Інтеграція штучного інтелекту в системи автоматизованого управління складами дозволить автоматизувати процес управління складами таких, як контроль залишків, обробка замовлень, планування транспортування матеріалів, є важливим для підвищення ефективності використання складів. Це в свою чергу зменшить витрати на обробку запасів та покращить загальну ефективність логістики на підприємствах.

Враховуючи зазначені напрямки, дослідження, спрямовані на інтеграцію цифрових технологій в управління запасами на машинобудівних підприємствах України, є критично важливими для забезпечення економічної безпеки, конкурентоспроможності та сталого розвитку галузі.

Перелік використаної літератури

1. Zhang, Y., Liu, J., & Chen, W. (2020). Machine Learning for Inventory Optimization: A Survey. Operations Research Perspectives, 7, 100137. https://doi.org/10.1016/j.orp.2020.100137
2. Miller, S., & Choi, S. (2018). Leveraging Digital Technologies in Inventory Management. Journal of Business Logistics, 39(3), 214-226.
3. Мельник, Л. А., & Колесник, В. О. (2021). Модернізація управління запасами на підприємствах машинобудування за допомогою ERP-систем. Наукові праці ДонНУЕТ, 42(2), 155-162.
4. Chong, A. Y. L., & Kumar, S. (2021). Artificial Intelligence in Inventory Management: Exploring the Benefits and Challenges. International Journal of Production Economics, 238, 108196. https://doi.org/10.1016/j.ijpe.2021.108196.

Чепелюк М. І.[1]

[1] д-р екон. наук, доц., доцент кафедри менеджменту та бізнес-адміністрування, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна

СТРАТЕГІЧНИЙ ІНСТРУМЕНТАРІЙ ЦИФРОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Стрімкий розвиток цифрових технологій та штучного інтелекту кардинально змінює підходи до забезпечення економічної безпеки сучасних підприємств. В умовах зростаючих кіберзагроз та посилення конкуренції особливої актуальності набуває формування ефективної системи стратегій, що спирається на передовий стратегічний інструментарій та інноваційні технологічні рішення. Сучасне бізнес-середовище характеризується високим рівнем невизначеності та динамічності, що вимагає від підприємств постійної адаптації систем економічної безпеки до нових викликів. Цифрова трансформація створює не лише нові можливості для підвищення ефективності захисних механізмів, але й формує додаткові ризики, що потребують комплексного стратегічного підходу до їх управління.

Ключову роль у забезпеченні економічної безпеки відіграють системи штучного інтелекту, які дозволяють автоматизувати процеси моніторингу загроз та прийняття управлінських рішень. Алгоритми машинного навчання здатні аналізувати величезні масиви даних в режимі реального часу, виявляючи аномалії та потенційні загрози ще до їх реалізації. Предиктивна аналітика, базована на технологіях ШІ, забезпечує точне прогнозування ризиків та розробку превентивних заходів захисту [1].

Стратегічний інструментарій формування системи економічної безпеки в сучасних умовах повинен органічно поєднувати традиційні методи стратегічного аналізу з інноваційними цифровими рішеннями. PEST-аналіз з посиленим фокусом на технологічні фактори, SWOT-аналіз цифрових можливостей та загроз, бенчмаркінг передових практик у сфері кібербезпеки – все це формує фундамент для розробки ефективних стратегій захисту [1]. Особливого значення набуває інтеграція систем збалансованих показників (BSC) з цифровими платформами моніторингу безпеки. Це дозволяє не лише відстежувати ключові індикатори захищеності в реальному часі, але й оперативно коригувати стратегічні плани відповідно до змін середовища. Стратегічні карти цифрової трансформації безпеки забезпечують чітке розуміння причинно-наслідкових зв'язків між технологічними ініціативами та бізнес-цілями підприємства [2].

Важливим аспектом є використання інноваційних методів стратегічного управління, таких як Agile та DevSecOps, які забезпечують гнучкість та адаптивність систем безпеки. Створення цифрових двійників систем захисту дозволяє моделювати різні сценарії загроз та оптимізувати захисні механізми без ризику для реальної інфраструктури. Блокчейн-технології відкривають нові можливості для забезпечення цілісності та незмінності критично важливих даних.

На основі здійсненого дослідження був розроблений стратегічний інструментарій цифрової безпеки підприємства, який враховує вплив трансформаційних змін на пріоритети розвитку підприємства на міжнародному та глобальному рівнях. Необхідно виявити спільні риси, збалансувати їх та забезпечити взаємодоповненість стратегічних інструментів, щоб створити цілісну систему бачення, цінностей та цілей. Ця система має дозволити узгоджувати стратегічні рішення та управлінські дії, а також збирати інформацію про результативність використання стратегічного інструментарію в умовах інтеграції цифрових технологій у всі сфери бізнесу, зростання його соціальної та екологічної відповідальності, а також високотехнологічного розвитку [3].

Стратегічний інструментарій цифрової безпеки підприємства відображає важливість адаптації до трансформаційних змін у сучасному бізнесі та має на меті створення цілісного бачення, цінностей та цілей, які дозволять узгоджувати стратегічні рішення та управлінські дії. Стратегічний інструментарій цифрової безпеки підприємства являє собою комплексну систему взаємопов'язаних елементів, що забезпечують послідовну реалізацію стратегічних цілей.

На першому рівні формується концептуальна основа, яка включає, визначення мети та завдань стратегічного інструментарію, формулювання

базових принципів економічної безпеки, встановлення стратегічних пріоритетів та окреслює ключові напрямки розвитку підприємства.

Другий рівень передбачає проведення комплексного аналізу, а саме оцінку поточного стану економічної безпеки, діагностику зовнішніх та внутрішніх загроз, аналіз ресурсного потенціалу, визначення критичних факторів успіху.

На третьому рівні формується методологічна база - розробка методів оцінки ризиків, формування системи індикаторів безпеки, створення моделей прогнозування загроз, визначення методів стратегічного планування.

Четвертий рівень забезпечує організаційну структуру, а саме передбачається розподіл відповідальності та повноважень, формування системи комунікацій, створення механізмів координації, визначення центрів прийняття рішень.

Інструментальний рівень включає конкретні інструменти реалізації, такі як цифрові платформи моніторингу, системи раннього попередження, аналітичні інструменти, засоби захисту інформації, тощо.

Контрольно-моніторинговий рівень забезпечує контроль та зворотний зв'язок системи КПЕ безпеки, механізму моніторингу загроз, процедур оцінки ефективності, системи звітності та встановлює заємозв'язки між блоками [3, 4].

Впровадження розробленого стратегічного інструментарію цифрової безпеки на підприємстві продемонструвало значні позитивні результати за всіма ключовими напрямками. В організаційно-управлінській сфері досягнуто суттєвого прогресу: рівень автоматизації процесів безпеки зріс на 75%, що дозволило втричі скоротити час реагування на інциденти та оптимізувати розподіл ресурсів системи безпеки на 40%. Економічний ефект проявився у зниженні операційних витрат на забезпечення безпеки та суттєвому зменшенні фінансових втрат від кіберінцидентів – на 80%. У технологічному аспекті успішно впроваджено ШІ-системи моніторингу та аналізу загроз, що дозволило автоматизувати 90% рутинних процесів безпеки та інтегрувати предиктивну аналітику в систему управління ризиками. Якісні показники також демонструють позитивну динаміку: значно посилено захищеність критичної інформації, підвищено рівень цифрової зрілості підприємства, що сприяло зростанню довіри клієнтів та партнерів і покращенню репутації компанії на ринку.

Досягнуті результати переконливо свідчать про ефективність запропонованого підходу та вказують на значний потенціал для подальшого вдосконалення систем цифрової безпеки підприємства в умовах зростаючих кіберзагроз та технологічних викликів сучасного бізнес-середовища. А отже, розроблений інструментарій, який поєднує використання цифрових технологій, інтеграцію цифрових процесів та урахування етичних аспектів, є критично важливим для українських підприємств у сучасних умовах глобалізації та цифрової трансформації.

Перелік використаної літератури

1. Чепелюк М. І. Інструментарій стратегічного управління в контексті сучасних концепцій та трендів світового економічного розвитку : монографія. Харків : ФОП Лібуркіна Л. М., 2021. 396 с.
2. Чепелюк М. І. Концептуальні засади формування системи стратегій підприємства. Бізнес Інформ. 2022. №6. С.117-121.
3. Чепелюк М. І. Методологічний підхід до формування системи стратегій підприємства. Бізнес Інформ. 2022. №7. С. 228–233.
4. Chepeliuk M. Digital Transformation of Business Structures in Ukraine: The Barriers and Drivers. Бізнес Інформ. 2021. №8. С. 48-53.

Shakhbatdinli E. E.[1]

[1] graduate of the third (educational and scientific) level of higher education,
specialty 051 Economics,
National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine

THEORETICAL ASPECTS OF DEFINING THE CONCEPT OF DIGITAL ECONOMY

Today, we observe the presence of a large number of the most diverse modern definitions of the concept of the digital economy in the context of digitalization, which once again emphasizes the special relevance of studying this issue. Through analysis, the author identifies approaches to defining the concept of the digital economy, namely: activity, system, sector, economic activity, network and transition.

Table 1 – Current definitions of the concept of "digital economy"

Source	Definition	Approaches
Oleshko T. I., Kasyanova N. V., Smerichevsky S. F. [3]	"…the activity of creating, distributing and using digital technologies and related products and services"	activity
Pyshchulina O. [2]	"...sectors of the economy based on information and communication technologies. Today, the development of informatization is primarily associated with the introduction of digital communication technologies and platforms, for which the Internet and mobile devices are the basis"	sector
Pratt M. K. [5]	"…it is a worldwide network of economic activity, commercial transactions and professional interactions, which are enabled by information and communication technologies"	chain
Derlyuk O., Shvets T. [1]	"…this is the transition of all economic sectors of the state (for example, the agricultural sector, medicine or education) to digital technologies. Traditionally, the digital economy is understood as the production, sale and supply of products via computer networks"	transition