DOI: 10.58423/2786-6742/2025-10-133-145
УДК 330.131.7:005.44:658.5:69

Марина КРАВЧЕНКО
доктор економічних наук, професор,
професор кафедри менеджменту підприємств
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна
ORCID ID: 0000-0001-5405-0159
Scopus Author ID: 57197853409

Федір НЕМИРОВСЬКИЙ
аспірант кафедри економіки і підприємництва
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Київ, Україна
ORCID ID: 0009-0008-0219-8029
e-mail: nemyrovskyifedir@gmail.com
(Corresponding author)

АНАЛІЗ СТАНУ ЦИФРОВІЗАЦІЇ ТА ІННОВАЦІЙНОЇ АКТИВНОСТІ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ У КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Анотація. *У межах дослідження здійснено комплексний аналіз цифровізації та інноваційної активності підприємств будівельної галузі в контексті забезпечення їх економічної безпеки. Метою роботи є ідентифікація ключових тенденцій цифрового розвитку підприємств галузі, оцінка їхньої спроможності протидіяти сучасним інформаційним загрозам і виявлення потенціалу використання інноваційних технологій як чинників зміцнення економічної безпеки. Методологічну основу дослідження становлять положення теорії економічної безпеки підприємства, системного та структурно-функціонального підходів, із застосуванням методів статистичного аналізу, групування, порівняння та графічної інтерпретації даних.*

У ході аналізу виявлено наявність помірного, але поступального зростання рівня цифрової зрілості підприємств будівельної галузі. Зафіксовано збереження практики зовнішнього делегування ІКТ-функцій, незначне поширення заходів формалізованого навчання персоналу з питань інформаційної безпеки, а також недостатній рівень впровадження сучасних цифрових інструментів, зокрема багатофакторної автентифікації, систем моніторингу загроз, технологій шифрування даних тощо. Проаналізовано масштаби використання штучного інтелекту та робототехнічних систем за функціональними напрямами. Встановлено, що їх застосування переважно зосереджене у виробничих процесах і сфері управління, тоді як використання в контексті забезпечення інформаційної безпеки залишається вкрай обмеженим.

This is an Open Access article distributed under the terms of the Creative Commons CC BY-NC 4.0

Практичне значення отриманих результатів полягає у можливості їх використання для розроблення стратегій цифрової трансформації будівельних підприємств з урахуванням вимог економічної безпеки, удосконалення систем управління інформаційною безпекою, а також впровадження ефективних механізмів оцінювання та мінімізації цифрових ризиків. Запропоновані аналітичні підходи можуть бути використані в процесі формування корпоративної політики щодо впровадження інноваційних технологій, підготовки внутрішніх нормативних документів з питань кіберзахисту, а також при розробці галузевих рекомендацій для підвищення рівня цифрової стійкості підприємств.

Ключові слова: *цифровізація, будівельні підприємства, економічна безпека, інформаційна безпека, інноваційна активність, цифрові ризики.*

JEL Classification: D83, L74, O33

Absztrakt. *A kutatás keretében átfogó elemzés történt az építőipari vállalatok digitalizációs és innovációs aktivitás gazdasági biztonságának szempontjából. A tanulmány célja az iparági vállalkozások digitális fejlődésének kulcsfontosságú trendjeinek azonosítása, a modern információs fenyegetésekkel szembeni képességük felmérése, valamint az innovatív technológiák gazdasági biztonságot erősítő tényezők felhasználási lehetőségeinek azonosítása. A kutatás módszertani alapját a vállalkozás gazdasági biztonságának elméleti rendelkezései, a szisztematikus és strukturális-funkcionális megközelítések képezik, statisztikai elemzési, csoportosítási, összehasonlítási valamint grafikai adatértelmezési módszerek alkalmazásával.*

A kutatás során mérsékelt, de fokozatos növekedés mutatkozott az építőipari vállalatok digitális érettségi szintjén. Megerősítést nyert, hogy az információs-kommunikációs technológiai (IKT) funkciók külső delegálásának gyakorlata továbbra is fennáll, az információbiztonságról szóló formalizált képzési intézkedések terjedése csekély, valamint a modern digitális eszközök, mint például a többfaktoros hitelesítés, a fenyegetésfigyelő rendszerek és az adat titkosítási technológiák bevezetése is elégtelen. Elemzésre került a mesterséges intelligencia és robotikai rendszerek funkcionális irányok szerinti használatának mértéke. Megállapításra került, hogy alkalmazásuk elsősorban a termelési folyamatokban és a menedzsment területén koncentrálódik, míg az információbiztonság biztosításában való használatuk rendkívül korlátozott.

Az elért eredmények gyakorlati jelentősége abban rejlik, hogy felhasználhatók az építőipari vállalkozások digitális átalakulására vonatkozó stratégiák kidolgozásához, figyelembe véve a gazdasági biztonság követelményeit, fejlesztve az információbiztonsági irányítási rendszereket, valamint hatékony mechanizmusokat vezetve be a digitális kockázatok felmérésére és minimalizálásra.

A javasolt analitikai megközelítések felhasználhatók az innovatív technológiák bevezetésére vonatkozó vállalati politika kialakításában, a kiberbiztonsággal kapcsolatos belső szabályozási dokumentumok elkészítésében, valamint az iparági ajánlások kidolgozásában a vállalatok digitális ellenálló képességének növelése érdekében.

Kulcsszavak: *digitalizáció, építőipari vállalatok, gazdasági biztonság, információbiztonság, innovációs aktivitás, digitális kockázatok.*

Abstract*. The study presents a comprehensive analysis of the digitalization and innovation activity of construction enterprises in the context of ensuring their economic security. The purpose of the work is to identify key trends in the digital development of the industry, assess the ability of enterprises to counter modern information threats, and determine the potential of using innovative technologies as drivers of economic security enhancement. The methodological basis of the study is grounded in the theory of enterprise economic security, as well as systemic and structural-functional approaches, with the application of statistical analysis, grouping, comparative methods, and graphical data interpretation.*

The analysis revealed a moderate but steady increase in the level of digital maturity of construction enterprises. The practice of outsourcing ICT functions remains prevalent, while

formalized employee training in information security is still limited. The level of adoption of advanced digital instruments—such as multi-factor authentication, threat monitoring systems, and data encryption technologies—remains insufficient. The use of artificial intelligence and robotics was also examined across functional areas. It was found that these technologies are primarily applied in production processes and management, whereas their implementation in the field of information security remains extremely limited.

The practical value of the obtained results lies in their applicability for developing digital transformation strategies for construction enterprises in line with economic security requirements, improving information security management systems, and implementing effective mechanisms for assessing and minimizing digital risks. The proposed analytical approaches can be applied in the formation of corporate policies on the adoption of innovative technologies, the development of internal regulatory documents on cybersecurity, as well as in the creation of industry-specific recommendations to strengthen the digital resilience of enterprises.

***Keywords**: digitalization, construction enterprises, economic security, information security, innovation activity, digital risks.*

Постановка проблеми. У сучасних умовах функціонування національної економіки, що характеризуються високим рівнем турбулентності зовнішнього середовища, ускладненням доступу до ресурсів, посиленням інформаційних загроз та необхідністю адаптації до цифрової трансформації, питання забезпечення економічної безпеки підприємств набувають особливої актуальності. Це в повній мірі стосується й суб'єктів господарювання будівельної галузі, які, з одного боку, залишаються ключовими учасниками процесів інфраструктурного розвитку держави, а з іншого — зазнають суттєвого впливу цифрових ризиків, викликаних недостатнім рівнем технологічної адаптації та організаційно-інформаційної захищеності.

Незважаючи на наявність окремих досліджень, присвячених цифровізації підприємств та інформаційній безпеці в галузевому розрізі, комплексна оцінка стану цифрової зрілості будівельних підприємств, рівня впровадження інноваційних рішень, характеру ІКТ-загроз і практик реагування на них у контексті економічної безпеки залишається недостатньо розробленою. Зокрема, актуальною є потреба у вивченні динаміки цифрової трансформації підприємств галузі, визначенні слабких місць в організації інформаційного захисту та окресленні потенційних точок зростання на основі впровадження інноваційних технологій.

Аналіз останніх досліджень і публікацій. Проблематика цифровізації, інноваційного розвитку та забезпечення економічної безпеки підприємств, у тому числі будівельної галузі, набула значної уваги у працях як вітчизняних, так і зарубіжних науковців. Так, В. Чешук [1] акцентує увагу на інноваційному аспекті моніторингу економічної безпеки будівельних підприємств, підкреслюючи необхідність інтеграції оцінки поточного стану з інструментами ефективного управління інноваціями. У дослідженні В. Воронкової та Є. Ніколаєнко [2] цифрова трансформація розглядається як ключовий чинник стабільності та сталого розвитку підприємств, що супроводжується розробленням практичних рекомендацій щодо підвищення результативності

цифровізації. Д. Бондаренко та К. Калашнікова [3] детально проаналізували кроки, які здійснюються на державному рівні з метою стимулювання цифровізації будівельної галузі, виокремивши основні бар'єри, виклики та можливості у цьому процесі. У працях О. Марченка та Р. Коляденка [4] доведено, що реалізація повоєнної відбудови України значною мірою залежить від впровадження BIM-технологій, цифрових сервісів та інструментів Єдиної державної електронної системи у сфері будівництва, що має стати підґрунтям для цифрової трансформації та підвищення конкурентоспроможності галузі.

Водночас, попри наявність значної кількості наукових напрацювань, питання оцінки рівня цифрової зрілості будівельних підприємств, визначення їхньої здатності протидіяти інформаційним загрозам та ефективно інтегрувати інноваційні технології у систему забезпечення економічної безпеки залишаються дискусійними та потребують подальшого дослідження.

Виділення невирішених раніше частин загальної проблеми. Таким чином, існуючий науковий доробок формує теоретичну основу для подальшого вивчення цифровізації і інноваційної активності будівельних підприємств у контексті економічної безпеки, проте питання інтеграції сучасних інформаційних технологій у практики управління економічною безпекою залишається недостатньо дослідженим і вимагає подальшого наукового опрацювання.

Формулювання цілей статті (постановка завдання). Метою роботи є ідентифікація ключових тенденцій цифрового розвитку підприємств галузі, оцінка їхньої спроможності протидіяти сучасним інформаційним загрозам і виявлення потенціалу використання інноваційних технологій як чинників зміцнення економічної безпеки.

Виклад основного матеріалу дослідження. З огляду на активізацію цифрової трансформації та потребу в удосконаленні інформаційної інфраструктури, особливої уваги заслуговує вивчення рівня залучення підприємств будівельної галузі до процесів, пов'язаних з інформаційно-комунікаційними технологіями (ІКТ), що представлені на рис. 1. Дослідження зазначених аспектів дозволить оцінити рівень цифрової зрілості підприємств галузі та виявити потенційні напрями посилення їх інформаційної безпеки й інноваційного розвитку.

Упродовж 2018–2022 років динаміка цифровізації будівельних підприємств через показники, пов'язані з ІКТ, засвідчує нерівномірне, проте поступове зростання за окремими напрямами. Частка підприємств, що проводили навчання у сфері ІКТ, коливалася в межах 1,3–2,3%, демонструючи найбільше значення у 2020 році, що може бути пов'язано з адаптаційними заходами в умовах пандемії. Аналогічно, зростала частка підприємств, що наймали фахівців у сфері ІКТ — з 2,7% у 2018 році до 3,4% у 2022 році, що свідчить про підвищення попиту на відповідні компетенції. Водночас найбільш стабільною залишалася частка підприємств, які делегували виконання ІКТ-функцій зовнішнім постачальникам — цей показник утримувався на рівні близько 14%, що вказує на сталу практику

аутсорсингу цифрових послуг у галузі. Загалом такі тенденції демонструють повільний, але сталий рух будівельних підприємств у напрямі зміцнення інформаційно-цифрового потенціалу.

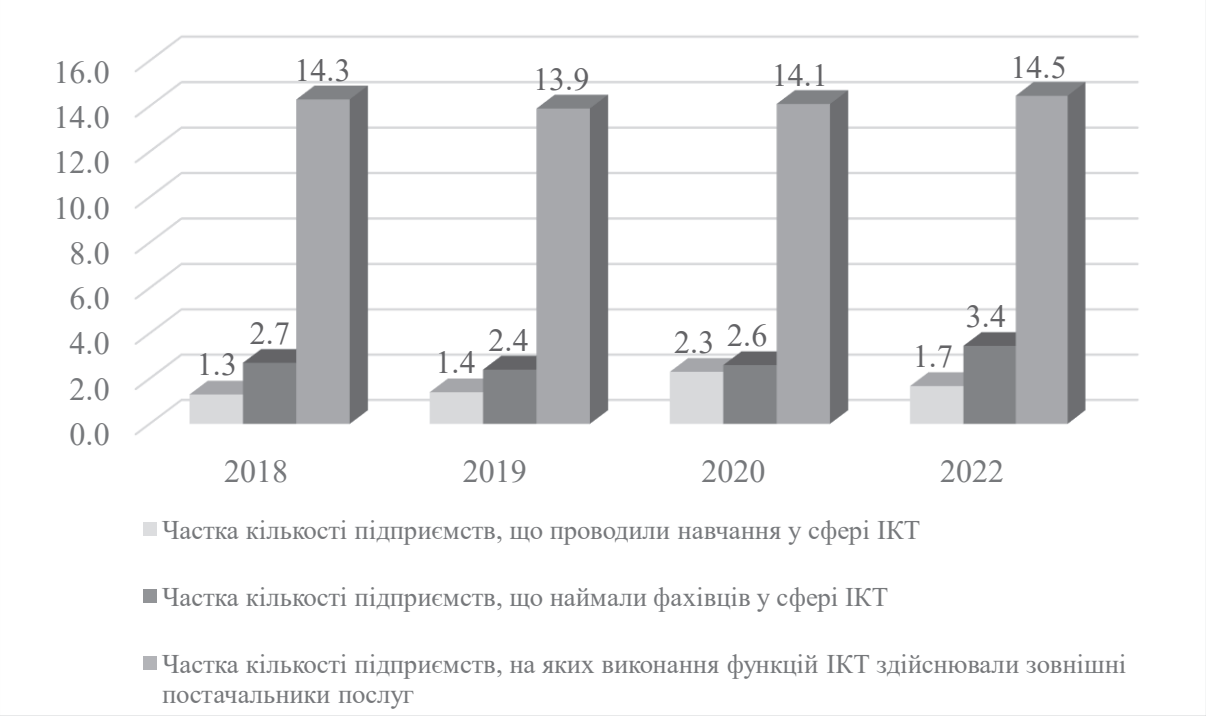

Рис.1 Рівень ІКТ на підприємствах будівельної галузі за 2018-2022 роках, % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Для подальшого аналізу варто звернути увагу на частку підприємств, які зіткнулися з проблемами через інциденти безпеки ІКТ (рис. 2). Цей показник є важливим індикатором ризиків для інформаційної безпеки, оскільки вказує на рівень уразливості підприємств до кіберзагроз. Враховуючи значну роль цифрових технологій у сучасному бізнес-середовищі, дослідження інцидентів безпеки ІКТ допомагає оцінити готовність підприємств до реагування на можливі загрози та визначити потребу у посиленні захисту інформаційних систем.

У 2023 році аналіз частки підприємств, які стикалися з проблемами через інциденти безпеки ІКТ, показав, що найбільша частка випадків стосувалася недоступності послуг ІКТ через збої апаратного або програмного забезпечення, що становить 16,8%.

Це свідчить про значну вразливість підприємств до технічних проблем, пов’язаних з обладнанням та програмним забезпеченням, які можуть спричиняти значні бізнес-втрати. Окрім цього, атаки ззовні, зокрема програм-вимагачів і відмови в обслуговуванні, мали місце на рівні 3,0%, що також є серйозною загрозою для інформаційної безпеки підприємств. Інші проблеми, такі як

знищення або пошкодження даних через технічні збої (4,1%) або через шкідливе програмне забезпечення та несанкціоноване проникнення (1,7%), також мали місце, хоча і у меншій кількості випадків. Водночас, випадки розкриття конфіденційних даних через проникнення, фармінг або фішингові атаки залишаються досить рідкісними (0,4%), що може свідчити про покращення захисту від таких загроз.

Також варто зазначити, що незначний відсоток інцидентів був спричинений ненавмисними діями працівників підприємств (0,7%), що вказує на важливість навчання і підвищення рівня обізнаності серед персоналу.

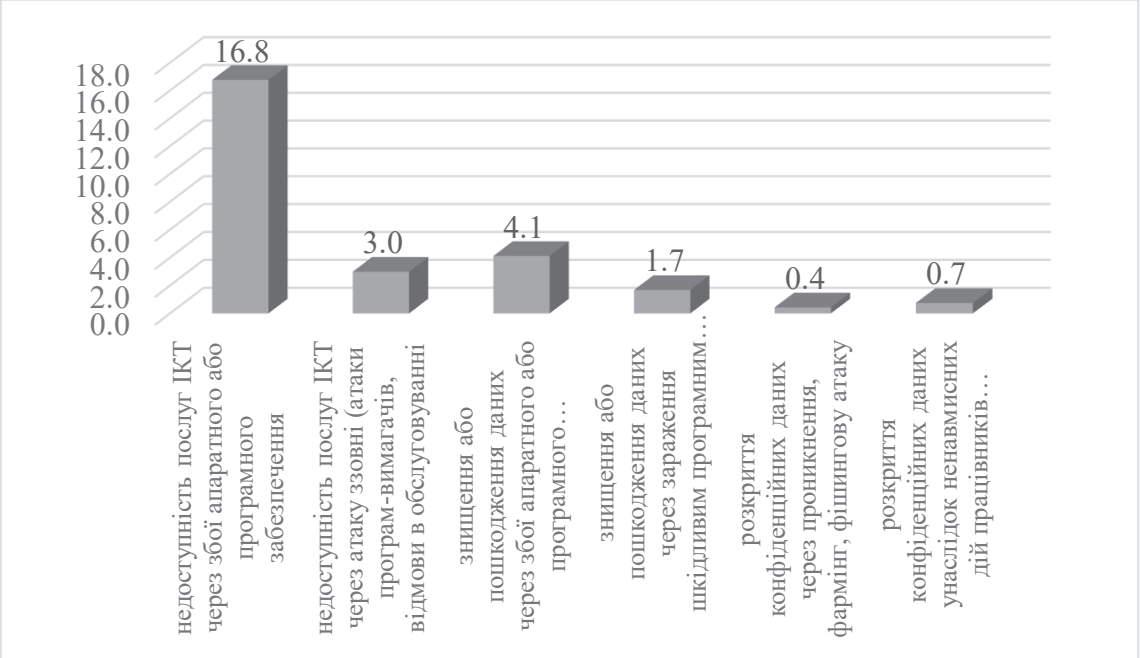

Рис. 2 Частка будівельних підприємств, які стикалися з проблемами через інциденти безпеки ІКТ у 2023 р., % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Забезпечення інформаційної безпеки на підприємствах є не лише питанням технічного захисту, а й важливою складовою управлінської практики, що включає інформування працівників про можливі загрози в галузі ІКТ (рис. 3). Аналіз різних способів інформування дозволить оцінити рівень підготовленості працівників та ефективність проведених заходів для запобігання потенційним інцидентам безпеки.

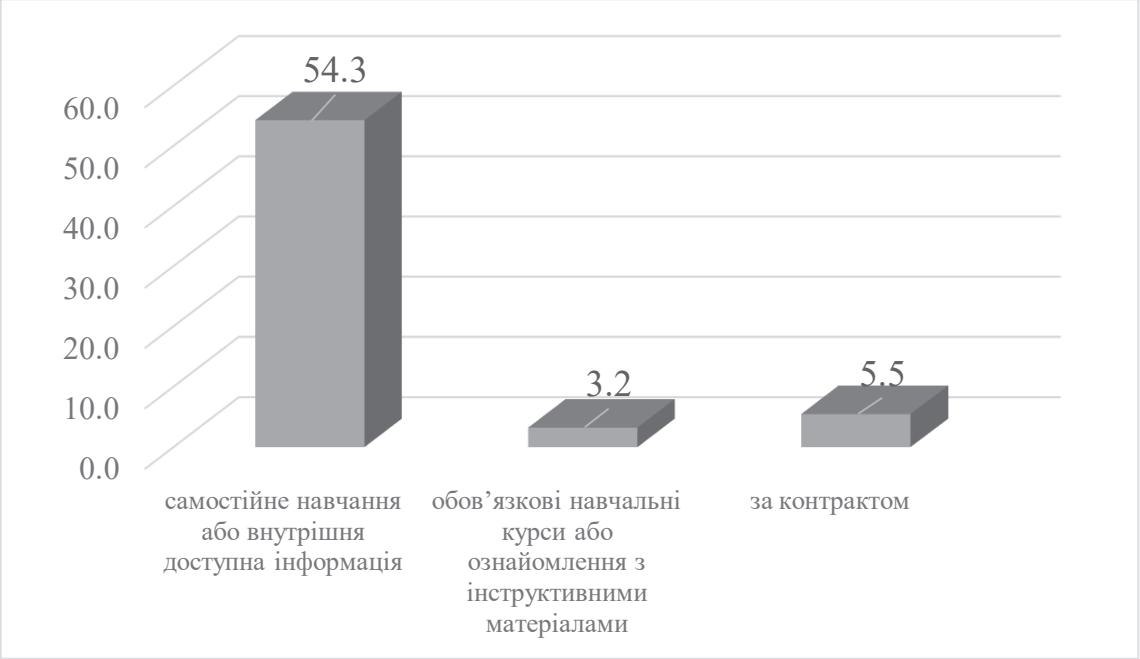

Рис. 3 Частка підприємств, що інформують працівників щодо питань безпеки ІКТ у 2023 р., % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Аналіз даних щодо частки підприємств демонструє, що 54,3% підприємств надають можливість працівникам здійснювати самостійне навчання або використовувати внутрішньо доступну інформацію для ознайомлення з аспектами безпеки ІКТ. Це свідчить про популярність гнучких форм навчання, які дозволяють співробітникам організувати свій час та інтенсивність навчання. Проте значно менша частка — лише 3,2% підприємств — забезпечують обов'язкові навчальні курси або ознайомлення з інструктивними матеріалами, що може вказувати на відсутність систематичності у підходах до безпеки ІКТ на цих підприємствах. Крім того, лише 5,5% підприємств мають договори, що передбачають інформування працівників з питань безпеки ІКТ. Ці дані вказують на необхідність більш активного впровадження формального навчання та зовнішніх інструментів підвищення обізнаності працівників щодо загроз у галузі ІКТ для посилення захисту інформаційних ресурсів підприємств.

Для продовження аналізу, наступним етапом є розгляд частки підприємств, що мають документи щодо безпеки ІКТ (рис. 4). Це дозволить оцінити, наскільки актуальні та оперативно оновлюються політики і процедури безпеки в компаніях, що є важливим чинником для збереження високого рівня інформаційної безпеки.

Аналіз даних щодо часу створення документів з безпеки ІКТ на будівельних підприємствах у 2023 році показує, що частина підприємств турбується про інформаційну безпеку. Зокрема, 1,1% підприємств мають документи, створені більше ніж 24 місяці тому, що вказує на довгострокове

планування та передбачення потенційних ризиків у сфері інформаційної безпеки. Наявність документів, створених протягом останніх 12 місяців (0,9%) або 12-24 місяців (0,3%), також підтверджує актуальність безпеки ІКТ в умовах сучасного цифрового середовища. Таким чином, можна зробити висновок, що будівельні підприємства належно реагують на виклики безпеки ІКТ, що забезпечує стабільність і ефективність їхніх інформаційних систем.

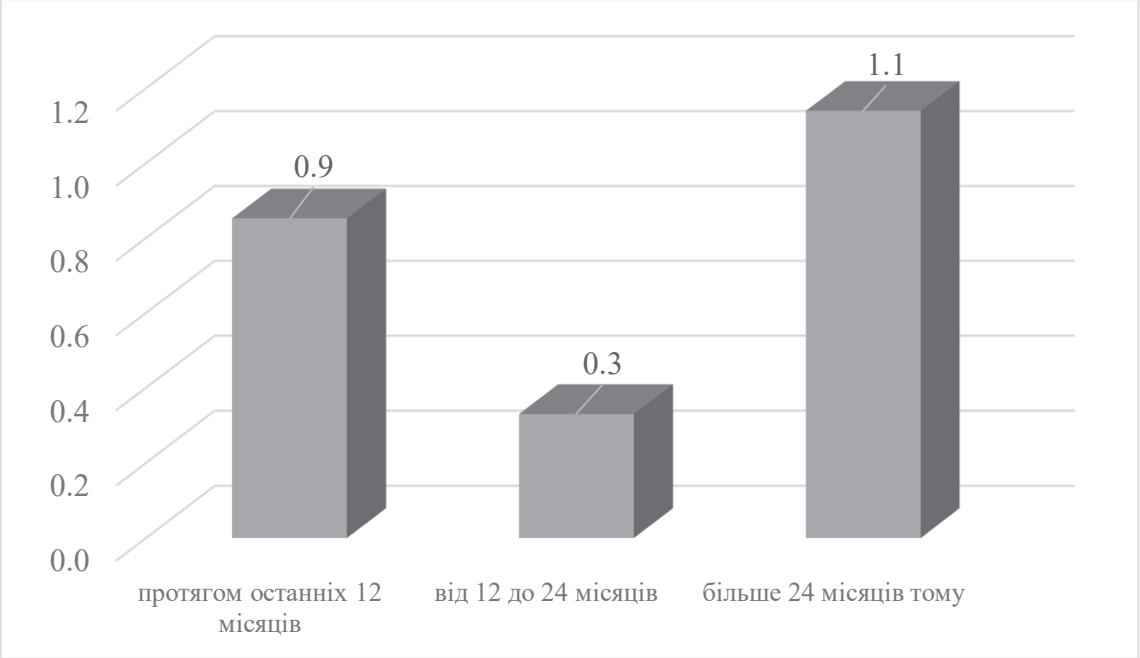

Рис. 4 Частка будівельних підприємств, що мають документи щодо безпеки ІКТ за часом створення документів у 2023 р., % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Для подальшого аналізу доцільно перейти до вивчення частки підприємств, що застосовують заходи безпеки ІКТ в інформаційно-комунікаційних системах (табл. 1). Це дозволить оцінити, які саме заходи безпеки вживаються на підприємствах для забезпечення захисту їхніх інформаційних ресурсів.

Аналіз даних щодо застосування заходів безпеки ІКТ на будівельних підприємствах у 2023 році демонструє широкий спектр інструментів і технологій, спрямованих на захист інформаційних систем. Найпоширенішим методом є автентифікація за допомогою надійного пароля, що застосовується на 59,4% підприємств, що свідчить про основний акцент на простоту та доступність цього заходу. Однак, менш поширеними є більш складні методи автентифікації, такі як біометричні методи (2,4%) та комбіновані методи (12%), що вказує на низький рівень впровадження сучасних методів доступу. Загалом, дані свідчать про значний розрив між базовими методами безпеки, такими як автентифікація та резервне копіювання, та більш складними заходами, такими як використання біометричних методів або систем моніторингу, що може бути результатом

різних рівнів інвестицій та технологічних можливостей підприємств у будівельній галузі.

Таблиця 1.

Частка будівельних підприємств, що застосовують заходи безпеки ІКТ за видами заходів безпеки у 2023 р., у %*

Види заходів безпеки ІКТ	***% підприємств***
автентифікація за допомогою надійного пароля	59,4
автентифікація за допомогою біометричних методів, які використовуються для доступу до інформаційно-комунікаційних систем підприємства	2,4
автентифікація на основі комбінації принаймні двох механізмів автентифікації	12,0
шифрування даних, документів або електронної пошти	16,2
резервне копіювання даних в окреме місце	42,5
контроль доступу до мережі	33,1
VPN	11,9
система моніторингу безпеки ІКТ, яка дозволяє виявити підозрілу активність в інформаційно-комунікаційних системах і сповіщає про це підприємство	11,2
ведення журналів реєстрації подій (лог-файлів), які дозволяють проводити аналіз після інцидентів безпеки ІКТ	8,7
оцінка ризику ІКТ	6,9
тести безпеки ІКТ	9,0

**Узагальнено автором на основі [5]*

Наступним етапом аналізу є вивчення частки підприємств, які використовують технології штучного інтелекту, з розподілом за цілями їх застосування (рис. 5). Це дозволить оцінити, які саме напрямки бізнес-процесів сприяють впровадженню інноваційних технологій та як штучний інтелект впливає на підвищення ефективності підприємств. Дослідження цих даних допоможе виявити ключові сфери застосування ШІ, визначити пріоритети підприємств та спрогнозувати подальший розвиток технологічних тенденцій у галузі.

Аналіз частки підприємств, що використовують технології штучного інтелекту (ШІ) за цілями застосування, виявляє чітку тенденцію до впровадження інтелектуальних технологій у різних сферах діяльності. Найбільше використання ШІ спостерігається у виробничих процесах, де частка становить 3,1%, що вказує на значний потенціал автоматизації та оптимізації виробничих ліній. Для організації процесів ділового адміністрування та управління підприємствами використання ШІ досягає 2,8% та 2,3% відповідно, що свідчить про активне використання інтелектуальних систем для підтримки управлінських рішень.

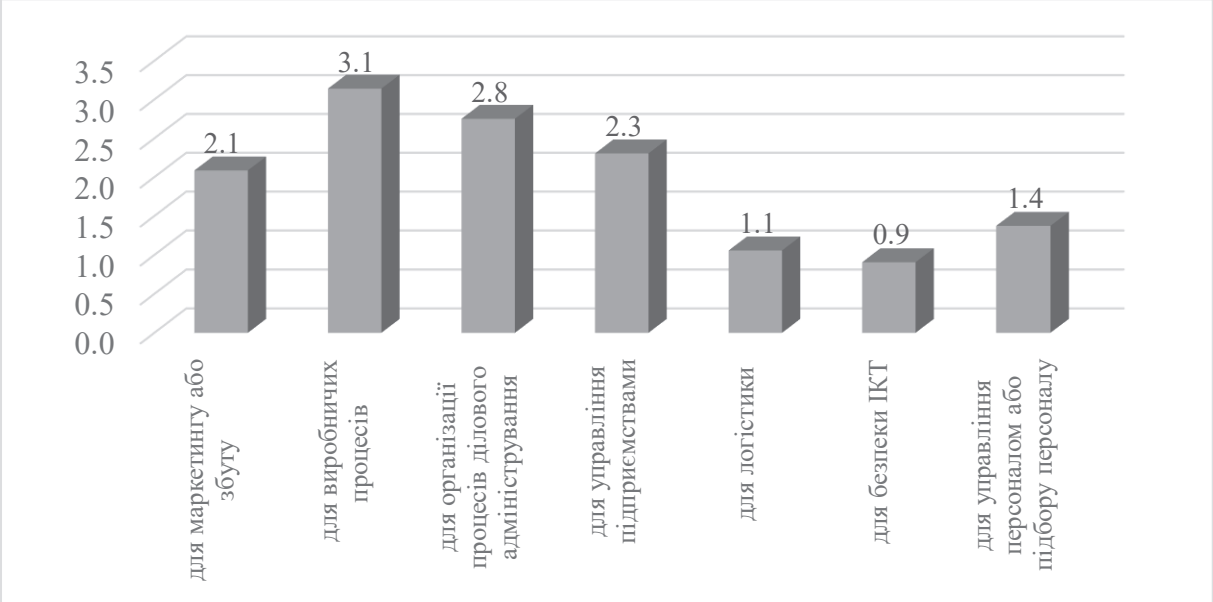

Рис. 5 Частка будівельних підприємств, що використовують технології штучного інтелекту за цілями використання штучного інтелекту у 2023 р., % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Застосування ШІ у маркетингу та збуті складає 2,1%, що підтверджує його роль у поліпшенні ефективності взаємодії з клієнтами та підвищенні результативності комерційних операцій. У той же час, технології ШІ у сфері логістики використовуються лише 1,1% підприємств, а в сфері безпеки ІКТ – 0,9%, що вказує на значний резерв для розвитку цих напрямків. Нарешті, для управління персоналом і підбору кадрів технології ШІ застосовуються у 1,4% підприємств, що свідчить про поступовий процес впровадження автоматизованих систем у кадрову діяльність. Таким чином, дані свідчать про різноманітне застосування ШІ на підприємствах, зокрема в управлінні та виробничих процесах, і вказують на значний потенціал для подальшого розвитку в інших сферах.

Окрім штучного інтелекту, підприємства будівельної галузі також активно впроваджують робототехніку (рис. 6), що є важливою складовою для підвищення ефективності виробничих процесів та забезпечення економічної безпеки. Використання роботів не лише оптимізує операційні витрати та скорочує час виконання завдань, але й сприяє зменшенню трудових травм та підвищенню рівня безпеки на підприємствах.

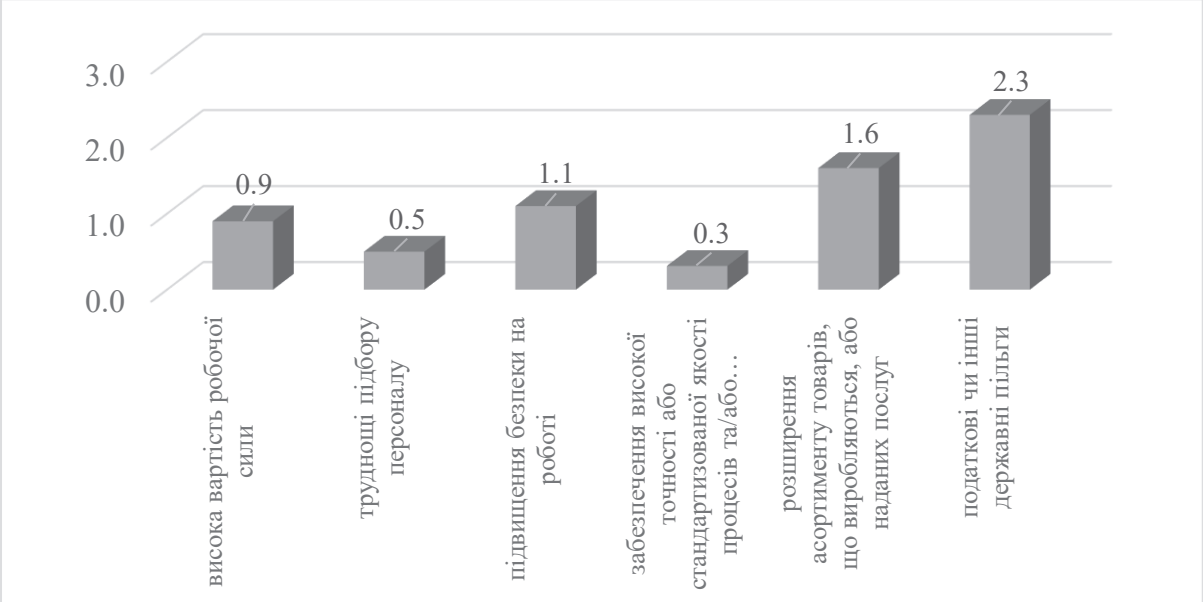

Рис. 6 Частка будівельних підприємств, що використовують робототехніку за причинами у 2023 р., % від загальної кількості підприємств*

**Узагальнено автором на основі [5]*

Аналіз даних щодо причин використання робототехніки будівельними підприємствами показує, що найбільша частка підприємств впроваджує роботів через економічні та організаційні фактори. Однією з важливих причин є висока вартість робочої сили, що змушує підприємства шукати способи оптимізації витрат та автоматизації процесів. Проте, в контексті економічної безпеки, особливо важливою є причина, що пов'язана з підвищенням безпеки на роботі — 1,1 % підприємств вказали саме цей фактор як основний мотив для використання роботів. Це свідчить про те, що роботизація може суттєво знизити рівень ризиків, пов'язаних із фізичними травмами, нещасними випадками та іншими небезпеками, що можуть виникати на будівельних майданчиках, тим самим забезпечуючи стабільність та безпеку підприємства в цілому.

Узагальнений аналіз статистичних та структурних даних засвідчив складну, але динамічну трансформацію будівельної галузі України в умовах зростаючих викликів економічній безпеці. Особливої актуальності набувають питання фінансової стійкості, інноваційного розвитку та захищеності цифрової інфраструктури підприємств. Виявлені тенденції свідчать про необхідність глибшого вивчення внутрішніх факторів стабільності на рівні окремих суб’єктів господарювання. Це зумовлює перехід до більш деталізованого аналізу показників діяльності будівельних підприємств на основі їх фінансової звітності.

Висновки та перспективи подальших досліджень. Результати проведеного аналізу дозволяють зробити висновок про наявність сталих, хоча й помірних тенденцій цифрової трансформації у будівельній галузі України. Встановлено, що переважна більшість підприємств зосереджується на базових

інструментах цифрової безпеки (наприклад, автентифікація за допомогою паролів, резервне копіювання даних), у той час як сучасні технології захисту, такі як багатофакторна автентифікація, шифрування, системи виявлення загроз та штучний інтелект, впроваджуються вкрай обмежено. Практики інформування персоналу з питань ІКТ-безпеки залишаються несистемними, а значна частина підприємств взагалі не має формалізованих політик або документів з інформаційної безпеки.

Ідентифіковано ключові виклики для економічної безпеки будівельних підприємств, серед яких – низька цифрова компетентність персоналу, обмежені інвестиції в інноваційну інфраструктуру, фрагментарність підходів до управління цифровими ризиками. Водночас підтверджено наявність потенціалу для розширення сфери застосування штучного інтелекту, автоматизованих систем і робототехніки не лише у виробничих, але й у захисно-інформаційних функціях підприємств.

Перспективами подальших досліджень є розроблення індикаторів цифрової готовності підприємств у контексті економічної безпеки; моделювання взаємозв'язку між рівнем цифровізації та стійкістю підприємств до інформаційних загроз.

Практичне значення отриманих результатів полягає у можливості їх використання для розроблення стратегій цифрової трансформації будівельних підприємств з урахуванням вимог економічної безпеки, удосконалення систем управління інформаційною безпекою, а також впровадження ефективних механізмів оцінювання та мінімізації цифрових ризиків. Запропоновані аналітичні підходи можуть бути використані в процесі формування корпоративної політики щодо впровадження інноваційних технологій, підготовки внутрішніх нормативних документів з питань кіберзахисту, а також при розробці галузевих рекомендацій для підвищення рівня цифрової стійкості підприємств.

Список використаних джерел

1. Чешук В. Сучасні підходи моніторингу економічної безпеки будівельних підприємств: інноваційний аспект. *Економічний часопис Волинського національного університету імені Лесі Українки.* 2019. №1(17). С. 62-67.
2. Воронкова В., Ніколаєнко Є. Цифрова трансформація підприємств як стратегічний інструмент сталого розвитку та економічної стабільності в умовах війни та післявоєнного відновлення. *Цифрова економіка та економічна безпека.* 2025. №1(16). С. 9-17.
3. Бондаренко Д., Калашнікова К. Цифровізація будівельної галузі України: аналіз стану, проблем та перспектив розвитку. *Економіка та суспільство.* 2024. № 65.
4. Марченко О., Коляденко Р. Цифрова трансформація будівельного бізнесу: тенденції та перспективи. Цифрова економіка та економічна безпека. 2023. № 4(04). С. 20-26.
5. Державна служба статистики України. URL: https://ukrstat.gov.ua (дата звернення: 12.06.2025).

References

1. Cheshuk, V. (2019). Suchasni pidkhody monitorynhu ekonomichnoi bezpeky budivelnykh pidpryiemstv: innovatsiinyi aspekt [Modern approaches to monitoring the economic security of construction enterprises: innovative aspect]. *Ekonomichnyi chasopys Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky, 1*(17), 62-67 [in Ukrainian].
2. Voronkova, V., Nikolaienko, Y. (2025). Tsyfrova transformatsiia pidpryiemstv yak stratehichnyi instrument staloho rozvytku ta ekonomichnoi stabilnosti v umovakh viiny ta pisliavoiennoho vidnovlennia [Digital transformation of enterprises as a strategic tool for sustainable development and economic stability in the conditions of war and post-war recovery]. *Tsyfrova ekonomika ta ekonomichna bezpeka, 1*(16), 9-17 [in Ukrainian].
3. Bondarenko, D., Kalashnikova, K. (2024). Tsyfrovizatsiia budivelnoi haluzi Ukrainy: analiz stanu, problem ta perspektyv rozvytku [Digitalization of the construction industry of Ukraine: analysis of the state, problems and development prospects]. *Ekonomika ta suspilstvo,65* [in Ukrainian].
4. Marchenko, O., Koliadenko, R. (2023). Tsyfrova transformatsiia budivelnoho biznesu: tendentsii ta perspektyvy [Digital transformation of the construction business: trends and prospects]. *Tsyfrova ekonomika ta ekonomichna bezpeka, 4*(04), 20-26 [in Ukrainian].
5. State Statistics Service of Ukraine. URL: https://ukrstat.gov.ua [in Ukrainian].

Отримано:	*05.08.2025*	*Beérkezett:*	*2025.08.05*	*Received:*	*05.08.2025*
Прийнято до друку:	*19.08.2025*	*Elfogadva:*	*2025.08.19*	*Accepted:*	*19.08.2025*
Опубліковано:	*30.09.2025*	*Megjelent:*	*2025.09.30*	*Published:*	*30.09.2025*