Офісна IT-система – комп'ютери співробітників, локальні сервери, HR-системи, фінансовий облік, електронна пошта.

Актив	***Рівень критичності***	***Обґрунтування класифікації***
Хмарні сервери	*Високий*	*Ці сервери є основою бізнесу, оскільки безпосередньо хостять клієнтські дані та застосунки. Будь-який збій або компрометація призведе до зупинки сервісів для клієнтів, фінансових втрат та репутаційних ризиків. Розподіл по регіонах забезпечує відмовостійкість, але робить їх високопріоритетними для захисту.*
Системи зберігання даних	*Високий*	*Зберігають чутливі клієнтські та корпоративні дані. Витік або втрата даних може призвести до юридичних санкцій (наприклад, GDPR), штрафів та втрати довіри клієнтів. Резервне копіювання є ключовим, але вразливості в доступі посилюють критичність.*
Мережева інфраструктура	*Високий*	*Забезпечує безперервний доступ до всіх ресурсів. Компрометація (наприклад, через DDoS) блокує комунікації, впливаючи на операції та клієнтів. Як "ворота" до системи, вона є первинною лінією оборони.*
Клієнтські застосунки	*Середній*	*Дозволяють доступ користувачам, але не є ядром зберігання даних. Вразливості можуть призвести до фішингу чи неавторизованого доступу, але вплив обмежений порівняно з серверами (можна тимчасова ізоляція).*
Офісна IT-система	*Середній/ Низький*	*Підтримує внутрішні операції (HR, фінанси), але не безпосередньо впливає на клієнтські сервіси. Ризики обмежені внутрішніми процесами; низький рівень для не критичних компонентів, як пошта, але середній для локальних серверів через можливий вхідний вектор для атак.*

2. Ідентифікація загроз і вразливостей

Основні загрози та вразливості

На основі вхідних даних (інциденти, сканування вразливостей), ідентифіковано 5 основних загроз/вразливостей:

DDoS-атаки – перевантаження мережі для блокування доступу.
Витоки даних через неповну DLP-систему – несанкціоноване шеринг даних (наприклад, посилання на G-Drive).
Інфікування шкідливими програмами (malware) – віруси на офісних ПК та серверах.
Неправильне управління доступом – надмірні привілеї або слабка аутентифікація (виявлено в 20% серверів).
Неоновлене програмне забезпечення – вразливості середньої/високої критичності на хмарних серверах.

Оцінка вірогідності реалізації

Загроза/ Вразливість	***Вірогідність***	***Обґрунтування***
DDoS-атаки	*Середня*	*2 випадки на рік без наслідків, з ростом з 0 до 2 за 3 роки. Хмарні сервіси є привабливою метою для конкурентів чи хакерських груп, але існуючі IDS/IPS та файєрволи знижують ймовірність успіху.*
Витоки даних через неповну DLP	*Висока*	*5 випадків на рік стабільно (4-5 за 3 роки). Google DLP контролює шеринг, але не є повноцінним, що робить витоки через людський фактор (помилки співробітників) дуже ймовірними в хмарному середовищі.*
Інфікування шкідливими програмами	*Висока*	*15 випадків на рік, з невеликим зниженням (з 20). Захист кінцевих точок є на ПК, але не на всіх серверах; віддалена робота через VPN збільшує вектори атаки (фішинг, USB).*
Неправильне управління доступом	*Середня*	*Виявлено в 20% серверів під час сканування. MFA та політика паролів впроваджені, але розподілена інфраструктура ускладнює контроль, роблячи ймовірність середньою.*
Неоновлене програмне забезпечення	*Висока*	*20% серверів вразливі; регулярні оновлення не завжди вчасні в розподіленій системі, що робить це системною проблемою з високою ймовірністю експлуатації.*

3. Оцінка ризиків за методологією OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – це методологія, що фокусується на активах, загрозах та вразливостях з операційної перспективи. Вона включає етапи: ідентифікацію активів (виконано вище), профілювання загроз, ідентифікацію вразливостей та оцінку ризиків. Нижче – застосування до даних.

Тип загрози	*Частота (на рік)*	*Повторюваність (за 3 роки)*	*Аналіз*
DDoS-атаки	*2*	*Зростання (0 → 2)*	*Низька частота, але тенденція до збільшення вказує на ескалацію інтересу до хмарних сервісів. Ризик для мережі високий.*
Витоки даних	*5*	*Стабільна (4-5)*	*Висока повторюваність через неповну DLP; впливає на дані клієнтів, критичні активи.*
Malware-інфікування	*15*	*Зниження (20 → 15)*	*Найвища частота, але покращення завдяки оновленням ПЗ; все ж високий ризик для офісних систем та серверів.*
Неправильне управління доступом	*Не кількісно*	*Виявлено в скануваннях*	*Пов'язане з 20% серверів; повторюваність через людський фактор.*
Неоновлене ПЗ	*Не кількісно*	*Виявлено в скануваннях*	*Системна проблема, повторюється без автоматизованих оновлень.*

Аналіз вразливостей з сканувань
Сканування показало 20% хмарних серверів з вразливостями середньої/високої критичності:

- **Неправильне управління доступом**: Дозволяє ескалацію привілеїв, загрожує серверам та даним.
- **Неоновлене ПЗ**: Відкриті CVE (наприклад, в Apache чи MySQL), дозволяють RCE (remote code execution). Ці вразливості посилюють загрози malware та витоків, оскільки сервери – висококритичні активи.

Стратегії мінімізації ризиків

- **Для DDoS**: Автоматизоване масштабування трафіку (Cloudflare або AWS Shield) для розподілу навантаження.
- **Для витоків даних**: Повна DLP-система (наприклад, Microsoft Purview) з автоматизованим моніторингом шерингу.
- **Для malware**: Розширення EDR (Endpoint Detection and Response) на сервери, регулярні пентести.
- **Для доступу та оновлень**: Автоматизоване керування конфігураціями (Ansible) та CI/CD для оновлень ПЗ.

План заходів для покращення безпеки

Технічні заходи:

- Впровадити SIEM-систему (наприклад, Splunk) для централізованого моніторингу логів.
- Автоматизувати патч-менеджмент для серверів (щотижневі оновлення).
- Інтегрувати AI-детекцію аномалій в IDS/IPS.

Організаційні заходи:

- Проводити щорічні тренінги з фішингу для співробітників.
- Оновити план реагування на інциденти з симуляціями (tabletop exercises) раз на квартал.
- Аудит постачальників хмарних сервісів для відповідності ISO 27001.

Ці заходи знижують ризик на 30-50% за оцінкою OCTAVE, фокусуючись на операційних пріоритетах.

Ризик (загроза)	***Підхід до обробки***	***Обґрунтування***	***Конкретні заходи***
DDoS-атаки	*Зменшення*	*Ризик середньої вірогідності, але високий вплив на доступність; уникнення неможливе (хмарні сервіси критичні), передача – часткова, але компанія повинна контролювати.*	*Впровадити DDoS-мітигацію через провайдера (AWS Shield), моніторинг трафіку 24/7; бюджет: 10% від IT.*
Витоки даних	*Зменшення*	*Висока вірогідність та вплив на репутацію/штрафи; повне уникнення порушить бізнес, прийняття неприйнятне для клієнтських даних.*	*Розгорнути повну DLP (Symantec DLP) з правилами для G-Drive; аудит доступів щомісяця.*
Malware-інфікування	*Зменшення*	*Висока частота, але контрольована; передача на страхування кіберризику доповнює, але основний контроль внутрішній.*	*Розширити антивірус (CrowdStrike) на сервери; сегментація мережі для ізоляції інфікованих.*
Неправильне управління доступом	*Зменшення*	*Середня вірогідність, критичний для активів; уникнення – надто радикально (прийняття – ризиковано).*	*Впровадити RBAC (Role-Based Access Control) з автоматизацією; MFA для всіх доступів.*
Неоновлене ПЗ	*Уникнення/ Зменшення*	*Висока вірогідність, системний ризик; уникнення для критичних серверів шляхом міграції на managed services.*	*Міграція на оновлювані хмарні платформи (Azure Update Management); заборона неоновленого ПЗ.*