DOI: https://doi.org/10.32782/2524-0072/2025-82-189

УДК 65.012.8:005.96

ФОРМУВАННЯ КАДРОВОЇ БЕЗПЕКИ ТА ОРГАНІЗАЦІЙНОЇ СТІЙКОСТІ ОРГАНІЗАЦІЇ В УМОВАХ ЦИФРОВИХ ВИКЛИКІВ

BUILDING PERSONNEL SECURITY AND ORGANIZATIONAL RESILIENCE IN THE CONTEXT OF DIGITAL CHALLENGES

Глєбова Алла Олександрівна
кандидат економічних наук, доцент кафедри менеджменту і логістики,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORSID: https://orcid.org/0000-0002-7030-948X

Гришко Володимир Васильович
доктор економічних наук, професор,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORSID: https://orcid.org/0000-0001-9183-4008

Hliebova Alla, Hryshko Volodymyr
National University «Yuri Kondratyuk Poltava Polytechnic»

Стаття присвячена комплексному дослідженню процесу формування кадрової безпеки організації у умовах цифровізації, що дозволить забезпечити організаційну стійкість. Визначено, що кадрова безпека повинна базуватися на взаємозв'язку психологічної безпеки, цифрової грамотності, технологій командної роботи та культури безпеки в умовах стрімкого розвитку інформаційно- комунікаційних технологій. Запропоновано підхід до формування політики кадрової безпеки на основі інтеграції вимог міжнародних стандартів ISO 9001:2015, ISO 45003:2021 та ISO/IEC 27001, що дозволяє поєднати управління HR-процесами, психологічну безпеку, цифрову компетентність, цифрову та інформаційну безпеку у єдину комплексну модель, яка орієнтована на забезпечення організаційної стійкості. Доведено доцільність переходу від часткових заходів кадрової безпеки до комплексної моделі формування культури безпеки, що є важливою складовою процесу формування організаційної стійкості в умовах цифровізації та дозволяє зменшити кількість репутаційних ризиків та їх наслідки на основі сучасних стандартів системи якості ISO.

Ключові слова: команда, кадрова безпека, психологічна безпека, цифрові компетентності, стійкість.

The article presents a comprehensive examination of the challenges associated with the formation of personnel security in organizations under the conditions of global transformations, including digitalization, pandemics, and wartime disruptions. It is substantiated that effective personnel security should be grounded in the systemic interrelation between psychological safety, digital literacy, collaborative work technologies, and the development of a sustainable safety culture amid the rapid evolution of information and communication technologies and ongoing digital transformation. An integrated approach to the development of a personnel security policy is proposed, based on the harmonization of the requirements of international standards ISO 9001:2015, ISO 45003:2021, and ISO/IEC 27001. Such integration enables the consolidation of HR management processes, psychological well-being, and information security into a unified, comprehensive framework aimed at strengthening organizational resilience and adaptive capacity. The proposed personnel security model is built upon a process-oriented approach, risk-based thinking, and the principles of continuous improvement (PDCA) embedded in the ISO 9000 and ISO/IEC 27000 standards. It encompasses three interconnected levels: strategic (integration of personnel security into the overall development strategy of the organization); tactical (alignment of internal procedures, regulations, and policies with digital competencies and psychological safety requirements); and operational (implementation of practical measures related to recruitment, onboarding, training, performance evaluation, access control, and monitoring of behavioral and information-related incidents). The implementation of personnel security based on international standards ensures protection against internal threats, reduces risks of human error and data breaches, prevents professional burnout, strengthens ethical behavior and trust within teams, and enhances the investment attractiveness and reputational reliability of modern organizations. The study substantiates the necessity of transitioning from fragmented personnel security measures to a holistic model for developing an integrated security culture.

Keywords: team, personnel security, psychological safety, digital competencies, resilience.

© Глєбова А. О., Гришко В. В., 2025

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій, які проникають у всі сфери життєдіяльності людини, економіки, суспільства, де основним джерелом коштів стає не продаж товарів і послуг, а увага, емоції та час споживачів (користувачів) актуалізується питання забезпечення стійкості розвитку сучасних організацій. Адже суттєво змінюється середовище сучасного бізнесу, яке стає не просто складним і мінливим, але й складнопрогнозованим і турбулентним, що має велику кількість не тільки можливостей, але і загроз та ризиків. Це, в свою чергу, впливає на систему менеджменту та технології управлінської діяльності, які повинні забезпечувати не тільки ефективне функціонування, але й стійкий організаційний розвиток у довгостроковій перспективі. Виконати таке управлінське завдання неможливо без цифрових технологій, ефективної кадрової політики, потужного кадрового потенціалу та сучасних технологій командної роботи, які дозволяють в умовах глобальних викликів (війни, пандемії, природних катаклізмів тощо) досягати поставленої мети використовуючи всі сучасні здобутки НТП та менеджменту.

Одночасно із цим зростає потреба у формуванні системної політики та культури безпеки організації, яка буде інтегрована у кадрову безпеку, оскільки за умов цифровізації саме персонал (його потенціал) виступає не лише ключовим ресурсом забезпечення конкурентоспроможності та стійкості, а й потенційним джерелом вразливостей, пов'язаних із витоками інформації, внутрішніми загрозами, помилками персоналу, цифровою некомпетентністю та професійним вигоранням. Це обумовлює об'єктивну необхідність пошуку шляхів формування моделі кадрової безпеки, здатної забезпечити адаптивність, надійність і безперервність функціонування організацій в умовах цифрових трансформацій й зростання багаторівневих ризиків.

Аналіз останніх досліджень і публікацій. У сучасних наукових працях та аналітичних звітах [1-4] цифровізація розглядається як ключовий фактор забезпечення стійкості та конкурентоспроможності не тільки організацій, але й економіки загалом. Організації, бізнеси, міста, країни стають цифровими. Українські науковці (Касич А.О. [5], Коптєва Г.В. [6], Швед В.В. [7] та інші) підкреслюють роль і значення кадрової безпеки в умовах цифровізації. Водночас цифрова трансформація суттєво ускладнює середовище функціонування організацій, формуючи нові ризики, пов'язані з людським фактором, інформаційною вразливістю та психологічною нестійкістю персоналу. У наукових дослідженнях дедалі частіше підкреслюється, що кадрова безпека в умовах цифрових викликів виходить за межі традиційного управління персоналом і трансформується у комплексну управлінську категорію, що інтегрує HR-менеджмент, інформаційну безпеку, психологічну безпеку та управління ризиками [8].

У працях Шведа Н.М. [9], Горбунової В.В. [10] та інших розглядається командна робота у контексті сучасних технологій організації роботи організацій в умовах глобальних викликів (пандемії, війни, цифровізації). Автори підкреслюють, що ефективність командної діяльності дедалі більше залежить від рівня цифрових компетентностей, розвитку емоційного інтелекту, довіри, відповідальності та психологічної безпеки працівників, що безпосередньо впливає на стабільність функціонування організації.

Виділення невирішених раніше частин загальної проблеми. Невирішеними залишаються питання методологічного обґрунтування зв'язку між кадровою безпекою організації, психологічною безпекою, цифровою та інформаційною безпекою, цифровою компетентністю, технологіями командної роботи в умовах стрімкого розвитку інформаційно-комунікаційних технологій та цифровізації.

Формулювання цілей статті (постановка завдання). Метою дослідження є обґрунтування та розробка практично орієнтованих рекомендацій щодо формування кадрової безпеки організації на основі інтеграції вимог міжнародних стандартів систем менеджменту ISO, зокрема ISO 9001:2015 (система управління якістю), ISO 45003:2021 (управління психосоціальними ризиками), ISO/IEC 27001 (інформаційна безпека) в умовах цифровізації.

Виклад основного матеріалу дослідження. В умовах глобальних викликів набуває важливого значення забезпечення кадрової безпеки, яка повинна не тільки забезпечувати захист організації від ризиків і загроз, пов'язаних із персоналом, але й сприяти розвитку трудових та етичних відносин між адміністрацією та персоналом, зі зовнішніми та внутрішніми стейкхолдерами, формувати сприятливе соціально-психологічне середовище, підтримувати довіру та відповідальну поведінку працівників, запобігати виникненню внутрішніх конфліктів, професійному виго-

ранню й деструктивним формам опортуністичної поведінки, а також створювати передумови для стійкого розвитку організації в умовах цифровізації та зростання невизначеності зовнішнього середовища. Однак, сучасний розвиток організації складно розглядати без використання технологій командної роботи, які є інтегрованими у сучасні інформаційні CRM, що є основою побудови комунікацій в організаціях й дозволяють на основі гібридних форматів зайнятості вирішувати не тільки питання безпеки, особливо в умовах глобальних викликів (цифровізації, пандемії, війни, природних катаклізмів тощо), але й досягати амбітних цілей за рахунок підвищення рівня гнучкості та адаптивності організації до динамічних змін зовнішнього середовища.

За таких умов командні технології перетворюються не лише на інструмент координації індивідуальної праці, а й на ключовий елемент системи організаційної стійкості, здатної забезпечувати безперервність бізнес-процесів і підтримку стабільність управлінських рішень [11]. Водночас, актуалізуються питання інформаційного перенавантаження, цифрових компетенцій, навичок кібергігієни, психологічного клімату, рівня довіри між членами команди, здатності до конструктивної комунікації та управління конфліктами, а також дотримання норм інформаційної й цифрової безпеки, етичної поведінки у цифровому середовищі. Все це є важливими компонентами культури безпеки, яка відіграє ключову роль у організаційній стійкості.

За відсутності системного підходу до розвитку зазначених складових у цифровій економіці в умовах зростання інформаційних та цифрових загроз зростає ймовірність виникнення помилок у прийнятті управлінських рішень, витоків конфіденційної інформації, втрати даних, репутаційних ризиків, зниження продуктивності праці та посилення соціально-психологічної напруги в колективі, що призводить не тільки до зниження прибутковості та рентабельності бізнесу, але й банкрутства.

У зв’язку з цим, доцільно запропонувати розглядати кадрову безпеку не лише як сукупність заходів контролю та запобігання внутрішнім загрозам, а як комплексну управлінську модель, яка ґрунтується на основі розвитку людського капіталу та цифрової грамотності персоналу, підтримці психологічної безпеки та забезпеченні відповідності поведінкових практик працівників стратегічним цілям організації. Такий підхід обумовлений тим, що сучасний бізнес зазнає найбільших збитків саме від репутаційних ризиків, які виникають у процесі використання цифрових комунікацій у професійній діяльності. Так, за останні роки (2018- 2025 рік) частка організацій у світі, які постраждали від атак програм- вимагачів має тенденцію до зростання (рис. 1).

Основним сектором у світі, який найбільш постраждав у 2025 році є виробництво, потім сфера медицини і третє місце державні установи та організації [13]. Саме даний вид загроз актуалізує питання навичок кібергігієни та цифрової грамотності. Адже, у результаті цих дій втрачаються не тільки кошти і дані, але руйнується довіра у клієнтів, постачальників, працівників тощо. Знижується довіра між всіма стейкхолдерами, що призводить до зниження інвестиційної привабливості організацій, галузей, економік тошо. Згідно аналізу кібератак у 2025 році середня вартість витоку даних у 2025 році знизилася до ~4,44 мільйона доларів, що приблизно на 9% менше, ніж у 2024 році. Однак у США витрати різко зросли до 10,22 мільйона доларів за інцидент, оскільки зловмисники зосереджуються на великих цілях. Вартість одного викраденого запису також зросла в середньому приблизно до 169 доларів, що відображає зростання цінності персональних даних [14]. Людська помилка та соціальна інженерія продовжують бути основними причинами порушень, що призводять до зростання репутаційних та фінансових ризиків. Фішинг є найпоширенішим методом соціальної інженерії, що приблизно становить 15–20% від загальних порушень та коштує організаціям в середньому ~4,9 млн доларів США за інцидент.

Понад 57% організацій стикаються зі спробами фішингу щотижня або щодня, що свідчить про високий потенціал методів соціальної інженерії. Зловмисники також дедалі частіше використовують викрадені облікові дані, невиправлені вразливості програмного забезпечення, що призводить до компрометації інформаційних ланцюгів у 2025 році вартістю у середньому вартістю 4,91 млн доларів США [13].

В Україні ці тенденції також простежуються. Так, у першому півріччі 2025 року порівняно з попереднім періодом знизилася кількість інцидентів за типом “Розповсюдження ШПЗ (Malware distribution)” – з 43% від загальної кількості до 33%, а ось інтенсивність фішингових атак збільшилась – з 19% у другому півріччі 2024 року до 27% у першій половині цього року [15]. Таким чином, роль і значення роль

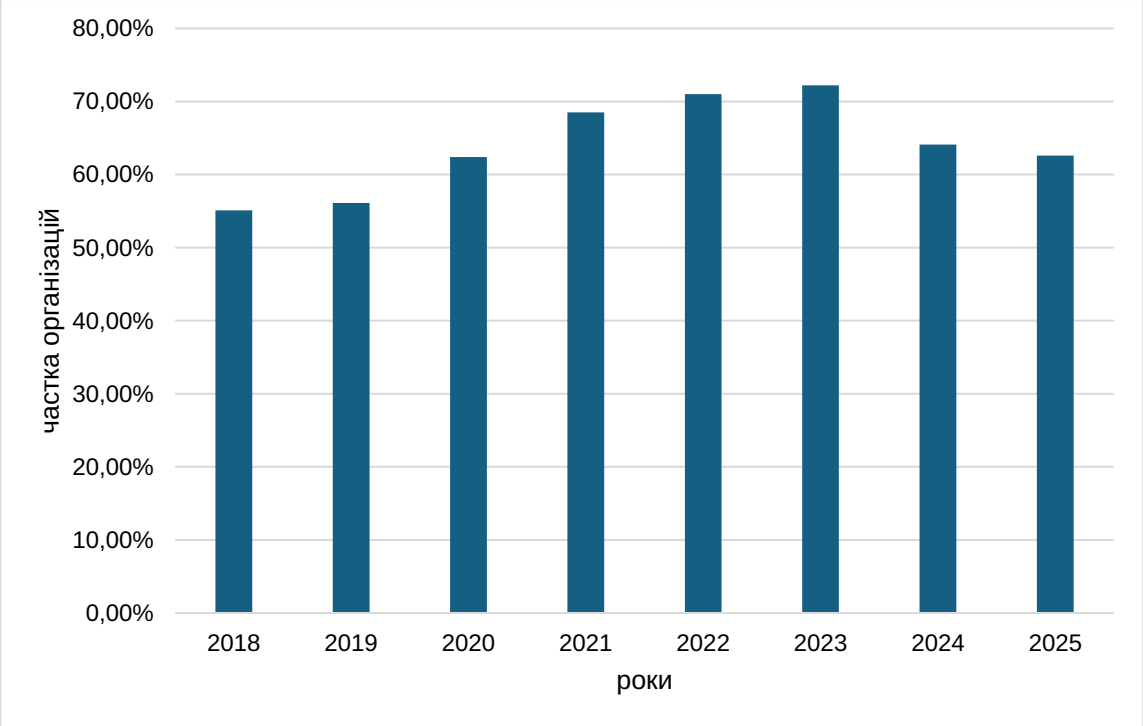

Рис. 1. Частка організацій, які постраждали від атак програм-вимагачів у всьому світі з 2018 по 2025 рік

Джерело: сформовано авторами на основі [12]

кадрової безпеки в умовах цифрових викликів суттєво зростає, оскільки саме персонал виступає одночасно ключовим суб'єктом забезпечення цифрової та інформаційної безпеки і є найбільш уразливим елементом системи захисту організації.

Високий рівень фішингових атак, поширення програм-вимагачів і зростання вартості витоків даних свідчать про необхідність переорієнтації управлінських підходів від суто технічних заходів кіберзахисту до комплексного розвитку людського чинника безпеки та формування культури безпеки в умовах інтенсивного розвитку інформаційно-комунікаційних технологій, які є важливою складовою сучасного суспільства.

У цьому контексті кадрова безпека повинна охоплювати процедури добору, контролю та мотивації персоналу з урахуванням системного формування цифрових компетенцій, навичок кібергігієни, культури відповідального поводження з інформаційними ресурсами, а також психологічної стійкості працівників у стресових і кризових умовах. Оскільки використання великої кількості інформаційно-комунікаційних технологій призводить до швидкого емоційного вигорання, а з часом і професійного. Це негативно впливає на продуктивність працівників та організаційну стійкість, адже результатом виснаження є звільнення працівника, тобто втрата його креативного, творчого, особистісного та професійного потенціалу, що дозволяє отримувати організації синергетичний ефект від взаємодії працівника, технологій та ресурсів. При цьому зростає роль і значення психологічної безпеки, яка здатна мінімізувати негативні наслідки інтенсивного розвитку інформаційно-комунікаційних технологій шляхом формування культури безпеки. Вона створює передумови для розвитку креативності, критичного мислення, взаємодії та співпраці, внутрішнього спокою, зворотного зв'язку, зменшення масових та індивідуальних панічних реакцій.

Особливого значення набуває питання психологічної безпеки у умовах збільшення практики командної роботи, де в межах команд реалізуються ключові бізнес-процеси, приймаються оперативні рішення та здійснюється обмін критично важливою інформацією, реалізуються функції планування, організації, мотивації та контролю. Проєкти, які створюються і виконуються сучасними організаціями майже всі передбачають використання командних технологій, які посилюються саме в умовах цифровізації. І з кожним роком їх

кількість збільшується, як і кількість взаємодій як в середині команди, так і команди із іншими стейкхолдерами.

Посилюється питання емоційного та професійного вигорання у результаті збільшення інформаційного навантаження та зростання кількості комунікацій, що в свою чергу призводить, до розмивання меж між робочим і особистим часом. Це призводить до зниження продуктивності діяльності, збільшення кількості людських помилок, що впливає на організаційну стійкість та здатність протидіяти внутрішнім і зовнішнім загрозам та зберігати репутаційну надійність. З огляду на це, доцільно запропонувати використання «тріади» положень міжнародних стандартів ISO 9001:2015, ISO 45003:2021 та ISO/IEC 27001 як методологічної основи для формування інтегрованої моделі кадрової безпеки, що дозволяє комплексно вирішити питання психологічної та цифрової безпеки, цифрових компетенцій, командної технології у контексті забезпечення організаційної стійкості (табл. 1).

Оскільки в сучасних умовах досить складно уявити організацію роботи сучасного управлінця без командних технологій, які є інтегрованими у сучасні інформаційно-комунікаційні

Таблиця 1

Запропонована політика кадрової безпеки організації на основі стандартів міжнародних стандартів ISO 9001:2015, ISO 45003:2021 та ISO/IEC 27001

Напрям політики кадрової безпеки	Відповідний стандарт ISO	Стратегічна мета	Основні цілі	Ключові інструменти реалізації	Очікуваний результат
Управління якістю HR-процесів	ISO 9001:2015	Підвищення керованості та надійності системи управління персоналом	стандартизація HR-процесів; підвищення прозорості відповідальності; зниження кадрових ризиків	Регламенти HR-процесів, KPI персоналу, внутрішні аудити, матриці компетенцій, процесний підхід	Стабільність управлінських рішень, зниження помилок, прогнозованість результатів
Психологічна безпека персоналу	ISO 45003:2021	Забезпечення психо-соціальної стійкості працівників і команд	зниження рівня стресу; профілактика вигорання; зменшення конфліктів	Оцінка психосоціальних ризиків, програми well-being, психологічна підтримка, навчання керівників soft skills	Підвищення лояльності персоналу, продуктивності та командної згуртованості
Інформаційна та кібер-безпека	ISO/IEC 27001	Захист інформаційних ресурсів від внутрішніх загроз	мінімізація людського чинника; формування культури кібергігієни	Політики доступу, MFA, навчання персоналу, фішинг-симуляції, моніторинг інцидентів	Зниження кількості інцидентів, збереження репутації, довіра клієнтів
Розвиток цифрових компетенцій	Інтегровано у всі стандарти	Підвищення цифрової зрілості персоналу	підвищення цифрової грамотності; безпечне використання ІКТ	Навчальні програми, сертифікації, e-learning, оцінка цифрових навичок	Зменшення операційних і кіберризиків
Командна стійкість	Комплексно	Забезпечення безперервності діяльності	підвищення адаптивності; ефективна взаємодія	Цифрові платформи командної роботи, кризові тренінги, командні регламенти	Операційна стабільність і швидка адаптація

Джерело: сформовано авторами на основі [16; 17]

платформи, сервіси, додатки, то організація та управління кадровим потенціалом набуває ключової ролі.

Так, міжнародний стандарт системи якості ISO 9001:2015 дозволить визначити чітко процеси кадрової безпеки та їх формалізувати; стандарт ISO 45003:2021 у контексті кадрової безпеки визначити критерії, інструменти та процеси у контексті психологічної безпеки та інформаційної безпеки, що відображені у стандарті ISO/IEC 27001. Отже, буде сформована можливість інтегрувати вимоги до інформаційної та цифрової безпеки та сформувати культуру безпеки. Як результат, така модель дозволить поєднати управлінські, соціально-психологічні та інформаційно-технологічні компоненти в єдиний комплекс забезпечення організаційної стійкості організації і отримати наступні конкурентні переваги (рис. 2).

Запропонована модель кадрової безпеки на основі «тріади» положень міжнародних стандартів ISO 9001:2015, ISO 45003:2021 та

Рис. 2. Основні переваги від впровадження кадрової безпеки організації на основі міжнародних стандартів ISO 9001:2015, ISO 45003:2021 та ISO/IEC 27001

Джерело: сформовано авторами на основі [16; 17]

ISO/IEC 27001 дозволить поступово вирішувати наступні проблеми кадрової безпеки на підприємствах України: економічні (недостатнє фінансування програм навчання персоналу з цифрової грамотності та кібергігієни; низький рівень оплати праці, що знижує мотивацію працівників дотримуватися політик безпеки; високі витрати на програмне забезпечення, аудит, консультаційні послуги та технічні засоби захисту); технічні (відсутність інтегрованих цифрових платформ для командної роботи та безпечного обміну даними; нестача технічних спеціалістів з інформаційної безпеки; фрагментарність інформаційних систем і відсутність єдиних стандартів обробки даних); організаційні (формальний підхід до впровадження стандартів ISO; слабка координація між HR-підрозділом, службою безпеки та IT-службою; відсутність внутрішніх регламентів і процедур управління ризиками, пов'язаними з персоналом; нестача досвіду впровадження систем менеджменту за міжнародними стандартами).

Адже, використання міжнародних стандартів системи якості ISO сприятиме формуванню системного вирішення зазначених проблем, оскільки вона створена на основі процесного підходу, ризик-орієнтованого мислення та принципів безперервного вдосконалення (PDCA), закладених у стандартах ISO серії 9000 та ISO/IEC 27000 дозволить охопити наступні рівні: стратегічний (інтегрувати політику кадрової безпеки у загальну стратегію розвитку організації); тактичний (забезпечити взаємозв'язок між процедурами, регламентами, політиками із цифровими компетенціями та психологічною безпекою); оперативний (сформувати практичну реалізацію заходів з відбору, адаптації, навчання, оцінювання персоналу, забезпечення контролю доступу, моніторингу поведінкових та інформаційних інцидентів). Отже, особливістю запропонованого підходу є інтеграція психологічної безпеки та цифрових компетенцій, зокрема навичок кібергігієни у систему управління людськими ресурсами, що дозволяє розглядати персонал не лише як об'єкт захисту, але і як активний суб'єкт формування культури безпеки в організації.

Висновки. Таким чином, кадрова безпека в умовах цифрових трансформацій набуває системного характеру та розглядається як ключова складова забезпечення організаційної стійкості у довгостроковій перспективі в умовах інтенсивного розвитку інформаційно-комунікаційних технологій. Вона орієнтована не лише на інструменти контролю та мінімізації внутрішніх загроз, а й на системну роботу щодо цілеспрямованого розвитку цифрових компетенцій персоналу, забезпечення психологічної безпеки, формування культури безпеки на основі технологій командної взаємодії.

Інтеграція вимог стандартів ISO 9001:2015, ISO 45003:2021 та ISO/IEC 27001 у кадрову безпеку дозволить створити методологічне підґрунтя для формування культури безпеки та підвищення адаптивності організації до багаторівневих ризиків цифрового середовища. Реалізація такого підходу дозволить підвищити надійність управлінських рішень, зменшити ймовірність інформаційних і соціально-психологічних інцидентів, забезпечити безперервність бізнес-процесів і зберегти довгострокову конкурентоспроможність організацій в умовах зростаючої турбулентності зовнішнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. OECD Digital Transformation Strategy 2020–2025: A Digital Government for a Digital Society. Paris: OECD Publishing, 2020. 48 p. (дата звернення: 14.01.2026)

2. Проєкт «Цифрова Аджета-2020. Концептуальні засади. URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (дата звернення: 14.01.2026)

3. Розпорядження КМУ Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках від 31 грудня 2024 р. № 1351-р. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (дата звернення: 14.01.2026)

4. Повідомлення комісії до європейського парламенту, ради, європейського економічно-соіального комітету та комітету регіонів. Цифровий компас 2030: європейський шлях для цифрового десятиліття. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (дата звернення: 14.01.2026)

5. Касич А.О., Медвідь Г.С. Управління кадровою безпекою на українських підприємствах через призму макроекономічних процесів. *Ефективна економіка*. № 11, 2019. URL: http://www.economy.nayka.com.ua/pdf/1_2019/11.pdf. (дата звернення: 18.01.2026)

6. Коптєва Г. М. Кадрова безпека підприємства: сутність, складові та забезпечення. *Вісник Національного технічного університету "ХПІ".* Сер.: Економічні науки: зб. наук. пр. Харків : НТУ "ХПІ", 2020. № 2. С. 119-124. (дата звернення: 18.01.2026)

7. Швед В.В., Чорнокозинська О.А. Теоретико-методологічні засади кадрової політики на підприємстві. *Східна Європа: економіка, бізнес та управління*. Випуск 3 (36), 2022. URL: https://www.easterneurope-ebm.in.ua/journal/36_2022/18.pdf (дата звернення: 18.01.2026)

8. Anna Sutton, Lisa Tompson. Towards a cybersecurity culture-behaviour framework: a rapid evidence revier. URL: https://www.sciencedirect.com/science/article/pii/S0167404824004152 (дата звернення: 06.02.2026)

9. Швед Н.М. Прикладні аспекти організації командної роботи в публічній організації. Актуальні проблеми публічного управління та адміністрування: Колективна монографія. Т. : ФОП Паляниця В. А. С. 236–254. URL: https://elartu.tntu.edu.ua/bitstream/lib/32390/2/monograph_PU_2020_TNTU_Shveda_N_M-Practical_aspects_of_teamwork_236-254.pdf (дата звернення: 20.01.2026)

10. Горбунова В. В. Психологія командотворення: ціннісно-рольовий підхід до формування та розвитку команд: монографія. Житомир : Вид-во ЖДУ ім. І. Франка, 2014. 380 с. (дата звернення: 21.01.2026)

11. Глєбова А. Організація командної роботи в умовах глобальних викликів у контексті цифрової та кадрової безпеки. *Економіка і регіон Economics and Region*, (4(99), 2025. с184–193. https://doi.org/10.26906/EiR.2025.4(99).4171 (дата звернення: 20.01.2026)

12.Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2025. URL: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/?srsltid=AfmBOopsHRWPxINiegyWfpa72AA3V6tA7JGyRxia1q0nBuoTVwENwHbe (дата звернення: 21.01.2026)

13. Global ransomware attacks rose 32% in 2025, as manufacturers emerged as top target. URL: https://industrialcyber.co/reports/global-ransomware-attacks-rose-32-in-2025-as-manufacturers-emerged-as-top--target/ (дата звернення: 25.01.2026)

14. Mohammed Khalil. Malware Statistics 2025: Global Cyber Threat Trends and Costs. URL: https://deepstrike.io/blog/Malware-Attacks-and-Infections-2025 (дата звернення: 25.01.2026)

15. Інтенсивність фішингових атак зросла, але люди стали більш обізнаними в питаннях кібергігієни: аналітичний звіт CERT-UA. URL: https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh--obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua (дата звернення: 24.01.2026)

16. Міжнародний стандарт системи якості ISO 9001:2015. URL: https://iso-certify.com/ua/iso-9001/?gad_source=1&gad_campaignid=2081778400&gbraid=0AAAAADmroGyfBAqQpVFds1l2o2vUWjCrl&gclid=Cj0KCQiA-hOfLBhCCARIsAJPiopOyNOfxn6_r0te704Gh-4N-Z-G9AycybrO0ugM-IdDYRgmuS9fcSuwaAkyMEALw_wcB (дата звернення: 16.01.2026)

17. ISO 45003 – Управління психосоціальними ризиками у вашому бізнесі. URL: https://tms.ua/sistemy-menedzhmenta/iso-45001/iso-45003/(дата звернення: 16.01.2026)

REFERENCES:

1. OECD. (2020). *OECD Digital Transformation Strategy 2020–2025: A Digital Government for a Digital Society* (48 p.). OECD Publishing.

2. Ukrainian Chamber of Commerce and Industry. (2020). *Digital Agenda 2020 Project. Conceptual Framework*. Retrieved from https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf [in Ukrainian]

3. Cabinet of Ministers of Ukraine. (2024). *Resolution No. 1351-r "On Approval of the Strategy for Digital Development of Innovation Activity of Ukraine until 2030 and the Action Plan for Its Implementation in 2025–2027"*. Retrieved from https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text [in Ukrainian]

4. European Commission. (2021). *Digital Compass 2030: The European Way for the Digital Decade*. Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

5. Kasych, A. O., & Medvid, H. S. (2019). Upravlinnia kadrovoiu bezpekoiu na ukrainskykh pidpryiemstvakh cherez pryzmu makroekonomichnykh protsesiv [Personnel security management at Ukrainian enterprises through the prism of macroeconomic processes]. *Efektyvna ekonomika*, (11). Retrieved from http://www.economy.nayka.com.ua/pdf/1_2019/11.pdf [in Ukrainian]

6. Koptieva, H. M. (2020). Kadrova bezpeka pidpryiemstva: sutnist, skladovi ta zabezpechennia [Personnel security of the enterprise: essence, components and provision]. *Bulletin of the National Technical University "KhPI". Series: Economic Sciences*, (2), 119–124. [in Ukrainian]

7. Shved, V. V., & Chornokozynska, O. A. (2022). Teoretyko-metodolohichni zasady kadrovoi polityky na pidpryiemstvi [Theoretical and methodological foundations of personnel policy at the enterprise]. *Eastern Europe:*

Economy, Business and Management, 3(36). Retrieved from https://www.easterneurope-ebm.in.ua/journal/36_2022/18.pdf [in Ukrainian]

8. Sutton, A., Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*. 2025. Vol. 148. Art. 104110. DOI: 10.1016/j.cose.2024.104110. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404824004152

9. Shved, N. M. (2020). Prykladni aspekty orhanizatsii komandnoi roboty v publichnii orhanizatsii [Applied aspects of organizing teamwork in a public organization]. In *Current Issues of Public Administration and Management* (pp. 236–254). Ternopil: FOP Palyanytsia V. A. Retrieved from https://elartu.tntu.edu.ua/bitstream/lib/32390/2/monograph_PU_2020_TNTU_Shveda_N_M-Practical_aspects_of_teamwork_236-254.pdf [in Ukrainian]

10. Horbunova, V. V. (2014). *Psykholohiia komandotvorennia: tsinnisno-rolovyi pidkhid do formuvannia ta rozvytku komand* [Psychology of team building: value-role approach to team formation and development]. Zhytomyr: Zhytomyr Ivan Franko State University Publishing House. [in Ukrainian]

11. Hliebova, A. (2025). Orhanizatsiia komandnoi roboty v umovakh hlobalnykh vyklykiv u konteksti tsyfrovoi ta kadrovoi bezpeky [Organization of teamwork under global challenges in the context of digital and personnel security]. *Economics and Region*, 4(99), 184–193. https://doi.org/10.26906/EiR.2025.4(99).4171 [in Ukrainian]

12. Statista Research Department. (2025). *Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2025*. Retrieved from https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

13. Industrial Cyber. (2025). *Global ransomware attacks rose 32% in 2025, as manufacturers emerged as top target*. Retrieved from https://industrialcyber.co/reports/global-ransomware-attacks-rose-32-in-2025-as-manufacturers-emerged-as-top-target/

14. Khalil, M. (2025). *Malware Statistics 2025: Global Cyber Threat Trends and Costs*. Retrieved from https://deepstrike.io/blog/Malware-Attacks-and-Infections-2025

15. CERT-UA. (2025). Intensyvnist fishynhovykh atak zrosla, ale liudy staly bilsh obiznanymy v pytanniakh kiberhihiieny [Phishing intensity increased, but people became more aware of cyber hygiene issues]. Retrieved from https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua [in Ukrainian]

16. International Organization for Standardization. (2015). *ISO 9001:2015 Quality Management Systems – Requirements*. Retrieved from https://iso-certify.com/ua/iso-9001/

17. International Organization for Standardization. (2021). *ISO 45003: Occupational health and safety management – Psychological health and safety at work*. Retrieved from https://tms.ua/sistemy-menedzhmenta/iso-45001/iso-45003/

Дата надходження статті: 06.12.2025
Дата прийняття статті: 17.12.2025
Дата публікації статті: 29.12.2025