

ІНТЕГРАЦІЯ СИСТЕМ УПРАВЛІННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОЮ БЕЗПЕКОЮ У СТРАТЕГІЧНИЙ МЕНЕДЖМЕНТ СУБ'ЄКТІВ АГРАРНОГО БІЗНЕСУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ТА ВОЄННО-ЕКОНОМІЧНИХ ВИКЛИКІВ

©2026 САБАДАШ І. В., БЕРЕЗА В. В., СЕЛІХОВ С. В.

УДК 338.436:339

JEL Classification: H56; M10; O33; Q12

Сабадаш І. В., Береза В. В., Селіхов С. В.

Інтеграція систем управління організаційно-правовою безпекою у стратегічний менеджмент суб'єктів аграрного бізнесу в умовах цифрової трансформації та воєнно-економічних викликів

Статтю присвячено дослідженню теоретичних і прикладних аспектів інтеграції організаційно-правової безпеки у систему стратегічного менеджменту суб'єктів аграрного бізнесу в умовах цифрової трансформації та воєнно-економічних викликів. Обґрунтовано, що активне впровадження цифрових технологій, систем точного землеробства, штучного інтелекту, Інтернету речей, автоматизованих платформ управління та цифрових сервісів, поряд із підвищенням ефективності виробничих процесів, зумовлює появу нових організаційних, правових, інформаційних і кібернетичних ризиків. Встановлено, що сучасні умови функціонування аграрних підприємств вимагають переходу від фрагментарного реагування на окремі загрози до комплексної інтеграції механізмів організаційно-правової безпеки в систему стратегічного управління. У роботі проаналізовано сучасні тенденції розвитку цифровізації аграрного сектора, вплив воєнно-економічних чинників на діяльність суб'єктів аграрного бізнесу та основні організаційно-правові ризики, що виникають у процесі цифрової трансформації. На основі статистичних даних досліджено динаміку цифрових інвестицій і зростання кіберзагроз як чинників трансформації систем управління безпекою. Узагальнено ключові організаційно-правові ризики цифрової трансформації аграрних підприємств і визначено стратегічні механізми їх мінімізації. Запропоновано модель інтеграції організаційно-правової безпеки у систему стратегічного менеджменту аграрного підприємства, яка передбачає комплексне поєднання правового забезпечення, комплаєнс-менеджменту, ризик-орієнтованого управління, кібербезпеки, кадрового розвитку та внутрішнього контролю. Обґрунтовано, що реалізація запропонованого підходу забезпечує своєчасне виявлення та мінімізацію ризиків, підвищує адаптивність підприємств до змін зовнішнього середовища, сприяє зміцненню економічної стійкості, конкурентоспроможності та безперервності господарської діяльності в умовах цифрової трансформації й воєнно-економічної нестабільності. Практичне значення результатів дослідження полягає у можливості використання запропонованих рекомендацій під час розроблення стратегій розвитку, удосконалення систем управління організаційно-правовою безпекою та впровадження сучасних цифрових технологій у діяльність суб'єктів аграрного бізнесу.

Ключові слова: організаційно-правова безпека; стратегічний менеджмент; аграрний бізнес; цифрова трансформація; кібербезпека; ризик-менеджмент.

DOI: <https://doi.org/10.32983/2222-0712-2026-2-280-288>

Рис.: 3. Табл.: 1. Бібл.: 19.

Сабадаш Інна Володимирівна – кандидат юридичних наук, докторант, Інститут тваринництва НААН України (вул. Тваринників, 1а, Харків, 61026, Україна)

E-mail: inna.sabadash@tuta.com

ORCID: <https://orcid.org/0009-0001-5267-9153>

Береза Валерій Володимирович – доктор філософії, докторант, Інститут тваринництва НААН України (вул. Тваринників, 1а, Харків, 61026, Україна)

E-mail: bereza.vv@meta.ua

ORCID: <https://orcid.org/0009-0006-6698-2889>

Селіхов Сергій Володимирович – кандидат економічних наук, докторант, Інститут тваринництва НААН України (вул. Тваринників, 1а, Харків, 61026, Україна)

E-mail: info@lfi-naas.org.ua

ORCID: <https://orcid.org/0009-0009-4040-2235>

UDC 338.436:339

JEL Classification: H56; M10; O33; Q12

Sabadash I. V., Bereza V. V., Selikhov S. V. Integration of Organizational and Legal Security Management Systems into the Strategic Management of Agrarian Business Entities in the Conditions of Digital Transformation and Wartime-Economic Challenges

The article is focused on studying the theoretical and practical aspects of integrating organizational and legal security into the strategic management system of agrarian business entities amid digital transformation and wartime-economic challenges. It is substantiated that the active implementation of digital technologies, precision farming systems, artificial intelligence, the Internet of Things, automated management platforms, and digital services, along with improving production efficiency, leads to the emergence of new organizational, legal, informational, and cyber risks. It is found that the current operating conditions of agrar-

ian enterprises require moving from a fragmented response to individual threats to a comprehensive integration of organizational and legal security mechanisms into the strategic management system. The study analyzes current trends in the digitalization of the agrarian sector, the impact of wartime-economic factors on the activities of agrarian business entities, and the main organizational and legal risks that arise during digital transformation. Based on statistical data, the study examines the dynamics of digital investments and the rise of cyber threats as factors transforming security management systems. The key organizational and legal risks of digital transformation in agrarian enterprises are summarized, and strategic mechanisms to minimize them are identified. A model for integrating organizational and legal security into the strategic management system of an agrarian enterprise is proposed, which involves a comprehensive combination of legal support, compliance management, risk-oriented management, cybersecurity, personnel development, and internal control. It has been substantiated that implementing the proposed approach ensures timely risk detection and minimization, enhances the adaptability of enterprises to changes in the external environment, and contributes to strengthening economic resilience, competitiveness, and continuity of business operations under conditions of digital transformation and wartime-economic instability. The practical significance of the research results lies in the possibility of using the proposed recommendations when elaborating development strategies, improving organizational and legal security management systems, and implementing modern digital technologies in the activities of agribusiness entities.

Keywords: organizational and legal security; strategic management; agribusiness; digital transformation; cybersecurity; risk management.

Fig.: 3. **Tabl.:** 1. **Bibl.:** 19.

Sabadash Inna V. – Candidate of Sciences (Law), Candidate on Doctor Degree, Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine (1a Tvarynykiv Str., Kharkiv, 61026, Ukraine)

E-mail: inna.sabadash@tuta.com

ORCID: <https://orcid.org/0009-0001-5267-9153>

Bereza Valerii V. – PhD, Candidate on Doctor Degree, Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine (1a Tvarynykiv Str., Kharkiv, 61026, Ukraine)

E-mail: bereza.vv@meta.ua

ORCID: <https://orcid.org/0009-0006-6698-2889>

Selikhov Serhii V. – Candidate of Sciences (Economics), Candidate on Doctor Degree, Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine (1a Tvarynykiv Str., Kharkiv, 61026, Ukraine)

E-mail: info@lfi-naas.org.ua

ORCID: <https://orcid.org/0009-0009-4040-2235>

Вступ. З огляду на прогнози ООН щодо зростання чисельності населення планети майже до 10 мільярдів осіб до 2050 року, навантаження на світові сільськогосподарські системи досягло історичного максимуму. Необхідність виробляти значно більші обсяги продовольства за умов суттєвого скорочення доступних ресурсів змушує аграрний сектор шукати нові технологічні рішення. Відповіддю на ці глобальні виклики стає концепція «розумного сільського господарства» (Smart Agriculture), що передбачає інтеграцію цифрових інструментів – датчиків Інтернету речей (IoT), безпілотних літальних апаратів, аналітики на базі штучного інтелекту та робототехніки – для оптимізації управління фермерськими господарствами.

Проте для України глобальний тренд технологічної модернізації розгортається на тлі руйнівних воєнно-економічних викликів. Вітчизняні суб'єкти агробізнесу змушені одночасно адаптуватися до умов воєнного стану, долати наслідки руйнування інфраструктури та інтегрувати складні цифрові системи у свою діяльність. За таких обставин критичного значення набуває організаційно-правова безпека підприємств, яка повинна бути не просто ізольованою функцією юридичного відділу, а базовим елементом стратегічного менеджменту агробізнесу.

Аналіз останніх досліджень і публікацій показує, що проблематика інтеграції систем управління безпекою в сучасні моделі стратегічного менеджменту дедалі частіше стає предметом наукових досліджень, що зумовлено активною цифровою трансформацією економіки, зростанням кіберзагроз та необхідністю підвищення стійкості під-

приємств до зовнішніх ризиків. Теоретичні та прикладні аспекти забезпечення економічної, організаційної й інформаційної безпеки знайшли відображення у працях українських і зарубіжних учених, які сформували методологічне підґрунтя сучасних концепцій безпеки.

Серед вітчизняних дослідників вагомий внесок у розвиток теорії економічної безпеки підприємств зробила О. І. Вівчар [10], яка обґрунтувала стратегічні підходи до забезпечення економічної безпеки суб'єктів господарювання в соціогуманітарному контексті та запропонувала механізми її інтеграції у загальну систему управління. Для подолання ризиків та невизначеності у воєнний період науковці дедалі частіше звертаються до гнучких моделей управління. Зокрема, дослідження активних та пасивних стратегій захисту, сформульовані у працях Н. В. Зачосової, О. В. Ковалю та Д. В. Сафонова [12], дозволяють поєднати проактивне виявлення інноваційних загроз із регулярним моніторингом для зміцнення стійкості сучасних суб'єктів господарювання.

Останніми роками суттєво зросла увага науковців до інтеграції систем управління інформаційною безпекою із загальною системою менеджменту підприємства. Зокрема, Giovanna Culot, Guido Nassimbeni, Matteo Podrecca та Marco Sartor [2; 3] у систематичному огляді наукових досліджень, присвячених стандарту ISO/IEC 27001, доводять, що ефективність системи управління інформаційною безпекою визначається не лише технічними засобами захисту, а й рівнем її інтеграції зі стратегічним управлінням, системою управління ризиками та корпоративним управлінням

підприємства. Автори наголошують, що сучасні системи безпеки мають розглядатися як невід'ємний елемент стратегічного розвитку організації та адаптуватися до змін зовнішнього середовища. Практичне значення такого підходу підтверджується подальшими дослідженнями авторів, які встановили позитивний вплив впровадження ISO/IEC 27001 на результати діяльності підприємств, їхню стійкість до інформаційних ризиків та довіру зацікавлених сторін.

Водночас аналіз наукових праць свідчить, що більшість досліджень присвячена окремим аспектам економічної, інформаційної або кібербезпеки підприємств. Натомість питання комплексної інтеграції організаційно-правової безпеки у систему стратегічного менеджменту суб'єктів аграрного бізнесу з урахуванням цифрової трансформації, поширення технологій Smart Agriculture та воєнно-економічних викликів залишаються недостатньо розробленими, що й зумовлює необхідність подальших досліджень.

Мета статті – обґрунтування теоретико-прикладних засад інтеграції організаційно-правової безпеки в систему стратегічного менеджменту суб'єктів аграрного бізнесу в умовах цифрової трансформації та воєнно-економічних викликів.

Викладення основного матеріалу дослідження. Сучасний етап розвитку агропромислового комплексу (АПК) визначається концепцією точного землеробства – дата-центричного підходу, що забезпечує точкове управління ресурсами. Використання датчиків IoT дозволяє здійснювати моніторинг стану ґрунту та посівів у реальному часі, аерофотозйомка з дронів допомагає виявляти проблемні зони на ранніх етапах, а безпілотні трактори та GPS-керовані роботизовані системи автоматизують капіталомісткі процеси оранки, пропонування, збирання врожаю та обприскування. При цьому мінімізуються втрати сировини, зменшується екологічне навантаження та підвищення врожайності.

Динаміка світових інвестицій у цифрову трансформацію свідчить про перехід підприємств до цифрових моделей управління (рис. 1). Для аграрного сектору це означає не лише підвищення ефективності виробництва, а й виникнення нових організаційно-правових ризиків, пов'язаних із використанням цифрових платформ, алгоритмів штучного інтелекту та обробкою даних. Проте технологічний прогрес супроводжується серйозними компромісами та системни-

ми ризиками. Переваги точного землеробства найчастіше концентруються в руках великих, висококапіталізованих холдингів, оскільки вартість комплексних smart-систем залишається недоступною для дрібних фермерів. Високі початкові витрати, складність освоєння технологій та тривалий період окупності інвестицій гальмують цифрову трансформацію малих господарств. До того ж жорстка залежність від стабільного інтернет-зв'язку та енергопостачання стає критичною вразливістю для віддалених аграрних регіонів.

Існують також екологічні та агрономічні суперечності. Прагнення максимізувати прибутки за допомогою цифрових систем стимулює розвиток масштабних монокультур, якими простіше керувати за допомогою алгоритмів, що створює загрозу для біорізноманіття. Крім того, екологічна вигода від скорочення обсягів використання води й добрив має зіставлятися з високим рівнем споживання енергії самими цифровими пристроями та серверами для обробки даних.

Для вітчизняних суб'єктів господарювання глобальні виклики ускладнюються катастрофічними наслідками бойових дій. Станом на кінець 2024 року загальні прямі та непрямі втрати українського агропромислового комплексу внаслідок повномасштабного вторгнення оцінювалися майже у 84 млрд доларів США, а сукупна потреба у фінансуванні процесів відновлення становила 55,5 млрд доларів США. Найглибших руйнувань зазнали господарства у прифронтових та тимчасово окупованих областях, зокрема Херсонській, Запорізькій, Донецькій та Харківській, де обсяг прямих втрат сягнув 11,2 млрд доларів США [5; 14].

Блокада портів, руйнування логістичних ланцюгів та безпосередні бойові дії спричинили різке скорочення експорту й падіння доходів аграріїв, що потребує системного аналізу регіональних наслідків війни. Як зазначено у науково-аналітичній доповіді Інституту регіональних досліджень імені М. І. Долишнього НАН України [11], подолання кризових явищ та формування передумов для повоєнного відновлення безпосередньо залежить від адаптивності місцевих економічних систем та інтеграції безпекових контурів у стратегічне управління ключовими секторами, зокрема АПК.

У Харківській області масштаб руйнувань є критичним для регіональної економічної стабільності. Понад 500 сільськогосподарських підприємств зазнали суттєвих пошкоджень або були повністю зруйновані, а понад 1600 одиниць спеціалізованої техніки було знищено [19]. Додатковим тягарем стали довгострокові екологічні збитки, які в області перевищили пів трильйона гривень: бойовими діями забруднено та засмічено понад 7,34 млн квадратних метрів земельних ресурсів (оцінка шкоди становить 502,276 млрд грн), а викиди понад 542,5 тис. тонн забруднюючих речовин в атмосферне повітря завдали збитків ще на 3,856 млрд грн [13].

Проблема протимінної діяльності залишається одним із головних факторів, що блокують ведення господарської діяльності. На кінець 2025 року понад 40 тис. гектарів земель у Харківській області вважалися потенційно небезпечними або замінованими. Протягом 11 місяців 2025 року державні оператори протимінної діяльності змогли розмінувати понад 9 тис. гектарів (з них понад 6 тис. гектарів – землі сільськогосподарського призначення), тоді як не-

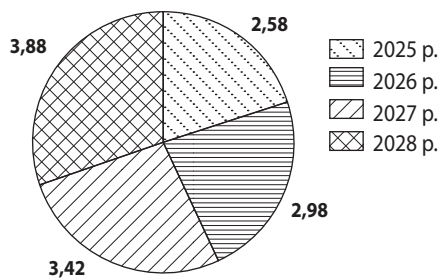


Рис. 1. Витрати на технології та послуги цифрової трансформації у всьому світі з 2025 по 2028 рр., трлн дол. США

Джерело: сформовано на основі [4]

урядові оператори обстежили 41 тис. гектарів та очистили близько 8,2 тис. гектарів [18].

Ситуація ускладнюється руйнуванням логістичних ланцюгів. Понад 50 атак на портову інфраструктуру призвели до пошкодження більш ніж 280 об'єктів та знищення понад 100 тис. тонн сільськогосподарської продукції. Блокада портів спричинила скорочення експорту зернових культур у період 2022–2023 років на 13%, що різко знизило платоспроможність аграріїв та їхню спроможність інвестувати у відновлення земельного фонду та закупівлю сучасних технологій⁶. Близько 60% дрібних фермерів повідомили про падіння доходів (з яких 46% зафіксували критичне зниження), а заборгованість серед малих господарств зростає з 6 % у 2021 році до 9 % у 2022 році. Водночас у 2024 році ринок землі продемонстрував дивовижну адаптивність: середня ціна гектара землі зростає на 21% до 46 678 грн, а кількість зареєстрованих угод збільшилася на 34% порівняно з попереднім роком [9].

Організаційно-правова безпека є фундаментом стабільного функціонування підприємства в умовах перманентної економічної нестабільності, змін законодавства та рейдерських загроз та забезпечує відповідність бізнес-процесів нормативно-правовим вимогам, мінімізуючи юридичні ризики, штрафні санкції та втрату активів. Структурно такий вид безпеки охоплює управління матеріальними, фінансовими, трудовими та інформаційними ресурсами, а також процеси модернізації обладнання, залучення інвестицій і підвищення кваліфікації кадрів [6; 7].

Однак емпіричні дослідження свідчать про критично низький рівень уваги менеджменту до таких питань. Українські аграрні підприємства залучають елементи функціональних систем менеджменту для забезпечення своєї економічної, екологічної та організаційно-правової безпеки лише на 19–35%. Підприємства переважно ігнорують показники ефективності розвитку (такі як ринковий успіх продукції та стійкі конкурентні переваги) у своїй планово-економічній діяльності та стратегічному плануванні.

Для подолання розривів у воєнний період найефективнішою визнано змішану стратегію управління безпекою, яка поєднує елементи активної оборони (проактивне виявлення вразливостей, правове моделювання загроз) та пасивного захисту (регуляторний комплаєнс, страхування ризиків). Стратегічний менеджмент має формувати довгострокові орієнтири, місію та візію безпеки, тоді як командний менеджмент повинен забезпечувати оперативну гнучкість, координацію зусиль та швидкий розподіл ролей у кризових ситуаціях [12].

Впровадження цифрових технологій в українських реаліях стримується не лише фінансовим дефіцитом, а й жорсткими регуляторними та воєнними обмеженнями, які безпосередньо впливають на організаційно-правову безпеку підприємств.

По-перше, використання безпілотних літальних апаратів (БПЛА) для потреб АПК ускладнене відсутністю єдиного порядку отримання дозволів на польоти. Вимоги різняться залежно від регіону та відомства, що приймає рішення (СБУ, військові адміністрації або підрозділи ЗСУ), а тривалі терміни розгляду заявок унеможливають оперативне планування сезонних робіт. При цьому державні

органи значно охочіше погоджують польоти, якщо суб'єкт господарювання може чітко обґрунтувати їхню значущість для продовольчої безпеки держави (наприклад, оптимізація витрат палива чи підвищення врожайності в умовах дефіциту ресурсів).

По-друге, чинне законодавство встановлює жорсткі правила експлуатації авіаційної техніки. Згідно з Повітряним кодексом України, обов'язковий реєстрації у Державному реєстрі цивільних повітряних суден підлягають усі комерційні дрони, а також БПЛА, чия злітна вага перевищує 20 кг. Крім того, необхідно отримати унікальний операторський номер у Національній інформаційній системі. Для безпілотників вагою до 20 кг, які використовуються у наукових, спортивних чи розважальних цілях, державна реєстрація не потрібна, проте вони підлягають обліку в уповноважених організаціях. Будь-які польоти без спеціального дозволу обмежені висотою до 120 метрів, заборонено наближатися ближче ніж на 500 метрів до інших повітряних суден та на 150 метрів до скупчень людей, а порушення цих норм тягне за собою сувору адміністративну та кримінальну відповідальність (зокрема у разі виникнення авіаційних подій з тілесними ушкодженнями або пошкодженням майна).

По-третє, серйозною проблемою залишається захист персональних та комерційних даних. Зйомка полів за допомогою дронів часто охоплює суміжні земельні ділянки, що без письмової згоди їхніх власників є прямим порушенням Закону України «Про захист персональних даних» і може призвести до штрафів до 17 000 грн або тривалих судових позовів. Ситуація ускладнюється тим, що в Україні досі відсутній спеціальний комплексний закон про БПЛА, регулювання базується на застарілих нормах, а адаптація національного законодавства до європейських стандартів (таких як GDPR та Artificial Intelligence Act) перебуває на початковій стадії. Хоча у 2020 році уряд ухвалив Концепцію розвитку штучного інтелекту, правовий статус алгоритмічних рішень в агросекторі залишається неврегульованим, що створює значні юридичні ризики для інвесторів.

Глобальна цифрова трансформація відкриває бізнес для нових загроз. Світові витрати на цифровізацію зростають (з 2.58 трлн доларів США у 2025 році до прогнозованих 3.88 трлн у 2028 році), паралельно збільшуючи площу кібератак. Очікується, що глобальні збитки від кіберзлочинності зростуть з 9,22 трлн доларів у 2024 році до 15,63 трлн у 2029 році (рис. 2). Найбільш вразливими є промислові сектори, де близько 70% усіх інцидентів припадає на атаки вірусів-вимагачів. У відповідь на це компанії нарощують бюджети на ІТ-безпеку (середнє зростання у 2024 році склало 5,7%), роблячи ключовий акцент на підвищенні кіберстійкості команд.

Стрімке зростання кіберзлочинності трансформувє кібербезпеку з технічної функції в ключовий елемент організаційно-правової безпеки підприємства.

Динаміка світових інвестицій у цифрову трансформацію свідчить про перехід підприємств до дата-центричних моделей управління. Оцінюючи економічні переваги цифрової трансформації аграрного сектору, Б. Мельник [17] наголошує на важливості автоматизації бізнес-процесів та оптимізації використання ресурсів за допомогою smart-

Збитки, трлн дол. США

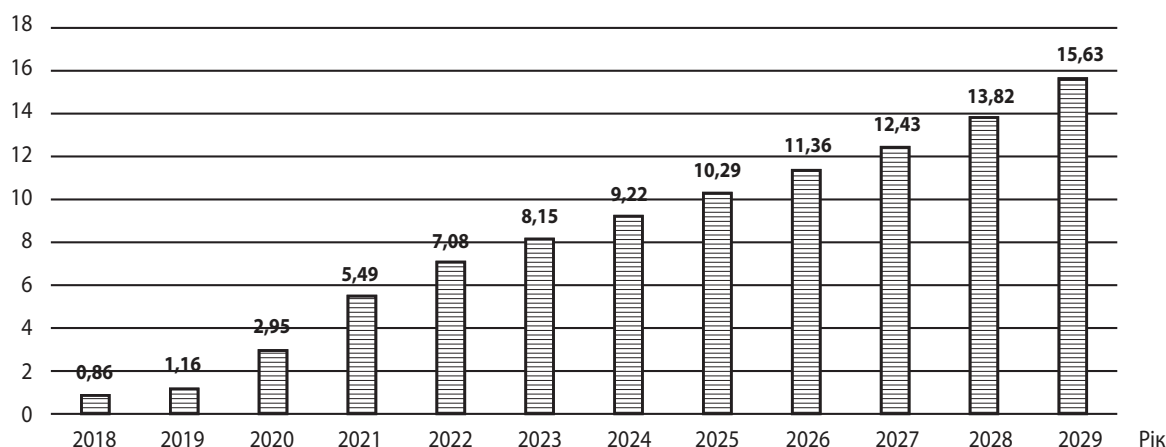


Рис. 2. Орієнтовні збитки від кіберзлочинності у світі за 2018-2029 рр., трлн дол. США

Джерело: сформовано на основі [1]

систем. Водночас стрімке впровадження IoT-пристроїв та штучного інтелекту породжує специфічні виклики. Досліджуючи цей аспект, В. Карбівський [15] доводить, що стабільне функціонування та фінансова безпека аграрних підприємств в умовах цифровізації потребують превентивного управління кіберризиками, оскільки будь-які збої у цифрових інфраструктурах призводять до значних фінансових втрат.

В українському агросекторі впровадження IoT та хмарних платформ супроводжується значними технічними труднощами: обмеженою ємністю локальних енергомереж, нестабільним покриттям інтернету та вразливістю хмарних сховищ до атак. Збої в роботі систем та цілеспрямовані кібератаки вже сьогодні завдають аграріям значних фінан-

сових втрат.

Для запобігання подібним інцидентам системи стратегічного менеджменту повинні передбачати превентивні інструменти захисту інформації. Проведення регулярних аудитів кібербезпеки дозволяє знизити ризик успішних хакерських атак до 80%. Організаційно-правовий контур безпеки має включати обов'язкове використання надійних паролів (12+ символів), двофакторної автентифікації, регулярне оновлення прошивок дронів та програмного забезпечення, а також підписання договорів про нерозголошення та використання шифрування даних. Для захисту критичної цифрово-технологічної інфраструктури великих підприємств доцільно впроваджувати спеціалізовані SIEM-системи виявлення загроз і орієнтуватися на міжна-

Таблиця 1

Основні організаційно-правові ризики цифрової трансформації суб'єктів аграрного бізнесу та напрями їх інтеграції у стратегічний менеджмент

Організаційно-правова загроза	Прояв у діяльності аграрного підприємства	Стратегічний механізм реагування
Кіберризики	Несанкціонований доступ до інформаційних систем, витік даних, кібератаки на цифрову інфраструктуру	Впровадження системи кібербезпеки, регулярний аудит інформаційних систем, резервне копіювання даних
Правові ризики	Часті зміни земельного, податкового, екологічного та воєнного законодавства	Постійний правовий моніторинг, комплаєнс-контроль, юридичний супровід управлінських рішень
Технологічні ризики	Збої в роботі IoT-пристроїв, цифрових платформ, безпілотних систем, програмного забезпечення	Верифікація постачальників, аудит цифрових рішень, страхування технологічних ризиків
Кадрові ризики	Недостатній рівень цифрових компетентностей персоналу, порушення правил інформаційної безпеки	Систематичне навчання персоналу, підвищення цифрової грамотності, розвиток культури кібергігієни
Логістичні та воєнні ризики	Пошкодження інфраструктури, порушення транспортних маршрутів, тимчасова окупація територій	Диверсифікація логістичних маршрутів, кризове планування, страхування ризиків, створення резервних ланцюгів постачання

Джерело: розроблено на основі [3]

родні стандарти ISO/IEC 27001, 27017, 27018.

Проведений аналіз свідчить, що організаційно-правові ризики, зумовлені цифровою трансформацією та воєнно-економічними викликами, мають комплексний характер і потребують інтегрованого управління. Їхня мінімізація неможлива шляхом реалізації окремих заходів, а потребує системного поєднання правових, організаційних, інформаційних та управлінських механізмів.

Узагальнення організаційно-правових ризиків цифрової трансформації аграрного бізнесу, наведених у табл. 1, стало основою для розроблення моделі інтеграції організаційно-правової безпеки у систему стратегічного менеджменту аграрного підприємства (рис. 3).

Запропонована модель інтеграції організаційно-правової безпеки в систему стратегічного менеджменту аграрного підприємства ґрунтується на принципі комплексного поєднання управлінських, правових, організаційних та цифрових механізмів забезпечення стійкого функціонування суб'єктів аграрного бізнесу. На відміну від традиційних підходів, у межах яких питання безпеки розглядаються як окремий напрям діяльності підприємства, запропонована модель передбачає інтеграцію безпекової складової в усі етапи стратегічного управління – від формування місії та стратегічних цілей до контролю результативності реалізації управлінських рішень.

Вихідною ланкою моделі є зовнішнє середовище функціонування аграрного підприємства, яке в сучасних умовах характеризується високим рівнем невизначеності та динамічності. До основних факторів зовнішнього впливу належать цифрова трансформація економіки, воєнно-економічні виклики, зміни національного та міжнародного законодавства, розвиток цифрових технологій, кіберзагрози, глобалізація аграрних ринків, кліматичні зміни та трансформація вимог до продовольчої безпеки. Сукупність зазначених факторів формує нові ризики для діяльності

аграрних підприємств і потребує системного перегляду підходів до забезпечення їхньої організаційно-правової безпеки.

Наступним елементом моделі є система стратегічного менеджменту підприємства, яка визначає місію, стратегічні цілі, напрями розвитку та механізми адаптації до змін у зовнішньому середовищі. Саме на цьому рівні доцільно інтегрувати організаційно-правову безпеку як одну з функціональних підсистем управління, що забезпечує врахування безпекових аспектів під час ухвалення стратегічних управлінських рішень. Такий підхід дозволяє перейти від реагування на окремі загрози до їх системного прогнозування та попередження.

Центральним елементом моделі є інтегрована система управління організаційно-правовою безпекою, що поєднує взаємопов'язані функціональні компоненти. До її складу входять правове забезпечення діяльності підприємства, комплаєнс-менеджмент, система управління ризиками, інформаційна та кібербезпека, кадрова безпека, внутрішній контроль і корпоративне управління. Їх комплексне функціонування забезпечує своєчасне виявлення потенційних загроз, оцінювання їх можливого впливу на діяльність підприємства та розроблення превентивних управлінських заходів.

Особливу роль відіграє ризик-орієнтований підхід до управління. На відміну від традиційного реагування на вже реалізовані загрози, інтеграція механізмів управління ризиками в стратегічний менеджмент дає змогу прогнозувати ймовірність виникнення організаційно-правових, технологічних, інформаційних і воєнних ризиків, визначати їх пріоритетність та формувати систему превентивних заходів. Водночас функціонування комплаєнс-системи забезпечує постійний контроль за відповідністю діяльності підприємства вимогам чинного законодавства, корпоративних стандартів та міжнародних норм у сфері цифрової

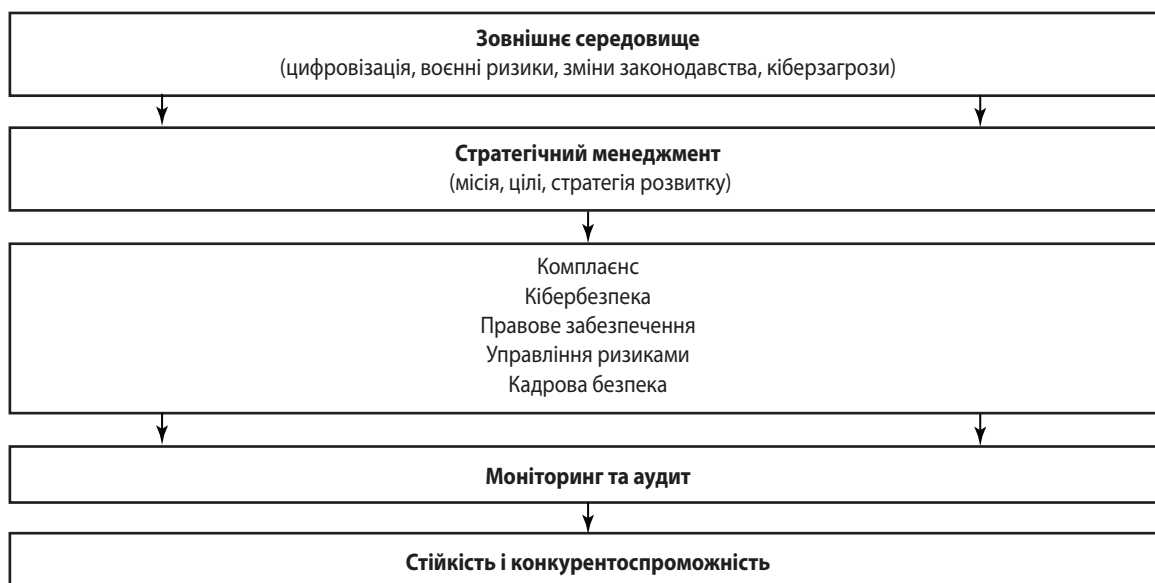


Рис. 3. Модель інтеграції організаційно-правової безпеки у систему стратегічного менеджменту аграрного підприємства

Джерело: розроблено автором

безпеки, захисту персональних даних і використання цифрових технологій.

Завершальним етапом є система моніторингу, внутрішнього аудиту та оцінювання ефективності, яка забезпечує постійний контроль за реалізацією стратегічних цілей і результативністю функціонування інтегрованої системи організаційно-правової безпеки. Отримані результати використовуються для коригування управлінських рішень, удосконалення внутрішніх процедур і своєчасної адаптації підприємства до змін у зовнішньому середовищі.

Практична реалізація запропонованої моделі сприятиме формуванню цілісної системи стратегічного управління безпекою аграрного підприємства, підвищенню рівня його організаційної стійкості, мінімізації правових і кібернетичних ризиків, забезпеченню безперервності виробничих процесів і зміцненню конкурентних позицій на внутрішньому та міжнародних аграрних ринках. Таким чином, інтеграція організаційно-правової безпеки до системи стратегічного менеджменту повинна розглядатися не як окремий напрям діяльності, а як невід'ємна складова довгострокового розвитку суб'єктів аграрного бізнесу в умовах цифрової трансформації та воєнно-економічних викликів.

Успішна адаптація суб'єктів аграрного бізнесу до сучасних умов господарювання потребує докорінної трансформації управлінських моделей, що передбачає інтеграцію організаційно-правової безпеки до системи стратегічного менеджменту. Такий процес має здійснюватися комплексно та охоплювати кілька взаємопов'язаних напрямів. Насамперед важливим є перехід до гнучкого стратегічного планування змішаного типу, яке поєднує активні заходи захисту, зокрема постійний моніторинг змін земельного, податкового та воєнного законодавства, впровадження антирейдерських механізмів і диверсифікацію логістичних та експортних маршрутів, із пасивними комплаєнс-процедурами, що передбачають неухильне дотримання вимог щодо використання повітряного простору, ліцензування програмного забезпечення та інших нормативно-правових регламентів.

Не менш важливим напрямом є впровадження інтегрованих критеріїв оцінювання організаційно-правової безпеки. Стратегічні плани розвитку підприємств мають містити не лише традиційні фінансово-економічні показники, а й систему індикаторів, що характеризують рівень організаційно-правової стійкості. До таких індикаторів доцільно віднести рівень захищеності комерційної інформації, ступінь відповідності цифрових систем вимогам міжнародних стандартів захисту персональних даних, рівень готовності інформаційної інфраструктури до кіберзагроз, а також ефективність функціонування внутрішньої системи комплаєнсу.

Важливим елементом інтегрованої системи управління є здійснення правової та технологічної верифікації постачальників цифрових послуг і технологічних рішень. Укладання договорів із постачальниками IoT-пристроїв, розробниками програмного забезпечення, провайдерами аналітичних платформ і операторами безпілотних літальних апаратів повинно супроводжуватися комплексною оцінкою рівня кібербезпеки, перевіркою відповідності

нормативним вимогам та визначенням юридичної відповідальності сторін за можливі технічні збої. Особливу увагу необхідно приділяти закріпленню в договорах механізмів відшкодування збитків у разі виникнення помилок у роботі цифрових систем, які можуть призвести до фінансових втрат підприємства.

Окремим стратегічним напрямом є кадровий та організаційний розвиток підприємства. З огляду на те, що людський фактор залишається одним із ключових джерел інформаційних ризиків, система управління персоналом повинна передбачати регулярне навчання працівників основам кібергігієни, формування навичок розпізнавання фішингових атак, дотримання правил захисту облікових даних, а також безпечної експлуатації цифрових платформ, роботизованої техніки та інших інтелектуальних систем, що використовуються у сучасному аграрному виробництві. Комплексна реалізація зазначених заходів сприятиме формуванню інтегрованої системи організаційно-правової безпеки, здатної забезпечити стійкість функціонування суб'єктів аграрного бізнесу в умовах цифрової трансформації та воєнно-економічних викликів.

Інтеграція систем управління організаційно-правовою безпекою у загальну стратегію розвитку дозволить суб'єктам українського агробізнесу не лише вистояти під впливом воєнно-економічних ударів, а й створити надійний плацдарм для майбутнього високотехнологічного відновлення на базі стандартів «Сільського господарства 4.0».

Висновки. У результаті дослідження встановлено, що ефективне функціонування аграрних підприємств у сучасних умовах неможливе без інтеграції організаційно-правової безпеки у систему стратегічного управління. Такий підхід забезпечує своєчасне виявлення та мінімізацію внутрішніх і зовнішніх загроз, підвищує адаптивність підприємств до змін нормативно-правового середовища, сприяє формуванню стійких механізмів управління ризиками та створює передумови для безперервності господарської діяльності.

За результатами аналізу сучасних тенденцій цифрової трансформації та воєнно-економічних викликів запропоновано авторський підхід до інтеграції систем управління організаційно-правовою безпекою у стратегічний менеджмент аграрних підприємств, який ґрунтується на поєднанні правового моніторингу, комплаєнс-менеджменту, ризик-орієнтованого управління, кібербезпеки, кадрового розвитку та безперервного контролю ефективності управлінських рішень. Запропонована модель забезпечує узгодження безпекових заходів зі стратегічними цілями підприємства та сприяє підвищенню його економічної стійкості, конкурентоспроможності й інвестиційної привабливості.

БІБЛІОГРАФІЯ

1. Estimated cost of cybercrime worldwide 2018–2029 // Statista. URL: <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide/>
2. Culot G., Nassimbeni G., Podrecca M., Sartor M. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*. 2021.

Vol. 33. No. 7. P. 76–105. DOI: <https://doi.org/10.1108/TQM-09-2020-0202>

3. Podrecca M., Culot G., Nassimbeni G., Sartor M. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*. 2022. Vol. 142. Article 103744. DOI: <https://doi.org/10.1016/j.compind.2022.103744>

4. Spending on digital transformation technologies and services worldwide from 2025 to 2028 // Statista. URL: <https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/>

5. Аналітичний звіт та дані інфографічного довідника «Агробізнес України» (2025/2026). Загальні втрати українського АПК від повномасштабного вторгнення сягнули майже \$84 млрд // SuperAgronom. URL: <https://superagronom.com/news/21979-zagalni-vtrati-ukrayinskogo-apk-vid-povnomasshtabnogo-vtorgnennya-syagnuli-mayje-84-mlrd>

6. Богданюк І. Виклики та чинники формування механізму управління організаційно-правовою безпекою аграрних підприємств. *Актуальні питання економічних наук*. 2024. № 5. DOI: <https://doi.org/10.5281/zenodo.14200373>

7. Богданюк І. В. Механізми управління економічною та організаційно-правовою безпекою аграрних підприємств. *Енергозбереження. Енергетика. Енергоаудит*. 2024. № 2. Р. 45–52.

8. Вівчар О. І. Управління економічною безпекою підприємств: соціогуманітарні контексти : монографія. Тернопіль : ФОП Паляниця В. А., 2018. 515 с.

9. Виклики економічного розвитку регіонів України в умовах війни та повоєнного відновлення. Науково-аналітична доповідь // Інститут регіональних досліджень ім. М. І. Долішнього НАН України. URL: <https://ird.gov.ua/irdp/e20230002.pdf>

10. Вівчар О. І. Управління економічною безпекою підприємств: соціогуманітарні контексти : монографія. Тернопіль : ФОП Паляниця В. А., 2018. 474 с.

11. ДУ «Інститут регіональних досліджень імені М. І. Долішнього НАН України». Виклики економічного розвитку регіонів України в умовах війни та післявоєнного відновлення. Науково-аналітична доповідь. URL: <https://ird.gov.ua/irdp/e20230002.pdf>

12. Зачосова Н. В., Коваль О. В., Сафонов Д. В. Активні та пасивні стратегії управління економічною безпекою суб'єктів господарювання в умовах традиційних та інноваційних загроз. *Економіка, управління та адміністрування*. 2023. № 1 (103). С. 43–48. DOI: [https://doi.org/10.26642/ema-2023-1\(103\)-43-48](https://doi.org/10.26642/ema-2023-1(103)-43-48)

13. Екологічні втрати Харківської області внаслідок агресії росії перевищили 500 мільярдів гривень // 25tv. URL: <https://25tv.com.ua/content/ekologichni-zbitki-harkivschi-cherez-agresiyu-rf-perevischili-piv-trilyona-griven/>

14. Загальні втрати українського АПК від повномасштабного вторгнення сягнули майже \$84 млрд // SuperAgronom. URL: <https://superagronom.com/news/21979-zagalni-vtrati-ukrayinskogo-apk-vid-povnomasshtabnogo-vtorgnennya-syagnuli-mayje-84-mlrd>

15. Карбівський В. Фінансова безпека аграрних підприємств в умовах цифровізації економіки. *Сталій розвиток економіки*. 2025. № 2 (53). С. 318–323. DOI: <https://doi.org/10.32782/2308-1988/2025-53-44>

16. Ключко Т. Фінансова безпека як умова фінансової стійкості підприємства. *Економіка та суспільство*. 2021. № 23. DOI: <https://doi.org/10.32782/2524-0072/2021-23-17>

17. Мельник Б. Економічні переваги цифрової трансформації аграрного сектору: аналіз інструментів і практик. *Економіка та суспільство*. 2025. № 78. DOI: <https://doi.org/10.32782/2524-0072/2025-78-99>

18. На Харківщині за 2025 рік розміновано понад 6 тисяч гектарів земель аграрного призначення // SuperAgronom. URL: <https://superagronom.com/news/21867-na-harkivschi-na-2025-rik-rozminovano-ponad-6-tisyach-gektariv-zemel-agrarnogo-priznachennya>

19. На Харківщині зруйновано понад 500 агропідприємств – ОВА // Куркуль. URL: <https://kurkul.com/news/41064-na-harkivschi-zruynovano-ponad-500-agropidpriyemstv--ova>

Додаткові матеріали: Не передбачені.

Джерела фінансування: Дослідження не отримувало зовнішнього фінансування.

Вдячності: Не передбачені.

Конфлікт інтересів: Автори заявляють про відсутність конфлікту інтересів.

Використання ШІ: Генеративні інструменти штучного інтелекту не використовувалися для генерації чи суттєвого редагування наукового змісту статті.

Supplementary Materials: Not applicable.

Funding: This research received no external funding.

Acknowledgments: Not applicable.

Conflict of Interest: The authors declare no conflict of interest.

Use of Artificial Intelligence: No generative AI tools were used to generate or substantively edit the scholarly content of this article.

REFERENCES

25tv. Ekologichni vtraty Kharkivskoi oblasti vnaslidok ahresii rosii perevyschly 500 miliardiv hryven [Environmental losses of Kharkiv region as a result of russian aggression exceeded 500 billion hryvnias]. <https://25tv.com.ua/content/ekologichni-zbitki-harkivschi-cherez-agresiyu-rf-perevischili-piv-trilyona-griven/>

Bohdaniuk I. V. (2024). Mekhanizmy upravlinnia ekonomichnoiu ta orhanizatsiino pravovoiu bezpekoiu ahrarnykh pidpriyemstv [Mechanisms of managing economic, organizational and legal security of agricultural enterprises]. *Enerhozbezrehennia. Enerhetyka. Enerhoaudyt*, 2, 45–52.

Bohdaniuk I. (2024). Vyklyky ta chynnyky formuvannia mekhanizmu upravlinnia orhanizatsiino pravovoiu bezpekoiu ahrarnykh pidpriyemstv [Challenges and factors in the formation of the management mechanism of organizational and legal security of agricultural enterprises]. *Aktualni pytannia ekonomichnykh nauk*, 5. <https://doi.org/10.5281/zenodo.14200373>

Culot G., Nassimbeni G., Podrecca M. & Sartor M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 7(33), 76–105. <https://doi.org/10.1108/TQM-09-2020-0202>

DU «Інститут регіональних досліджень імені М. І. Долішнього НАН України». (2023). Vyklyky ekonomichnoho rozvytku rehioniv Ukrainy v umovakh viiny ta pislavoiennoho vidnovlennia. Naukovo analitychna dopovid [Challenges of economic development of Ukrainian regions under conditions of war and post-war recovery. Scientific and analytical report]. <https://ird.gov.ua/irdp/e20230002.pdf>

Інститут регіональних досліджень ім. М. І. Долішнього НАН України. (2023). Vyklyky ekonomichnoho rozvytku rehioniv Ukrainy v umovakh viiny ta povoiennoho vidnovlennia. Naukovo analitychna dopovid [Challenges of economic development of Ukrainian regions under conditions of war and post-war recovery. Scientific and analytical report]. <https://ird.gov.ua/irdp/e20230002.pdf>

Karbyvskiy V. (2025). Finansova bezpeka ahrarnykh pidpriyemstv v umovakh tsyfrovizatsii ekonomiky [Financial security of

agricultural enterprises under conditions of digitalization of the economy]. *Stalyi rozvytok ekonomiky*, 2 (53), 318–323. <https://doi.org/10.32782/2308-1988/2025-53-44>

Klochko T. (2021). Finansova bezpeka yak umova finansovoi stiiosti pidpriemstva [Financial security as a condition of financial stability of the enterprise]. *Ekonomika ta suspilstvo*, 23. <https://doi.org/10.32782/2524-0072/2021-23-17>

Kurkul. Na Kharkivshchyni zruinovano ponad 500 ahropidpriemstv – OVA [In Kharkiv region, over 500 agricultural enterprises were destroyed – RMA]. <https://kurkul.com/news/41064-na-harkivschini-zruinovano-ponad-500-agropidpriemstv--ova>

Melnyk B. (2025). Ekonomichni perevahy tsyfrovoy transformatsii aharnoho sektoru: analiz instrumentiv i praktyk [Economic advantages of digital transformation of the agricultural sector: analysis of tools and practices]. *Ekonomika ta suspilstvo*, 78. <https://doi.org/10.32782/2524-0072/2025-78-99>

Podrecca M., Culot G., Nassimbeni G. & Sartor M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142, 103744. <https://doi.org/10.1016/j.compind.2022.103744>

Statista. Estimated cost of cybercrime worldwide 2018–2029. <https://www.statista.com/forecasts/1280009/cost-cyber-crime-worldwide/>

Statista. Spending on digital transformation technologies and services worldwide from 2025 to 2028. <https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/>

SuperAgronom. Analitichnyi zvit ta dani infografichnoho dovidnyka «Ahrobiznes Ukrainy» (2025/2026). Zahalni vtraty ukrainskoho APK vid povnomasshtabnoho vtornhennia siahnuly maizhe \$84 mlrd [Analytical report and data of the infographic handbook «Agribusiness of Ukraine» (2025/2026). Total losses of the Ukrainian agro-industrial complex from the full-scale invasion reached almost \$84 billion]. <https://superagronom.com/news/21979-zagalni-vtraty-ukrayinskogo-apk-vid-povnomasshtabnogo-vtornhennia-siahnuly-maizhe-84-mlrd>

zagalni-vtraty-ukrayinskogo-apk-vid-povnomasshtabnogo-vtornhennia-syagnuli-mayje-84-mlrd

SuperAgronom. (2025). Na Kharkivshchyni za 2025 rik rozminovano ponad 6 tysiach hektariv zemel aharnoho pryznachennia [In Kharkiv region, over 6 thousand hectares of agricultural land were demined in 2025]. <https://superagronom.com/news/21867-na-harkivschini-za-2025-rik-rozminovano-ponad-6-tisyach-gektariv-zemel-agrarnogo-pryznachennia>

SuperAgronom. Zahalni vtraty ukrainskoho APK vid povnomasshtabnoho vtornhennia siahnuly maizhe \$84 mlrd [Total losses of the Ukrainian agro-industrial complex from the full-scale invasion reached almost \$84 billion]. <https://superagronom.com/news/21979-zagalni-vtraty-ukrayinskogo-apk-vid-povnomasshtabnogo-vtornhennia-syagnuli-mayje-84-mlrd>

Vivchar O. I. (2018). *Upravlinnia ekonomichnoiu bezpekoiu pidpriemstv: sotsiohumanitarni konteksty* [Management of economic security of enterprises: socio-humanitarian contexts]. Ternopil: FOP Palianytsia V. A.

Vivchar O. I. (2018). *Upravlinnia ekonomichnoiu bezpekoiu pidpriemstv: sotsiohumanitarni konteksty* [Management of economic security of enterprises: socio-humanitarian contexts]. Ternopil: FOP Palianytsia V. A.

Zachosova N. V., Koval O. V. & Safonov D. V. (2023). Aktyvni ta pasyvni stratehii upravlinnia ekonomichnoiu bezpekoiu subiektyv hospodariuvannia v umovakh tradytsiinykh ta innovatsiinykh zahroz [Active and passive strategies for managing the economic security of business entities in conditions of traditional and innovative threats]. *Ekonomika, upravlinnia ta administruvannia*, 1 (103), 43–48. [https://doi.org/10.26642/ema-2023-1\(103\)-43-48](https://doi.org/10.26642/ema-2023-1(103)-43-48)

Стаття надійшла до редакції 28.05.2026 р.

Статтю прийнято до публікації 16.06.2026 р.

Оприлюднено 11.08.2026 р.