УДК 004.8.056:005.8

МЕХАНІЗМИ МІНІМІЗАЦІЇ РИЗИКІВ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІТ-ПРОЄКТАХ У МЕЖАХ БАЗОВОГО GENERAL DATA PROTECTION REGULATION

Кузнєцов Д.О.
e-mail: dmytro.kuznietsov@nure.ua
Науковий керівник – д.т.н., проф. Євланов М.В.
Харківський національний університет радіоелектроніки, каф. ІУС
м. Харків, Україна

This paper looks at the main risks connected with the use of AI in modern IT projects under GDPR requirements. It focuses on how AI solutions are integrated to automate and optimize business and project processes, but also shows that such integration can create legal, organizational, and technical issues related to personal data. To reduce these risks, the paper considers a risk-based approach that includes privacy by design, data minimization, risk assessment, and human oversight. It also refers to the general principles of ISO 31000 and ISO/IEC 42001. The results show that effective AI implementation requires not only technical development, but also proper management and compliance control.

У сучасному ІТ-бізнесі дотримання вимог General Data Protection Regulation (GDPR) є ключовим елементом роботи із персональними даними на усіх рівнях надання послуг – від продуктових компаній до аутсорсинг-стартапів. Переважна більшість продуктів або сервісів у цих організаціях має потребу в інтеграціях та обміні приватною інформацією у мережі поза межами первинного сервісу, що значно підвищує ризики втрати або розкриття даних на усіх рівнях трансферу інформації та її отримання. Таким чином, масштабування, збереження та використання інформації підвищує вірогідність її втрати, що не відповідає вимогам законодавства про використання та обмін персональними даними та безпосередньо підриває довіру і безпеку до надавача послуг. Саме з цієї причини світові тенденції та бізнеси потребували чіткої доктрини безпеки. Регламент GDPR [1] визначає базові принципи обробки даних, зокрема законність, прозорість, обмеження мети, мінімізацію даних, точність, обмеження строків зберігання, а також цілісність і конфіденційність.

Використання GDPR стандартизовано передбачено на етапі аналізу потреб та концепції проєкту перед створенням архітектури обміну та організації даних з метою урахування основних методів безпеки даних, таких як data protection by design and by default. Такий підхід допомагає взяти під контроль усі потенційні ризики обробки даних та врахувати їх в організації первинних бізнес-потреб проєкту та подальшої його імплементації. Таким чином, регламент GDPR використовується на усіх етапах реалізації продукту – від ініціації до завершення та видалення

даних, що надає можливість проконтролювати усі потенційні прогалини у безпеці продукту та запобігти законодавчим і репутаційним наслідкам.

Із появою рішень від OpenAI почався надвисокий попит на їх використання в усіх потенційних галузях. Можливість не тільки використовувати базу знань, таку як пошукові системи, а й надавати можливість виведення логічних висновків на підставі вже існуючого досвіду надала людям можливість зменшити витрати ресурсів на зайві базові процеси та змістити пріоритети на більш важливі та комплексні задачі у безлічі напрямків. Паралельно із цим компанії почали створювати все більше ШІ-агентів та дозволяти робити інтеграції цих сервісів у свої продукти з метою автоматизації та підвищення попиту на нейромережі. Не менш важливим є фактор того, що така інтеграція допомагає ШІ ще краще навчатися, надавати більш валідну відповідь і тим самим ще більше підвищувати цікавість до його використання у різноманітних напрямках.

Автоматизація передбачає пряму або часткову інтеграцію ШІ-сервісу у систему продукту та прямий обмін даними між базами даних і сервісом нейромережі, що гарантовано створює трансфер даних від сервера, який належить компанії-постачальнику послуг, до сторонніх проміжних серверів ШІ-агентів та різноманітних хмарних систем, які оптимізують використання сторонніх сервісів і не є частиною первинного сховища даних. Таким чином, кожен такий крок є потенційним ризиком втрати даних, а навчання моделей підвищує ризик використання приватних даних поза зоною основного внутрішнього функціоналу, що означає, що в подальшому ці дані можуть стати основою для відповідей ШІ для інших користувачів. Це прямо суперечить базовим принципам GDPR, зокрема обмеженню мети, мінімізації даних і вимозі забезпечення їх цілісності та конфіденційності. Окремо ризик посилюється тоді, коли AI бере участь в автоматизованому прийнятті рішень без достатнього людського контролю, оскільки GDPR встановлює обмеження для таких випадків.

На поточний час багато ШІ-провайдерів підпадають під вимоги щодо безпечної організації даних та надають можливість мінімізувати частину ризиків [2]. Таким чином, частина нейромережевих провайдерів на рівні політики користування надає можливість відмовитися від використання даних сервісом для навчання. Також вкрай важливо відокремити частини сервісу, які оброблюють конфіденційні дані, та надавати доступ до них виключно за потребою прямої обробки окремих даних ШІ-агентом, що допомагає ізолювати сховище та запобігти потенційній втраті даних. Із додаткових методів безпеки важливо використовувати шифрування даних, їх мінімізацію та вести постійний контроль статусів ШІ-продукту задля вчасного ізолювання продукту у разі збоїв або масових втрат даних, оскільки подібні інциденти можуть призводити до репутаційних, безпекових і фінансових наслідків для компанії.

Основними механізмами мінімізації ризиків використання ШІ в ІТ-проєктах у межах базових вимог GDPR є насамперед обмеження обсягу даних, чітке визначення мети їх обробки та відокремлення конфіденційної інформації від загального функціоналу сервісу. Ще на етапі проєктування доцільно застосовувати підхід data protection by design and by default, який передбачає використання лише необхідних даних, обмеження доступів, скорочення строків зберігання, а також технічні засоби захисту, зокрема псевдонімізацію та шифрування. Якщо ШІ інтегрується через зовнішнього провайдера, важливо окремо контролювати умови використання сервісу, зокрема можливість відмови від використання даних для навчання моделей, а також перевіряти, куди саме передаються дані і хто має до них доступ.

Додатково ефективним механізмом є використання локальних або ізольованих рішень для обробки чутливих даних там, де це можливо, щоб зменшити залежність від сторонньої інфраструктури.

Не менш важливими є й організаційні механізми, оскільки без них технічний захист сам по собі не гарантує безпеки. Для проєктів, у яких обробка даних може створювати високий ризик для прав і свобод людини, доцільно проводити Data Processing Impact Assessment (DPIA) ще до запуску рішення, а також зберігати людський контроль у тих процесах, де ШІ бере участь в автоматизованому прийнятті рішень [3].

У практичному значенні це означає, що безпечна інтеграція ШІ повинна спиратися на попередню оцінку ризиків, контроль провайдерів, моніторинг роботи сервісу після запуску та зрозумілу відповідальність команди за обробку даних. Отже, мінімізація ризиків використання ШІ в ІТ-проєктах полягає не в відмові від автоматизації, а в її правильній організації відповідно до базових вимог GDPR.

Список використаних джерел:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 10.03.2026).

2. What does data protection “by design” and “by default” mean? European Commission: вебсайт. URL: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (дата звернення: 10.03.2026).

3. ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system. 2023-12-01. Geneva, 2023. 51 p. URL: https://www.iso.org/standard/81230.html (дата звернення: 10.03.2026).