Технології штучного інтелекту та безпека даних

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

Лекція 7. Дані як актив і ризик: типи даних, персональні дані за законом

Мета лекції: пояснити подвійну природу даних у сучасній економіці — цінний актив і водночас джерело серйозних ризиків — і закласти понятійний та юридичний фундамент (класифікація даних, тріада безпеки, визначення персональних даних, основи законодавства), на якому будуватимуться всі наступні лекції блоку про безпеку.

Зв'язок з попередніми лекціями: лекції 1–6 показали технологічні можливості й обмеження ШІ. Починаючи з цієї лекції, курс переходить до другого блоку — як безпечно й відповідально працювати з даними, які проходять через ці технології.

1. Місток від технологій до безпеки

- Впродовж лекцій 1–6 ми детально розібрали, що таке ШІ, як він працює, де помиляється і як його застосовують в економіці.
- Кожне з розглянутих застосувань — від чат-бота підтримки до фінансового скорингу (лекція 6) — працює з **даними**: даними клієнтів, співробітників, комерційною інформацією.
- Друга половина курсу відповідає на питання: що таке ці дані, чому вони настільки цінні й ризиковані одночасно, і як з ними поводитися правильно — організаційно та юридично.
- Ця лекція закладає понятійний фундамент, на якому будуватимуться всі наступні: класифікація даних, базова термінологія безпеки, основи законодавства про персональні дані.

2. Дані як економічний актив

- У сучасній економіці дані дедалі частіше називають «новою нафтою» — ресурсом, що набуває цінності через переробку (аналіз, поєднання з іншими даними, використання для навчання моделей).
- На відміну від фізичних активів, дані можна копіювати необмежену кількість разів практично без витрат, використовувати одночасно багатьма сторонами, і їхня цінність часто зростає з обсягом — так званий мережевий ефект: більше даних дають точніші прогнози й персоналізацію.
- Приклади: дата-брокери купують і продають споживчі профілі; технологічні компанії оцінюються ринком значною мірою через обсяг і якість зібраних даних про користувачів; для тренування сучасних ШІ-моделей (пор. лекцію 2) якісні дані стали дефіцитним і дорогим ресурсом.

Практичний висновок для економіста: дані варто розглядати як актив на балансі уваги компанії, навіть якщо бухгалтерськи вони рідко відображаються як такі.

3. Тріада інформаційної безпеки: конфіденційність, цілісність, доступність

- Класична модель «CIA-тріада» (Confidentiality, Integrity, Availability) — основа для розуміння, що взагалі означає «захищати дані».
- **Конфіденційність** — дані доступні лише тим, хто має на це право (протилежність — витік чи несанкціонований доступ).
- **Цілісність** — дані точні, повні й не змінені без дозволу (протилежність — підробка, помилкове чи зловмисне редагування).
- **Доступність** — дані та системи доступні уповноваженим користувачам тоді, коли потрібно (протилежність — збої, DDoS-атаки, шифрувальники-вимагачі).
- Ці три властивості часто конфліктують між собою: надмірні заходи конфіденційності (складні паролі, багатофакторна автентифікація) можуть знижувати доступність. Баланс між ними — управлінське рішення, а не суто технічне.

Дидактична примітка: *Хороша вправа для аудиторії: попросіть навести особистий приклад ситуації, де довелося пожертвувати зручністю (доступністю) заради безпеки (конфіденційності) — наприклад, складний пароль чи двофакторна автентифікація.*

4. Класифікація даних за чутливістю

- Практично будь-яка організація працює з даними різного рівня чутливості, і поводитися з усіма однаково — або небезпечно, або невиправдано дорого.

Рівень	Приклади	Наслідки витоку
Публічні	Прес-релізи, публічна звітність, маркетингові матеріали	Відсутні
Внутрішні	Внутрішні процедури, робоче листування	Помірні
Конфіденційні / комерційна таємниця	Фінансові показники до публікації, стратегічні плани, клієнтські бази, вихідний код	Серйозні
Персональні дані	Будь-яка інформація про фізичну особу	Юридичні (найсуворіші)

Практична порада: перш ніж вводити будь-яку інформацію в загальнодоступний ШІ-інструмент (пор. майбутню лекцію 8), варто подумки класифікувати її за цією шкалою.

5. Що таке персональні дані: визначення і приклади

- **Персональні дані** — будь-яка інформація, що відноситься до фізичної особи, яку прямо чи опосередковано ідентифіковано або можна ідентифікувати.
- Прямі ідентифікатори: ім'я, номер паспорта чи ІПН, номер телефону, домашня адреса.
- Непрямі ідентифікатори (стають персональними даними в комбінації з іншою інформацією): дата народження + поштовий індекс, IP-адреса, фотографія обличчя, геолокація пристрою, унікальний ідентифікатор пристрою чи облікового запису.

- Важливий нюанс: дані можуть бути **знеособленими (анонімізованими)** — тоді вони втрачають статус персональних, якщо повторну ідентифікацію особи справді неможливо здійснити розумними зусиллями.
- **Псевдонімізація** (заміна імені на код) — це НЕ повна анонімізація: такі дані все ще вважаються персональними, якщо ключ де-псевдонімізації існує.

Приклад із життя студента: список учасників групового проєкту з іменами й email — це вже персональні дані; той самий список, зведений до узагальненої статистики без імен, — уже ні.

6. Особливі категорії персональних даних

- Деякі категорії персональних даних отримують посилений правовий захист через високий потенціал шкоди в разі витоку чи зловживання.
- До таких категорій традиційно відносять: дані про стан здоров'я, біометричні дані (відбитки пальців, скани обличчя, голос), генетичні дані, дані про расове чи етнічне походження, політичні погляди, релігійні переконання, членство у профспілках, дані про сексуальне життя чи орієнтацію.
- Обробка таких даних, як правило, вимагає додаткових підстав (явна згода, законодавчо визначені виключення) і посилених заходів захисту порівняно зі «звичайними» персональними даними.

Приклад ризику саме для теми курсу: якщо студент чи співробітник вводить у загальнодоступний чат-бот медичну довідку «для перевірки формулювань» — це вже може бути передачею особливої категорії персональних даних третій стороні (лекція 8 розбере це детальніше).

7. Правове регулювання в Україні: Закон «Про захист персональних даних»

- В Україні базовим документом є Закон України «Про захист персональних даних» (№2297-VI, ухвалений 2010 року, з подальшими змінами).
- Закон визначає персональні дані, встановлює права суб'єктів даних, обов'язки тих, хто обробляє дані (володільців і розпорядників), і повноваження органу контролю.
- Україна також рухається в напрямку гармонізації з європейським регулюванням (GDPR) у межах євроінтеграційного курсу — тому багато принципів, які ми розглянемо, збігаються з європейськими, хоча деталі правозастосування різняться.

Дидактична примітка: *На момент підготовки цього курсу тривають законодавчі процеси з оновлення українського законодавства про захист даних для більшого узгодження з GDPR — тому варто перевіряти актуальний стан законодавства окремо, якщо це критично для конкретної практичної ситуації.*

8. Основні принципи обробки персональних даних

Незалежно від конкретної юрисдикції, сучасне законодавство про персональні дані спирається на спільний набір принципів:

Принцип	Що означає
Законність і прозорість	Обробка має правову підставу; суб'єкт даних розуміє, як дані використовують
Обмеження мети	Дані збираються для конкретної, заздалегідь визначеної мети
Мінімізація даних	Збирається лише те, що справді необхідно для мети — не «про всяк випадок»
Точність	Дані точні й актуальні; неточні — виправляються чи видаляються
Обмеження зберігання	Дані не зберігаються довше, ніж потрібно для мети обробки
Цілісність і конфіденційність	Належні технічні й організаційні заходи захисту (пор. тріаду CIA)
Підзвітність	Організація повинна вміти довести дотримання всіх принципів, а не лише декларувати

9. Ролі: володілець, розпорядник і суб'єкт даних

- **Суб'єкт персональних даних** — фізична особа, якої стосуються дані (наприклад, клієнт, співробітник, студент).
- **Володілець персональних даних** — фізична чи юридична особа, яка визначає мету й засоби обробки даних (наприклад, сама компанія-роботодавець чи університет).
- **Розпорядник персональних даних** — особа, якій володілець доручив обробку даних від свого імені (наприклад, хмарний сервіс, що зберігає дані компанії на своїх серверах, чи ШІ-сервіс, що обробляє введений текст).

Це розмежування критично важливе для практики роботи зі ШІ: коли компанія вводить персональні дані клієнтів у сторонній ШІ-інструмент, вона не перестає бути володільцем цих даних і залишається відповідальною за їх захист, навіть якщо технічну обробку виконує зовнішній розпорядник (постачальник ШІ-сервісу).

10. Права суб'єкта персональних даних

- **Право на доступ** — знати, чи обробляються твої дані, і отримати їх копію.
- **Право на виправлення** — вимагати виправлення неточних даних.
- **Право на видалення** («право бути забутим») — вимагати видалення даних за певних умов.
- **Право на заперечення** — заперечити проти певних видів обробки (наприклад, для маркетингових цілей).
- **Право на обмеження обробки** — тимчасово «заморозити» обробку даних у спірних ситуаціях.
- **Право на портативність даних** — отримати свої дані у зручному форматі для передачі іншому постачальнику послуг (де застосовно).

Ці права безпосередньо стосуються студентів як споживачів цифрових сервісів, включно з ШІ-інструментами: варто знати, що можна вимагати від постачальника щодо власних даних.

11. Дані як ризик: чому витік даних дорого коштує

- Витік персональних чи конфіденційних даних має щонайменше три виміри наслідків для організації.
- **Юридичний вимір** — штрафи регуляторів, судові позови від постраждалих осіб, обов'язок публічно повідомити про витік (у багатьох юрисдикціях це законодавчо закріплений обов'язок).
- **Фінансовий вимір** — прямі витрати на розслідування інциденту, усунення вразливості, компенсації постраждалим, зростання страхових премій на кіберризики.
- **Репутаційний вимір** — втрата довіри клієнтів і партнерів, що часто має довші й важче вимірювані наслідки, ніж прямі штрафи.

Важливо: ці ризики стосуються не лише великих корпорацій — будь-яка організація, включно з малим бізнесом чи навіть навчальним закладом, що обробляє персональні дані, потенційно перебуває під ризиком.

12. Зв'язок зі ШІ: чому тема даних стала критичною саме зараз

- Генеративний ШІ загострив тему захисту даних одразу з кількох напрямків, які ми вже розглядали технологічно (лекції 1–6), а тепер розглянемо з погляду ризику.
- **Навчальні дані** (лекція 2, RLHF): мовні моделі тренуються на величезних масивах тексту, зібраних з інтернету й діалогів користувачів — питання, чи потрапляють туди персональні дані і на яких підставах, залишається предметом активних судових суперечок у різних юрисдикціях.
- **Введені дані** (тема лекції 8): кожен запит користувача до чат-бота потенційно містить персональну чи комерційно чутливу інформацію, яка залишає межі організації.
- **Упередженість** (лекція 4): якісні, репрезентативні й водночас етично зібрані дані — дефіцитний ресурс, тому спокуса використовувати «все, що є під рукою», включно з даними сумнівного походження, зростає.

Висновок: тема захисту даних — це не окрема від теми ШІ дисципліна, а необхідна умова відповідального використання ШІ, яку курс тепер розглядає системно.

13. Практичний чек-лист класифікації даних

Перш ніж працювати з будь-яким набором інформації (зокрема, перед тим як ввести її в ШІ-інструмент), корисно поставити собі кілька запитань:

- Чи стосується ця інформація конкретної фізичної особи, яку можна ідентифікувати прямо чи опосередковано?
- Якщо так — чи належить вона до особливої категорії (здоров'я, біометрія, політичні/релігійні погляди тощо)?

- Чи є в мене законна підстава й дозвіл використовувати ці дані саме так, як я планую?
- Чи є ця інформація комерційною таємницею чи конфіденційною діловою інформацією, навіть якщо вона не є персональними даними?
- Якби ця інформація стала публічною завтра, які були б наслідки — для мене, для компанії, для людини, якої вона стосується?

Якщо на будь-яке з цих питань відповідь викликає сумнів чи занепокоєння — це сигнал зупинитися і проконсультуватися, перш ніж ділитися інформацією з третіми сторонами, включно зі ШІ-сервісами.

Місток до наступної лекції: ми розібрали, що таке дані, чому вони цінні й ризиковані, і які базові юридичні поняття та принципи регулюють роботу з персональними даними. Наступна лекція застосовує ці поняття безпосередньо до діалогу з генеративним ШІ: куди насправді йдуть введені дані, хто їх бачить, і як мінімізувати ризик випадкового розкриття чутливої інформації через звичайний чат з ШІ-асистентом. Це тема лекції 8.

Контрольні питання для самоперевірки студентів

- Поясніть своїми словами, чому дані водночас є активом і ризиком для організації.
- Наведіть приклад для кожного з трьох елементів тріади CIA з власного досвіду (навчання, підробіток тощо).
- Класифікуйте за рівнем чутливості: (а) розклад занять групи, (б) власна залікова книжка, (в) свій список контактів у телефоні.
- Чим псевдонімізація відрізняється від анонімізації даних? Чому це розрізнення юридично важливе?
- Поясніть різницю між володільцем і розпорядником персональних даних на прикладі університету, що використовує хмарний сервіс для зберігання оцінок студентів.
- Яким із прав суб'єкта персональних даних ви скористалися б, якби дізналися, що компанія зберігає застарілу інформацію про вас? Обґрунтуйте.