Герасименко О. О.
кандидат економічних наук, доцент,
доцент кафедри менеджменту інноваційної
та інвестиційної діяльності,
Київський національний університет імені Тараса Шевченка

DOI: https://doi.org/10.36059/978-966-397-438-5-2

БЕЗПЕКОВА КОМПОНЕНТА СТІЙКОГО РОЗВИТКУ ПІДПРИЄМСТВ ЯК ІМПЕРАТИВ ТЕХНІКО-ТЕХНОЛОГІЧНИХ ТРАНСФОРМАЦІЙ В УМОВАХ «ІНДУСТРІЇ 4.0»

Глобальний розвиток економіки та соціуму в третьому десятилітті XXI століття, коли «Індустрія 4.0» створює нові масштабні можливості та продукує різновекторні ризики і загрози, загострює науковий та прикладний фокус стійкого розвитку підприємств. Традиційні його компоненти – економічна, соціальна, екологічна, які кореспондують з Цілями сталого розвитку, ухваленими в рамках 70-ї сесії Генеральної Асамблеї ООН та підтриманими щодо їх досягнення і результатів адаптації з урахуванням специфіки розвитку України [4] – закономірно та об'єктивно доповнюються безпековою складовою.

Реалії сьогодення засвідчили, що примноження та посилення економічного потенціалу підприємств стало неможливим без управління ризиками, які викликані ефектами й наслідками заміщення людського ресурсу високими технологіями Четвертої промислової революції; дотримання належного соціального контуру на тлі складно передбачуваного професійного та соціально-трудового майбутнього ускладнюється в частині гарантування стабільності в зайнятості, оплаті праці, наданні соціальних благ, дотриманні морально-етичних принципів; ресурсоощадливі технології та безвідходні виробництва, як квінтесенція екологічного розвитку, актуалізують інвестування в поновлювальні джерела енергії.

Нині реальністю є те, що в умовах Четвертої промислової революції до тріади компонент сталого розвитку підприємств додається безпековий елемент, передусім як цифрова та інформаційна безпека. Особливо гостро постає проблема конфіденційності інформації та кібербезпеки з актуальною потребою попередження витоків даних про підприємства та персональні дані їх працівників. Віртуальний світ ділових комунікацій будується на системах передавання інформації, які працюють з цифровими даними та електронними каналами, що наражає користувачів на додаткові ризики несанкціонованого доступу до конфіденційної,

службової чи таємної інформації, що містить комерційну таємницю або персональні дані, поширення яких може завдати матеріальних та репутаційних збитків.

При цьому, до викликів, що продукуються інноваціями Четвертої промислової революції, додається досить низький рівень довіри до використання штучного інтелекту в різних сферах діяльності [1].

Новітні техніко-технологічні рішення, що продукуються «Індустрією 4.0», істотно змінюють організаційну структуру та бізнес-процеси у внутрішньому середовищі підприємств, а також їх взаємодію з агентами зовнішнього середовища на основі гібридних форм співпраці та змішаних каналів комунікацій. Технології Четвертої промислової революції постають не лише як інструментарій автоматизації, комп'ютеризації, роботизації численних бізнес-процесів та прийняття управлінських рішень, а й як віртуальний партнер у досягненні намічених цілей та поставлених завдань, сприяючи створенню продуктивних моделей діяльності, що задовольняють потреби клієнтів, ділових партнерів, працівників підприємств.

Поділяємо точку зору авторів, які доводять, що інтеграція сучасних технологій штучного інтелекту в бізнес-середовищі створює передумови для отримання конкурентних переваг на різних рівнях, зниження затрат часу на виконання стандартних, рутинних операцій, підвищення продуктивності й якості послуг з обслуговування клієнтів [2].

Використання проривних технологій Четвертої промислової революції набуває широких масштабів, які динамічно збільшуються. За оновленими у 2024 році аналітичними оцінками консалтингової компанії McKinsey від 50 % до 60 % усіх організацій використовують штучний інтелект [3].

Цифровізація бізнес-процесів з використанням штучного інтелекту, CRM-систем, комунікаційних ботів, Big Data, хмарних технологій, гейміфікації, віртуальної реальності посилює вимоги щодо надійності кібербезпеки.

Одним з найбільш потужних та загрозливих викликів сьогодення є дотримання етичних норм в цифрову епоху, оскільки з появою високих сучасних технологій – штучного інтелекту, розпізнавання облич, соціальних мереж, біоінженерних технологій – на різних рівнях (від індивідуального до глобального, включаючи корпоративний та національний) виникає питання про моральну відповідальність та етичну поведінку.

Завдяки віртуальним каналам люди та підприємства як суб'єкти різнопланової діяльності активно використовують потенціал соціальних мереж, мобільних додатків, інструментарію онлайн-комерції, що не може не викликати занепокоєння щодо кібербезпеки та масштабів поширення конфіденційної інформації.

Усе викладене дає підставу для висновку, що до усталеної комбінації складових сталого розвитку підприємств в умовах «Індустрії 4.0» додається безпекова компонента, передусім, цифрова та інформаційна безпека, що має стати відповіддю на виклики і загрози техніко-технологічного характеру.

Література:

1. Андрощук Г.О. Рівень довіри до штучного інтелекту: аналіз результатів глобальних досліджень та стан в Україні. *Інформація і право*. 2023. № 4. С. 217–231. DOI: https://doi.org/10.37750/2616-6798.2023.4(47).291675

2. Дриньов Д.М. Загородніх В.В., Зінченко О.М. Застосування штучного інтелекту у системі управління підприємством. *Економічний простір*. 2023. № 188. С. 79–82. DOI: https://doi.org/10.32782/2224-6282/188-13

3. Статистика ШІ за 2024 рік: зростання, використання та впровадження. URL: https://mspoweruser.com/uk/ai-statistics/ (дата звернення: 06.11.2024).

4. Цілі сталого розвитку та Україна. URL: https://www.kmu.gov.ua/diyalnist/cili-stalogo-rozvitku-ta-ukrayina (дата звернення: 08.11.2024).