

ЗАТВЕРДЖЕНО

Рішення правління АТ «НСТУ»

від 10 лютого 2024 року № 4/4

**Принципи використання
штучного інтелекту в АТ «НСТУ»**

1. Загальні положення

Акціонерне товариство «Національна суспільна телерадіокомпанія України» (далі – АТ «НСТУ», Суспільне) з метою реалізації Стратегії розвитку Національної суспільної телерадіокомпанії України на 2023–2025 роки, затвердженої рішенням Наглядової ради АТ «НСТУ» від 26.04.2023 № 77 (далі – Стратегія), місії Суспільного, враховуючи Концепцію розвитку штучного інтелекту в Україні, схвалену розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р, планує впровадження інноваційних інформаційних технологій у роботі, зокрема через використання штучного інтелекту (далі – ШІ).

Суспільне прагне позитивно вплинути на розвиток інформаційних технологій у медіа та поширення практик відповідального використання ШІ. Також АТ «НСТУ» очікує, що впровадження інструментів ШІ зробить ефективнішими виробничі процеси створення та дистрибуції контенту.

Використання ШІ Суспільним ніколи не має ставити під загрозу довіру суспільства до АТ «НСТУ». Будь-які технологічні рішення мають ухвалюватися з огляду на пріоритети Суспільного: збереження й поглиблення довіри суспільства, тісніша взаємодія із суспільством на засадах незалежної та добросовісної журналістики, виробництво контенту, спрямованого на поширення достовірної та збалансованої інформації про Україну й світ, зміцнення української мови та культури, особистості й народу України.

Суспільне усвідомлює, що розвиток ШІ та, зокрема, поява генеративного штучного інтелекту (Generative Artificial Intelligence) створюють нову хвилю технологічних інновацій, що вплинуть майже на всі сфери людської діяльності.

Суспільне досліджуватиме, як можна використовувати ШІ в роботі для реалізації Стратегії, місії та головної мети діяльності АТ «НСТУ», а саме: задоволення інформаційних і культурних потреб суспільства, залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань, забезпечення національного діалогу, сприяння формуванню громадянського суспільства, забезпечення права кожного на свободу думки та слова, на отримання повної, достовірної та оперативної інформації, відкрите й вільне обговорення суспільних питань.

Суспільне вивчатиме походження рішень на базі ШІ з метою запобігання використанню редакціями рішень, із розробленням та використанням яких асоційовані ризики підзвітності, добросовісності та безпеки обробки даних. За результатами досліджень Суспільне формуватиме й регулярно оновлюватиме регламентний перелік рекомендованих і нерекomenдованих рішень, інструментів, моделей та сервісів на базі ШІ для застосування редакціями, з якими будуватиметься робота на зазначених нижче принципах.

2. Принципи використання ШІ в АТ «НСТУ»

1. Прозорість та відповідальність.

У разі використання ШІ для виробництва контенту Суспільне завжди повідомлятиме про це користувачів на тій платформі, де представлений цей контент. За кожним елементом контенту, що створений за допомогою ШІ, стоїть людина, яка несе відповідальність за кінцевий результат і відповідність контенту вимогам законодавства, редакційним засадам, редакційному статуту АТ «НСТУ» і стандартам інформаційного мовлення АТ «НСТУ».

2. Ефективність.

Суспільне використовуватиме ШІ, щоб вивільнити ресурси журналістів і працівників творчих підрозділів для виробництва контенту. Команда Суспільного за допомогою ШІ автоматизує у своїй роботі такі процеси: транскрибування (розшифрування) аудіо / відео, субтитрування, озвучування, пошук та збір інформації, формування чернеток за шаблоном на основі цифрових даних, аналіз великих масивів даних з метою виявлення тенденцій, закономірностей, гіпотез, що можна використати в роботі з аналітичними матеріалами та розслідуваннями, перевірка фактів, переклад. Усі перелічені процеси перевірятимуться та/або адаптуватимуться людиною.

3. Доцільність.

З огляду на дотримання стандартів журналістики АТ «НСТУ» вирішуватиме, чи сприятимуть ті чи інші рішення оптимізації роботи команди Суспільного. АТ «НСТУ» не використовуватиме інструменти ШІ, які несуть потенційні ризики для подання інформації та можуть призвести до створення «інформаційних бульбашок», упередженості та ін. Суспільне також відмовляється від інструментів, доцільність використання яких не виправдана витратою ресурсів і часу.

4. захист даних користувачів.

Якщо Суспільне збиратиме персональні дані користувачів, то водночас інформуватиме, які саме дані збирає і як вони використовуватимуться. Крім того, Суспільне в межах своєї компетенції та вимог законодавства вживатиме заходів для захисту персональних даних користувачів.

5. Пріоритет команди та захист прав інтелектуальної власності.

Суспільне завжди надаватиме перевагу творчості й рішенням команди. Робота журналістів, редакторів, дизайнерів, відеографів, фотокореспондентів та інших працівників творчих підрозділів є основою Суспільного. Інструменти ШІ для журналістів і працівників творчих підрозділів будуть допоміжними, а не трансформаційними. Суспільне не має на меті замінити людину рішеннями на базі ШІ. Водночас Суспільне усвідомлює, що технологічний прогрес означатиме переосмислення посад, обов'язків і функціоналу. Будь-які доповнення наявних посадових обов'язків або створення нових мають здійснюватися відповідно до

трудового законодавства України. АТ «НСТУ» під час використання ШІ також дотримуватиметься вимог законодавства у сфері авторського права та суміжних прав.

6. Використання об'єктів інтелектуальної власності Суспільного для навчання моделей ШІ.

Передача прав на використання об'єктів інтелектуальної власності АТ «НСТУ» третім особам для навчання моделей ШІ здійснюється в порядку, передбаченому законодавством.

7. Дотримання загальних світових стандартів щодо ШІ.

Наразі в Європейському Союзі (далі – ЄС) розробляються окремі правила використання ШІ, які встановлюють зобов'язання для провайдерів і користувачів залежно від рівня ризику ШІ. Попри те, що багато систем ШІ становлять мінімальний ризик, їх потрібно оцінювати за такими критеріями:

1) неприйнятний ризик.

Системи ШІ з неприйнятним ризиком – це системи, які вважаються загрозою для людей і будуть заборонені. Вони включають:

- когнітивне поведінкове маніпулювання людьми або окремими вразливими групами;
- соціальну оцінку: класифікацію людей на основі поведінки, соціально-економічного статусу чи особистих характеристик;
- біометричну ідентифікацію та категоризацію людей, системи біометричної ідентифікації в режимі реального часу та віддалені (наприклад, розпізнавання обличчя);

2) високий ризик.

Системи ШІ, які негативно впливають на безпеку або фундаментальні права, вважатимуться високоризиковими. Зокрема, йдеться про системи ШІ, що належать до певних сфер і повинні бути зареєстровані в базі даних ЄС: управління та експлуатація критичної інфраструктури; освіта та професійна підготовка; працевлаштування, управління працівниками та доступ до самозайнятості; доступ і користування основними приватними та державними послугами й перевагами; правозастосування; управління міграцією, притулком і прикордонним контролем; допомога в правовому тлумаченні та застосуванні законодавства.

Усі системи ШІ з високим рівнем ризику оцінюватимуться перед виведенням на ринок ЄС, а також протягом усього життєвого циклу.

Розрізняють ШІ загального призначення та генеративний. Генеративний ШІ (наприклад, ChatGPT) повинен відповідати таким вимогам прозорості:

- розкриття інформації про те, що контент створено ШІ;
- розроблення моделі для запобігання створенню незаконного вмісту;

– публікація зведень захищених авторським правом даних, які використовуються для навчання.

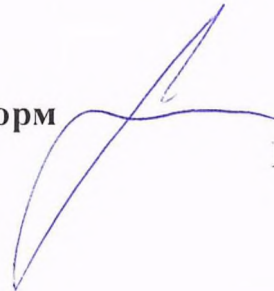
Моделі ШІ загального призначення з високим впливом, які можуть становити системний ризик (наприклад, GPT-4), повинні пройти ретельне оцінювання, а про будь-які серйозні інциденти потрібно буде повідомляти Європейську комісію;

3) обмежений ризик.

Системи ШІ з обмеженим ризиком повинні відповідати мінімальним вимогам щодо прозорості, що забезпечує можливість користувачам приймати обгрунтовані рішення. Після взаємодії з додатками ШІ користувач може вирішити, чи хоче він продовжувати ним користуватися. Користувачі повинні бути обізнані з особливостями роботи з ШІ, що включає системи ШІ, які створюють або обробляють зображення, аудіо- чи відеовміст, наприклад «глибокі фейки» (deepfake). Основним аспектом відповідності вимогам для ШІ є сертифікат захисту ШІ та даних від міжнародно визнаної організації. Така сертифікація може охоплювати багато тем, зокрема конфіденційність і безпеку даних, а також допомогти отримати повне розуміння нюансів ШІ та відповідних нормативних стандартів.

Суспільне під час вибору та роботи з ШІ керуватиметься згаданими принципами (щодо рівня ризику та сертифікації ШІ) та не використовуватиме у своїй діяльності ШІ з неприйнятним або високим рівнем ризику та/або такий, що не пройшов відповідної сертифікації.

**Головний продюсер цифрових платформ
Дирекції цифрових платформ**



Вікторія МУРОВАНА