Управління інформаційною безпекою в умовах впровадження великих мовних моделей у CRM-системи

УДК 004.056

Ігор Ралік[1]

Тернопільський національний технічний університет, [1]tntuihor@gmail.com

Впровадження великих мовних моделей у CRM-системи створює нові виклики для управління інформаційною безпекою на корпоративному рівні [1]. Перехід від статичних комунікаційних шаблонів до динамічної генерації тексту вимагає розробки рішень для контролю за поведінкою алгоритмів штучного інтелекту.

Генерація персоналізованих комунікаційних сценаріїв у реальному часі несе ризики порушення корпоративних політик, розголошення чутливої інформації або надання клієнтам юридично некоректних даних. Відповідно, ефективне управління інформаційною безпекою вимагає механізмів, які б регулювали генеративний процес, забезпечуючи його контрольованість та запобігаючи появі небажаних відповідей.

У запропонованій архітектурі CRM-системи управління безпекою реалізується превентивно через механізм динамічного структурованого промпту, за інформаційну безпеку відповідають два блоки, а саме:

- Блок системних обмежень. Виконує функцію системного метарегулятора, який визначає універсальні рамки безпеки. Управління ризиками тут відбувається через суворі інструкції, такі як заборону на використання чутливої інформації, уникнення припущень щодо особистих даних клієнта та обмеження на інтерпретацію юридичної інформації. Цей рівень управління спрямований на мінімізацію ризиків, безпосередньо пов'язаних з автоматизованою генерацією тексту.
- Блок бізнес-правил. Забезпечує управління дотриманням вимог на рівні конкретної організації. Цей компонент містить політики підтримки, внутрішні процедури, регламенти та юридичні обмеження компанії. Завантажуючись одноразово як системний промпт, він гарантує повну відповідність згенерованих сценаріїв бізнес-політиці, забезпечуючи функціональну та операційну надійність взаємодії.

Управління інформаційною безпекою у CRM-системах має базуватися на проактивному вбудовуванні політик безпеки безпосередньо в логіку генерації відповідей. Поєднання блоку універсальних обмежень та суворого дотримання доменних бізнес-правил дозволяє зберігати контроль над системою, відкриваючи перспективи для подальшої розробки механізмів контролю генеративних сценаріїв.

1. HOCHI C. The Impact of Large Language Model Integration on Customer Relationship Management in Small and Medium-Sized Enterprises: An Empirical Study of a Medium-Sized Printing Company. Journal of International Social Science. 2025. p. 177.