IThingy Labs — Whitepaper з політики інформаційної безпеки та конфіденційності AI-інфраструктури

Версія 1.0 | 2025

1. Загальні положення

Цей документ визначає політику безпеки, стандарти конфіденційності та підходи до захисту даних у діяльності компанії **IThingy Labs** — AI-native software house, який поєднує людську експертизу з автономними можливостями штучного інтелекту.

Метою документа є забезпечення довіри між компанією та її клієнтами, партнерами й співробітниками через впровадження системного підходу до управління інформаційною безпекою.

2. Місія та принципи діяльності

2.1. Місія

IThingy Labs створює ефективні, безпечні та технологічно прозорі рішення у сфері розробки програмного забезпечення, використовуючи моделі штучного інтелекту для підвищення продуктивності команд.

2.2. Основні принципи

1. **Пріоритет безпеки:** будь-яка автоматизація не може зменшувати рівень контролю доступу чи загрожувати інтелектуальній власності клієнта.
2. **AI як інструмент, а не ризик:** використання моделей відбувається лише у контрольованих середовищах, без підключення до відкритих API.
3. **Прозорість і відповідальність:** кожна дія в AI-інфраструктурі має трасованість і технічне підтвердження.
4. **Конфіденційність за замовчуванням:** Усі дані клієнтів, партнерів і співробітників обробляються відповідно до принципу *“Privacy by Design”*.

3. Технічна архітектура безпеки

3.1. AI-інфраструктура

Інфраструктура IThingy Labs базується на приватному кластері моделей, розгорнутих у внутрішній мережі компанії (Docker + Kubernetes + vLLM).

Моделі: **Mistral-7B-Instruct**, **Llama-3-Code**, **DeepSeek-Coder**.
Усі обчислення виконуються **локально або на виділених приватних VPS**, розташованих у ЄС.

3.2. Ізоляція клієнтських середовищ

Кожен клієнтський проєкт розміщується у власному контейнері, що має окремий файловий простір, мережеву ізоляцію та окремий AI-endpoint.
Між клієнтами **не існує жодного каналу обміну даними**.

3.3. Доступ та аутентифікація

1. Авторизація здійснюється через **JWT-токени** з двофакторною перевіркою.
2. Права доступу призначаються за ролями (RBAC).
3. Всі з’єднання — **TLS 1.3**, ключова довжина 4096 біт.
4. Усі дії користувачів журналюються в системі **AuditTrail**, яка зберігає лише метадані без змісту промптів.

4. Політика “Zero Retention & Zero Leak”

1. AI-моделі не мають постійної пам’яті. Кожен запит обробляється одноразово.
2. Дані промптів і відповідей не зберігаються у сховищі, якщо клієнт не вимагає зворотного.
3. Регулярне очищення тимчасових даних відбувається кожні **72 години**.
4. Заборонено підключення до публічних AI-провайдерів (ChatGPT, Claude, Gemini тощо).
5. Усі внутрішні API мають фільтрацію запитів на предмет передачі потенційно чутливих даних.

5. Управління ключами та токенами

1. Ключі доступу зберігаються у **HashiCorp Vault** з апаратним шифруванням (AES-256).
2. Доступ до Vault мають лише адміністратори безпеки з рівнем доступу L3.
3. Ключі змінюються не рідше ніж раз на 30 днів або після кожного інциденту.
4. Передача токенів через особисті канали зв'язку (месенджери, пошту) суворо заборонена.

6. Політика конфіденційності клієнтів

1. Всі коди, документи, дизайн-матеріали, API-ключі та бізнес-дані клієнта належать виключно клієнту.
2. IThingy Labs не має права використовувати їх поза межами проєкту без письмової згоди.
3. Копії даних, зроблені з метою резервування, зберігаються в зашифрованому вигляді не довше ніж 90 днів.
4. Після завершення контракту дані видаляються з усіх сховищ з підтвердженням клієнту.
5. У разі запиту клієнт може отримати акт про знищення копій та журнал доступу.

7. Відповідність міжнародним стандартам (Compliance)

Інфраструктура IThingy Labs розроблена з урахуванням:

1. **GDPR (EU Regulation 2016/679)** — принцип мінімізації даних і контроль суб'єкта.
2. **ISO/IEC 27001:2022** — управління ризиками інформаційної безпеки.
3. **SOC 2 Type I** — контроль доступу, журналювання, моніторинг та реагування.
4. **NIST SP 800-53** — рекомендації щодо захисту інформаційних систем.

8. Процедури моніторингу та реагування

8.1. Безперервний моніторинг

Система **Security Watchdog** здійснює контроль доступів у режимі 24/7, реєструє спроби несанкціонованих дій і повідомляє адміністратора безпеки.

8.2. Протокол реагування (SIP-01)

1. Виявлення інциденту.
2. Автоматична ізоляція контейнера.
3. Повідомлення керівництва та клієнта протягом **1 години**.
4. Технічне розслідування з формуванням звіту.
5. Усунення наслідків і перевірка системи.

9. Аудит і перевірка безпеки

1. Внутрішній аудит політики безпеки проводиться **щоквартально**.
2. Зовнішній аудит може ініціювати будь-який стратегічний клієнт.
3. Результати аудитів фіксуються у внутрішньому звіті з доступом “read-only”.

10. Відповідальність співробітників

1. Кожен співробітник зобов’язаний дотримуватись політики **AI Security Policy** та **Employee Confidentiality Agreement**.
2. За порушення — дисциплінарне стягнення, матеріальна відповідальність або розірвання контракту.
3. Повідомлення про потенційний інцидент має бути зроблене **протягом 60 хвилин** після виявлення.

11. Переваги для клієнтів та інвесторів

1. **Прозора архітектура безпеки.** Кожен етап контролю можна перевірити документально.
2. **Прискорений цикл розробки.** Завдяки AI-асистентам терміни скорочуються на 30–40 %.

3. **Вартість, що виглядає вигідно.** Загальна економія бюджету до 10 % за рахунок підвищення ефективності.
4. **Повна юридична захищеність.** Кожен проєкт супроводжується NDA і технічним актом про ізоляцію середовища.

12. Висновок

IThingy Labs поєднує інновації у сфері штучного інтелекту з класичними принципами інформаційної безпеки.
Наші системи побудовані за принципом **“Безпека — перед ефективністю”**, але завдяки AI ми досягаємо обох одночасно.

Ми переконані, що майбутнє аутсорсу — це **AI-native підхід**, де конфіденційність є нормою, а швидкість — конкурентною перевагою.

IThingy Labs — AI-Native Software House
contact@ithingy.ai