УДК 658.589:005.35:339.9

Пирог В. В.
здобувач ступеня доктора філософії
Приватне акціонерне товариство «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
м. Київ, Україна

ОРГАНІЗАЦІЙНІ ІННОВАЦІЇ ЯК ВІДПОВІДЬ НА ГЛОБАЛЬНІ ГІБРИДНІ ЗАГРОЗИ В УМОВАХ ЕКОНОМІЧНОЇ ГЛОБАЛІЗАЦІЇ

Зростаюча взаємозалежність економік, зумовлена глобалізацією, значно посилила вразливість корпоративного сектору до гібридних загроз. Ці загрози, що поєднують кіберризики, економічний тиск та дезінформаційні кампанії, виходять за межі національних кордонів та впливають на корпорації незалежно від їхнього масштабу чи галузі. Глобальний характер фінансових потоків й ланцюгів постачання підсилює ці ризики, створюючи складні виклики, які підривають стійкість, порушують операційну діяльність та загрожують довгостроковій стабільності. У зв'язку з цим виникає критична потреба у впровадженні інноваційних організаційних стратегій, спрямованих на вирішення цих викликів, збереження конкурентоспроможності та забезпечення безперервності роботи. Глобальний характер гібридних загроз вимагає системної відповіді, яка включає не лише технологічні рішення, але й адаптивні та стратегічні інновації на організаційному рівні.

Гібридні загрози представляють багатовимірний виклик, посилений динамікою економічної глобалізації. З розширенням міжнародної присутності та участі в транскордонних операціях корпорації стають дедалі вразливішими до різних загроз, таких як кібернапади на інтелектуальну власність, економічні санкції, які порушують операційну стабільність, та розриви у ланцюгах постачання через геополітичні напруження [2]. Дослідження показують, що гібридні загрози мають мультиплікативний ефект, значно збільшуючи ризики на взаємопов'язаних глобальних ринках та дестабілізуючи традиційні бізнес-моделі [2]. Наприклад, один кібернапад на глобальний ланцюг постачання може мати каскадні наслідки, порушуючи логістику, підриваючи довіру клієнтів і спричиняючи фінансові втрати на міжнародному рівні. Ці загрози не лише порушують поточні бізнес-процеси, але й змушують організації переглядати свої рамки управління ризиками та розробляти інноваційні відповіді, орієнтовані на глобалізоване середовище.

Організаційні інновації відіграють ключову роль у забезпеченні адаптації до швидкозмінного глобального середовища. Ці інновації охоплюють створення гнучких управлінських структур, впровадження передових цифрових систем захисту та адаптивних стратегій, спрямованих на підвищення стійкості корпоративних систем [1]. Одним із таких підходів є концепт «цифрового імунітету», який передбачає створення проактивних систем для виявлення та нейтралізації кіберзагроз до їх виникнення. Концепт «цифрової вакцинації», наприклад, дозволяє організаціям захищати свою інфраструктуру від вразливостей, забезпечуючи більшу стійкість до зовнішніх шоків. Ці підходи зменшують час реагування та мінімізують потенційний вплив гібридних загроз на операційну діяльність, особливо у секторах, які залежать від цифрових технологій і глобальної взаємопов'язаності.

Глобалізація фінансових потоків і зростаюча взаємозалежність економік вимагають інтеграції інноваційних бізнес-моделей, які підвищують ефективність, адаптивність і гнучкість. Використання передових технологій, таких як штучний інтелект, прогнозна аналітика та блокчейн, дозволяє корпораціям оптимізувати глобальні операції, одночасно вирішуючи нові ризики та невизначеності [3]. Передова аналітика, наприклад, дозволяє компаніям у реальному часі відстежувати коливання ринку та геополітичні ризики, забезпечуючи швидкість і точність прийняття стратегічних рішень. Автоматизація та диджиталізація додатково сприяють розвитку стійких операційних структур, знижуючи витрати та підвищуючи ефективність глобальних транзакцій. Ці технології є особливо

важливими для подолання складності гібридних загроз, оскільки дозволяють корпораціям виявляти вразливості, прогнозувати потенційні збої та впроваджувати превентивні заходи.

Кіберзагрози, як ключовий компонент гібридних атак, є одним із найбільших глобальних викликів для корпорацій у диджиталізованій економіці. Ці загрози мають широкі наслідки: від порушення цифрової інфраструктури до підриву довіри на міжнародних ринках. Дослідження підкреслюють важливість багаторівневих систем безпеки, які використовують міждисциплінарні підходи для виявлення, оцінки та пом'якшення ризиків [5]. Застосування штучного інтелекту та аналітики великих даних виявилося особливо ефективним для посилення заходів кібербезпеки, дозволяючи прогнозувати потенційні загрози та швидко на них реагувати. Ці технології не лише захищають цифрові активи, але й підтримують прийняття рішень, надаючи організаціям актуальну інформацію про нові ризики.

У контексті України та інших країн, що розвиваються, глобальний характер гібридних загроз створює додаткові виклики та можливості. Залежність від міжнародних фінансових систем та ланцюгів постачання робить локальні корпорації особливо вразливими до зовнішнього тиску, економічної нестабільності та вторинних наслідків глобальних криз [4]. Наприклад, геополітичні напруження, які впливають на міжнародні торговельні маршрути, можуть серйозно порушувати локальні ланцюги постачання, посилюючи вразливість корпоративного сектору. Для вирішення цих проблем корпорації мають пріоритизувати розвиток локалізованих інновацій, які посилюють їхню здатність орієнтуватися у глобальних ринках, одночасно мінімізуючи ризики. До таких інновацій відносяться розробка регіонально специфічних рамок управління ризиками, впровадження адаптивних моделей управління та розширення співпраці з міжнародними партнерами для зміцнення стійкості.

Організаційні інновації є критично важливими для корпорацій, які прагнуть ефективно орієнтуватися у складнощах глобалізованої економіки, формованої гібридними загрозами. Впроваджуючи інноваційні практики та інтегруючи передові технології у свої операційні структури, компанії можуть підвищити свою стійкість до гібридних загроз, зберегти операційну стабільність і використовувати можливості на нестабільних ринках. Ці інновації створюють основу для розвитку сучасних бізнес-моделей, які не лише відповідають на глобальні виклики, але й забезпечують стале зростання в умовах економічної невизначеності та геополітичної нестабільності.

Література:

1. Hybrid threats against industry 4.0: adversarial training of resilience / O. Kaikova et al. E3S web of conferences. 2022. Vol. 353. P. 03004. URL: https://doi.org/10.1051/e3sconf/202235303004 (date of access: 19.11.2024).

2. Mazaraki A., Kalyuzhna N., Sarkisian L. Multiplicative effects of hybrid threats*. Baltic journal of economic studies. 2021. Vol. 7, no. 4. P. 136–144. URL: https://doi.org/10.30525/2256-0742/2021-7-4-136-144 (date of access: 19.11.2024).

3. Perilla Maluche R. B., Orozco Castro L. A. Organizational innovation and business model innovation: bridges from a systematic literature review. *International journal of innovation science*. 2023. URL: https://doi.org/10.1108/ijis-08-2022-0143 (date of access: 18.11.2024).

4. Shyra T. Corporate sector: development trends and threats of corporate security of enterprises. Eastern Europe: economy, business and management. 2019. № 6(23). URL: https://doi.org/10.32782/easterneurope.23-66 (дата звернення: 19.11.2024).

5. Trim P. R. J., Lee Y.-I. Managing cybersecurity threats and increasing organizational resilience. Big data and cognitive computing. 2023. Vol. 7, no. 4. P. 177. URL: https://doi.org/10.3390/bdcc7040177 (date of access: 19.11.2024).