

УДК 004.056:339.9

Лазнева І.О.<sup>1</sup>, Лук'янова М.А.<sup>2</sup>

<sup>1</sup> канд. іст. наук, доц. НУ «Запорізька політехніка»

<sup>2</sup> студ. гр. БТЕЗ-1912 НУ «Запорізька політехніка»

## **КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ МІЖНАРОДНОГО БІЗНЕСУ**

Сучасний міжнародний бізнес функціонує в умовах стрімкої цифрової трансформації, що охоплює виробничі процеси, міжнародну торгівлю, фінансові операції, логістику, маркетинг, управління персоналом і взаємодію з клієнтами. Хмарні технології, великі дані, штучний інтелект, цифрові платформи, електронна комерція та автоматизація бізнес-процесів створюють нові можливості для глобального масштабування компаній, зниження трансакційних витрат і підвищення швидкості прийняття управлінських рішень. Водночас цифровізація посилює вразливість компаній до кіберзагроз, оскільки розширення цифрової інфраструктури автоматично збільшує площу потенційної атаки, а отже кібербезпека перетворюється з технічної функції на стратегічну умову стабільного розвитку міжнародного бізнесу.

Цифрова трансформація міжнародного бізнесу означає не лише впровадження окремих технологічних рішень, а глибоку зміну бізнес-моделей, способів створення вартості, каналів взаємодії зі споживачами та механізмів міжнародної координації. Сучасні дослідження з міжнародного бізнесу наголошують, що цифрова трансформація вже є центральною темою для міжнародних компаній, оскільки впливає на їхню глобальну стратегію, структуру управління та інтернаціоналізацію. У цьому контексті цифрова інфраструктура стає ключовим активом компанії, а її захист - умовою збереження конкурентоспроможності на міжнародних ринках.

Саме тому кібербезпеку доцільно розглядати не як допоміжний елемент ІТ-підтримки, а як одну з базових складових цифрової трансформації. У міру того як бізнес переходить до платформних моделей, дистанційного управління, цифрових ланцюгів постачання, електронних платежів і хмарних сервісів, кіберризики стають системними.

Для міжнародного бізнесу це особливо важливо з кількох причин. По-перше, глобальні компанії працюють одночасно в різних юрисдикціях, а отже повинні враховувати відмінності в регуляторних вимогах щодо захисту даних, управління кіберризиками та реагування на інциденти. По-друге, міжнародний бізнес часто залежить від складних мереж підрядників, логістичних операторів, фінансових посередників і цифрових платформ, що створює додаткові ризики через атаки на ланцюги постачання. По-третє, цифрова трансформація активізує використання штучного інтелекту, хмарної інфраструктури та Інтернету речей, а це вимагає нових підходів до управління доступом, захисту даних і безперервності операцій. OECD у своєму рамковому документі з цифрової безпеки прямо розглядає цифрову безпеку як економічне та соціальне питання, а не лише як технічну проблему.

У практичному вимірі кібербезпека виконує щонайменше п'ять ключових функцій у цифровій трансформації міжнародного бізнесу: захист цифрових активів, зокрема баз даних, комерційної таємниці, фінансової інформації, клієнтських профілів та інтелектуальної власності; забезпечення безперервності операцій, оскільки кіберінциденти можуть зупинити виробництво, транскордонні поставки, платежі чи клієнтський сервіс; дотримання регуляторних вимог у різних країнах і юрисдикціях; підтримка довіри до бренду, адже в цифровій економіці довіра до безпечності сервісів прямо впливає на лояльність споживачів і партнерів; підтримка інновацій, оскільки компанії значно охочіше впроваджують нові цифрові рішення тоді, коли мають зрозумілі механізми управління кіберризиками. Цей висновок узгоджується і з сучасними дослідженнями, які пов'язують цифрову трансформацію, кіберстійкість і бізнес-резильєнтність.

Разом із тим цифрова трансформація міжнародного бізнесу загострює низку нових проблем. Серед них - дефіцит кваліфікованих кадрів у сфері кібербезпеки, зростання залежності від сторонніх провайдерів цифрових послуг, складність оцінювання ризиків у глобальних мережах, а також поява нових векторів атак, пов'язаних із генеративним ШІ, автоматизованими фішинговими кампаніями та компрометацією постачальників програмного забезпечення. WEF звертає увагу на нерівномірність кіберспроможностей між організаціями та секторами, що особливо небезпечно в міжнародному бізнесі, де вразливість одного елемента мережі може створити ризики для всієї екосистеми.

У цих умовах ефективна цифрова трансформація міжнародного бізнесу має спиратися на принцип кіберстійкості. Йдеться не лише про запобігання атакам, а й про здатність організації виявляти загрози, швидко реагувати, мінімізувати збитки та відновлювати діяльність. Кіберстійкість доцільно розглядати як складову загальної організаційної стійкості компанії. Це передбачає інтеграцію кібербезпеки в корпоративну стратегію, ризик-

менеджмент, аудит, підготовку персоналу, роботу з контрагентами та систему безперервності бізнесу.