

Технології штучного інтелекту та безпека даних

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

Лекція 12. Підсумок курсу: зведений чек-лист і підготовка до контролю

Мета лекції: звести весь матеріал 11 попередніх лекцій у єдину практичну систему — наскрізні принципи й зведені чек-листи — і підготувати до підсумкового контролю. Ця лекція не вводить нового матеріалу, а синтезує вже вивчене.

Формат: на відміну від попередніх лекцій, тут немає «місточка до наступної теми» — натомість кожен розділ явно посилається назад на конкретні лекції курсу, щоб допомогти зібрати цілісну картину перед контролем.

1. Погляд назад: карта курсу

- Курс складався з двох рівних блоків по 6 лекцій: **технологічного** (лекції 1–6) і **безпекового** (лекції 7–11), а ця дванадцята лекція — підсумкова.
- Технологічний блок** пройшов шлях від «що таке ШІ» (лекція 1) через механіку генеративних моделей (лекція 2), побічні ефекти масового впровадження (лекція 3), надійність і обмеження (лекція 4), практичний інструментарій промпт-інжинірингу (лекція 5) до екосистеми застосувань в економіці (лекція 6).
- Безпековий блок** пройшов шлях від базових понять про дані (лекція 7) через приватність у діалозі з ШІ (лекція 8), право і відповідальність (лекція 9), кібербезпеку (лекція 10) до організаційного управління (лекція 11).

Ця остання лекція не вводить нового матеріалу, а зводить усе вивчене в єдину практичну систему й готує до підсумкового контролю.

№	Лекція	Ключовий фокус
1	Що таке штучний інтелект	ШІ $\supset$ ML $\supset$ DL $\supset$ Generative AI; статистичне передбачення тексту
2	Як ми навчили машину говорити	RLHF; чому мова живіша за формальні правила
3	Виклики масового ШІ	Крива Гартнера; когнітивний борг; людина-оператор
4	Надійність генеративного ШІ	Цільова функція генерації; галюцинації; чорна скринька
5	Промпт-інжиніринг	5 стовнів промпта; шаблони CRAFT, RACE, CARE та інші
6	Екосистема ШІ в економіці	Модальності, агенти, матриця цінність/складність
7	Дані як актив і ризик	Тріада CIA; класифікація даних; персональні дані за законом
8	Приватність у діалозі з ШІ	Шлях запиту; канали витоку приватності; GDPR, AI Act
9	Право і регулювання ШІ	Авторське право на контент; відповідальність за рішення
10	Кібербезпека, посилена ШІ	Фішинг, дипфейки, BEC-шахрайство; захист
11	Організація впровадження ШІ	AI governance; політики; ролі; тіньовий ШІ
12	Підсумок курсу	Наскрізні принципи; зведені чек-листи; підготовка до

№	Лекція	Ключовий фокус
		контролю

2. Наскрізнi теми, якi проходили через увесь курс

- **«Людина-оператор, ШІ-інструмент»** (вперше сформульовано в лекції 3, юридично закріплено в лекції 9): відповідальність за результат завжди лежить на людині, яка дала завдання чи ухвалила рішення.
- **Ефект чорної скриньки й довіра** (лекція 4, застосовано в лекціях 8–9): неможливість повністю пояснити рішення моделі ускладнює і довіру до неї, і юридичне обґрунтування відповідальності.
- **Дуальність технології** (вперше в лекції 4 — дипфейки, розгорнуто в лекціях 8 і 10): та сама технологія, що дає користь, дає і шкоду.
- **Дані як актив і ризик** (лекція 7, застосовано в лекціях 8–11): подвійна природа даних проходить через увесь безпековий блок.
- **Крива Гартнера і динамічність технології та регулювання** (лекція 3, повторено в лекціях 9 і 11): те, що правильно сьогодні, може застаріти завтра — і в технології, і в законі.

3. Зведений чек-лист: генеративний ШІ (лекції 1–6)

- Пам'ятайте: модель передбачає ймовірне продовження тексту, а не «знає» правильну відповідь (лекції 1–2).
- Впевнений тон ≠ правильна відповідь; перевіряйте важливі факти в незалежних джерелах (лекція 4).
- Формулюйте запит конкретно, з контекстом і форматом; ставтеся до першої відповіді як до чернетки (лекція 5).
- Обирайте рівень автономності інструменту (чат-бот проти агента) відповідно до ціни можливої помилки (лекція 6).
- Пам'ятайте про побічні ефекти масового використання — когнітивний борг, інформаційний шум (лекція 3).

4. Зведений чек-лист: дані і приватність (лекції 7–8)

- Перш ніж ділитися інформацією — класифікуйте її: публічна, внутрішня, конфіденційна чи персональна (лекція 7).
- Не вводьте в загальнодоступний ШІ те, що не хотіли б показати сторонньому (лекція 8).
- Перевіряйте, чи є в конкретного інструменту угода про обробку даних і чи можна вимкнути використання діалогів для тренування.
- Пам'ятайте про особливі категорії персональних даних (здоров'я, біометрія тощо) — вони вимагають ще більшої обережності.

5. Зведений чек-лист: право і кібербезпека (лекції 9–10)

- Документуйте творчий внесок при роботі зі ШІ, якщо плануєте комерційне використання результату (лекція 9).
- Перевіряйте умови використання (ToS) сервісу перед комерційним застосуванням контенту.
- Не довіряйте виключно тексту чи голосу як підтвердженню особи — використовуйте протокол зворотного дзвінка для фінансових запитів (лекція 10).
- Звертайте увагу на елементи терміновості й тиску в підозрілих повідомленнях — це класична ознака соціальної інженерії.

6. Зведений чек-лист: організаційний рівень (лекція 11)

- Компанія повинна мати чітку, конкретну матрицю «що можна вводити в які інструменти».
- Заборона без альтернативи веде до тіньового використання ШІ — краще дати реалістичні правила.
- Відповідальність за впровадження ШІ (навіть готового рішення) лежить на компанії-впроваджувачі, а не лише на розробнику технології.
- Психологічна безпека повідомляти про помилки — умова ефективного виявлення й виправлення проблем.

7. Єдина матриця рішень: коли довіряти, а коли перевіряти

- Синтез усього курсу можна звести до однієї практичної матриці на основі двох вимірів: **ціна помилки** (низька/висока) і **оборотність рішення** (легко виправити/важко виправити).

	Легко виправити	Важко виправити
Низька ціна помилки	Довіряйте ШІ без глибокої перевірки (напр. чернетка допису)	Помірна перевірка (напр. внутрішня нотатка, що піде в архів)
Висока ціна помилки	Перевірка людиною перед публікацією (напр. клієнтський лист)	Обов'язкова перевірка, документування, формальний процес (напр. фінансове рішення, персональні дані)

Ця матриця — практичний інструмент, який студенти можуть застосовувати в будь-якій новій ситуації, не пам'ятаючи напам'ять усі 11 лекцій.

8. Що залишилось за рамками курсу

- Курс свідомо уникав глибокого занурення в математику й код, зосереджуючись на концептуальному й управлінському рівні для економістів.
- Для тих, хто хоче поглибитися технічно: основи статистики й лінійної алгебри, конкретні архітектури нейронних мереж, практичне програмування.

- Для тих, хто хоче поглибитися юридично: детальне вивчення конкретного національного законодавства (не лише загальні принципи), спеціалізовані курси з ІТ-права.

Курс дав понятійний фундамент і практичні евристики — але не замінює спеціалізованого поглибленого вивчення для тих, хто працюватиме безпосередньо з розробкою ШІ чи юридичним супроводом складних кейсів.

9. Куди рухається технологія й регулювання

- Пор. лекцію 3 (крива Гартнера): будь-який прогноз про майбутнє ШІ має короткий термін придатності.
- Загальні напрямки, які варто відстежувати самостійно: розвиток ШІ-агентів і зростання їх автономності (лекція 6); подальша гармонізація законодавства різних країн з підходами на кшталт GDPR і AI Act (лекції 7–9); можлива поява нових регуляторних вимог щодо прозорості згенерованого контенту.

Практична порада на майбутнє: оскільки і технологія, і регулювання змінюються швидше, ніж будь-який курс встигає оновлюватися, найважливіша навичка — не запам'ятовані факти, а вміння застосувати наскрізні принципи (п. 2) до нової, ще не побаченої ситуації.

10. Як застосовувати ці знання в кар'єрі економіста чи аналітика

- **Особистий рівень:** як самому ефективно й безпечно користуватися ШІ в щоденній роботі.
- **Професійний рівень:** як оцінювати ШІ-рішення у своїй предметній галузі — фінанси, аналітика, маркетинг.
- **Управлінський рівень:** якщо доведеться брати участь у впровадженні ШІ чи розробці політик компанії.

Приклад: аналітик, що готує звіт за допомогою ШІ, застосовує чек-лист з п. 3 (перевірка фактів); той самий аналітик, оцінюючи новий ШІ-інструмент для відділу, застосовує чек-листи з пп. 5–6 (юридична перевірка, договірні умови).

11. Підготовка до підсумкового контролю

- Підсумковий контроль курсу перевірятиме розуміння понятійного апарату (лекції 1, 7), здатність застосувати наскрізні принципи (п. 2) до нових ситуацій, а не відтворення дослівних визначень.
- **Корисна стратегія підготовки:** пройтися контрольними питаннями наприкінці кожної лекції і спробувати відповісти на них без підказок конспекту.
- **Типи завдань, яких можна очікувати:** класифікація наведеної ситуації (напр. «до якого рівня ризику за AI Act належить ця система?»); аналіз кейсу із застосуванням кількох чек-листів одночасно; пояснення наскрізного принципу на новому прикладі.

12. Наскрізний приклад: розбір кейсу

Щоб побачити, як усі чек-листи працюють разом, розглянемо наскрізний приклад: **невеликий стартап хоче використати чат-бот на основі публічної LLM для попередньої обробки звернень клієнтів, включно з інформацією про платежі.**

- **Крок 1 — класифікація даних (лекція 7):** інформація про платежі клієнтів — це персональні й потенційно конфіденційні фінансові дані, тобто найвищий рівень чутливості з чотирьох.
- **Крок 2 — правило мінімізації (лекція 8):** дані такого рівня чутливості не можна вводити в загальнодоступну версію чат-бота без окремої угоди про обробку даних (DPA).
- **Крок 3 — договірна перевірка (лекція 9):** перш ніж підписувати з постачальником, потрібно перевірити умови обробки даних, гарантії безпеки й межі договірної відповідальності за помилку моделі.
- **Крок 4 — оцінка ризику за AI Act (лекції 8–9):** якщо чат-бот лише відповідає на загальні запитання — це «обмежений ризик» (потрібна прозорість); якщо ж він автоматично ухвалює рішення про повернення коштів — рівень ризику підвищується.
- **Крок 5 — організаційна політика (лекція 11):** стартап повинен формально визначити, до якого рівня доступу (1, 2 чи 3 з лекції 11) належить цей інструмент, і хто відповідає за його впровадження.
- **Крок 6 — матриця рішень (п. 7 цієї лекції):** оскільки ціна помилки висока (фінансові дані, можлива шкода репутації) і виправити наслідки складно (витік вже стався), цей кейс потрапляє в квадрант «обов'язкова перевірка, документування, формальний процес».

Висновок кейсу: жоден із чек-листів окремо не дає повної відповіді — лише послідовне застосування знань із кількох лекцій дає цілісну картину ризиків і необхідних дій. Саме такого типу аналізу очікує підсумковий контроль.

13. Заключне слово

- Генеративний ШІ — це не тимчасова мода, а технологія, з якою нинішні студенти працюватимуть протягом усієї кар'єри в тій чи іншій формі (пор. лекцію 3, п'ятий висновок).
- Курс не намагався зробити зі студентів технічних спеціалістів чи юристів — мета полягала в тому, щоб дати достатньо розуміння для відповідального, критичного й ефективного використання ШІ як інструменту економіста й аналітика.

Найважливіше практичне вміння, яке курс сподівається залишити: звичка ставити правильні питання перед тим, як довіритися відповіді ШІ, поділитися інформацією чи впровадити нове рішення — а не намагання запам'ятати кожен окремий факт.

Контрольні питання для самоперевірки студентів

- Оберіть будь-яку тему з блоку ШІ (лекції 1–6) і поясніть, як вона пов'язана з відповідною темою з блоку безпеки (лекції 7–11).

- Проаналізуйте уявний кейс (компанія хоче впровадити ШІ-чат-бот для консультування клієнтів банку) із застосуванням щонайменше трьох чек-листів із цієї лекції.
- Поясніть своїми словами матрицю «ціна помилки / оборотність рішення» і наведіть власний приклад для кожного з чотирьох квадрантів.
- Який наскрізний принцип курсу, на вашу думку, найважливіший для вашої майбутньої професійної діяльності? Обґрунтуйте.
- Назвіть одну тему, яка залишилась поза рамками курсу, але видається вам цікавою для подальшого самостійного вивчення.
- Сформулюйте для себе три конкретні дії, які ви будете практикувати після цього курсу при роботі зі ШІ.