https://doi.org/10.31891/2307-5740-2024-334-69
УДК 330

ЛЮБОХИНЕЦЬ Лариса
Хмельницький національний університет
https://orcid.org/0000-0003-1578-615X
e-mail: lubohinets@ukr.net
ПОПЛАВСЬКА Ольга
Хмельницький національний університет
https://orcid.org/0000-0001-5539-5845
e-mail: l-o-v-88@ukr.net
ВІНСКЕВИЧ Олександр
Хмельницький національний університет
https://orcid.org/0009-0008-4464-1287

КОНВЕРГЕНЦІЯ МАРКЕТИНГУ ТА ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

В статті досліджено взаємозв'язок маркетингу та фінансово-економічної безпеки в умовах розвитку інформаційних технологій, так як їх конвергенція є невід'ємною частиною сучасного бізнесу. Цифрові трансформації значно змінюють ландшафт маркетингу та фінансово-економічної безпеки, щоб успішно працювати в нових умовах, підприємства повинні інвестувати в цифрові технології, захищати дані клієнтів та системи від кібератак та шахрайських дій, постійно адаптуватися до нових технологій та ринкових умов. В умовах сьогодення економічність, раціональність та максимальна ефективність на основі використання сучасних інформаційних та мультимедійних технологій є запорукою не лише якісного управління, а й загальної конкурентоспроможності компанії на ринках.

Ключові слова: конвергенція, маркетинг, фінансово-економічна безпека, економічна безпека, маржа безпеки, методи ситуаційного управління, метод аналізу чутливості, коефіцієнт чутливості небезпеки, шахрайство, індикатори функціональних компонент економічної безпеки

LIUBOKHYNETS Larysa, POPLAVSKA Olga, VINSKEVYCH Oleksandr
Khmelnytskyi National University

CONVERGENCE OF MARKETING AND FINANCIAL AND ECONOMIC SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION

The article examines the relationship between marketing and financial and economic security in the context of the development of information technologies, as their convergence is an integral part of modern business. Digital transformations significantly change the landscape of marketing and financial and economic security, in order to work successfully in new conditions, enterprises must invest in digital technologies, protect customer data and systems from cyber attacks and fraudulent actions, constantly adapt to new technologies and market conditions. In today's conditions, economy, rationality and maximum efficiency based on the use of modern information and multimedia technologies are a guarantee not only of quality management, but also of the company's overall competitiveness in the markets.

Marketing plays a key role in ensuring the financial and economic security of the enterprise, i.e. constant monitoring of the market, analysis of competitors and study of customer needs allow timely detection of potential threats and development of effective strategies to neutralize them. Thanks to a deep understanding of customer needs and market dynamics, marketing contributes to the development of effective strategies that allow the enterprise to adapt to changes and maintain its competitiveness, optimize its costs, improve product quality and strengthen its position in the market. In the conditions of growing global competition, companies must understand the development trends of international markets, cultural characteristics and take into account legislative norms in their activities. In this case, marketing helps to adapt business to new conditions, and economic security provides protection from external threats. The rapid development of digital technologies is changing the rules of the game in the market, while marketing allows effective use of digital channels to interact with customers, and economic security provides protection against cyber threats and other risks related to digital technologies. Consumers increasingly expect a personalized approach and high quality products and services, so marketing helps to understand the needs of customers and develop appropriate offers, and financial and economic security ensures that these offers will be fulfilled with quality and time. New players are constantly entering the market, which complicates competition, so there is a need to stand out among competitors, determine the company's competitive advantages, build a positive image and effectively manage crisis situations. In this case, economic security protects against unfair competition, ensures business stability in conditions of uncertainty, helps protect company data from cyber attacks and fraudulent actions, and prevents financial losses.

Therefore, ensuring financial and economic security during marketing operations is a complex task that requires a complex approach. The convergence of marketing and financial and economic security allows you to minimize risks, ensure sustainable business development and effective promotion of goods and services, and protect the reputation of the company and its assets. The interaction of marketing and economic security helps prevent crisis situations related to security breaches that can negatively affect the company's image, as well as avoid ineffective spending on marketing campaigns related to unsafe or unethical practices

Key words: convergence, marketing, financial and economic security, economic security, margin of safety, methods of situational management, method of sensitivity analysis, risk sensitivity coefficient, fraud, indicators of functional components of economic security

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Швидкий розвиток інформаційних технологій створює нові виклики для бізнесу, підвищуючи рівень невизначеності, тому для успішного функціонування в умовах цифрових трансформацій компанії змушені постійно вдосконалювати свої процеси, як щодо маркетингових технологій, так і забезпечення фінансово-економічної безпеки бізнесу. Застосування сучасних маркетингових інструментів та методів управління дозволяє підприємствам стати більш гнучкими, адаптуватися до змін ринку та забезпечити свою фінансову стабільність.

Маркетинг відіграє ключову роль у забезпеченні фінансово-економічної безпеки підприємства, тобто постійний моніторинг ринку, аналіз конкурентів та вивчення потреб клієнтів дозволяють своєчасно виявляти потенційні загрози та розробляти ефективні стратегії їх нейтралізації. Конвергенція маркетингу та фінансово-економічної безпеки є невід'ємною частиною сучасного бізнесу. Завдяки глибокому розумінню потреб клієнтів та динаміки ринку, маркетинг сприяє розробці ефективних стратегій, які дозволяють підприємству адаптуватися до змін та зберігати свою конкурентоспроможність, оптимізувати свої витрати, підвищити якість продукції та зміцнити свою позицію на ринку. Конвергенція дозволяє не тільки захистити компанію від загроз, але й підвищити ефективність маркетингових кампаній, зміцнити довіру клієнтів та забезпечити сталий розвиток бізнесу

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Теоретичні основи категорії конвергенції закладені в працях представників інституційного напряму розвитку економічної думки таких як Арон Р., Тінберген Ян, Ростоу У., Дракер П., Гелбрейт Дж., Балаша Б., при цьому ідею конвергенції вчені поширювали на всі сфери суспільного розвитку, але її основна теза була у поступовому стиранні економічних, політичних і соціальних розбіжностей між різними економічними системами, які в перспективі об'єднаються у високорозвинене постіндустріальне суспільство. Так, Дж. Гелбрейт до проблеми «конвергенції» двох систем підходить з погляду розмірів виробництва, його техніко-організаційної сторони і ігнорує відмінності у сферах власності, Р. Арон висував ідею плюралізму всесвітнього розвитку, для якого характерним є існування індустріальних суспільств різного типу, М. Дюверже майбутнє різних економічних систем уявляв як систему «демократичного соціалізму», яка утвориться в результаті неминучих процесів лібералізації на Сході і соціалізації на Заході [1, с.261]. Ключовим мотивом теорії конвергенції було прагнення уникнути глобальної катастрофи. Вчені попереджали, що протистояння двох протилежних економічних систем може призвести до неконтрольованої ескалації конфлікту, аж до ядерної війни. Тому пропонувалося знайти спільну основу для співпраці, об'єднавши найкращі аспекти обох систем. Сьогодні ми спостерігаємо швидку конвергенцію різних технологій (наприклад, біотехнології, нанотехнології, інформаційні технології), що призводить до появи нових продуктів і послуг. Проблеми конвергенції маркетингу за умов сталого розвитку досліджує Садченко О. [2], конвергенцію економічного потенціалу та економічної безпеки – ВасильцівТ., Міценко Н., Мульська О., Зайченко В. [3], конвергенцію бенчмаркетингу і стандартів якості – Тельнов А. [4], Орлик О. аналізує можливості підвищення економічної безпеки підприємств на основі інтернет-технологій маркетингу [5]. Тому конвергенція маркетингу та фінансово-економічної безпеки бізнесу в умовах постійних змін бізнес-середовища, пов'язаних з розвитком цифрових технологій є актуальним напрямком дослідження

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження напрямів взаємозв'язку та взаємодії маркетингу та фінансово-економічної безпеки підприємств за умов трансформації сучасних цифрових технологій

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В умовах зростання глобальної конкуренції компаній мають розуміти тенденції розвитку міжнародних ринків, культурних особливостей та враховувати в своїй діяльності законодавчі норми. В цьому випадку маркетинг допомагає адаптувати бізнес до нових умов, а економічна безпека забезпечує захист від зовнішніх загроз. Швидкий розвиток цифрових технологій змінює правила гри на ринку, при цьому маркетинг дозволяє ефективно використовувати цифрові канали для взаємодії з клієнтами, а економічна безпека забезпечує захист від кіберзагроз та інших ризиків, пов'язаних з цифровими технологіями. Споживачі все більше очікують персоналізованого підходу та високої якості продуктів і послуг, тому маркетинг допомагає зрозуміти потреби клієнтів та розробити відповідні пропозиції, а фінансово-економічна безпека гарантує, що ці пропозиції будуть виконані якісно та вчасно. На ринок постійно виходять нові гравці, що ускладнює конкуренцію, тому виникає потреба виділитися серед конкурентів, визначити конкурентні переваги компанії, побудувати позитивний імідж та ефективно управляти кризовими ситуаціями. В цьому випадку економічна безпека захищає від недобросовісної конкуренції, забезпечує стабільність бізнесу в умовах невизначеності, допомагає захистити дані компанії від кібератак та шахрайських дій та запобігти фінансовим втратам.

Забезпечення фінансово-економічної безпеки підприємств передбачає використання найбільш адекватних науково-методичних підходів та інструментів, які відповідають існуючим умовам ведення бізнесу [6]. Серед основних методів, які використовуються для побудови і подальшого функціонування механізму забезпечення економічної безпеки промислових підприємств використовуються такі: метод системного аналізу, метод ситуаційного аналізу, метод імітаційного моделювання, аналіз чутливості, метод діагностики, метод аналогій, метод теорії ігор, нейронні мережі. Наявність значної кількості методів не означає доцільність одночасного їх використання, оскільки побудова механізму доволі кропіткий процес, який передбачає відповідний рівень гнучкості управлінських рішень. Такі рішення реалізуються за допомогою використання інструментального забезпечення управлінських процесів, причому Scrum, Kanban, Bug tracker, Index cards, Agile project management tool, Wireframes, Timecards, Spreadsheet доцільно використовувати для забезпечення належного рівня гнучкості системи управління підприємством в цілому і системи економічної безпеки зокрема.

В основі формування механізму забезпечення економічної безпеки промислових підприємств, на основі використання інструментів гнучкого управління, мають стояти методи ситуаційного управління, тобто сукупність прийомів і способів впливу на об'єкт управління для досягнення поставлених цілей підприємства. Частіш за все, в ситуаційному управлінні використовують методи системного та ситуаційного аналізу, метод діагностики, аналогій, методи імітаційного моделювання, теорії ігор тощо. На нашу думку, в основі цих методів повинен бути аналіз чутливості, який є одним з методів проведення розрахунків в умовах невизначеності. Цей метод управління використовується менеджерами з метою визначення зміни результату, якщо початково заплановані події чи основні передумови змінились.

В основі аналізу чутливості лежить метод аналізу даних, який більше зустрічається в інженерній економіці і теорії прийняття управлінських рішень під назвою «ранжування параметрів» та передбачає розрахунок базової моделі на основі припустимих значень вхідних змінних, для якого визначається стан фінансово-економічної безпеки за функціональними компонентами економічної безпеки. Наступним кроком проведення аналізу чутливості є визначення аналізу критичних змін параметрів, причому критичним називають значення змінної, за якого підприємство буде потрапляє у високу зону небезпеки. Таким чином, суть даного методу полягає у вимірювані чутливості основних результуючих показників до зміни факторів. Аналіз чутливості привабливий при виявленні факторів, оскільки дозволяє виділити найбільш важливі з них, що відповідає положенням рівноважного підходу до забезпечення економічної безпеки підприємства. В центрі аналізу чутливості лежать коефіцієнт чутливості небезпеки та «маржа безпеки». В загальному вигляді коефіцієнти чутливості небезпеки $К_{чн}$ обчислюється формулою (1):

$$Кчн = \frac{Тпр_y}{Тпр_x} \quad (1)$$

де $Тпр_y$ – темпи приросту (зниження) індексу функціональної компоненти економічної безпеки;
$Тпр_x$ – темпи приросту (зниження) фактор-аргументу.

Після формування найбільш важливих факторів для підприємства, рекомендується провести безпосередньо аналіз чутливості функціональних компонент економічної безпеки відповідно до запропонованої методики, метою якого є визначення впливу цих факторів на кінцеві результати діяльності підприємства в умовах невизначеності. Таким чином, можна передбачити можливий вплив факторів небезпеки на стан економічної безпеки підприємства та у випадку фактичної зміни параметра бути готовим до нейтралізації загроз.

В основі аналізу чутливості функціональних компонент економічної безпеки є категорія «маржа безпеки» (margin of safety). Зазначимо, концепція «маржі безпеки» була розроблена Бенджаміном Грехемом (Benjamin Graham) з метою зниження ризиків і набула широкого розповсюдження в сфері інвестування [7]. Б. Грехем був інвестором та наставником інвестування і його вважають батьком аналізу безпеки та інвестування вартості. Під маржою безпеки Б. Грехем розумів рівень ціни, яку обирав інвестор для придбання акцій, або відсоток від реальної вартості цінного паперу, за якого її можна купувати [7].

На думку багатьох фахівців у сфері зменшення ризиків в інвестуванні концепція «маржі безпеки» є важливим інструментом в процесі формування оптимального портфеля якісних облігацій та привілейованих акцій. Згідно з концепцією, здатність компанії у минулому періоді генерувати прибуток, розмір якого значно перевищує її відсоткові виплати, створює так звану «маржу безпеки», яку можна розглядати як захист інвестора від втрат внаслідок неочікуваних коливань на фінансовому ринку.

З позиції формування механізму забезпечення економічної безпеки підприємства концепція «маржі безпеки» також набуває особливої актуальності, звичайно в контексті використання інструментів гнучкого управління. В цьому контексті «маржа безпеки» – перевищення фактичного значення індикаторів функціональних компонент економічної безпеки над пороговими (рис. 1).

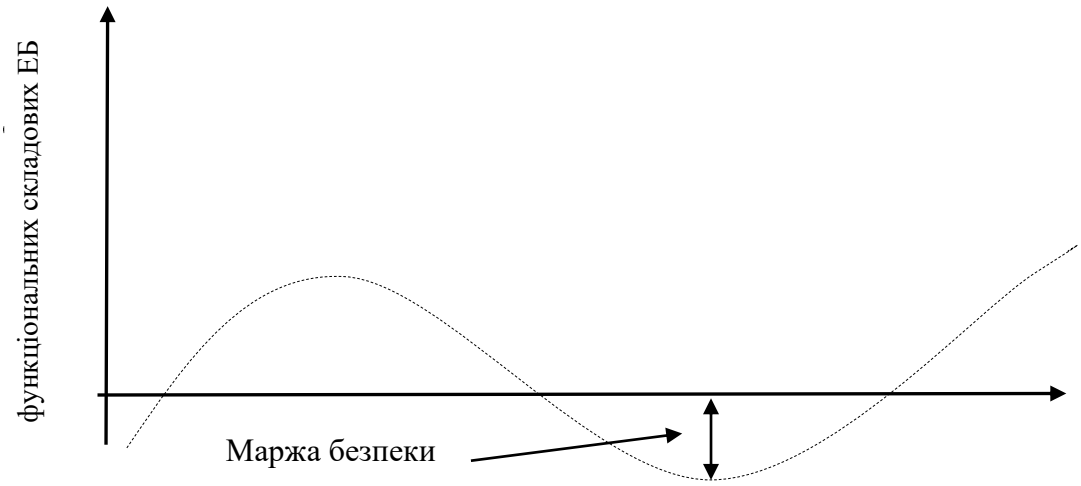

Рис. 1. Маржа безпеки [6]

Використання «маржі безпеки» дозволить працівникам служби економічної безпеки (СЕБ) здійснювати постійний моніторинг за рівнями функціональних компонент економічної безпеки. Крім того, порівнюючи порогові значення індикаторів з фактичними, аналітики зможуть виявляти потенційні загрози та рівень «маржі безпеки». Використовуючи інструментарій аналізу чутливості, можна здійснювати імітаційне моделювання та прогнозування впливу відповідних управлінських рішень на рівень економічної безпеки підприємства.

Розроблення механізму забезпечення економічної безпеки промислових підприємств на основі використання інструментів гнучкого управління потребує формування відповідного переліку індикаторів економічної безпеки в розрізі її функціональних проекцій, а саме: ресурсна, фінансово-економічна, організаційно-правова, управлінська, технологічна, інформаційна, кадрова та соціальна безпека (Таблиця 1).

Зазначимо, що запропонований в таблиці 1 інструментарій враховує природу загроз економічній системі промислового підприємства та забезпечить можливість їх виявлення, аналізу та нейтралізації з врахуванням їх сили та інтенсивності.

Розглянемо функціональні компоненти економічної безпеки більш детально.

Ресурсна безпека промислового підприємства – це забезпеченість виробництва основними видами ресурсів, а саме: основними засобами, матеріальними та енергетичними ресурсами, а також розроблення заходів щодо подолання загрозливих явищ внаслідок зростання цін на них. В цілому, ресурсна безпека забезпечує стійкий стан захищеності підприємства від негативного впливу зовнішніх та внутрішніх загроз, дестабілізуючих факторів, за якого забезпечується ефективний рух матеріальних потоків.

Під фінансово-економічною безпекою промислового підприємства розуміють ступінь захищеності фінансових інтересів підприємства на всіх рівнях його фінансових відносин. Фінансова-економічна безпека є функціональною компонентою економічної безпеки, проте має своє специфічне значення, оскільки її зміст безпосередньо пов’язаний з основною метою функціонування промислового підприємства – отримання прибутку. Основними її завданнями є: формування здатності фінансової системи підприємства забезпечити ефективне функціонування його економічної системи та стійке економічне зростання; можливість протистояти загрозам внаслідок формування відповідного фінансового забезпечення; формування відповідного рівня забезпеченості підприємства фінансовими ресурсами, достатніми для задоволення його потреб та виконання існуючих зобов’язань.

Індикатори фінансової безпеки є системою показників, динаміка яких дозволяє зробити висновок про тенденції її розвитку, на основі яких доцільно формувати комплекс заходів щодо попередження та усунення загроз фінансовій безпеці промислового підприємства.

Організаційно-правова безпека промислового підприємства – це комплекс заходів, направлених на захист підприємства від нестабільного законодавства, постійний моніторинг правил та умов взаємодії з контрагентами й державними контролюючими та правоохоронними органами, мінімізація негативного впливу надмірного податкового тиску, а також контроль якості взаємодії усіх територіальних підрозділів із головним офісом.

Забезпечення управлінської безпеки промислового підприємства полягає в участі працівників служби економічної безпеки у створенні та підтримці ефективного функціонування його структури управління, попередження та мінімізації конфліктів співвласниками з менеджментом підприємства, організації взаємодії та координації між усіма структурними підрозділами системи задля досягнення поставлених цілей.

Технологічна складова економічної безпеки промислового підприємства та необхідність її забезпечення стає дедалі важливішим стратегічним напрямом в сучасних умовах. Забезпечення

технологічної безпеки має ґрунтуватись на основі визначених цілей та пріоритетів промислового підприємства, а саме забезпечувати їхню реалізацію. Однак при цьому необхідно враховувати результати дослідження стану зовнішнього та внутрішнього середовищ для своєчасного виявлення та запобігання існуючим загрозам. Напрями та обсяги інвестицій, а також терміни їх вкладення вимагають чіткої класифікації науково-обґрунтованих індикаторів технологічної складової економічної безпеки підприємства. Сутність оцінювання технологічної складової економічної безпеки промислового підприємства полягає в тому, наскільки рівень технологій на підприємстві відповідає найкращим світовим аналогам.

Таблиця 1

Характеристика індикаторів функціональних компонент економічної безпеки [6]

Функціональна складова економічної безпеки	**Індикатор**	**Порогове значення**	**Суб'єкт експертного оцінювання**
Ресурсна	Рівень придатності основних засобів	> 0,5	Працівники СЕБ, керівник відділу матеріально-технічного забезпечення
	Забезпеченість матеріальними ресурсами	100 %	
	Забезпеченість енергетичними ресурсами	100 %	
	Забезпеченість технологічними ресурсами	100 %	
Фінансово-економічна	Рентабельність активів	> 15 %	Працівники СЕБ, працівники фінансового управління
	Коефіцієнт покриття	> 1,2	
	Коефіцієнт абсолютної ліквідності	> 0,2	
	Приріст обсягів реалізованої продукції	> 10 %	
Організаційно-правова	Відповідність установчих документів вітчизняному законодавству та видам діяльності	1	Працівники СЕБ, керівник юридичного управління
	Відсутність неузгодженостей з контрагентами	1	
	Відсутність проблем взаємодії з державними контролюючими та правоохоронними органами	1	
	Платоспроможність партнерів	1	
Управлінська	Відсутність розбіжностей серед співвласників	1	Працівники СЕБ, власники, керівник юридичного управління
	Відсутність розбіжностей між співвласниками та менеджментом	1	
	Рівень компетентності вищого менеджменту	1	
	Якість взаємодії структурних підрозділів із службою економічної безпеки	1	
Технологічна	Відсоток нової продукції в загальному обсязі	> 10 %	Працівники СЕБ, керівник технічного управління
	Динаміка інвестицій у модернізацію обладнання	> 10 %	
	Частка продукції без рекламацій щодо якості	> 95 %	
	Коефіцієнт використання виробничої потужності	> 0,8	
Інформаційна	Рівень захисту інформації	1	Працівники СЕБ, керівник інформаційно-технічного відділу
	Захист від вірусної шкоди інформаційним ресурсам підприємства	1	
	Бізнес-репутація підприємства	1	
	Рівень захисту інформаційної інфраструктурі	1	
Кадрова	Коефіцієнт стабільності кадрів	1	Працівники СЕБ, керівник відділу кадрів
	Середня заробітна плата на підприємстві порівняно із середньою заробітною платою в галузі (регіоні)	1	
	Продуктивність праці	1	
	Забезпеченість трудовими ресурсами	1	
Соціальна	Ступінь задоволення соціальним пакетом на підприємстві	1	Працівники СЕБ, голова профкому
	Стан техніки безпеки на підприємстві	1	
	Ступінь задоволеністю оплатою праці	1	
	Ступінь задоволеністю умовами праці	1	

Система кадрової безпеки промислового підприємства є взаємозв'язком процесів запобігання негативним впливам на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з людськими ресурсами промислового підприємства, їх інтелектуальним потенціалом та трудовими відносинами. Система кадрової безпеки має спиратися на 3 ключові аспекти: перспективний рекрутинг, лояльність до персоналу і контроль персоналу. Суб'єктами кадрової безпеки є вищий менеджмент, співробітники служби управління персоналом та працівники служби економічної безпеки.

Соціальна безпека промислового підприємства має на меті не тільки його розвиток та реалізацію інтересів, а й задоволення матеріальних і нематеріальних потреб працівників.

Інформаційна безпека промислового підприємства – це стан інформаційної системи, за якого вона найменш уразлива до втручання та заподіяння шкоди з боку третіх осіб. Безпека даних також має на увазі управління ризиками, пов'язаними з розголошенням інформації або впливом на апаратні та програмні модулі захисту. Загрози інформаційної безпеки являють собою певні дії, які можуть призвести до порушення стану захисту інформації на підприємстві, або потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам. Залежно від різних способів

класифікації, всі можливі загрози інформаційної безпеки можна згрупувати за такими ознаками: небажаний контент, несанкціонований доступ, витік інформації, втрата даних, кібертероризм.

Порушення режиму інформаційної безпеки може бути спричинене як спланованими операціями зловмисників, так і недосвідченістю працівників. Користувачі інформації за усіма каналами її обігу повинні володіти відповідними знаннями щодо правил користування та обміном інформацією, а також запобігати випадкам появи шкідливого програмного забезпечення, яке може завдати значних збитків для економічної системи підприємства. Такі інциденти, як втрата або витік інформації, можуть бути обумовлені цілеспрямованими діями співробітників підприємства, які зацікавлені в отриманні вигоди в обмін на цінні дані.

Світ цифрових технологій відкриває нові можливості, але водночас створює сприятливе середовище для шахраїв. Конвергенція маркетингу та фінансово-економічної безпеки є життєво необхідною для сучасних підприємств. Однак, ця взаємодія також породжує певні ризики та загрози, які необхідно враховувати та нейтралізувати. Постійно з'являються нові, досконаліші схеми обману, які становлять серйозну загрозу як для споживачів, так і для бізнесу. Основними джерелами загроз є окремі зловмисники («хакери»), кіберзлочинні групи, які застосовують весь арсенал доступних кіберзасобів. Для отримання доступу до потрібної інформації використовуються слабкі місця та помилки в роботі програмного забезпечення та вебзастосунків, вдаються до прослуховування каналів зв'язку та використання клавіатурних шпигунів.

В сучасному невизначеному та нестабільному конкурентному середовищі боротьба з корпоративним шахрайством стає важливою умовою економічної стійкості суб'єктів господарювання, так як шахрайство залишається однією із значних проблем для компаній як на національному, так і міжнародному рівнях. При цьому корпоративне шахрайство спрямоване на розкрадання активів найманими працівниками, менеджерами чи власниками компаній шляхом обману або зловживанням довірою в особистих цілях на шкоду інтересам компанії і характеризується навмисним втручанням у фінансово-економічну діяльність компанії з метою здійснення або приховування шахрайських дій. Як показують статистичні дослідження Association of Certified Fraud Examiners (ACFE) світові компанії втрачають щорічно близько 5% прибутку через несумлінні дії своїх співробітників [8]. Відповідно до світової статистики внаслідок економічних злочинів і шахрайства щорічно втрачається 6,3 трлн доларів США [9]. Щодо України, то ця цифра в деяких випадках досягає 10-15%. В Україні 61,5 % компаній зазнавали шахрайства. При цьому 20% компаній оцінили свої збитки від шахрайства в сумі від $100 тис. до $5 млн на рік. Україна посідає 5 місце в рейтингу країн світу за рівнем корпоративного шахрайства [9].

Серед ризиків, що призводять до шахрайських дій відносять: відсутність систем внутрішніх контролів; самоусунення власника від прямого управління компанією; відсутність критеріїв виміру ефективності бізнесу; особисте небажання власника впроваджувати заходи протидії шахрайству; акцент на готівку при проведенні фінансових транзакцій. За результатами Всесвітнього дослідження економічних злочинів та шахрайства 2020-2024 компанії PwC до Топ-5 видів шахрайств відносять: незаконне привласнення майна (47%), хабарництво та корупція (47%), шахрайство з боку клієнтів (31%), кіберзлочини (31%), шахрайство у закупівлях (31%) [10]. 70% опитаних організацій в Україні зазначили, за результатами опитування PwC 2024 року, що шахрайство у закупівлях є поширеною проблемою, при цьому лише невелика частка опитаних організацій використовує інструменти для виявлення шахрайства чи його протидії [11]. За результатами «Глобального дослідження економічної злочинності 2024» компанії PwC Global, шахрайство під час закупівель, зокрема, входить до трійки найбільш руйнівних економічних злочинів, з якими стикалися компанії в усьому світі за останні 24 місяці – відразу після кіберзлочинності та корупції [12]. За даними Торгової палати США, 75% працівників крали у свого роботодавця принаймні один раз. Палата також встановила, що до 30% невдач у бізнесі можуть бути наслідком шахрайства та зловживань співробітників [13]. За результатами опитування PwC 2024 року **41% респондентів з України жодного разу не проводили перевірку доброчесності своїх контрагентів** [11]. Тому власникам компаній необхідно постійно проводити процедури спрямовані на захист бізнесу, які включають аналіз та моніторинг всіх змін, що відбуваються в ході діяльності компанії та можуть впливати на її результативність по забезпеченню економічної безпеки. Хоча майже половина національних компаній не проводить взагалі або проводить лише неформальну перевірку доброчесності своїх респондентів, лише 59% українських організацій провели розслідування виявлених випадків шахрайства. Як показали дослідження економічних злочинів та шахрайства 2020 компанії PwC, кожна четверта організація в Україні не має спеціальної програми з управління ризиками і 22% респондентів не проводили жодної оцінки ризиків за останні два роки [10]. За даними дослідження 2024 року 84% респондентів з України висловили впевненість у тому, що їх програми комплаєнсу здатні мінімізувати потенційні корупційні ризики, в той же час, 25% респондентів або взагалі не мають формалізованої програми управління ризиками взаємодії з контрагентами, або, навіть якщо і мають її - не проводять оцінку ризиків такої співпраці [11], на глобальному рівні таких респондентів 42% [12].

В умовах розвитку цифрових технологій національні компанії застосовують сучасні інформаційні технології і методи для виявлення шахрайських дій і все ж залишаються не захищені від кібератак. З'ясовано, що лише третина організацій в Україні має програму кіберзахисту, хоча *кожне порушення*

механізму захисту бази даних може паралізувати роботу великих фірм та об'єднань, призвести до значних матеріальних втрат. Як приклад можна привести дві самі великі кібер-атаки WannaCry та GoldenEye/Petya, що були проведені в першій половині 2017 року і від яких постраждали майже всі країни світу і велика кількість компаній, більше 230 000 комп'ютерів. За різними оцінками експертів, втрати від цих атак склали від 1 до 4 млрд. дол. США, тобто від 4300 до 17000 дол. в розрахунку на кожний комп'ютер [14]. Одна із найбільших кібератак в Україні DDoS-атака 15лютого 2022 року привела до того, що сайти майже 15 банків і держорганів були недоступні протягом п'ятьох годин. З лютого 2022 року відбулося орієнтовно 10 тисяч кібератак та критичних інцидентів [15]. Тому звичайно піднімається питання про розробку програм захисту інформаційного ресурсу компаній, баз даних, національного інформаційного простору, створення умов для якісного й ефективного інформаційного забезпечення всіх зацікавлених сторін, підтримку проєктів і програм інформатизації, страхування інформаційних ризиків. За даними брокера Marsh, до 2022 року ціни на страхування кіберризиків зросли на 150%, зараз вони збільшились ще в середньому на 10-15%. У деяких випадках спостерігається зниження від 10% до 25% [16].

Так як нестабільність економічного розвитку та вимушене переведення співробітників на віддалену роботу збільшує масштаби внутрішнього шахрайства в компаніях, забезпечення економічної безпеки вимагає пошуку перспективних шляхів тісної взаємодії й координації державних та недержавних структур у системі запобігання шахрайських дій. Ризики шахрайства можуть виникнути і через нестабільний фінансовий стан постачальників та покупців, тому вкрай важливо здійснювати моніторинг зміни фінансового становища таких компаній і визначати нові траєкторії їх розвитку.

Не останнє місце в програмах розвитку бізнесу займає і соціальна відповідальність всіх зацікавлених сторін. За даними ООН United Nations Global Compact, компанії, які враховують ESG-фактори (інформація про екологічні, соціальні, управлінські чинники підприємства), є більш привабливими для інвесторів та партнерів. Вони отримують на 12% більшу маржу й на 19% більшу ринкову вартість та кредитоспроможність у довгостроковій перспективі [17]. Якщо серед світових трендів розвитку бізнесу 2022 року виділяють вимогу врахування ESG-факторів у бізнес-стратегії компанії, необхідність проведення діджеталізації бізнесу, кооперацію та інтеграцію бізнес-процесів, то до 19 технологічних трендів 2024 року відносять поширення генеративного ШІ, злиття ІТ-підрозділів з підрозділами безпеки, Інтернет речей, технології сталості, роботизовану автоматизацію процесів (RPA) [18]. При цьому оптимізація процесів допоможе звільнити величезну кількість ресурсу та розподіляти час більш ефективніше, а також допоможе визначати шляхи протидії корпоративному шахрайству й усунення процесуальних недоліків, які дали змогу нанести компанії збиток.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, забезпечення фінансово-економічної безпеки при проведенні маркетингових операцій є складним завданням, яке вимагає комплексного підходу. Конвергенція маркетингу та фінансово-економічної безпеки дозволяє мінімізувати ризики, забезпечити сталий розвиток бізнесу та ефективне просування товарів та послуг, захист репутації компанії та її активів. Взаємодія маркетингу та економічної безпеки допомагають запобігти кризовим ситуаціям, пов'язаним з порушеннями безпеки, які можуть негативно вплинути на імідж компанії, а також уникати неефективних витрат на маркетингові кампанії, пов'язані з небезпечними або неетичними практиками.

В умовах сьогодення економічність, раціональність та максимальна ефективність на основі використання сучасних інформаційних та мультимедійних технологій є запорукою не лише якісного управління, а й загальної конкурентоспроможності компанії на ринках. Більшість провідних компаній світу еволюційним шляхом дійшли до розуміння відсутності уніфікованих мультипроєктних інструментів ведення бізнесу і використовують комбінації найбільш придатних інструментів у конкретний період часу для вирішення чітко сформульованих завдань. Розробка власного інструментарію та комбінування найкращих практик дозволяє реалізовувати стратегічні завдання та забезпечувати спроможність до конкуренції за споживача товарів, робіт та послуг

Література

1. Любохинець Л.С. Історія політичних та економічних вчень: навч.посіб / Л.С.Любохинець, В.М. Шавукн, Л.М.Бабич – К.: «Центр учбової літератури», 2021. – 294с.
2. Садченко О.В. (2024). Конвергенція в умовах сталого розвитку на прикладі підприємництва органічних добрив. *Сталий розвиток економіки.* №3(50). С.87-93
3. Васильців Т.Г., Міценко Н.Т., Мульска О.Г., Зайченко В.В. (2023) Економічний потенціал vs економічна безпека підприємства: точки конвергенції та дивергенції. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. Випуск 36. С.23-29
4. Тельнов А. (2022) Конвергенція бенчмаркінгу і стандартів якості як базис забезпечення фінансово-економічної безпеки суб'єктів господарської діяльності в умовах інформаційного суспільства. *Економічний аналіз*. Том 32. №1. С.282-289

5. Орлик О.В. (2019) Підвищення економічної безпеки підприємств на основі інтернет-технологій маркетингу. *Міжнародний науково-виробничий журнал Сталий розвиток економіки*. № 2 (43). С. 84–92

6. Любохинець Л. С. Методологія гнучкого управління у забезпеченні економічної безпеки промислових підприємств: оцінювання та моделювання : монографія / Л. С. Любохинець – Хмельницький : ХНУ, 2022. – 288 с.

7. Graham B. The intelligent investor: a book of practical counsel / B. Graham, J. Zweig. – 6th Ed. – New York : Collins Business Essentials, 2005. – 623 p

8. Report to the Nations 2018 Global Study on Occupational Fraud and Abuse. URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

9. Борис С. Шахрайство на підприємстві: причини та наслідки, виявлення та протидія. URL: https://uz.ligazakon.ua/ua/magazine_article/EA012486

10. Всесвітнє дослідження економічних злочинів та шахрайства 2020: результати опитування українських організацій. URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf

11. Всесвітнє дослідження економічних злочинів та шахрайства 2024: результати опитування українських організацій. URL: https://www.pwc.com/ua/uk/survey/2024/global-economic-crime-survey.html

12. Глобальне дослідження економічної злочинності 2024 URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

13. Ivy Walker. Your Employees Are Probably Stealing from You. Here are Five Ways to Put an End to It. URL: https://www.forbes.com/sites/ivywalker/2018/12/28/your-employees-are-probably-stealing-from-you-here-are-five-ways-to-put-an-end-to-it/?sh=3d27ebc93386

14. Panda labs - Звіт за 2 квартал 2017. URL: https://pandasecurity.bitrix24.ru/docs/pub/1c3e16b44b7eced067ca1ceb9ae381ce/default/?&

15. Кібервійна росії проти України URL: https://speka.media/kiberviina-rosiyi-proti-ukrayini-9qy4ok?utm_source=google&utm_medium=cpc&utm_campaign=21107681931&gad_source=1

16. Паращук О. Війна в Україні та системні кіберзагрози створюють проблеми для глобального ринку страхування URL: https://interfax.com.ua/news/blog/935615.html

17. 5 довгострокових тенденцій, які допоможуть вирости бізнесу у 2022 році. URL: https://youcontrol.com.ua/blog/yctrends2022/

18. 10 технологічних трендів 2024 року URL: https://wezom.com.ua/ua/blog/10-tehnologichnih-trendiv-2024-roku

References

1. Liubokhynets L.S. Istoriia politychnykh ta ekonomichnykh vchen: navch.posib / L.S.Liubokhynets, V.M. Shavukn, L.M.Babych – K.: «Tsentr uchbovoi literatury», 2021. – 294s.

2. Sadchenko O.V. (2024). Konverhentsiia v umovakh staloho rozvytku na prykladi pidpryiemnytstva orhanichnykh dobryv. Stalyi rozvytok ekonomiky. №3(50). S.87-93

3. Vasyltsiv T.H., Mitsenko N.T., Mulska O.H., Zaichenko V.V. (2023) Ekonomichnyi potentsial vs ekonomichna bezpeka pidpryiemstva: tochky konverhentsii ta dyverhentsii. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. Seriia yurydychna. Vypusk 36. S.23-29

4. Telnov A. (2022) Konverhentsiia benchmarkinhu i standartiv yakosti yak bazys zabezpechennia finansovo-ekonomichnoi bezpeky subiektiv hospodarskoi diialnosti v umovakh informatsiinoho suspilstva. Ekonomichnyi analiz. Tom 32. №1. S.282-289

5. Orlyk O.V. (2019) Pidvyshchennia ekonomichnoi bezpeky pidpryiemstv na osnovi internet-tekhnolohii marketynhu. Mizhnarodnyi naukovo-vyrobnychyi zhurnal Stalyi rozvytok ekonomiky. № 2 (43). S. 84–92

6. Liubokhynets L. S. Metodolohiia hnuchkoho upravlinnia u zabezpechenni ekonomichnoi bezpeky promyslovykh pidpryiemstv: otsiniuvannia ta modeliuvannia : monohrafiia / L. S. Liubokhynets – Khmelnytskyi : KhNU, 2022. – 288 s.

7. Graham B. The intelligent investor: a book of practical counsel / B. Graham, J. Zweig. – 6th Ed. – New York : Collins Business Essentials, 2005. – 623 r

8. Report to the Nations 2018 Global Study on Occupational Fraud and Abuse. URL: https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

9. Borys C. Shakhraistvo na pidpryiemstvi: prychyny ta naslidky, vyiavlennia ta protydiia. URL: https://uz.ligazakon.ua/ua/magazine_article/EA012486

10. Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraistva 2020: rezultaty opytuvannia ukrainskykh orhanizatsii. URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf

11. Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraistva 2024: rezultaty opytuvannia ukrainskykh orhanizatsii. URL: https://www.pwc.com/ua/uk/survey/2024/global-economic-crime-survey.html

12. Hlobalne doslidzhennia ekonomichnoi zlochynnosti 2024 URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

13. Ivy Walker. Your Employees Are Probably Stealing from You. Here are Five Ways to Put an End to It. URL: https://www.forbes.com/sites/ivywalker/2018/12/28/your-employees-are-probably-stealing-from-you-here-are-five-ways-to-put-an-end-to-it/?sh=3d27ebc93386

14. Panda labs - Zvit za 2 kvartal 2017. URL: https://pandasecurity.bitrix24.ru/docs/pub/1c3e16b44b7eced067ca1ceb9ae381ce/default/?&

15. Kiberviina rosii proty Ukrainy URL: https://speka.media/kiberviina-rosiyi-proti-ukrayini-9qy4ok?utm_source=google&utm_medium=cpc&utm_campaign=21107681931&gad_source=1

16. Parashchuk O. Viina v Ukraini ta systemni kiberzahrozy stvoriuiut problemy dlia hlobalnoho rynku strakhuvannia URL: https://interfax.com.ua/news/blog/935615.html

17. 5 dovhostrokovykh tendentsii, yaki dopomozhut vyrosty biznesu u 2022 rotsi. URL: https://youcontrol.com.ua/blog/yctrends2022/

18. 10 tekhnolohichnykh trendiv 2024 roku URL: https://wezom.com.ua/ua/blog/10-tehnologichnih-trendiv-2024-roku