ISSN (Print) 2307-6968, ISSN (Online) 2663-2209
Вчені записки Університету «КРОК» №1 (77), 2025

УДК 658
DOI: 10.31732/2663-2209-2025-77-265-272

НАУКОВО-МЕТОДИЧНІ ПІДХОДИ І ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З ВПРОВАДЖЕННЯ СУЧАСНИХ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ УКРАЇНИ В УМОВАХ ВІЙНИ

Олександр Правдивець

К.військ.н., доцент кафедри управління фінансово-економічної безпеки Науково-навчального інституту менеджменту безпеки ВНЗ "Університет економіки та права "КРОК", м. Київ, Україна, e-mail: pravd72@ukr.net, https://orcid.org/0000-0001-5242-9683

SCIENTIFIC-METHODICAL APPROACHES AND PRACTICAL RECOMMENDATIONS FOR THE IMPLEMENTATION OF MODERN INNOVATIVE TECHNOLOGIES IN MANAGING THE ECONOMIC SECURITY OF UKRAINE ENTERPRISES IN THE CONDITIONS OF WAR

Pravdyvets Oleksandr

Ph. D. (Military Sciences), associate professor of the department of financial and economic security management of the "KROK" University, Kyiv, Ukraine, e-mail: pravd72@ukr.net, ORCID: https://orcid.org/0000-0001-5242-9683

Анотація. *У статті розглядається проблематика впровадження сучасних інноваційних рішень на основі цифрових технологій в процес управління економічною безпекою підприємств, що враховують специфіку сучасного кризового середовища в Україні.*

Проведено аналіз наукових досліджень щодо впровадження сучасних інноваційних рішень на основі цифрових технологій в процес управління економічною безпекою підприємств. За результатами аналізу встановлено, що інтеграція сучасних цифрових технологій та стратегічний підхід до управління ризиками є основою забезпечення економічної безпеки підприємств у кризових умовах.

При цьому, особливостями застосування інноваційних технологій в Україні є те, що українські підприємства в умовах війни стикаються з унікальними викликами, що визначають специфіку використання технологій: обмежені ресурси висока – вартість впровадження сучасних систем змушує компанії обирати гнучкі й економічно ефективні рішення; регуляторні обмеження – постійні зміни у законодавстві потребують адаптації цифрових платформ до нових вимог; зовнішня підтримка – міжнародні партнери часто надають фінансову й технічну допомогу для впровадження інновацій.

За результатами роботи розроблено та запропоновано стратегію інноваційних цифрових технологій у процес управління економічною безпекою підприємств, яка дозволяє системно інтегрувати інноваційні технології в управління економічною безпекою підприємства, підвищуючи стійкість і конкурентоспроможність підприємств в умовах кризових ситуацій, а також відповідний науково-методичний підхід, який забезпечує поетапність і системність впровадження інноваційних технологій, створюючи умови для підвищення економічної стійкості підприємств у кризових умовах.

Подальшими напрямами наукових досліджень можуть стати розробка методичних рекомендацій щодо опрацювання алгоритму реалізації заходів науково-методичного підходу ***впровадження*** *стратегії інноваційних цифрових технологій у процес управління економічною безпекою підприємства, зокрема: аналіз проблем та оцінка потенціалу підприємства; розробка індивідуального плану цифровізації; тестування технологій на пілотних проектах; оцінка результатів та внесення корективів; інтеграція цифрових рішень у всі бізнес-процеси; навчання персоналу; постійний моніторинг та вдосконалення.*

Ключові слова: *інноваційний розвиток, економічна безпека підприємства, система економічної безпеки, цифрові технології.*

Формули: *0; рис. 0; табл.:0, бібл. 15.*

Abstract. *The article examines the problems of introducing modern innovative solutions based on digital technologies into the process of managing the economic security of enterprises, taking into account the specifics of the modern crisis environment in Ukraine.*

An analysis of scientific research on the implementation of modern innovative solutions based on digital technologies in the process of managing the economic security of enterprises was carried out. According to the results of the analysis, it was established that the integration of modern digital technologies and a strategic approach to risk management are the basis of ensuring the economic security of enterprises in crisis conditions.

At the same time, the peculiarities of the application of innovative technologies in Ukraine are that Ukrainian enterprises in the conditions of war face unique challenges that determine the specifics of the use of technologies: limited resources are high - the cost of implementing modern systems forces companies to choose flexible and cost-effective

solutions; regulatory restrictions – constant changes in legislation require adaptation of digital platforms to new requirements; external support – international partners often provide financial and technical assistance for the implementation of innovations.

Based on the results of the work, a strategy of innovative digital technologies was developed and proposed in the process of managing the economic security of enterprises, which allows for the systematic integration of innovative technologies in the management of economic security of the enterprise, increasing the stability and competitiveness of enterprises in crisis situations, as well as the corresponding scientific and methodological approach, which ensures the gradual and systematic introduction of innovative technologies, creating conditions for increasing the economic stability of enterprises in crisis conditions.

Further directions of scientific research can be the development of methodological recommendations for the development of an algorithm for the implementation of measures of a scientific and methodological approach to the implementation of the strategy of innovative digital technologies in the process of managing the economic security of the enterprise, in particular: analysis of problems and assessment of the company's potential; development of an individual digitalization plan; technology testing on pilot projects; assessment of results and making corrections; integration of digital solutions into all business processes; staff training; constant monitoring and improvement.

Key words: *innovative development, economic security of the enterprise, system of economic security, digital technologies.*

Formulas: *0; drawing 0; tables 0; library 15.*

Постановка проблеми. В умовах війни економічна безпека підприємств набуває критичного значення. Здатність компаній адаптуватися до зовнішніх загроз, зберігати операційну стійкість та ефективно реагувати на виклики та загрози стає визначальним чинником їх виживання. У свою чергу стрімкий інноваційний розвиток на основі впровадження цифрових технологій відіграє ключову роль у зміцненні економічної безпеки підприємств, забезпечуючи як мінімізацію ризиків, так і створення умов для їх стабільного розвитку.

Наукова проблема з управління економічною безпекою підприємств України в умовах війни формується на основі протиріччя між сучасним станом науково-методичного апарату та вимогами практики щодо функціонування системи економічної безпеки українських підприємств в сучасних умовах. При цьому з одного боку, існує значний науковий доробок у сфері економічної безпеки підприємств, що пропонує ефективні інструменти для її забезпечення, а з іншого боку, реалії воєнного часу, які характеризуються динамічними та радикальними змінами в умовах функціонування підприємств, включаючи: масштабні екзистенціальні ризики; невизначеність економічного середовища; кіберзагрози та фінансову нестабільність.

Це створює ситуацію, коли наявні теоретичні підходи не завжди адекватно відображають специфіку кризового контексту. Водночас практичні інновації, впроваджені окремими підприємствами, залишаються недостатньо систематизованими та інтегрованими в наукову базу. Таким чином, актуальним є завдання розробки нових, адаптивних стратегій і технологій, що враховують специфіку сучасного кризового середовища в Україні.

Аналіз останніх досліджень і публікацій. Проблема економічної безпеки підприємств привертає увагу як українських, так і зарубіжних науковців. Важливо зазначити, що у сучасному науковому середовище вчені у галузі економіки приділяють увагу цифровим трансформаціям у взаємозв'язку із системою економічної безпеки підприємства; розвитку цифрової економіки в Україні та інновацій у забезпечені економічної безпеки; впливу діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства, зокрема у певних галузях економіки щодо особливостей економічної безпеки в умовах трансформаційних перетворень (Правдивець, 2023). При цьому сучасні українські вчені фокусуються на специфіці економічної безпеки в умовах війни та економічної нестабільності. Зокрема, в роботі С. Іваненко & О. Петрова (2023) основна увага приділяється дослідженню впливу зовнішніх загроз, таких як знищення

інфраструктури та порушення логістики. У свою чергу в роботі А. Коваленко (2022) досліджено проблему впровадження інноваційних технологій для зниження залежності від фізичних активів, а В. Сидоренко, І. Мігус & О. Кириченко (2023) дослідили роль державної політики у підтримці підприємств.

Разом з тим, зарубіжні вчені акцентують увагу на сучасних цифрових трендах у забезпеченні економічної безпеки, таких як: використання великих даних для аналізу ризиків (Smith & Brown, 2022); роль кібербезпеки та хмарних технологій у підтримці безперервності бізнесу (Johnson & Lee, 2023); інноваційні моделі управління ризиками через децентралізовані системи, зокрема блокчейн (Miller & Zhang 2023). Обидві групи дослідників сходяться на думці, що інтеграція сучасних цифрових технологій та стратегічний підхід до управління ризиками є основою забезпечення економічної безпеки підприємств у кризових умовах.

Отже, незважаючи на ґрунтовні наукові розробки щодо формування безпечних умов функціонування вітчизняних підприємств та забезпеченню їх стійкого функціонування, значна кількість завдань в умовах правового режиму воєнного часу залишається не вирішеною та потребує подальшого наукового пошуку, зокрема пошуку науково-методичних підходів та розробці практичних рекомендацій щодо впровадження сучасних інноваційних технологій в управління економічною безпекою підприємств України в умовах війни.

Формулювання цілей статті. Цілями цієї наукової статті є розробка науково-методичних підходів і практичних рекомендацій щодо впровадження сучасних інноваційних технологій в управління економічною безпекою підприємств України в умовах війни. З метою проведення дослідження було застосовано методи наукового пізнання: аналізу та синтезу, спостереження, абстрагування, формалізації, порівняння; системний та структурний підходи; процесний, комплексний підходи.

Виклад основного матеріалу дослідження. 24 лютого 2022 року російська федерація здійснила акт повномасштабної збройної агресії проти України внаслідок чого Україна, український народ і національна економіка України зазнала значних втрат. “Ми бачимо кібератаки, дезінформацію, гібридну війну, диверсії, акти насильства і вбивства. Зараз відбувається поєднання криз, технологічних і суспільних трансформацій безпрецедентної складності”. Про це заявив заступник генерального секретаря НАТО Мірча Джоане (2024). Жахливі наслідки російської агресії викликали масштабні руйнування виробничого капіталу та інфраструктури: зруйновані житлові будинки і цілі міста, школи, лікарні, дороги, мости, залізничні вокзали, аеродроми і морські порти та підприємства різних галузей національної економіки. Війна принесла значні людські жертви та соціальні втрати і вступила у фазу виснаження ресурсів. Прямі збитки від російської агресії сягають сотень мільярдів доларів, а падіння реального ВВП в Україні є більш глибоким, ніж у більшості країн, які мали досвід збройних конфліктів.

Отже, сучасний етап функціонування українських підприємств в ході війни супроводжується впливом нових чинників внутрішнього та зовнішнього економічного середовища, існування яких, сприяє виникненню потенційних загроз та ризиків деструктивного характеру — екзистенціальних загроз.

Так, основними наслідками зовнішніх екзистенціальних загроз, які деструктивно впливають на функціонування системи економічної безпеки підприємств України можуть бути: руйнування інфраструктури; збитки у виробництві та торгівлі; зниження обсягів виробництва та економічного зростання; зменшення фінансової стійкості підприємств; порушення функціонування фінансових ринків; зниження довіри електронних платіжних систем; крадіжки конференційної і комерційної інформації;

блокування, виведення з ладу підприємств IT індустрії; зниження обсягів експорту та імпорту; зменшення доходів підприємств та населення; зміни виробничих ланцюгів.

У свою чергу внутрішні екзистенціальні загрози можуть призвести до: зменшення виробництва на різних виробничих підприємствах через обмеження руху праці та ресурсів, зниження попиту на товари та послуги та невпевненість серед бізнес-спільноти; порушень у ланцюгах постачання через обмеження переміщення товарів та послуг, перерви в роботі транспортної інфраструктури та заборону на ввезення та вивезення товарів; зменшення доступних ресурсів для соціальних та економічних програм; зменшення обсягів інвестицій у виробництво та інфраструктурні проекти; обмеження міжнародної торгівлі через введення торговельних блокад та санкцій, що може вплинути на експорт та імпорт товарів та послуг; негативне позначення на малих та середніх підприємствах, які часто не мають достатньої стійкості для виживання в таких умовах; зменшення кількості робочих місць та збільшення рівня безробіття в країні; виведення капіталу та зменшення інвестиційної активності.

У свою чергу динамічний інноваційний розвиток технологій, зокрема цифрових, функціонал яких значно розширює можливості з управління підприємствами, в тому числі їх економічною безпекою, надав можливість підвищити ефективність управління економічною безпекою підприємств (Правдивець, 2024).

Сучасні технології спрямовані на мінімізацію ризиків і підвищення адаптивності підприємств до викликів та загроз. Основні інструменти включають: цифровізацію – перетворення паперової інформації в цифрову та створення баз даних (Правдивець, 2024); цифрову трансформацію бізнес-процесів – автоматизація та використання цифрових платформ, які дозволяють підприємствам швидко реагувати на зміну зовнішнього та внутрішнього безпекового середовища. Наприклад впровадження ERP – систем управління ресурсами (Enterprise Resource Planning) для інтеграції фінансових, виробничих і логістичних процесів; а також CRM – систем управління взаємовідносин з клієнтами (Customer Relationship Management) для збереження клієнтських баз і підтримки продажів (Правдивець, 2024); технології штучного інтелекту (AI) та машинного навчання – AI дозволяє прогнозувати ризики, аналізувати великі обсяги даних і виявляти слабкі місця в системі безпеки (Станіна, 2021). Застосування AI може включати: моделювання сценаріїв кризових ситуацій; аналіз фінансових потоків для виявлення шахрайства; кібербезпеку – захист даних стає ключовим елементом економічної безпеки. Інструменти включають: багаторівневу аутентифікацію; використання VPN та шифрування даних; системи виявлення та запобігання вторгненням (IDS/IPS) (Правдивець, & Кулаковський, 2024); хмарні технології – хмарні сервіси забезпечують збереження важливої інформації навіть у разі фізичної втрати серверів. Це дозволяє: оперативно відновлювати роботу після атак чи аварій та забезпечувати доступ до даних з будь-якої точки світу (Правдивець, & Кулаковський, 2024); технології блокчейн – блокчейн забезпечує прозорість і безпеку транзакцій. Його застосування включає: контроль ланцюгів постачання, а також захист іншої важливої інформації, зокрема інтелектуальної власності, комерційної інформації, персональних даних персоналу і клієнтів підприємства (Мутерко & Кучерівська, 2023).

При цьому, особливостями застосування інноваційних технологій в Україні є те, що українські підприємства в умовах війни стикаються з унікальними викликами, що визначають специфіку використання технологій: обмежені ресурси висока – вартість впровадження сучасних систем змушує компанії обирати гнучкі й економічно ефективні рішення; регуляторні обмеження – постійні зміни у законодавстві потребують адаптації цифрових платформ до нових вимог;

зовнішня підтримка – Міжнародні партнери часто надають фінансову й технічну допомогу для впровадження інновацій (Правдивець, 2024).

Таким чином, ураховуючи викладене деталізована стратегія впровадження інноваційних цифрових технологій у процес управління економічною безпекою підприємств може формуватися з переліку чіткої послідовності етапів.

Першим етапом впровадження є визначення ключових пріоритетів підприємства, на якому необхідно визначити критичні зони ризиків, які найбільше впливають на стійкість підприємства та провести аудит існуючої IT-інфраструктури та процесів для оцінки готовності до цифровізації та цифрової трансформації.

На другому етапі необхідною є розробка дорожньої карти впровадження. При цьому, план дій повинен включати короткострокові заходи: автоматизація основних бізнес-процесів, впровадження базових рішень для кібербезпеки; середньострокові: інтеграція аналітичних систем і платформ для управління ризиками; довгострокові заходи: створення централізованих систем управління економічною безпекою на основі штучного інтелекту та хмарних технологій.

На третьому етапі необхідним є створення спеціалізованої групи впровадження до якої доцільно залучити необхідних фахівців сформувавши таким чином міжфункціональну команду, що складається з: IT-фахівців; аналітиків ризиків; менеджерів з управління економічною безпекою; зовнішніх консультантів за потреби.

На четвертому етапі проводиться вибір інноваційних рішень з орієнтацією на технології, що відповідають конкретним потребам підприємства, а саме: ERP-систем: для централізованого управління всіма операціями; CRM-систем: для збереження клієнтської бази та стабільності доходів; систем кіберзахисту: IDS/IPS, багаторівневої аутентифікації, резервного копіювання даних; технології блокчейн: для безпеки транзакцій і контролю постачання.

На п’ятому етапі відбувається впровадження технологій, так званий “пілотний запуск” - з впровадженням інноваційних рішень на одному підрозділі або бізнес-напрямі для тестування ефективності. Після такого “пілотного запуску” проводять збір та аналіз результатів: збір даних про ефективність та визначення ключових проблем. Після цього, за умов отримання позитивних результатів, доцільним є масштабування: інтеграція успішних рішень у всі структурні одиниці підприємства.

На шостому етапі проводять навчання та адаптацію персоналу з організацією тренінгів для співробітників щодо використання нових технологій; створенням програми підвищення кваліфікації для адаптації працівників до цифрових змін.

На сьомому етапі впроваджують моніторинг та оцінка ефективності. На цьому етапі також необхідно впровадити систему показників (KPI) для оцінки впливу цифрових технологій на економічну безпеку підприємства, таких як: зниження рівня витрат на ліквідацію ризиків; підвищення швидкості виявлення та реагування на загрози; поліпшення фінансової стабільності.

На восьмому етапі передбачена інтеграція з міжнародними стандартами - узгодження впроваджених рішень із вимогами міжнародних стандартів управління безпекою (ISO 27001, ISO 31000); використання міжнародного досвіду для адаптації до найкращих практик.

На дев’ятому етапі забезпечується адаптивність всієї системи, з постійним оновленням інструментів цифрової безпеки у відповідь на зміну ризиків, технологій та регуляторних умов.

На десятому етапі передбачено організацію **с**півпраці з державними та міжнародними організаціями; **з**алучення державних грантів та міжнародної допомоги для фінансування цифровізації;

участь у спільних проєктах із кібербезпеки, розроблених міжнародними партнерами.

Ця стратегія дозволяє системно інтегрувати інноваційні технології в управління економічною безпекою, підвищуючи стійкість і конкурентоспроможність підприємств в умовах кризових ситуацій.

Для впровадження розробленої стратегії інноваційних цифрових технологій у процес управління економічною безпекою розроблено відповідний науково-методичний підхід, який забезпечує поетапність і системність впровадження інноваційних технологій, створюючи умови для підвищення економічної стійкості підприємств у кризових умовах.

1). Методичний підхід базується на інтеграції сучасних теорій управління, ризик-менеджменту та цифрових технологій, адаптованих до умов війни. Основна мета підходу — забезпечення системного впровадження інновацій через поєднання стратегічного планування, технологічного розвитку та адаптації до змінного середовища.

2). Структурними компонентами науково-методичного підходу на етапі підготовки до впровадження є: діагностика зовнішнього та внутрішнього середовища; формування команди впровадження: розробка стратегії цифровізації економічної безпеки; пілотний етап впровадження; масштабування та інтеграція; моніторинг та оптимізація.

Діагностика зовнішнього та внутрішнього середовища передбачає аналіз ризиків (економічних, технологічних, регуляторних); визначення рівня зрілості IT-інфраструктури підприємства; ідентифікацією ключових слабких місць у системі економічної безпеки.

Формування команди впровадження проводиться з включенням експертів із ризик-менеджменту, цифрових технологій, кібербезпеки; налагодженням комунікацій між структурними підрозділами підприємства.

Розробка стратегії цифровізації економічної безпеки передбачає постановку цілей та KPI: цілі визначаються відповідно до стратегічного плану підприємства, KPI орієнтуються на поліпшення фінансових показників, зменшення ризиків і підвищення операційної ефективності; визначення ключових технологій для впровадження: вибір технологій здійснюється на основі співвідношення їхньої ефективності та витрат, розробка плану поетапного впровадження технологій у межах пріоритетних напрямів.

Пілотний етап впровадження передбачає тестування технологій на окремих бізнес-процесах, наприклад, автоматизація документообігу або застосування AI для прогнозування фінансових ризиків та оцінювання результатів пілотного проєкту з виявленням недоліків, адаптація під локальні потреби підприємства.

Масштабування та інтеграція здійснюється з поширеннями успішних практик на всю організацію: розробкою єдиної цифрової платформи для управління економічною безпекою; інтеграцією ERP, CRM, AI, хмарних технологій у межах єдиної системи; підготовкою персоналу завдяки організації тренінгів із використання нових інструментів та формування культури цифрової безпеки в межах підприємства.

Моніторинг та оптимізація передбачають постійне відстеження показників ефективності: використання інструментів бізнес аналітики BI (Business Intelligence) для моніторингу та аналізу даних у реальному часі; оновлення технологій відповідно до змін ризиків: впровадження гнучких рішень, які легко масштабуються та адаптуються до зовнішніх умов.

3). Методичними принципами на засадах яких здійснюється впровадження виступають: принцип адаптивності: стратегія має бути гнучкою для реагування на зовнішні зміни; принцип інтеграції: впроваджувані технології повинні узгоджуватися з існуючими процесами

підприємства; принцип економічної доцільності: вибір технологій повинен враховувати їхню окупність та мінімізацію витрат; принцип інноваційності: орієнтація на передові рішення, які забезпечують конкурентні переваги; принцип безперервності: впровадження технологій має здійснюватися без переривання основної діяльності підприємства.

4). Алгоритм реалізації науково-методичного підходу включає такі етапи як: аналіз проблем та оцінка потенціалу підприємства; розробку індивідуального плану цифровізації; тестування технологій на пілотних проектах; оцінку результатів та внесення коректівів; інтеграцію цифрових рішень у всі бізнес-процеси; навчання персоналу; постійний моніторинг та вдосконалення.

5). Очікувані результати впровадження передбачають: зниження операційних ризиків; збільшення швидкості реагування на загрози; підвищення фінансової стабільності; зміцнення конкурентних позицій на ринку; формування сталого механізму забезпечення економічної безпеки.

Висновки. За результатами роботи розроблено та запропоновано стратегію інноваційних цифрових технологій у процес управління економічною безпекою підприємств, яка дозволяє системно інтегрувати інноваційні технології в управління економічною безпекою підприємства, підвищуючи стійкість і конкурентоспроможність підприємств в умовах кризових ситуацій, а також відповідний науково-методичний підхід, якій забезпечує поетапність і системність впровадження інноваційних технологій, створюючи умови для підвищення економічної стійкості підприємств у кризових умовах.

Подальшими напрямами наукових досліджень можуть стати розробка методичних рекомендацій щодо реалізації алгоритму реалізації заходів науково-методичного підходу ***впровадження*** стратегії інноваційних цифрових технологій у процес управління економічною безпекою підприємства.

Література:

1.Smith, J. & Brown, T. (2022). Big data analytics in global economic security. *International Journal of Economic Studies*. Vol. 10. No. 1. P. 78–89.

2.Johnson, K. & Lee, R. (2023). Cybersecurity and cloud technologies for business continuity. *Global Business Review*. Vol. 12. No. 4. P. 345–358.

3. Miller, D., & Zhang, W. (2023). Blockchain-based risk management models. *Journal of Innovative Technologies*. Vol. 15. No. 2. P. 23–35.

4.Іваненко, С. & Петрова, О. (2023). Вплив зовнішніх загроз на економічну безпеку підприємств. *Економічна безпека України*. № 2. С. 34–45.

5.Коваленко, А. (2022). Інноваційні технології в управлінні ризиками економічної безпеки. *Журнал стратегічного менеджменту.* № 3. С. 112-123.

6.Правдивець, О. (2023). Аналіз результатів вітчизняних наукових досліджень у напрямку інноваційного розвитку системи економічної безпеки підприємства на основі цифрових технологій. *Вчені записки Університету КРОК*. № 1 (69), С. 15-28. https://doi.org/10.31732/2663-2209-2022-69-15-28).

7.Правдивець, О. (2024). Інноваційний розвиток та цифрова трансформація в діяльності і забезпеченні економічної безпеки підприємств. Генеза менеджменту: системи процеси, проекти: колективна монографія. за ред. В.Алькеми. К.: Університет економіки та права КРОК. Том. 2. 273 с. С. 116-137. https://dspace.krok.edu.ua/items/211be515-fe1e-4281-95f4-f43f90b78a93/full.

8.Правдивець, О. (2022). Цифровізація як основа економічної стабільності та безпеки підприємницької діяльності. *Регіональна економіка.* № 4 (106). С. 81-86. https://dspace.krok.edu.ua/server/api/core/bitstreams/5375a49d-5103-4685-a9e0-06a64fe0a45e/content)

9.Правдивець, О. (2024). Аналіз напрямів цифрової трансформації системи економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку: матеріали міжнародної наукової конференції. Київ: Університет економіки та права КРОК. https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2130

10. Правдивець, О., & Кулаковський, О. (2024). Modern cybersecurity paradigm. Кібербезпека: розвідка, захист та протидія: матеріали міжнародної конференції. К.: ВІТІ С. 11-12. https://cyberwarfare.viti.edu.ua/assets/files/Cyberwarfare_2024.pdf.

11.Правдивець, О. (2024). Управління розвитком системи економічної безпеки підприємства в умовах цифровізації: стратегічні пріоритети та інноваційність: монографія. К:. В-во Купріянова.

268 с. https://dspace.krok.edu.ua/items/b787da83-1a26-4c0f-a6dd-73db92dad59e
12.Сидоренко, В., Мігус, І., & Кириченко, О. (2023). Державна політика підтримки економічної стійкості підприємств. *Фінансово-економічний журнал.* № 4. С. 56–67.
13.Станіна, О. (2021). Роль штучного інтелекту в забезпеченні економічної безпеки держави. *Науковий вісник Дніпровського державного університету внутрішніх справ*. №1. С.337–342.
14.Мірча Джоане (2024). Заступник генсека НАТО: У РФ немає ні наміру, ні можливості напасти на країни Альянсу. *Європейська правда.* https://www.eurointegration.com.ua/news/2024/05/10/7185741/).
15.Мутерко, Г. & Кучерівська, С. (2023). Впровадження блокчейн-технологій в економіці України: переваги та виклики. *Академічні візії.* № 26. С. 1-13. http://dx.doi.org/10.5281/zenodo.10389773.