

Практична цінність ГШІ виявляється у сценаріях багатосторонньої взаємодії, де один фахівець може одночасно комунікувати з декількома ШІ-агентами, що мають власні суперечливі цілі та соціальні установки. Така симуляція дозволяє глибоко аналізувати процеси формування коаліцій та пошуку інтегративних рішень, які задовольняють інтереси всіх сторін конфлікту чи переговорів.

Використання генеративного штучного інтелекту для розвитку переговорних навичок є перспективним напрямом цифрової трансформації освіти. Це дозволяє перейти від епізодичного навчання до моделі безперервного вдосконалення майстерності. Впровадження ГШІ-симуляторів у корпоративний сектор та навчальні програми закладів вищої освіти дозволить виховувати нове покоління фахівців, здатних ефективно діяти у мінливих умовах цифрового суспільства.

### Список використаних джерел

1. Brynjolfsson, E., Li, D., & Raymond, L. (2024). *Replication data for: Generative AI at work* [Data set]. Harvard Dataverse. <https://doi.org/10.7910/DVN/FSV1X7>
2. Fisher, R., & Ury, W. (2011). *Getting to Yes: Negotiating Agreement Without Giving In*. Penguin Books.
3. Malhotra, D. (2007). *Negotiation Genius*. Harvard Business Review Press.
4. Voss, C., & Raz, T. (2017). *Never Split the Difference: Negotiating As If Your Life Depended On It*. HarperBusiness.

**Резуненко С.А.,**  
викладач,

ВСП «Фаховий коледж інформаційних систем і технологій  
Київського національного економічного університету імені Вадима Гетьмана»

**Помазун О.М.,**  
к.е.н., доцент,

Київський національний економічний університет імені Вадима Гетьмана

## АВТОМАТИЗАЦІЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТИ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ МАЛОГО І МІКРОБІЗНЕСУ

В умовах зростаючої конкуренції та інфляційного тиску малий і мікробізнес стикається з необхідністю підвищення операційної ефективності за обмежених ресурсів. На відміну від великих корпорацій, малі підприємства змушені шукати доступні інструменти оптимізації, здатні забезпечити відчутний результат за мінімальних інвестицій.

Саме автоматизація робочих процесів та впровадження інструментів на базі штучного інтелекту (ШІ) стають важливими механізмами формування конкурентних переваг. За даними дослідження Торгової палати США [1], 86% малих підприємств підтверджують, що технологічні платформи допомогли їхньому бізнесу працювати ефективніше, а 75% зазначають, що без доступу до технологій їхній бізнес не зміг би вижити.

Масштаб технологічної трансформації малого бізнесу є безпрецедентним. За даними опитування Торгової палати США (3 870 респондентів) [1], 99% малих підприємств використовують принаймні одну технологічну платформу, а 58% – чотири і більше. Технології застосовуються для маркетингу (46%), управління розрахунками із персоналом (44%), бухгалтерського обліку (42%), управління відносинами з клієнтами (34%), обробки продажів (28%) та безпосередньо для автоматизації завдань (24%) [1]. При цьому спостерігається чіткий кореляційний зв'язок між рівнем технологічного впровадження та бізнес-результатами: серед компаній із низьким рівнем впровадження зростання продажів зафіксували 77%, тоді як серед компаній із середнім рівнем – 86%.

Першим трендом є автоматизація робочих процесів (workflow automation), яка, за визначенням Deloitte [2], перетворюється з допоміжної ІТ-функції на стратегічний інструмент трансформації бізнесу. Звіт Deloitte та ServiceNow підкреслює, що автоматизація має виходити за межі ІТ-відділу та охоплювати HR, фінанси, ризик-менеджмент та обслуговування клієнтів. Практичний досвід компаній, що впровадили комплексну автоматизацію робочих процесів, демонструє приріст продуктивності на 20–60%, зростання задоволеності клієнтів на 10–20% та досягнення 4–5-кратної окупності інвестицій в операційну ефективність [2].

Для малого бізнесу цей тренд реалізується через no-code/low-code платформи – такі інструменти, як Zapier, Make, N8n, дозволяють підприємцям без технічної освіти самостійно створювати автоматизовані сценарії, що пов'язують різні сервіси.

Другим трендом є стрімке впровадження ШІ як складової автоматизації бізнес-процесів. За даними SBE Council (опитування 517 підприємців у лютому 2026 р.) [3], 82% малих підприємств вже використовують принаймні один ШІ-інструмент, а медіана кількості інструментів складає п'ять. Основні сфери застосування включають дослідження ринку (37%), створення контенту (30%), автоматизацію маркетингу, управління проектами та роботу з соціальними мережами (по 25%). При цьому 81% користувачів ШІ вважають його важливим для конкурентоспроможності та зростання, а 68% називають підвищення ефективності головною мотивацією впровадження [3].

За даними глобального опитування McKinsey [4], 88% організацій вже регулярно використовують ШІ принаймні в одній бізнес-функції (порівняно з 78% роком раніше), а 62% експериментують із ШІ-агентами. Проте дослідження виявляє парадокс: попри широке розповсюдження, більшість організацій все ще перебувають на етапі експериментування – лише третина розпочала масштабування. McKinsey підкреслює, що найуспішніші компанії не просто впроваджують технології, а реорганізують бізнес-процеси: 58% високоефективних організацій системно вбудовують ШІ-рішення у робочі процеси, тоді як серед решти цей показник складає лише 20% [4]. Deloitte підтверджує цей висновок, наголошуючи на необхідності побудови стійкої технологічної екосистеми замість накопичення ізольованих рішень [2].

Вплив автоматизації та ШІ на продуктивність малого бізнесу є кількісно вимірюваним. За даними SBE Council [3], власники малого бізнесу заощаджують у середньому 5 годин на тиждень особисто, а сукупна економія по організації складає 11,5 годин на тиждень. Дві третини підприємців повідомляють про зростання доходів, при цьому 22% фіксують приріст понад 10%. Зекономлені ресурси реінвестуються: 44% впровадили інноваційні практики та покращили клієнтський досвід, 35% інвестували у підвищення конкурентоспроможності, а 34% спрямували ресурси на нові можливості зростання [3]. Важливо, що 82% малих підприємств, які використовують ШІ, збільшили чисельність персоналу за останній рік [1], а 52% розглядають технологічні інструменти як доповнення до людської праці [3].

Водночас впровадження автоматизації супроводжується низкою специфічних викликів. За даними SBE Council [3], основними бар'єрами є обмеженість знань та навичок (23%), занепокоєння щодо конфіденційності даних (17%), ризики кібербезпеки (13%) та вартість впровадження (12%). McKinsey [4] констатує, що на рівні великих організацій 51% респондентів повідомили про принаймні один випадок негативних наслідків від використання ШІ, а основні ризики стосуються точності, кібербезпеки та інтелектуальної власності. Deloitte [2] акцентує увагу на розриві між інвестиціями та отриманою цінністю: багато компаній не можуть чітко оцінити ROI своїх технологічних впроваджень, що потребує системного підходу до вимірювання результатів.

Таким чином, автоматизація робочих процесів та впровадження ШІ для малого і мікробізнесу – це вже не розкіш, а необхідна умова конкурентоспроможності. 96% власників малого бізнесу планують впроваджувати нові технології [1], а 62% очікують збільшення витрат на ШІ-інструменти протягом наступного року [3]. Разом з тим, ключовим фактором успіху є не кількість впроваджених технологій, а якість їх інтеграції у бізнес-процеси. Як демонструє досвід Deloitte [2], максимальна цінність досягається через побудову єдиної

технологічної екосистеми з фокусом на конкретних галузевих потребах, а не через хаотичне накопичення точкових рішень. Впровадження має бути поетапним: починати з автоматизації найбільш рутинних процесів, забезпечуючи навчання персоналу та контроль якості на кожному етапі цифрової трансформації.

### Список використаних джерел

1. U.S. Chamber of Commerce. (2025). *Empowering small business: The impact of technology on U.S. small business* (4th ed.). <https://www.uschamber.com/technology/empowering-small-business-the-impact-of-technology-on-u-s-small-business>
2. Deloitte & ServiceNow. (2025). *2025 workflow automation outlook: Turn possibilities into progress with transformational outcomes*. <https://www.deloitte.com/us/en/about/press-room/servicenow-workflow-automation-outlook-2025.html>
3. SBE Council & TechnoMetrica. (2026, March). *Small business technology use survey*. <https://sbecouncil.org/2026/04/25/the-ai-tools-small-businesses-are-using/>
4. McKinsey & Company. (2025, November). *The state of AI in 2025: Agents, innovation, and transformation*. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>

**Рзаєва С.Л.,**

к.т.н, доцент,

**Костюк Ю.В.,**

доктор філософії (PhD), доцент,

Київський столичний університет імені Бориса Грінченка

## ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПРОГНОЗУВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У сучасних умовах цифрової трансформації підприємства дедалі більше залежать від інформаційних систем, хмарних технологій, корпоративних мереж та автоматизованих сервісів. Разом із розвитком цифрової інфраструктури стрімко зростає кількість кіберзагроз, серед яких особливу небезпеку становлять несанкціонований доступ до даних, шкідливе програмне забезпечення, фішингові атаки, витік конфіденційної інформації та атаки на корпоративні мережі. Навіть короточасне порушення роботи інформаційної системи може спричинити значні фінансові збитки та репутаційні втрати для підприємства. Традиційні засоби інформаційної безпеки переважно орієнтовані на реагування на вже відомі загрози. Проте сучасні кібератаки постійно змінюються, а їх структура стає складнішою та менш передбачуваною. Саме тому особливої актуальності набуває використання штучного інтелекту як інструменту прогнозування ризиків інформаційної безпеки. На відміну від класичних підходів, інтелектуальні системи здатні аналізувати великі обсяги даних, виявляти приховані закономірності та прогнозувати ймовірність виникнення кіберінцидентів ще до моменту їх реалізації.

Штучний інтелект у сфері інформаційної безпеки використовується для автоматизованого аналізу подій, оцінювання ризиків, прогнозування атак та підтримки прийняття рішень. Основу таких систем становлять алгоритми машинного навчання, які здатні навчатися на основі історичних даних та адаптуватися до нових типів загроз.

Оцінювання ризику інформаційної безпеки зазвичай базується на визначенні ймовірності реалізації загрози та можливих збитків від неї. Узагальнений показник ризику можна подати