УДК 004.056:004.85:342.7

Є. А. Садовник

РИЗИКИ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОРИСТАННІ ПУБЛІЧНИХ ШІ-МОДЕЛЕЙ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет

Анотація. *У роботі досліджено загрози конфіденційності, пов'язані з використанням публічних великих мовних моделей (LLM) у корпоративному середовищі. Проаналізовано ризики витоку комерційної таємниці, втрати інтелектуальної власності та порушення нормативних вимог, таких як GDPR, через використання запитів користувачів для навчання алгоритмів. Запропоновано заходи щодо мінімізації цих загроз та захисту корпоративних і персональних даних.*

Ключові слова: штучний інтелект, LLM, конфіденційність, комерційна таємниця, GDPR, витік даних, інтелектуальна власність.

Abstract. *The paper examines the privacy threats associated with the use of public large language models (LLMs) in a corporate environment. The risks of trade secret leakage, loss of intellectual property, and violation of regulatory requirements, such as GDPR, through the use of user queries to train algorithms are analyzed. Measures to minimize these risks and protect corporate and personal data are proposed.*

Keywords: artificial intelligence, LLM, privacy, trade secrets, GDPR, data leakage, intellectual property.

Вступ

Сьогодні впровадження штучного інтелекту (ШІ) стало невід’ємною частиною бізнес-процесів багатьох компаній. В той же час стрімке поширення генеративних великих мовних моделей (LLM) створює нові загрози для інформаційної безпеки та конфіденційності. Незважаючи на очевидні переваги автоматизації, використання публічних ШІ-моделей співробітниками часто призводить до неконтрольованого обміну даними. Метою цієї роботи є дослідження ризиків витоку комерційної таємниці, втрати інтелектуальної власності та порушення нормативно-правових вимог (зокрема GDPR) при взаємодії персоналу з публічними ШІ-системами.

Результати дослідження

Однією з головних проблем використання відкритих систем генеративного штучного інтелекту є загроза витоку конфіденційних даних та комерційної таємниці. Коли співробітники вводять чутливу інформацію або внутрішні документи в публічні LLM (наприклад, для перевірки коду, написання звітів чи аналізу), ці дані можуть бути збережені провайдером послуг та використані для подальшого навчання моделей [1]. У результаті така інформація здатна несподівано з'явитися у відповідях системи іншим користувачам, що нівелює будь-який контроль над нею.

Яскравим прикладом реалізації такої загрози став інцидент у компанії Samsung, співробітники якої випадково розкрили конфіденційну інформацію під час використання ChatGPT на робочому місці. Було зафіксовано три окремі випадки ненавмисного витоку чутливих даних: один працівник вставив конфіденційний вихідний код у чат для перевірки на помилки, другий надіслав код для оптимізації, а третій завантажив аудіозапис наради для створення нотаток до презентації. Оскільки політика ChatGPT передбачає збереження та використання введених даних для подальшого навчання моделі, ця надсекретна інформація компанії фактично опинилася у відкритому середовищі [2].

Цей інцидент став реальним підтвердженням ризиків, про які тривалий час попереджали експерти з захисту даних. Експерти попереджають, що подібна передача конфіденційних текстів може порушувати вимоги GDPR, що, до речі, стало однією з причин тимчасової заборони ChatGPT в Італії [2–3]. Як наслідок, Samsung була змушена негайно обмежити обсяг завантаження даних до 1024 байт на користувача та розпочати розслідування щодо причетних співробітників, а також розглянути можливість створення власного внутрішнього ШІ-чатбота для уникнення подібних проблем у майбутньому.

Значною загрозою є також втрата прав на інтелектуальну власність (ІВ). Оскільки права на ІВ, зокрема патенти та комерційні таємниці, великою мірою залежать від збереження їх секретності, необережне використання ШІ (як у випадку із вихідним кодом у компанії Samsung) може призвести до їх безповоротної втрати [4]. Наприклад, якщо працівник завантажує пропрієтарну інформацію у ШІ-систему, це може бути розцінено як публічне розголошення, що позбавляє компанію законної можливості захистити ці дані.

Щоб уникнути цих загроз, компаніям необхідно впроваджувати комплекси технічних та організаційних заходів. Поширеною практикою стає пряма заборона працівникам використовувати відкриті ШІ для робочих завдань. Натомість бізнесу варто переходити на корпоративні або приватні LLM, які гарантують ізоляцію середовища та відмову від використання введених даних для навчання базової моделі [5].

Висновки

Використання публічних ШІ-моделей у корпоративному середовищі несе критичні ризики для конфіденційності, включаючи витік комерційної таємниці, розголошення інтелектуальної власності та порушення нормативних вимог щодо захисту персональних даних (GDPR). Дані, які вносяться у такі системи у вигляді запитів, часто накопичуються та використовуються для їх подальшого навчання. Реальний випадок із витоком вихідного коду та корпоративних записів компанії Samsung наочно демонструє, як відсутність контролю за використанням публічних LLM може призвести до втрати стратегічно важливої інформації. Для мінімізації цих ризиків компанії повинні повністю переглянути свої підходи: впроваджувати жорсткі внутрішні регламенти та переходити на використання ізольованих приватних або корпоративних моделей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What happens to your data in public LLMs? A reality check for businesses. *Medium*. URL: https://medium.com/@rom_55053/what-happens-to-your-data-in-public-llms-a-reality-check-for-businesses-e6db7ebd01d6 (date of access: 05.05.2026).
2. Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT. *Mashable*. URL: https://mashable.com/article/samsung-chatgpt-leak-details (date of access: 05.05.2026).
3. Юридичні ризики «порад» штучного інтелекту та їх використання в бізнесі. *Юридична Газета*. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/yuridichni-riziki-porad-shtuchnogo-intelektu-ta-yih-vikoristannya-v-biznesi.html (дата звернення: 05.05.2026).
4. Navigating the Legal Risks of AI: Intellectual Property and Privacy Considerations. *Miller Nash LLP*. URL: https://www.millernash.com/industry-news/navigating-the-legal-risks-of-ai-intellectual-property-and-privacy-considerations (date of access: 05.05.2026).
5. What are the copyright and confidentiality issues arising from use of public and private Large Language Models (LLMs)? *Geldards*. URL: https://www.geldards.com/insights/what-are-the-copyright-and-confidentiality-issues-arising-from-use-of-public-and-private-large-language-models-llms/ (date of access: 05.05.2026).

Садовник Євгеній Анатолійович – студент групи 1БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: sadovnikevgenii@gmail.com

Науковий Керівник: ***Радченко Євгеній Валентинович*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: eradchenko@vntu.edu.ua

Sadovnyk Yevhenii A. – student of 1BS-24b group, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: sadovnikevgenii@gmail.com

Supervisor: ***Yevhenii Radchenko V.*** – Assistant professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: eradchenko@vntu.edu.ua