МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 65.011.12; 65.011.56 **JEL Classification: D81, M15**
DOI: https://doi.org/10.32515/2663-1636.2024.12(45).224-235

О.В. Хаджинова, проф., д-р екон. наук
ДВНЗ "Приазовський державний технічний університет", м. Дніпро, Україна
Р.І. Жовновач, проф., д-р екон. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
О. В. Щепка, *здобувач третього (освітньо-наукового) рівня вищої освіти,*
ДВНЗ "Приазовський державний технічний університет", м. Дніпро, Україна

Забезпечення економічної безпеки виробничого підприємства у цифровому середовищі

Публікацію присвячено дослідженню особливостей забезпечення економічної безпеки виробничого підприємства у цифровому середовищі. Досліджуються завдання фахівців з економічної безпеки виробничого підприємства в сучасних умовах, які формуються під впливом ризиків, що пов'язані із конкурентним тиском, нестабільністю ринкової кон'юнктури, технологічними змінами, посиленням інформаційних ризиків та зростанням кіберзагроз в умовах цифрової трансформації діяльності. Метою публікації є встановлення переліку та ідентифікування специфічних аспектів і викликів, пов'язаних із забезпеченням економічної безпеки виробничих підприємств у середовищі цифрової економіки, розробка ефективних підходів та інструментів для підвищення стабільності і стійкості підприємств.

Публікацію спрямовано на ідентифікацію новітніх ризиків цифрової економіки, що включають кіберзагрози, ризики цифровізації виробничих процесів, захист інтелектуальної власності та комерційної інформації; аналіз можливостей для забезпечення безпеки через впровадження цифрових технологій, таких як Blockchain, AI, IoT та Big Data, які можуть підвищити прозорість і захищеність внутрішніх процесів. Вивченню підлягають питання оцінювання ефективності поточних заходів забезпечення економічної безпеки в умовах цифрової трансформації виробничої діяльності, визначення їхніх сильних і слабких сторін, розробка рекомендацій для підвищення адаптивності підприємств до цифрових загроз.

Сформовано рекомендації щодо запровадження інноваційних підходів до побудови системи економічної безпеки, таких як кіберстратегія, аналітика Big Data, автоматизоване управління ризиками. Управління ланцюгами поставок і захист конфіденційної інформації розглядаються з точки зору покладання у основу процесів забезпечення економічної безпеки комплексних та адаптивних систем захисту, які відповідають сучасним викликам і забезпечують стійкість діяльності підприємства в умовах стрімкої та всебічної цифрової трансформації. Обґрунтовано авторську позицію щодо напрямів наукових досліджень у сфері забезпечення економічної безпеки підприємства в умовах цифрової економіки, спрямованих на підвищення рівня економічної безпеки виробничих підприємств та допомоги їм адаптуватися до викликів цифрової економіки, де економічна стабільність багато в чому залежить від здатності до швидкої адаптації, проактивного реагування на ризики та інтеграції новітніх цифрових рішень.

економічна безпека, виробниче підприємство, ланцюги постачання, штучний інтелект, великі масиви даних, блокчейн, ризики діяльності, цифрове середовище

Постановка проблеми. Основні завдання фахівців з економічної безпеки виробничого підприємства (ЕБВП) полягають у захисті його діяльності від ризиків, що пов'язані із конкурентним тиском, нестабільністю ринкової кон'юнктури, технологічними змінами, посиленням інформаційних ризиків та зростанням кіберзагроз як наслідку цифрової трансформації діяльності. ЕБВП є критичним аспектом для забезпечення стабільної та ефективної діяльності в умовах постійно зростаючих зовнішніх і внутрішніх загроз. Таким чином, основними напрямами забезпечення ЕБВП є запобігання загрозам, які формуються як всередині, так і ззовні підприємства: по-перше, зовнішнім ризикам глобальних та локальних економічних криз, політичної нестабільності, коливання цін на ресурси, інтенсивної конкуренції на відкритих ринках; по-друге, кіберзагрози та ризики функціонування "розширених" цифрових віртуальних

© О.В. Хаджинова, Р.І. Жовновач, О. В. Щепка, 2024

підприємств, які є диджитальними клонами реальних, і потенційно підпадають під загрози кібератак будь-якого походження, витоку конфіденційної інформації, що може призвести до фінансових збитків, зупинки виробництва або втрати важливих даних; по-третє, інноваційна вразливість та критична залежність підприємств від "високих" технологій, особливо, якщо воно не має над ними належного контролю; по-четверте, загрози фінансовій стабільності, яка підпадає впливу ризиків неплатоспроможності, нестачі обігових коштів, специфічних проблем інвестування та кредитування; по-п'яте, ризикам застосування по відношенню до підприємства правових санкцій за недотримання регуляторних вимог щодо охорони навколишнього середовища, умов праці, стандартів якості тощо. Важливість забезпечення ЕБВП засобами стратегічного планування, запровадження ризик-менеджменту, управління фінансовими ресурсами, розвитку кадрового потенціалу та впровадження безпечних цифрових технологій полягає у можливості для виробничих підприємств оперативно реагувати на зміни і захищати власні активи в умовах цифрової економіки.

Аналіз останніх досліджень і публікацій. Останні дослідження підкреслюють, що цифрова економіка суттєво змінює структуру загроз для підприємств, додаючи до їхнього переліку кіберризики та небезпеку інформаційних втрат. Збільшується роль інформаційної складової, оскільки цифровізація за умов розгортання Industry 4.0 охоплює всі бізнес-процеси ланцюга формування вартості підприємства – від виробництва до управління каналами постачання (Schwab K. [21]). Значні зміни відбуваються у зв'язку із впровадженням Інтернету речей (IoT) (Mattern F. & Floerkemeier C. [17]; Miorandi D., Sicari S., Pellegrini F., & Chlamtac I. [18]), можливостей машинного аналізу великих масивів даних (Big Data) (Schwarz T. [22]) та технологій блокчейн (Blockchain), які відкривають нові можливості для оптимізації, але одночасно потребують ефективних засобів захисту інформації. У публікації колективу авторів під керівництвом Atzori L. [6], Vermesan O. [25] розглядаються основні аспекти IoT, включаючи архітектуру, комунікаційні технології, виклики та перспективи, окреслюються базові концепції, які допомагають формувати подальші дослідження у цій галузі. Роботу колективу авторів Uckelmann D., Harrison M., Michahelles F. [24] присвячено вивченню архітектурних особливостей, питанням конфіденційності, безпеки та управління даними у середовищі IoT. При цьому автори пропонують комплексний підхід до розробки відповідної інфраструктури, описують послідовність створення IoT-мереж на прикладі виробничих підприємств. Технічним аспектам проблеми присвячено з'ясування ролі RFID (радіочастотної ідентифікації) як ключової технології, що використовується для ідентифікації та відстеження об'єктів як важливої частини IoT. Ці роботи не просто охоплюють ключові концепції, архітектурні моделі, приклади застосування та виклики, але є основою для дослідників, які працюють у дотичних сферах.

Численні наукові публікації свідчать про зростання значення штучного інтелекту (AI) для побудови систем ЕБВП. Алгоритми AI та методи аналітики Big Data дозволяють прогнозувати ризики, здійснювати моніторинг аномалій та оперативно реагувати на загрози. Це, зокрема, актуально для виявлення потенційних внутрішніх загроз, шахрайства або інших ризиків, що виникають у результаті взаємодії з Big Data. Так, Annosi M.C. та Foss N.J. [5], De Santis F. [10], Gershenfeld N. [13], кожен зі своєї точки зору, розглядають роль AI в бізнес-середовищі, зокрема його застосування для моніторингу ризиків та забезпечення ЕБВП, стверджуючи, що він може покращити управління ризиками і запобігти кризовим ситуаціям на підприємствах. У дописі De Santis F. [10] актуалізуються питання реалізації концепції ризик-менеджменту за допомогою AI в умовах Industry 4.0, обґрунтовуються засоби оптимізації процесів управління ризиками на виробничих підприємствах, забезпечення безпеки даних і

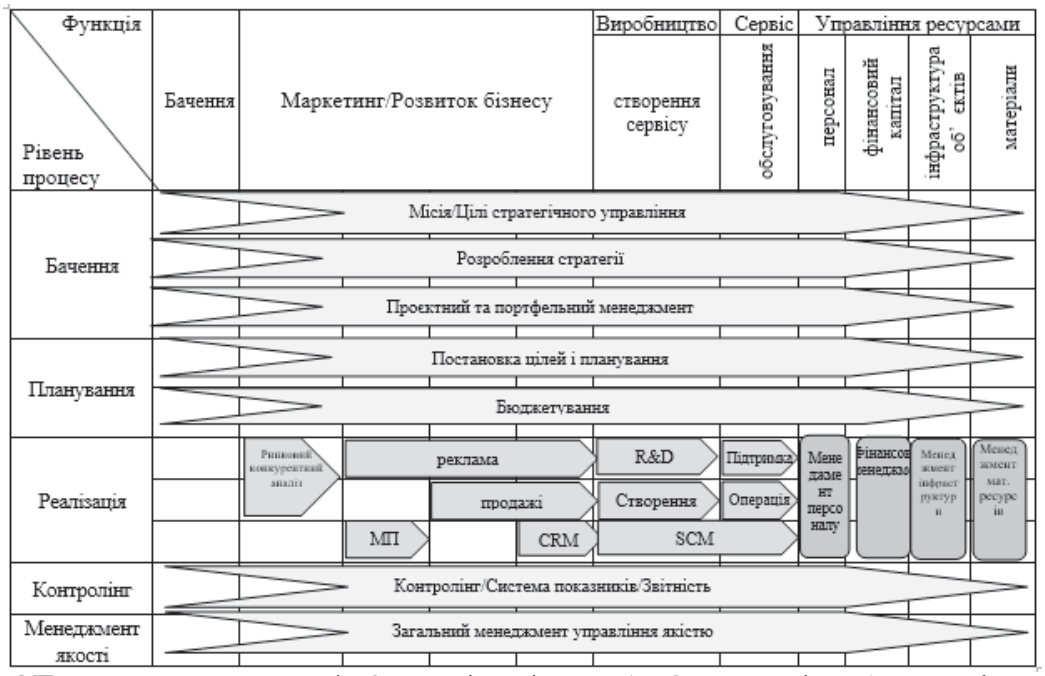
процесів. Творчий колектив Husain F. [14] описує методи машинного навчання (ML), що використовуються для забезпечення кібербезпеки у виробничих умовах, досліджує, як алгоритми ML здатні виявляти аномалії та відслідковувати підозрілу активність, що є важливим аспектом економічної безпеки. Роботи також містять підходи до проведення аналізу концепції прогнозного обслуговування, що використовує AI для мінімізації ризиків і підтримки безпеки на виробництві, показують, як алгоритми можуть передбачати збої обладнання, тим самим підвищуючи економічну безпеку та стабільність підприємства. Choi T.-M., Lambert J.H. [8] аналізують методи обробки масивів BigData, за допомогою яких AI може допомагати виявляти ризики та створювати економічно безпечне середовище на підприємстві. Ці публікації формують теоретичну та практичну базу для досліджень у сфері ЕБВП з використанням AI. Збільшення кількості та інтенсивності кібератак на виробничі підприємства змушує дослідників акцентувати увагу на кібербезпеці. В наукових роботах обговорюються методи захисту корпоративних мереж і збереження конфіденційної інформації від кібератак. Також підкреслюється необхідність багаторівневих систем захисту, включаючи шифрування даних, автентифікацію користувачів та контроль доступу. Питанням інтеграції децентралізованих блокчейн-технологій до системи управління ЕБВП присвячено останні роботи Mushtaq A. & Haq I.U. [19], колективу дослідників Wang M. [26], Sinha S. [23]. У роботах автори обговорюють роль блокчейну у забезпеченні безпеки в промисловості, аналізують, як децентралізовані мережі можуть підвищити надійність і захист даних, забезпечуючи прозорість і контроль за кожним етапом ланцюга постачання у контексті Індустрії 4.0, досліджують використання блокчейну та смарт-контрактів у ланцюгах постачання з метою забезпечення прозорості й достовірності інформації, що знижує ризики шахрайства і підвищує надійність взаємодії між постачальниками та виробниками. Спеціальні аспекти застосування блокчейну для захисту даних у промисловому IioT пов’язують з тим, як блокчейн може підтримувати децентралізовані системи довіри у виробничих процесах. Автори розглядають концепції “цифрового сліду”, що дозволяють відслідковувати всі операції на виробництві, підвищуючи безпеку і довіру до системи, описують можливості технології у протидії кібератакам, забезпеченні цілісності даних, а також можливість швидкого виявлення потенційних загроз.

Частина дослідників акцентує увагу на важливості інтеграції ризик-менеджменту до процесів економічної діяльності підприємства. Це включає розробку моделей для ідентифікації ризиків (Lam J. [15], Power M. [20], Frame J.D. [12]), оцінки та управління ними (Crouhy M. [9]). Ефективне управління ризиками забезпечує стійкість підприємства до зовнішніх і внутрішніх загроз, зокрема, шляхом впровадження процедур реагування на інциденти. Ці публікації формують основу сучасного розуміння інтеграції ризик-менеджменту в управління виробничими підприємствами, сприяючи розвитку більш безпечних і стійких бізнес-процесів. Вони досліджують методи і принципи, які дозволяють підприємствам не лише знижувати ризики, а й використовувати управління ризиками як конкурентну перевагу. В оприлюднених результатах досліджень зазначається важливість захисту інтелектуальної власності та конфіденційної інформації, особливо в умовах, коли цифрові платформи використовуються для управління інноваційною діяльністю підприємств. Інструменти правового захисту, такі як патентування технологій, а також технічні заходи, включаючи контроль доступу до даних, є важливими складовими економічної безпеки в умовах цифрової трансформації. Таким чином, сучасні дослідження вказують на необхідність здійснення комплексного підходу до забезпечення ЕБВП, що включає інтеграцію цифрових технологій, управління кіберризиками, захист інтелектуальної власності та адаптацію до нових викликів

цифрової економіки.

Постановка завдання. Наукове дослідження здійснюється з метою з'ясування специфічних аспектів і викликів, пов'язаних із забезпеченням ЕБВП у цифровій економіці, а також розробки ефективних підходів та інструментів для підвищення стабільності і стійкості підприємств. Публікацію спрямовано на ідентифікацію новітніх ризиків цифрової економіки, що впливають на ЕБВП, включаючи кіберзагрози, ризики цифровізації виробничих процесів, захист інтелектуальної власності та комерційної інформації; аналіз нових можливостей для забезпечення безпеки через впровадження цифрових технологій, таких як Blockchain, AI, IoT та Big Data, які можуть підвищити прозорість і захищеність внутрішніх процесів. Підлягатимуть вивченню питання оцінювання ефективності поточних заходів забезпечення ЕБВП в умовах глобальної цифрової трансформації, визначення їхніх сильних і слабких сторін, а також розробки рекомендацій для підвищення адаптивності підприємств до цифрових загроз. Формулювання рекомендацій щодо інноваційних підходів до побудови ЕБВП в цифрову епоху, таких як кіберстратегія, аналітика Big Data, автоматизоване управління ризиками, управління ланцюгами поставок і захист конфіденційної інформації передбачається розглянути з точки зору покладання у основу процесів створення комплексних та адаптивних систем забезпечення економічної безпеки, які відповідають сучасним викликам і забезпечують стійкість діяльності підприємства в умовах стрімкої та всебічної цифрової трансформації.

Виклад основного матеріалу. Виробнича корпорація, яка функціонує за новітніх умов розгортання цифрової економіки, протягом тривалого періоду використовує розгалужену системою зберігання даних, яка служить для різних цілей звітності та аналізу. Постійні зміни умов виробничої діяльності компанії вимагають переосмислення системи накопичення та зберігання масивів даних і майбутніх проектів у цьому середовищі. Для цього недостатньо просто аналізувати систему накопичення, зберігання та використання даних, оцінювати її архітектуру, якість інформації (рис. 1).



Примітки: МП – менеджмент продуктивності; R&D – дослідженні та розробки; CRM – управління зв'язками з клієнтами; SCM – управління ланцюгами постачань

Рисунок 1 – Традиційна карта використання виробничої інформації епохи Industry 3.0

Джерело: складено авторами

Такий підхід був частково виправданий за умов здійснення підходу до інформації як другорядного виробничого ресурсу, формування масивів даних з метою супроводження і обслуговування процесів використання більш пріоритетних трудових, матеріальних та грошових ресурсів корпорації (рис. 1). У повній відповідності до традиційного екстенсивно-ресурсного підходу до використання виробничого потенціалу, на підприємствах здійснювалась класифікація ризиків та загроз такій діяльності.

Поточний перехід до реалій господарювання в умовах розгортання цифрової економіки практично не вплинув на особливості класифікації різновидів ризиків виробничої діяльності (табл. 1), проте суттєво підвищив рівень вимог до управління специфічними ризиками, що виникають у процесі налагодження ланцюгів формування вартості продукції корпорації, яка має можливість підвищити рівень їхнього контролю у тому числі, а інколи і виключно, за рахунок використання цифрових інтелектуальних платформ.

Таблиця 1 – Класифікація ризиків виробничої діяльності

Критерії	Класи ризику	Пояснення
Відхилення в результатах	Чисті (асиметричні)	Цільові відхилення можливі лише в одну сторону
	Спекулятивні (симетричні)	Позитивні та негативні цільові відхилення
Рівні прийняття рішень	Стратегічні	Становлять небезпеку для компанії в цілому та перешкоджають реалізації довгострокових, глобальних цілей
	Тактичні та операційні	Стосуються середньо- та короткострокових рішень
Тимчасовий контекст	Постійні ризики проти тимчасової схильності до ризиків	Ризики тісно пов’язані з поставленими цілями, що є актуальними на певний момент часу або період
Сфера дії рішення	Індивідуальні	Виражає ризик, пов’язаний з ізольованим рішенням
	Загальні	Містить ризик прийняття усієї сукупності рішень
Об’єкт потоку ресурсів, до яких відносяться ризики	Матеріальні, товарні, фінансові, інформаційні та юридичні	Відхилення від цілей можуть виникати у зв’язку з операційними потоками товарів, грошей, інформації та законних прав
Зв’язок між окремими ризиками	Незалежні	Окремі ризики не впливають один на одного
	Залежні	Існує залежність між ризиками, за якої необхідно розрізняти ефект підсилення від ефекту компенсації окремих ризиків
Походження ризиків	Ендогенні	Причини ризиків криються всередині компанії або всередині ланцюга постачань
	Екзогенні	Причини ризиків формуються у корпоративному середовищі діяльності або в середовищі мережі ланцюгів постачань
Корпоративна сфера, в які існують ризики	Продуктивність	Ризики, пов’язані з процесом виробничої діяльності компанії, закупівлею факторів виробництва та/або продажем продукції
	Фінанси	Результат діяльності у фінансовій сфері компанії, який служить для підтримки фізичних процесів виробництва

Джерело: складено авторами на основі узагальнення [8-10; 16;20]

Отже, ми можемо класифікувати специфічні ризики виробничої діяльності, що пов’язані з подоланням загроз безперебійного налагодження ланцюгів постачань, інакше, ланцюгів формування вартості продукції корпорації в умовах розгортання цифрової економіки як асиметричні, стратегічні, постійні, загальні, змішані матеріально-інформаційні, залежні, екзогенні, пов’язані з продуктивною сферою

діяльності. Підходи до управління ризиками, що виникають у процесі налагодження ланцюгів постачань, визначаються цільовою спрямованістю елементів підходу та їхніми характерними особливостями (табл. 2). Цілісне управління ланцюгами постачань в режимі реального часу, відповідно, управління пов'язаними з цим ризиками в режимі on-line, у максимально повній мірі реалізується за можливості залучення до цього процесу інструментів відповідного програмного забезпечення складових елементів процесів електронного бізнесу (E-Business) – закупівель (E-Procurement), продажів (E-Commerce), торгівлі (E-Marketplace), електронного спілкування (E-Community) та кооперування (E-Company).

Таблиця 2 – Підходи до управління ризиками ланцюгів постачань у цифровому середовищі

Елемент підходу / Характерні особливості	Управління ризиками з орієнтацією на ланцюги постачань	Комплексний аналіз ризиків у ланцюгу постачань	Цілісне управління ризиками в ланцюзі постачань
Фокус процесу управління ризиками	Власна компанія		Ланцюг постачань
Співпраця в управлінні ризиками	–	З окремими компаніями-партнерами	З усіма компаніями-партнерами
Обмін інформацією про ризики	–	Нерегулярний, неформальний	Регулярний, офіційний, автоматичний
Інформаційна асиметрія щодо ризиків ланцюгів постачань	Висока	Середня	Незначна
Тип відносин між компаніями	Трансакційно орієнтований	Партнерство на основі підтвердженої довіри	
Фаза формування мережі	Побудова стосунків	Інтенсифікація стосунків	Налагодження співпраці
Спільні цілі та процеси планування	–	З обраною компанією-партнером	З усіма компаніями-партнерами
Інтенсивність довіри між компаніями	Незначна	Середня	Висока

Джерело: складено авторами на основі узагальнення [8-10; 12; 15; 20]

Суцільне охоплення усього ланцюга бізнес-процесів виробничої корпорації засобами цифрової підтримки одночасно сприяє формуванню "поля ризиків" використання цифрових технологій у виробничій діяльності. Елементами цього поля є:

– кіберзагрози та атаки, за яких IoT, автоматизовані системи управління виробництвом (SCADA), хмарні технології можуть стати для зловмисників джерелом доступу до конфіденційних даних з подальшим збитковим втручанням у роботу виробничих ліній, транспортних ланок, завданні фізичних збитків обладнанню;

– витік даних і порушення конфіденційності збережених та оброблених їхніх масивів (як внутрішніх, так і клієнтських) з загрозою подальшого потрапляння до конкурентів або використання для шахрайства;

– залежність інфраструктури та безпеки, хмарних платформ і програмного забезпечення, що надаються зовнішніми компаніями, від сторонніх постачальників та технологій, що може стати причиною збоїв у роботі сервісів;

– технологічних збоїв та використання ненадійних систем, що можуть виходити з ладу через технічні збої, проблеми з інтернет-з'єднанням або несумісність систем з можливими зупинками виробничих процесів і значними фінансовими збитками;

– проблеми з захистом IoT-пристроїв, що використовується для моніторингу і контролю бізнес-процесів на виробництві, які не мають належного рівня захисту, що робить їх легкою ціллю для хакерів;

– невідповідність практичних навичок персоналу високим вимогам до рівня знань і навичок у сфері кібербезпеки та управління сучасними технологіями, що може призвести до помилок або недостатнього використання систем.

Загальною умовою забезпечення економічної безпеки виробничого підприємства у цифровому середовищі є зміна стратегічного підходу до використання інформації як допоміжного ресурсу виробничої корпорації (рис. 2)

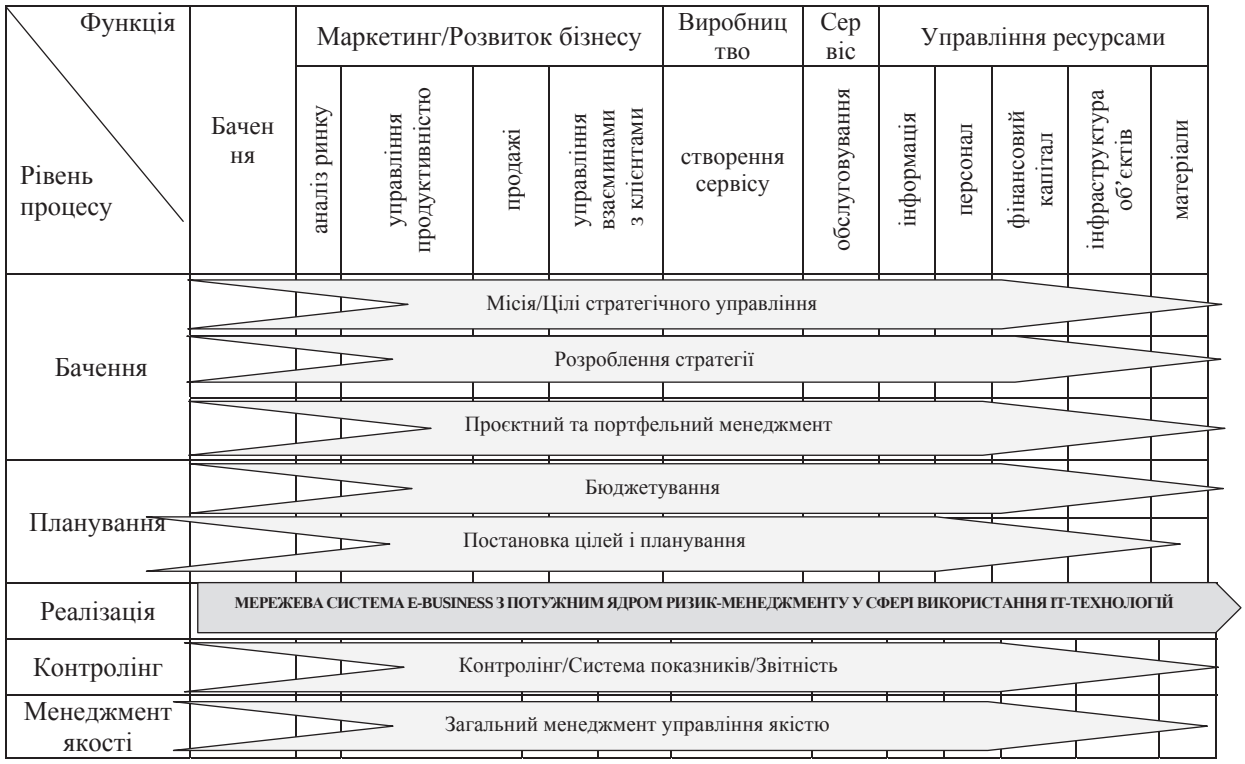


Рисунок 2 – Управління інформаційними ресурсами виробничої корпорації епохи Industry 4.0

Джерело: складено авторами на основі узагальнення [1-4; 7; 11]

Технічними способами запобігання ризикам безперебійного протікання бізнес-процесів ланцюгів постачань виробничої корпорації виступають:

1. Впровадження та інтеграція до системи кібербезпеки сучасних засобів: *брандмауерів* – систем на основі програмного або апаратного забезпечення, які є своєрідним "посередником" між безпечними та неперевіреними мережами, а також їх частинами, які поєднують функції пакетних фільтрів, фільтру стану з'єднання, фільтру інформації за допомогою усіх рівнів моделі OSI (Open Systems Interconnection), інших вбудованих додаткових систем безпеки – віртуальних приватних мереж (VPN), систем запобігання та виявлення вторгнень (IPS/IDS); *антивірусного програмного забезпечення* – спеціальних програм для знаходження комп'ютерних вірусів, не бажаних або шкідливих програм загалом, відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики (запобігання) зараження модифікацій файлів чи операційної системи шкідливим кодом. Важливо також мати регулярне оновлення ПЗ та здійснювати моніторинг систем у реальному часі (сканування файлів і програм; сканування комп'ютера за потребою; сканування інтернет-трафіку; сканування електронної пошти; захист від атак ворожих веб-вузлів; відновлення пошкоджених файлів).

2. Засоби *шифрування* (перетворення інформації в незрозумілі символи за допомогою математичного процесу, управління паролями) та *контролю доступу до баз даних* (на основі забезпечення вимог тріади безпеки – конфіденційності (confidentiality), цілісності (integrity), доступності (availability)), захист стільникових мереж на основі регістрів HLR (домашнього регістру місцеперебування) та VLR (регістру активних візитерів), що дозволяють здійснювати шифрування конфіденційних матеріалів і обмежувати доступ до них, тим самим знижувати ризик несанкціонованого використання. Слід також використовувати багаторівневу автентифікацію (multifactor authentication, MFA) та регулярні перевірки безпеки доступу в Amazon Web Services (AWS).

3. Створення резервних копій даних та планів на випадок аварій, плану програмного відновлення даних з фізичного сервера як окремого апаратного пристрою після збоїв, дозволяють оперативно відновити виробництво в разі втрати інформації або технічних проблем. Для цього може бути використано виділене обладнання для стійкості до відмов (дзеркальні жорсткі диски RAID); віртуалізація серверів; запасні сервери (failover); віддалене резервне копіювання (offsite backup); планування та тестування відновлень.

4. Зменшення залежності від сторонніх постачальників за рахунок врахування їхньої репутації в сфері безпеки, розроблення стратегію управління ризиками, пов’язаними з їхніми послугами (наприклад, укладення договорів з чіткими умовами щодо кібербезпеки та технічної підтримки).

5. Навчання персоналу та підвищення обізнаності співробітників з питань кібербезпеки, зокрема щодо розпізнавання фішингових атак та правильного поводження з конфіденційною інформацією.

6. Контроль і аудит IoT-пристроїв, що супроводжується ретельним контролем їх безпеки, включаючи встановлення надійних паролів, регулярне оновлення прошивок, і обмеження доступу до них.

Практичне використання стратегічних підходів у поєднанні з технічними засобами забезпечення ЕБВП у цифровому середовищі є надзвичайно важливим фактором забезпечення стійкості ланцюгів постачань.

Висновки та перспективи подальших досліджень. В умовах цифрової економіки забезпечення економічної безпеки підприємства набуває нових характеристик та вимог, оскільки інформаційні та комунікаційні технології кардинально змінюють традиційні підходи до бізнес-процесів. Основні особливості діяльності із забезпечення економічної безпеки підприємства в таких умовах включають:

1. Кібербезпеку як ключовий компонент економічної безпеки, що забезпечує захист від потенційних загроз цифровим системам і інформації підприємства. У цифровій економіці кожен аспект діяльності може стати вразливим до кібератак, від яких слід захищати фінансові операції, персональні дані клієнтів і співробітників, комерційні таємниці та інші важливі активи. Застосування багаторівневого захисту, шифрування даних, управління доступом та постійний моніторинг є обов’язковими для уникнення зловмисних дій та зламу даних.

2. Використання ШІ та аналітики Big Data дозволяють відстежувати й аналізувати великі обсяги інформації, що створює можливості для оперативного моніторингу ринкових змін, поведінки клієнтів і потенційних загроз. Аналітика даних дає змогу підприємствам прогнозувати ризики та загрози, а також моделювати різні сценарії розвитку подій. Це допомагає формувати проактивні стратегії та забезпечувати безперервність діяльності.

3. Інтеграція блокчейн-технологій для прозорості операцій створює нові можливості для економічної безпеки, забезпечуючи прозорість транзакцій та захист даних від несанкціонованих змін. Це особливо важливо для підприємств із довгими ланцюгами постачання, де кожна операція потребує підтвердження та захисту. Використання блокчейн-технологій дозволяє скоротити шахрайство, підвищити довіру між партнерами та мінімізувати ризики витоку інформації.

4. Адаптація до швидких змін і ризиків цифрового середовища. У цифровій економіці зміни відбуваються швидше, ніж у традиційних бізнес-моделях, що вимагає від підприємств готовності до швидкого реагування на нові загрози та адаптації до змін. Корпорації все частіше застосовують гнучкі підходи до управління та прийняття рішень, щоб миттєво відповідати на зміни у зовнішньому середовищі. Окрім того, виникає потреба у постійному вдосконаленні навичок співробітників для роботи з новими технологіями безпеки, а також у швидкому навчанні для підтримання конкурентоспроможності в умовах постійної цифровізації.

5. Економічна безпека в умовах мережевих структур та віддаленої роботи залежить від можливості уникнення нових загроз для підприємств через розширення віддаленої роботи та мережевих структур. У таких умовах економічна безпека підприємства залежить від захищеності каналів зв'язку, які використовують співробітники, і доступу до корпоративних систем. Підприємства повинні враховувати ризики витоку інформації через віддалені підключення, забезпечувати безпеку підключень VPN, а також застосовувати спеціальні політики безпеки для дистанційної роботи.

6. Інноваційні стратегії управління ризиками, орієнтовані на профілактику та попередження загроз, передбачають впровадження аналітичних систем, які дозволяють ефективно управляти фінансовими, операційними та стратегічними ризиками. Управління ризиками у цифровій економіці є комплексним процесом, що передбачає використання автоматизованих систем для контролю за операціями, управління фінансовими потоками та моніторингом змін у реальному часі.

Перспективні напрями наукових досліджень у сфері забезпечення економічної безпеки підприємства в умовах цифрової економіки охоплюють кілька ключових аспектів, що визначають особливості сучасних цифрових ризиків і можливостей для захисту економічних інтересів. Основні з них включають: по-перше, дослідження інноваційних рішень для кіберзахисту, що враховують постійно зростаючу кількість і складність кіберзагроз, включає створення багаторівневих і самонавчаючих систем захисту, що використовують AI і ML для виявлення та запобігання кібератакам у реальному часі, вивчення питань захисту даних у розподілених мережах та хмарних обчисленнях, зокрема підходів до забезпечення безпеки віддалених робочих місць та захисту критично важливих даних; по-друге, впровадження блокчейн-технологій для економічної безпеки, що мають забезпечити прозорість та відстеження транзакцій, знизити ризик шахрайства та економічних злочинів за рахунок використання смарт-контрактів у ланцюгах постачання та фінансових операціях як засобу підвищення захисту від несанкціонованих дій і покращення прозорості в бізнес-операціях; по-третє, прогнозування та управління ризиками за допомогою Big Data та AI для виявлення потенційних загроз на ранніх стадіях, завчасного відстеження ринкових змін, поведінки конкурентів і фінансових показників, що є критичними для економічної безпеки, розроблення моделей для автоматичного прийняття рішень щодо ризиків, що дає змогу підприємствам швидше реагувати на зміни в зовнішньому середовищ; по-четверте, у напрямі досліджень інтернету речей (IoT) та управління безпекою в умовах мережевих виробництв – покращення контролю над обладнанням, моніторинг операцій і запобігання аварійним ситуаціям, при цьому особлива увага приділяється забезпеченню

безпеки даних у мережевих виробничих структурах та захисту інформації про внутрішні процеси підприємства, вивченню особливостей захисту IoT-пристроїв і сенсорних мереж, які можуть бути вразливими до кібератак, що здатні впливати на операційну діяльність і безпеку; по-п’яте, у напрямі розробки концепцій цифрового суверенітету та незалежності, захисту підприємств і національних економік від зовнішнього контролю над їхніми цифровими системами, що особливо актуально для захисту економічної інформації і забезпечення незалежності від зовнішніх IT-сервісів та постачальників, дослідження можливостей локалізації критичних IT-систем для забезпечення захисту від ризиків, пов’язаних із залежністю від міжнародних постачальників програмного та апаратного забезпечення; по-шосте, адаптація до регуляторних змін і правових аспектів цифрової безпеки з акцентом на дослідженні правових аспектів забезпечення адаптації до міжнародних стандартів захисту даних і кібербезпеки, створенні механізмів для захисту прав власності на інформаційні активи, а також захисті персональних і комерційних даних відповідно до регуляторних вимог; по-сьоме, розроблення рекомендацій для підприємств щодо дотримання нових регуляторних стандартів цифрової безпеки, а також створення адаптивних систем управління ризиками.

Перераховані напрями наукових досліджень можуть суттєво підвищити рівень ЕБВП та допомогти їм адаптуватися до викликів цифрової економіки, де економічна стабільність багато в чому залежить від здатності до швидкої адаптації, проактивного реагування на ризики та інтеграції новітніх цифрових рішень.

Список літератури

1. Вєрсанова Г.А., Ксенофонтов Д.В., Савенчук І.С. Механізми підвищення рівня економічної безпеки підприємств в умовах цифровізації. *Вісник Східноєвропейського університетуекономіки і менеджменту.* Вип. № 2 (32), 2024 С. 145-137. URL: https://doi.org/10.58253/2078-1628-2024-2(32)-010.
2. Жовновач Р.І., Петленко Т.Г., Орлова А.А. Технології управління підприємством в системі менеджменту. *Український журнал прикладної економіки та техніки*. 2024. №1. С. 18-23. DOI: 10.36887/2415-8453-2024-1-2.
3. Кравченко М.С., Погорелов В.М., Будагян А.С. Цифрові технології управління ланцюгом постачань та підвищення конкурентного потенціалу виробничого підприємства. *Центральноукраїнський науковий вісник. Економічні науки.* 2024, №11(44). С. 126-137. URL:https://doi.org/10.32515/2663-1636.2024.11(44).145-156.
4. *Хаджинова О.В., Савенчук І.С., Хаджинова М.С.* Трансформація бізнес-процесів промислових підприємств в умовах цифровізації. *Центральноукраїнський науковий вісник. Економічні науки.* 2024, №11(44). С. 126-137. URL: https://doi.org/10.32515/2663-1636.2024.11(44).126-137.
5. Annosi M.C., Foss N.J. Artificial Intelligence in Business: From Research and Innovation to Market Deployment. *Procedia Computer Science.* 2020. 167(1). P. 2200-2210. URL: https://doi.org/10.1016/j.procs.2020.03.272.
6. Atzori L., Iera A., Morabito G. (2010) The Internet of Things: A Survey. *Computer Network*s. 2010. Volume 54. Issue 15. P. 2787-2805. DOI: 10.1016/j.comnet.2010.05.010.
7. Bath J., Winkler K. Hybrid Work. 1., Auflage. 2023. Freiburg, München, Stuttgart: Haufe Group. 280 s.
8. Choi T.-M., Lambert J.H. Advances in Risk Analysis with Big Data. *Risk Analysis.* 2017. 37(8). P. 1435-14442. URL: https://doi.org/10.1111/risa.12859.
9. Crouhy M., Galai D., Mark R. The Essentials of Risk Management. 2006. 414 p.
10. De Santis F. Artificial Intelligence for Risk Management. *Artificial Intelligence in Accounting and Auditing.* 2024. P. 139-154. URL: https://doi.org/10.1007/978-3-031-71371-2_6.
11. Erlhofer S. Suchmaschinen Optimierung. Das umfassende Handbuch. 11., aktualisierte Auflage. Rheinwerk Verlag GmbH, Bonn. 2023. 1232 s.
12. Frame J.D. Managing Risk in Organizations: A Guide for Managers. The Jossey-Bass business & management series 2003. 288 p.
13. Gershenfeld N. When Things Start to Think. Henry Holt and Company. 1999. 225 p.
14. Husain F., Husain R., Hassan S.A., Hossain E. at al. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials.* 2020. Volume 22. Issue 3. P. 1686-1721. URL: https://doi.org/10.1109/COMST.2020.2986444.

15. Lam J. Enterprise Risk Management: From Incentives to Controls. 2014. 476 p. URL: https://doi.org/10.1002/9781118836477.
16. Malakhovskyi Y., Gamaliy V., Zhovnovach R., Kulazhenko V, Cherednichenko M. Assessment of the risks of entrepreneurship as a prerequisite for the implementation of innovation projects. *Journal of Entrepreneurship Education.* 2019. Vol. 22. Issue 1, P. 127-133. URL: https://www.abacademies.org/articles/Assessment-of-the-risks-of-entrepreneurship-1528-2651-22-S1-351.pdf (дата звернення 24.10.2024).
17. Mattern F., Floerkemeier C. (2010). From the Internet of Computers to the Internet of Things. *From Active Data Management to Event-Based Systems and More. Lecture Notes in Computer Science* / Sachs, K., Petrov, I., Guerrero, P. (eds). Vol 6462. Springer, Berlin, Heidelberg. URL: https://doi.org/10.1007/978-3-642-17226-7_15.
18. Miorandi D., Sicari S., Pellegrini F., Chlamtac I. Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks.* 2012. Volume 10. Issue 7. P. 1497-1516. URL: https://doi.org/10.1016/j.adhoc.2012.02.016.
19. Mushtaq A., Haq I.U. Implications of Blockchain in Industry 4.O. *International Conference on Engineering and Emerging Technologies (ICEET).* 2019. URL: https://doi.org/10.1109/CEET1.2019.8711819
20. Power M. Risk Management and Corporate Governance. OECD. 2014. 90 p.
21. Schwab K. The Fourth Industrial Revolution. Penguin Group. 2016. 192 p.
22. Schwarz T. (Hrsg). Big Data im Marketing. Chancen und Möglichkeiten für eine effektive Kundenansprache. 1. Auflage. Freiburg, München: Haufe Gruppe. 2015. 324 s.
23. Sinha S. Blockchain for Enhancing IoT Privacy and Security. *International Journal of Innovative Research in Computer Science & Technolog*y. 2024. 12(2). 106-110. URL: https://doi.org/10.55524/ijircst.2024.12.2.18
24. Uckelmann D., Harrison M., Michahelles F. Architecting the Internet of Things. 2011. Springer. 384 p.
25. Vermesan O., Friess P. Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model. Springer. 2013. Springer. 359 p.
26. Wang M., Wu Y., Chen B., Evans M. Blockchain and Supply Chain Management: A New Paradigm for Supply Chain Integration and Collaboration. *OSCM Publication*s. 2021. Volume 14. Issue 1. URL: https://doi.org/10.31387/ oscm0440290.

References

1. Versanova H., Ksenofontov D., & Savenchuk I. (2024). Mechanisms for increasing the level of economic security of enterprises. *Visnyk Skhidnoievropeiskoho universytetu ekonomiky i menedzhmentu.* 2 (32), 145-137. [in Ukrainian]. https://doi.org/10.58253/2078-1628-2024-2(32)-010.
2. Zhovnovach, R.I., Petlenko, T.G., & Orlova, A.A. (2024). Enterprise management technologies in the management system. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky,* 1, 18-23. [in Ukrainian].https://doi.org/10.36887/2415-8453-2024-1-2.
3. Kravchenko M.S., Pogorelov V.M., & Budahian A.S. (2024). Digital supply chain management technologies and increasing the competitive potential of a manufacturing enterprise. *Tsentralnoukrainskyi naukovyi visnyk. Ekonomichni nauky.* 11(44)., 145-156. [in Ukrainian]. https://doi.org/10.32515/2663-1636.2024.11(44).145-156.
4. Khadzhinova O.V., Savenchuk I.S. & Khadzhinova M.S. (2024). Transformation of business processes of industrial enterprises in the context of digitalization. *Tsentralnoukrainskyi naukovyi visnyk. Ekonomichni nauky.* 11(44)., 126-137. [in Ukrainian]. https://doi.org/10.32515/2663-1636.2024.11(44).126-137.
5. Annosi, M.C., & Foss, N.J. (2020**).** Artificial Intelligence in Business: From Research and Innovation to Market Deployment. *Procedia Computer Science,* 167(1), 2200-2210. [In English]. https://doi.org/10.1016/j.procs.2020.03.272.
6. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. *Computer Network*s, 54, 15, 2787-2805. [In English]. https://doi.org/10.1016/j.comnet.2010.05.010.
7. Bath, J., & Winkler, K. (2023). *Hybrid Work.* Freiburg, München, Stuttgart: Haufe Group [In English].
8. Choi, T.-M., & Lambert, J.H. (2017). Advances in Risk Analysis with Big Data. *Risk Analysis.* 37(8), 1435-14442. [In English]. https://doi.org/10.1111/risa.12859.
9. Crouhy, M., Galai, D., & Mark, R. (2006). *The Essentials of Risk Management.* McGraw-Hill Professional [In English].
10. De Santis, F. (2024). Artificial Intelligence for Risk Management. *Artificial Intelligence in Accounting and Auditing,* 139-154. [In English]. https://doi.org/10.1007/978-3-031-71371-2_6 .
11. Erlhofer, S. (2023). *Suchmaschinen Optimierung. Das umfassende Handbuch*. Rheinwerk Verlag GmbH, Bonn. [In German].

12. Frame, J.D. (2003). *Managing Risk in Organizations: A Guide for Manager.* The Jossey-Bass business & management series. [In English].
13. Gershenfeld, N. (1999). *When Things Start to Think*. Henry Holt and Company [In English].
14. Husain, F., Husain, R., Hassan, S.A., Hossain, E. at al. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials, 22, 3, 1686-172.* [In English].https://doi.org/10.1109/COMST.2020.2986444.
15. Lam, J. (2014)**.** *Enterprise Risk Management: From Incentives to Controls* [In English]. https://doi.org/10.1002/9781118836477.
16. Malakhovskyi, Y., Gamaliy, V., Zhovnovach, R., Kulazhenko, V, & Cherednichenko, M. (2019). Assessment of the risks of entrepreneurship as a prerequisite for the implementation of innovation projects. *Journal of Entrepreneurship Education*, 22, 1S, 127-133. https://www.abacademies.org/articles/Assessment-of-the-risks-of-entrepreneurship-1528-2651-22-S1-351.pdf [In English].
17. Mattern, F., & Floerkemeier, C. (2010). *From the Internet of Computers to the Internet of Things. From Active Data Management to Event-Based Systems and More. Lecture Notes in Computer Science* / Sachs, K., Petrov, I., & Guerrero, P. (eds), 6462. Springer, Berlin, Heidelberg. [In English]. https://doi.org/10.1007/978-3-642-17226-7_15.
18. Miorandi, D., Sicari, S., Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks*, 10, 7, 1497-1516. [In English]. https://doi.org/10.1016/j.adhoc.2012.02.016.
19. Mushtaq, A., & Haq, I.U. (2019). Implications of Blockchain in Industry 4.O. *International Conference on Engineering and Emerging Technologies (ICEET).* [In English]. https://doi.org/10.1109/CEET1.2019.8711819.
20. Power, M. (2014). *Risk Management and Corporate Governance*. OECD [In English].
21. Schwab, K. (2016). *The Fourth Industrial Revolution*. Penguin Group [In English].
22. Schwarz, T. (Hrsg). (2015). *Big Data im Marketing. Chancen und Möglichkeiten für eine effektive Kundenansprache*. Freiburg, München: Haufe Gruppe [In English].
23. Sinha, S. (2024). Blockchain for Enhancing IoT Privacy and Security. *International Journal of Innovative Research in Computer Science & Technology*, 12(2), 106-110. [In English]. https://doi.org/10.55524/ijircst.2024.12.2.18.
24. Uckelmann, D., Harrison, M., & Michahelles, F. (2011). *Architecting the Internet of Things* [In English].
25. Vermesan, O., & Friess, P. (2013). *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model.* Springer [In English].
26. Wang, M., Wu, Y., Chen, B., & Evans, M. (2021). Blockchain and Supply Chain Management: A New Paradigm for Supply Chain Integration and Collaboration. *OSCM Publications*, 14, 1. [In English]. http://doi.org/10.31387/ oscm0440290/

Olena Khadzhynova, Professor, Doctor of Economic Sciences
State Higher Educational Institution "Pryazovskyi State Technical University", Dnipro, Ukraine
Ruslana Zhovnovach, Professor, Doctor of Economic Sciences
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
Oleksandr Shchepka, Postgraduate (student of the third (educational and scientific) level of higher education)
State Higher Educational Institution "Priazovskyi State Technical University", Dnipro, Ukraine

Ensuring the Economic Security of a Manufacturing Enterprise in the Digital Environment

The article is devoted to the study of the features of ensuring the economic security of a manufacturing enterprise in the digital environment**.** The study examines the tasks of economic security specialists in manufacturing enterprises under modern conditions, shaped by risks associated with competitive pressure, market instability, technological changes, increasing information risks, and growing cyber threats amid the digital transformation of business operations.The purpose of the publication is to establish a list and identify specific aspects and challenges related to ensuring the economic security of industrial enterprises in the digital economy environment, to develop effective approaches and tools to improve the stability and sustainability of enterprises.

The publication is aimed at identifying the latest risks of the digital economy, including cyber threats, risks of digitalization of production processes, protection of intellectual property and commercial information; analysis of opportunities to ensure security through the implementation of digital technologies such as Blockchain, AI, IoT, and Big Data, which can increase the transparency and security of internal processes. The study addresses the assessment of the effectiveness of current economic security measures in the context of the digital transformation of manufacturing activities, identifying their strengths and weaknesses, and developing recommendations to enhance enterprises' adaptability to digital threats.

Recommendations have been developed for the introduction of innovative approaches to building an economic security system, such as cyber strategy, Big Data analytics, and automated risk management. Supply chain management and the protection of confidential information are considered from the perspective of integrating comprehensive and adaptive security systems into economic security processes. These systems address modern challenges and ensure the resilience of enterprises in the face of rapid and extensive digital transformation. The author's position is substantiated regarding the directions of scientific research in the field of ensuring the economic security of enterprise in the digital economy, aimed at increasing the level of economic security of industrial enterprises and help them adapt to the challenges of the digital economy, where economic stability largely depends on the ability to quickly adapt, proactively respond to risks and integrate the latest digital solutions

economic security, supply chains, artificial intelligence, Big Data, blockchain, risks of activities in the digital environment

Одержано (Received) 24.10.2024 *Прорецензовано (Rewieved) 10.12.2024*
Прийнято до друку (Approved) 23.12.2024