УДК: 005.934:005.6:005.334:347.1 **doi: 10.20998/2313-8890.2026.01.09**

Береза Валерій Володимирович, докторант Інституту тваринництва НААН України, доктор філософії (PhD), +38(066)703-25-52, bereza.vv@meta.ua, ORCID ID: 0009-0006-6698-2889
Інститут тваринництва Національної академії аграрних наук України
вул. Тваринників, 1-А, м. Харків, Харківська область, 61026 (Кулиничі)

ЧИННИКИ ВПЛИВУ НА ІНТЕГРАЦІЮ МЕХАНІЗМІВ ТА СИСТЕМ УПРАВЛІННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОЮ БЕЗПЕКОЮ

Анотація. *У статті представлено комплексний аналіз чинників, що визначають успішність інтеграції систем управління організаційно-правовою безпекою в загальну структуру корпоративного менеджменту. В умовах глобальних економічних викликів, стрімкої цифровізації та зростаючої геополітичної турбулентності розрізнені заходи захисту більше не здатні ефективно протистояти комплексним загрозам сучасності. Дослідження ідентифікує та класифікує ключові детермінанти інтеграції за п'ятьма основними категоріями: правові, стратегічні, організаційні, людські та технологічні.*

Досліджено глибокий вплив міжнародних регуляторних інструментів, таких як Директива NIS2, GDPR та Регламент про цифрову оперативну стійкість (DORA), підкреслюючи їхню роль у трансформації безпеки з допоміжної реактивної функції у проактивний стратегічний пріоритет. Значну увагу приділено стратегічній ролі вищого керівництва та системному застосуванню циклу PDCA (Plan-Do-Check-Act) для гармонізації цілей безпеки із загальними завданнями розвитку бізнесу. Проаналізовано шляхи подолання «організаційних силосів» через впровадження інтегрованих систем менеджменту (ІСМ) на базі стандартів ISO 9001 та ISO/IEC 27001, наголошуючи на синергії між управлінням документацією (RIM) та кібербезпекою.

Технологічний вимір інтеграції проаналізовано крізь призму впровадження GRC-платформ, систем управління ідентифікацією (IAM), хмарних рішень та штучного інтелекту, які в сукупності підвищують організаційну стійкість та швидкість реагування на інциденти. Крім того, у статті наведено детальне економічне обґрунтування інтегрованого підходу, окреслено конкретні механізми економії витрат у сфері людських ресурсів, уніфікації документації та процесів сертифікації. Результати дослідження свідчать, що цілісна інтеграція доменів безпеки забезпечує точнішу пріоритезацію ризиків та суттєве зниження операційних витрат. Зроблено висновок, що інтегрована організаційно-правова безпека є критично важливим стратегічним активом, який гарантує довгострокову життєздатність, довіру зацікавлених сторін та сталий розвиток сучасних підприємств у високоневизначеному глобальному середовищі.

Ключові слова: *організаційно-правова безпека, інтегрована система управління (ІСМ), стратегічний менеджмент, цикл PDCA, регуляторний комплаєнс, організаційна стійкість, економічна ефективність.*

Bereza Valerii, Doctoral Student, Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine, +38(066)703-25-52, bereza.vv@meta.ua, ORCID ID: 0009-0006-6698-2889
Livestock Farming Institute of National Academy of Agrarian Sciences of Ukraine
1-A Tvarynnykyv Street, Kharkiv, Kharkiv region, 61026 (Kulynichi)

FACTORS INFLUENCING THE INTEGRATION OF ORGANIZATIONAL AND LEGAL SECURITY MANAGEMENT MECHANISMS AND SYSTEMS

Abstract. *The article provides a comprehensive analysis of the factors determining the successful integration of organizational and legal security management systems within the modern corporate governance framework. Amidst the landscape of global economic challenges, rapid digitalization, and growing geopolitical turbulence, fragmented security measures are no longer sufficient to counter complex modern threats. The research identifies and classifies key integration drivers into five primary categories: legal, strategic, organizational, human, and technological.*

The study examines the profound influence of international regulatory instruments, such as the NIS2 Directive, GDPR, and the Digital Operational Resilience Act (DORA), highlighting their role in shifting security from a reactive auxiliary function to a proactive strategic priority. A significant focus is placed on the strategic role of top management and the systematic application of the PDCA (Plan-Do-Check-Act) cycle to harmonize security objectives with overall business development goals. The elimination of "organizational silos" through the implementation of Integrated Management Systems (IMS) based on ISO 9001 and ISO/IEC 27001 standards is researched, emphasizing the synergy between Records and Information Management (RIM) and cybersecurity.

The technological dimension of integration is further analyzed through the adoption of GRC platforms, identity and access management (IAM), cloud solutions, and Artificial Intelligence, which collectively enhance organizational resilience and rapid incident response. Furthermore, the article provides a detailed economic justification for the integrated approach, outlining specific cost-saving mechanisms in human resources, unified documentation systems, and certification processes. The findings suggest that a holistic integration of security domains leads to more accurate risk prioritization and a significant reduction in operational overhead. It is concluded that integrated organizational and legal security is a critical strategic asset that ensures long-term sustainability, stakeholder trust, and sustainable development of modern enterprises in a highly uncertain global environment.

Keywords: *organizational and legal security, Integrated Management System, strategic management, PDCA cycle (Цикл PDCA), regulatory compliance, risk-oriented approach, economic efficiency.*

Постановка проблеми. У сучасному ландшафті глобальних економічних викликів, стрімкої цифровізації та зростаючої геополітичної турбулентності питання гарантування безпеки організацій трансформується з допоміжної функції в стратегічний пріоритет. Організаційно-правова безпека як синтетична категорія охоплює сукупність правових норм, управлінських рішень та організаційних структур, спрямованих на захист життєво важливих інтересів суб’єкта господарювання від внутрішніх і зовнішніх загроз. Процес інтеграції механізмів управління цією безпекою в загальну систему менеджменту стає критичним фактором виживання та розвитку, оскільки розрізнені заходи захисту більше не здатні протистояти комплексним ризикам сучасності.

Актуальність інтеграції зумовлена необхідністю створення єдиного інформаційно-управлінського простору, де правові інструменти захисту (договірна робота, комплаєнс, претензійно-позовна діяльність) поєднуються з організаційними заходами (управління персоналом, фізична безпека, захист активів). Така синергія дозволяє не лише мінімізувати втрати, а й оптимізувати використання ресурсів, що є надзвичайно важливим в умовах обмежених бюджетів та високої ризикованості підприємницької діяльності, особливо в контексті глобальних криз та воєнних станів.

Аналіз останніх досліджень і публікацій. Проблема формування інтегрованих систем управління безпекою останнім часом привертає все більше уваги наукової спільноти. Вагомий внесок у розробку теоретико-методологічних засад економічної та організаційної безпеки зробили українські та закордонні вчені, чиї праці заклали фундамент для розуміння безпеки як багаторівневої системи.

Дослідження Вівчар О. І. зосереджені на формуванні стратегій забезпечення економічної безпеки торговельних підприємств. Особливої уваги заслуговує запропонований дослідницею алгоритм імплементації соціогуманітарної стратегії забезпечення економічної безпеки підприємств в контексті протидії економічній злочинності, а також вдосконалення системного підходу до забезпечення економічної безпеки підприємств, що сприятиме створенню передумов ефективної роботи підприємницьких структур [1].

Чайкіна А. О. детально аналізує особливості інтеграції ризик-менеджменту в систему управління підприємством в умовах пандемії COVID-19 та воєнного стану в Україні. Вона доводить, що побудова ефективної системи протидії загрозам вимагає від менеджменту критичного та креативного мислення для створення альтернативних сценаріїв адаптації до динамічного середовища [2].

У сфері інформаційної безпеки фундаментальними є праці von Solms та von Solms, які одними з перших обґрунтували, що управління безпекою інформації є не технічним, а управлінським завданням (governance issue) [3]. Розвиваючи цю думку,

Knapp K. J. et al. [4] ідентифікували десять критичних факторів успіху, серед яких найважливішими є підтримка вищого керівництва та культура безпеки. Ahmad A. et al. [5] запропонували комплексні вимоги до ефективності СУІБ, включаючи аудит, навчання та відповідність регуляторним нормам.

Сучасні дослідження Marhad S. et al. [6], а також Hassan Y. et al. [7] розглядають інтеграцію систем управління інформаційною безпекою (СУІБ) через призму стратегічного менеджменту, підкреслюючи, що безпека має стати частиною екосистеми організації. Важливим є також внесок фахівців у галузі стандартизації, які розробили методики об'єднання стандартів ISO 9001 (якість) та ISO 27001 (безпека) у єдину інтегровану систему менеджменту (ІСМ) на основі структури високого рівня (HLS) [8].

Метою статті є комплексний науковий аналіз чинників, що визначають успішність інтеграції механізмів та систем управління організаційно-правовою безпекою. Дослідження спрямоване на виявлення причинно-наслідкових зв'язків між внутрішніми управлінськими процесами та зовнішніми регуляторними вимогами, а також на обґрунтування концептуальної моделі інтеграції, яка б забезпечувала стійкість організації до сучасних викликів.

Виклад основного матеріалу. Інтеграція механізмів управління організаційно-правовою безпекою не є одноразовим актом, а являє собою тривалий процес гармонізації різних функціональних сфер діяльності підприємства. Цей процес детермінується сукупністю чинників, які можна класифікувати за їхньою природою на правові, стратегічні, організаційні, людські та технологічні.

Основним зовнішнім стимулом для інтеграції виступає еволюція нормативно-правового поля. Сучасні міжнародні та національні вимоги стають дедалі складнішими, вимагаючи від організацій не просто формального дотримання законів, а побудови цілісних систем комплаєнсу. У Європейському Союзі ключовими регуляторами інтеграції стали Директива NIS2, GDPR та Акт про цифрову оперативну стійкість (DORA) [9]. Зазначені правові акти та їх вимоги щодо

інтеграції відображені у табл. 1.

Директива NIS2 суттєво розширює коло суб'єктів, для яких впровадження систем управління безпекою є обов'язковим, і встановлює жорсткі вимоги до ланцюгів постачання. Це змушує організації інтегрувати правову безпеку (аналіз контрактів, перевірка контрагентів) з технічними заходами кіберзахисту [10]. Правова підтримка в аграрному секторі, наприклад, фокусується на земельному законодавстві та контролі за дотриманням договорів з партнерами, що є невід'ємною частиною загальної економічної стійкості [11].

Таблиця 1 – Ключові вимоги нормативно-правових актів щодо інтеграції систем управління безпекою

Регуляторний інструмент	**Основна вимога щодо інтеграції**	**Вплив на організацію**
NIS2 Directive	Ризик-орієнтований підхід, звітність	Посилення відповідальності керівництва, інтеграція СУІБ
GDPR (Art. 15, 32)	Захист даних за замовчуванням	Злиття процесів IT-безпеки та юридичного комплаєнсу
DORA (EU)	Тестування стійкості систем	Створення єдиного механізму цифрової стійкості у фінансах
ISO/IEC 27001:2022	Управління активами та ризиками	Гармонізація технічних та організаційних контролів

Джерело: розроблено автором за [9; 10].

Юридична відповідність стає не лише інструментом захисту від штрафів, а й чинником підвищення ринкової вартості та довіри партнерів. Інтеграція правових механізмів у загальну систему управління дозволяє перетворити юридичний супровід з реактивного (гасіння пожеж) на проактивний інструмент запобігання конфліктам [11].

Інтеграція механізмів безпеки неможлива без активної підтримки вищого керівництва. Це підтверджується численними дослідженнями, які ставлять *executive support* на перше місце серед факторів успіху СУІБ. Керівництво повинно сприймати безпеку не як витратну статтю, а як інвестицію в безперервність бізнесу та конкурентну перевагу [6].

Важливим механізмом тут є цикл PDCA (Plan-Do-Check-Act), який забезпечує динамічність системи безпеки. На етапі *Plan* стратегічні цілі організації інтегруються з політиками безпеки. На етапі *Do* відбувається впровадження контролів. Етап *Check* передбачає моніторинг KPI та аудити, а *Act* – безперервне вдосконалення на основі отриманих даних [6]. Етапи циклу PDCA з огляду на інтеграцію та роль стратегічного менеджменту наведені у табл. 2.

Таблиця 2 – Реалізація циклу PDCA в системі стратегічного менеджменту організації

Етап циклу PDCA	**Діяльність з інтеграції**	**Роль стратегічного менеджменту**
Plan (Планування)	Визначення контексту, оцінка ризиків	Узгодження бюджетів та пріоритетів
Do (Впровадження)	Реалізація політик, навчання	Виділення ресурсів та повноважень
Check (Перевірка)	Внутрішні аудити, аналіз KPI	Оцінка ефективності інвестицій у безпеку
Act (Дія)	Коригувальні дії, інновації	Корекція стратегії розвитку організації

Джерело: розроблено автором за [6].

Отже, стратегічна інтеграція корпоративного управління (Strategic Integration Corporate Governance) забезпечує те, що безпека стає частиною бізнес-процесів, а не зовнішнім надбудовою. Це дозволяє організації бути адаптивною до змін ринку та технологічних інновацій, зберігаючи при цьому стійкість до загроз.

Однією з найбільших перешкод на шляху до інтеграції є «організаційні силоси» – ізольованість департаментів. Юристи, IT-фахівці, ризик-менеджери та HR-відділи часто працюють окремо, що створює зони безвідповідальності та дублювання функцій. Інтегрована система управління (ICM) на базі ISO 9001 та ISO 27001 дозволяє уніфікувати такі процеси, як управління документацією, внутрішні аудити та розгляд невідповідностей. [6].

Синергія між управлінням записами (Records and Information Management – RIM) та інформаційною безпекою є яскравим прикладом організаційної інтеграції. RIM забезпечує знання про те, де знаходяться дані та скільки їх є, що дозволяє

безпеці ефективніше захищати критичні активи. Зменшення обсягів непотрібної інформації автоматично знижує ризики її витоку [12].

Для успішної побудови інтегрованої моделі необхідно враховувати специфіку галузі. Наприклад, в аграрному бізнесі організаційна структура безпеки повинна адаптуватися до сезонності та залежності від природно-кліматичних умов. В IT-секторі акцент робиться на безперервності сервісів та захисті інтелектуальної власності.

Людський фактор залишається найбільш непередбачуваним чинником впливу. Співробітники можуть бути як джерелом внутрішніх загроз, так і головним активом у виявленні атак [13]. Тому інтеграція систем управління повинна включати психолого-педагогічні механізми формування культури безпеки.

Культура безпеки базується на трьох стовпах:

1. Обізнаність (Awareness): Розуміння персоналом важливості захисту активів та знання процедур реагування на інциденти.
2. Поведінкові наміри (Behavioral Intentions): Готовність дотримуватися правил навіть за відсутності прямого контролю. Це стимулюється як позитивними прикладами керівництва, так і системою санкцій.
3. Навчання та підготовка (Training): Безперервне підвищення кваліфікації у сфері економічної, правової та екологічної безпеки [13].

Інтеграція культури безпеки в загальну корпоративну культуру дозволяє знизити опір змінам під час впровадження нових технологій захисту. Коли працівники розуміють *навіщо* потрібна безпека, вони стають активними учасниками процесу вдосконалення систем управління [6].

Цифрова трансформація вимагає використання сучасних інструментів для інтеграції механізмів безпеки. Автоматизація дозволяє в реальному часі відстежувати стан захищеності, проводити оцінку ризиків та керувати доступом до активів (ACM). Використання великих даних (Big Data) стає ефективним інструментом підтримки прийняття рішень у складних та невизначених умовах,

допомагаючи долати неефективність застарілих правових норм. У таблиці 3 представлено аналіз технологічних рішень та їх переваг з огляду на безпеку.

Проте надмірна залежність від технологій також створює вразливості, особливо через використання готового комерційного програмного забезпечення (COTS), над яким організація має обмежений контроль [14]. Це підкреслює потребу в інтеграції технологічних заходів з правовими механізмами аудиту постачальників та контрактного захисту.

Таблиця 3 – Технологічні рішення та їх переваги для інтеграції процесів безпеки

Технологічний напрям	**Роль в інтеграції**	**Переваги для безпеки**
GRC-платформи	Об’єднання управління, ризиків та комплаєнсу	Єдина база даних інцидентів та контролів
Ідентифікація (IAM)	Централізоване управління доступом	Зниження ризиків несанкціонованого доступу
Хмарні технології	Забезпечення доступності та резервування	Підвищення стійкості до катастрофічних подій
Штучний інтелект	Прогнозна аналітика та виявлення аномалій	Швидка реакція на нові вектори загроз

Джерело: розроблено автором за [13].

Інтеграція систем управління є економічно вигідною стратегією. Створення інтегрованої системи менеджменту (ICM) дозволяє усунути дублювання ресурсів на підтримку окремих систем якості, безпеки та екології [15]. Оптимізація використання ресурсів (землі, води, техніки, людської праці) є основою економічної безпеки, особливо в агросекторі. У табл. 4 представлено аналіз статей економії ресурсів при впровадженні інтегрованого підходу до безпеки.

Інтеграція ризик-менеджменту в систему управління підприємством, як зазначає Чайкіна А. О., допомагає адаптуватися до змін внутрішнього та зовнішнього середовища, забезпечуючи сталий розвиток [2]. Незважаючи на очевидні переваги, процес інтеграції стикається з низкою викликів. Початкова складність об'єднання різних систем та потреба в значних короткострокових

ресурсах можуть зупиняти керівництво. Різниця в культурах департаментів якості та безпеки, розбіжності в методологіях оцінки ризиків та опір персоналу змінам – це типові перешкоди, які потребують виваженого управління змінами.

Таблиця 4 – Вплив інтеграції процесів на зниження операційних та фінансових витрат організації

Стаття економії при інтеграції	**Опис механізму**	**Ефект для підприємства**
Людські ресурси	Спільні команди для аудитів та комплаєнсу	Зниження витрат на персонал управління
Документація	Єдина політика та процедури для всіх стандартів	Спрощення адміністрування та доступу
Сертифікація	Комбіновані аудити від органів сертифікації	Пряме зменшення фінансових витрат на аудит
Управління ризиками	Єдиний реєстр ризиків для різних доменів	Більш точна пріоритезація витрат на захист

Джерело: розроблено автором за [15].

Важливо уникати *надмірної інтеграції* (over-integration), коли специфічні вимоги окремих стандартів втрачаються в загальних процедурах, що може призвести до невідповідності під час зовнішніх аудитів. Баланс між уніфікацією та збереженням спеціалізованих контролів є ключем до створення працездатної системи організаційно-правової безпеки.

Висновки. Інтеграція механізмів та систем управління організаційно-правовою безпекою є складним, багатовекторним процесом, успішність якого визначається синергією внутрішніх зусиль організації та її здатністю адаптуватися до зовнішніх регуляторних вимог. Проведене дослідження дозволяє зробити наступні висновки:

По-перше, домінуючим зовнішнім чинником є посилення правової регламентації у сфері безпеки (зокрема, стандарти ISO 27001, 45001 та директиви ЄС), що перетворює інтегроване управління з бажаної практики на юридичну необхідність. Правова безпека стає фундаментом, на якому будуються технічні та організаційні заходи захисту.

По-друге, стратегічна роль вищого керівництва та впровадження циклу PDCA є вирішальними для трансформації безпеки з реактивного механізму у проактивну стратегічну функцію. Без лідерської підтримки інтеграція залишається фрагментарною та малоефективною.

По-третє, формування культури безпеки та подолання організаційної ізольованості департаментів дозволяють використовувати людський капітал як ефективний бар'єр проти загроз. Інтеграція має відбуватися не лише на рівні документів, а й на рівні цінностей та щоденної поведінки співробітників.

По-четверте, використання технологічних інструментів автоматизації (GRC, Big Data) забезпечує необхідну швидкість та точність управління в умовах високої невизначеності, характерної для сучасного періоду.

Економічна вигода від створення інтегрованих систем менеджменту (ICM) у вигляді оптимізації ресурсів та зниження витрат на сертифікацію є вагомим аргументом на користь інтеграції. У підсумку, інтегрована організаційно-правова безпека стає не просто системою захисту, а стратегічним активом, що забезпечує стійкість, довіру зацікавлених сторін та сталий розвиток організації в умовах постійних глобальних викликів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Вівчар О. І. Управління економічною безпекою підприємств: соціогуманітарні контексти: монографія. Тернопіль: ФОП Паляниця В. А., 2018. 474 с.
2. Чайкіна А. О. Особливості інтеграції ризик-менеджменту в систему управління аідприємством. 2022. *Економіка та суспільство*. № 39. DOI: https://doi.org/10.32782/2524-0072/2022-39-5.
3. von Solms B., von Solms R. (2004). The 10 deadly sins ofinformation security management. *Computers & Security*. Vol. 23(5). Pp. 371–376. DOI: https://doi.org/10.1016/j.cose.2004.05.002.
4. Knapp K. J., Marshall T. E., Rainer R. K., Morrow D. W. The top information security issues facing organizations: Whatcan government do to help? *Information Security and Risk Management.* 2006. September/October, pp. 51–58. DOI: https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95124.5.
5. Ahmad A., Hadgkiss J., Ruighaver, A. B. Incident response teams – Challenges in supporting the organizationalsecurity function. *Computers & Security*. 2012. Vol. 31(5). Pp. 643–652. DOI: https://doi.org/10.1016/j.cose.2012.04.001.

6. Marhad S., Goni S., Sani M. Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*. 2024. Vol. 9. Pp. 197-203. DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5483.

7. Hassan Y., Ghazal T. M., Yasir S., Al-Adwan A. S., Younes S. S., Albahar M. A., Ahmad M., Ikram A. Exploring the mediating role of information security culture in enhancing sustainable practices through integrated systems infrastructure. *Sustainability*. 2025. Vol. 17(2), 687. DOI: https://doi.org/10.3390/su17020687.

8. Strahinja Stojanovic. How to integrate ISO 9001 and ISO 27001. Advisera. 2016. URL: https://advisera.com/9001academy/blog/2016/09/27/how-to-integrate-iso-9001-and-iso-27001/.

9. EU cybersecurity policies. Shaping Europe's digital future. European Union. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

10. Joseph S. EU Compliance Regulations: Key Guidelines & Updates. Scrut.io. 2025. URL: https://www.scrut.io/post/eu-compliance-regulations.

11. Богданюк І. В., Мандич С. М. Механізми управління економічною та організаційно-правовою безпекою аграрних підприємств: теоретичні аспекти. Енергозбереження. Енергетика. Енергоаудит. 2024. № 10(201). DOI: 10.20998/2313-8890.2024.10.04.

12. Information Management and Security Integration. Zasio. URL: https://zasio.com/records-and-information-management-information-security-two-risk-mitigation-peas-in-an-information-governance-pod/.

13. Gu L., Wang J. The impact of organizational factors on security behavioral intentions. *Issues in Information Systems*. 2024. Vol. 25, Iss. 3. pp. 26-35. DOI: https://doi.org/10.48009/3_iis_2024_103.

14. Park S., Ahmad A. Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. May 2010. Conference: Information Science and Applications (ICISA), 2010 International Conference. DOI: https://doi.org/10.1109/ICISA.2010.5480261.

15. Integrated Management Systems explained: ISO 27001, ISO 22301 and beyond. Evalian. URL: https://evalian.co.uk/integrated-management-systems-explained-iso-27001-iso-22301-and-beyond/.

REFERENCES:

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

2. Chaikina A. O. (2022). Osoblyvosti intehratsii ryzyk-menedzhmentu v systemu upravlinnia pidpryiemstvom [Features of risk management integration into the enterprise management system]. *Ekonomika ta suspilstvo – Economy and Society*, 39. https://doi.org/10.32782/2524-0072/2022-39-5.

3. von Solms B., von Solms R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002.

4. Knapp K. J., Marshall T. E., Rainer R. K., Morrow D. W. (2006). The top information security issues facing organizations: What can government do to help? *Information Security and Risk Management*, September/October, 51–58. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95124.5.

5. Ahmad A., Hadgkiss J., Ruighaver A. B. (2012). Incident response teams – Challenges in supporting the organizational security function. *Computers & Security*, 31(5), 643–652. https://doi.org/10.1016/j.cose.2012.04.001.

6. Marhad Siti, Goni Siti, Sani Mad. (2024). Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. Environment-Behaviour Proceedings Journal. 9. 197–203. https://doi.org/10.21834/e-bpj.v9iSI18.5483.

7. Hassan Y., Ghazal T. M., Yasir S., Al-Adwan A. S., Younes S. S., Albahar M. A., Ahmad M., Ikram A. (2025). Exploring the mediating role of information security culture in enhancing sustainable practices through integrated systems infrastructure. *Sustainability*, 17(2), 687. https://doi.org/10.3390/su17020687.

8. Stojanovic S. (2016, September 27). *How to integrate ISO 9001 and ISO 27001*. Advisera. Retrieved from https://advisera.com/9001academy/blog/2016/09/27/ how-to-integrate-iso-9001-and-iso-27001/.

9. European Union. (n.d.). *EU cybersecurity policies. Shaping Europe's digital future*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

10. Joseph S. (2025). *EU Compliance Regulations: Key Guidelines & Updates*. Scrut.io. Retrieved from https://www.scrut.io/post/eu-compliance-regulations.

11. Bohdaniuk I. V., Mandych S. M. (2024). Mekhanizmy upravlinnia ekonomichnoiu ta orhanizatsiino-pravovoiu bezpekoiu ahrarnykh pidpryiemstv: teoretychni aspekty [Mechanisms of economic and organizational-legal security management of agricultural enterprises: theoretical aspects]. *Enerhozberezhennia. Enerhetyka. Enerhoaudyt – Energy Saving. Power Engineering. Energy Audit*, 10(201). https://doi.org/10.20998/2313-8890.2024.10.04.

12. Zasio. (n.d.). *Information Management and Security Integration*. Retrieved from https://zasio.com/records-and-information-management-information-security-two-risk-mitigation-peas-in-an-information-governance-pod/.

13. Gu L., Wang J. (2024). The impact of organizational factors on security behavioral intentions. *Issues in Information Systems*, 25(3), 26–35. https://doi.org/10.48009/3_iis_2024_103.

14. Park S., Ahmad A. (2010, May). Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. *2010 International Conference on Information Science and Applications (ICISA)*. https://doi.org/10.1109/ICISA.2010.5480261.

15. Evalian. (n.d.). *Integrated Management Systems explained: ISO 27001, ISO 22301 and beyond*. Retrieved from https://evalian.co.uk/integrated-management-systems-explained-iso-27001-iso-22301-and-beyond/.

Стаття надійшла до редакції: 02.12.2025; рецензування: 22.12.2025;
прийнята до публікації 05.01.2026. Автори прочитали и дали згоду рукопису.
The article was submitted on 02.12.2025; revised on 22.12.2025; and accepted for publication on 05.01.2026. The authors read and approved the final version of the manuscript.