ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ТА БЕЗПЕКА ДАНИХ

Лекція 11

Організація безпечного впровадження ШІ в компанії

Освітня програма «Економіка і аналітика» · 1 курс · 4 кредити ECTS

ВІД ОСОБИСТОГО ДО СИСТЕМНОГО

Місток до організаційного рівня

- Лекція 10 показала індивідуальні загрози й особисті практики захисту
- Але окремі правильні дії співробітників не замінюють системного підходу організації

Без єдиної політики кожен працівник самостійно вирішує, як (і чи) безпечно користуватися ШІ — це і є ризик.

ВИЗНАЧЕННЯ

Що таке AI governance?

Сукупність політик, процесів, ролей і механізмів контролю, які визначають, як організація розробляє, впроваджує й використовує системи ШІ.

- Мета — не заборонити інновації, а забезпечити відповідність юридичним вимогам (лекції 7–9)
- Знижувати ризики (лекція 10) і водночас реалізовувати бізнес-цінність (лекція 6)

Без формального governance компанія покладається на випадкові рішення — це суперечить принципу підзвітності з лекції 7.

ПРИХОВАНА РЕАЛЬНІСТЬ

Проблема «тіньового ШІ» (Shadow AI)

Використання неавторизованих ШІ-інструментів для робочих задач без відома чи контролю ІТ-відділу й керівництва.

- Співробітники користуються ШІ незалежно від формальної політики — інструменти просто корисні й легкодоступні
- Ризик: чутливі корпоративні дані потрапляють у публічні ШІ-сервіси (пор. лекцію 8), а керівництво про це навіть не знає

Проста заборона — неефективна стратегія: працівники однаково користуватимуться, тільки прихованіше. Ефективніше — дати чіткі, реалістичні правила.

Що можна вводити в ШІ: матриця даних

Публічна інформація	→	Будь-який інструмент
Внутрішня операційна інформація	→	Лише схвалені корпоративні інструменти
Конфіденційна й персональні дані	→	Лише інструменти з підписаною DPA чи заборонено

Матриця має бути конкретною й застосовною за лічені секунди — інакше співробітники її ігноруватимуть.

Рівні дозволеного доступу до ШІ

1

Рівень 1: Публічні інструменти

Задачі без конфіденційних даних — дослідження, ідеї, публічний контент

2

Рівень 2: Корпоративні підписки

Внутрішня операційна робота з даними середньої чутливості

3

Рівень 3: Аудитовані рішення

Персональні дані, фінансові рішення, юридично значущий контент

ПОР. ЛЕКЦІЮ 7

Ролі в AI governance

Комітет з управління ШІ

ІТ, юридичний відділ, безпека, бізнес — визначає й переглядає політику

Відповідальний у підрозділі

Практичне дотримання політики в конкретному відділі

Кінцеві користувачі

Усі співробітники, що використовують ШІ у щоденній роботі

Організаційне віддзеркалення розмежування володілець/розпорядник/суб'єкт даних з лекції 7 — тепер застосоване до самого ШІ.

ДОКУМЕНТИ GOVERNANCE

Політика використання та перевірка постачальників

Acceptable Use Policy

- Перелік схвалених інструментів
- Класифікація дозволеного контенту
- Вимоги перевірки результату («чернетка, не фінал»)
- Процедура запиту нового інструменту

Vendor Vetting

- Умови обробки даних постачальника
- Відповідність AI Act за рівнем ризику
- Гарантії безпеки й доступності
- Договірна відповідальність за помилки

Політика повинна регулярно оновлюватися — крива Гартнера (лекція 3) означає, що статичний документ швидко застаріє.

СИСТЕМА, НЕ ПОДІЯ

Навчання співробітників

1

Онбординг

Базове навчання з політики для нових співробітників

2

Регулярне оновлення

Періодичне навчання з актуальними прикладами загроз

3

Рольове навчання

Поглиблені курси для тих, хто працює з чутливими даними

Моніторинг та аудит використання ШІ

Технічні механізми

Журналювання використання корпоративних інструментів; періодичні перевірки на тіньовий ШІ

Організаційні механізми

Регулярний перегляд реєстру схвалених інструментів; аудит відповідності політиці в підрозділах

Пряме застосування принципу підзвітності з лекції 7: організація повинна вміти довести дотримання політики, а не просто декларувати.

ПЛАН ДІЙ

Реагування на інциденти, пов'язані з ШІ

Канал повідомлення → **Визначений відповідальний** → **Розслідування** → **Сповіщення постраждалих і регуляторів**

Культура, що заохочує повідомляти про помилки без страху покарання, значно ефективніша за приховування — раннє виявлення завжди дешевше.

- Випадкове розкриття даних через чат-бот
- Помилкове чи упереджене автоматизоване рішення (пор. лекцію 4)
- Успішна атака з дипфейком чи клонованим голосом (пор. лекцію 10)

ПОР. ЛЕКЦІЮ 9

AI Act: обов'язки організацій-впроваджувачів

1. Використовувати систему відповідно до інструкцій розробника
2. Забезпечити людський нагляд на практиці, а не лише на папері
3. Моніторити роботу й повідомляти про виявлені проблеми
4. Зберігати автоматично згенеровані журнали роботи системи

Навіть компанія, яка сама не розробляє ШІ, а лише використовує готове рішення, несе власний, окремий набір юридичних обов'язків.

Культура відповідального використання ШІ

- **Психологічна безпека:**
  - можливість поставити питання чи повідомити про помилку без страху покарання
- **Приклад «згори»:**
  - керівництво, що ігнорує власну політику, підриває її дотримання іншими
- **Баланс інновацій і обережності:**
  - надто жорстко → тіньовий ШІ; надто ліберально → непередбачувані ризики

СИНТЕЗ

Чек-лист запуску AI governance

- ✓ Провести інвентаризацію фактичного використання ШІ (включно з тіньовим)
- ✓ Класифікувати дані компанії за чутливістю
- ✓ Сформувати міжфункціональний комітет з управління ШІ
- ✓ Розробити й затвердити політику прийнятного використання
- ✓ Запровадити процес схвалення нових інструментів
- ✓ Організувати системне навчання співробітників
- ✓ Впровадити моніторинг і план реагування на інциденти

ПІДСУМОВУЄМО

Що варто запам'ятати з цієї лекції

- AI governance — не заборона інновацій, а система політик, ролей і процесів
- Заборона ШІ штовхає до тіньового використання — краще дати чіткі правила
- Матриця даних і рівнева модель доступу роблять політику застосовною на практиці
- Компанія-впроваджувач має власні юридичні обов'язки за AI Act, навіть не розробляючи ШІ сама
- Культура психологічної безпеки — умова ефективного реагування на інциденти

Наступна (остання) лекція курсу: зведений чек-лист і підсумок перед контролем.