DOI: https://doi.org/10.32782/2524-0072/2026-85-172

УДК 005.93:004:332.1

ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ «ЗЕЛЕНОЇ» ТРАНСФОРМАЦІЇ

THEORETICAL FOUNDATIONS FOR FORMULATING ENTERPRISE INFORMATION SECURITY POLICY IN THE CONTEXT OF «GREEN» TRANSFORMATION

Косінський Петро Миколайович
доктор філософії, доцент, доцент кафедри економіки,
Луцький національний технічний університет
ORCID: https://orcid.org/0000-0002-3254-2379

Малишко Сергій Олекскандрович
аспірант,
Луцький національний технічний університет
ORCID: https://orcid.org/0009-0003-6989-8517

Kosinskyi Petro, Malyshko Serhii
Lutsk National Technical University

В статті наведено зміст політики інформаційної безпеки. Обґрунтовано роль та значення політики інформаційної безпеки сучасного підприємства в умовах «зеленої» трансформації та з'ясовано, що інтеграція «зелених» технологій, цифрових платформ управління ресурсами, систем моніторингу «зеленого» розвитку лише посилюють її значення. Охарактеризовано загальний стан і тенденцій формування інформаційної безпеки підприємств в умовах «зеленого» розвитку. Наведено підстави стверджувати про відсутність належної кадрової, освітньої основи інформаційної безпеки на вітчизняних підприємствах та наявність системної проблеми у цій сфері. Систематизовано етапи, принципи та завдання формування політики інформаційної безпеки підприємства в умовах «зеленої» трансформації. Сформовано відповідні висновки.

Ключові слова: інформаційна безпека, політика інформаційної безпеки, цифровізація, інформаційно-комунікаційні технології, «зелена» трансформація, «зелений» розвиток.

The processes of "green" transformation of enterprises taking place in our country necessitate the active use of digital tools, technologies, and devices, which increases the level of potential information risks and, accordingly, requires the identification of theoretical foundations for the formation of an information security policy. The absence of a unified approach to the development of an enterprise information security policy and its alignment with environmental objectives in the context of "green" transformation determines the relevance of this study. The article examines scholarly views on the interpretation of the category "information security policy," which indicates its multifaceted nature. The content of the information security policy is defined both in a broad sense and within the context of enterprise activity. The role and significance of the information security policy of a modern enterprise under conditions of "green" transformation are substantiated, and it is established that the integration of "green" technologies, digital resource management platforms, and monitoring systems for sustainable development further enhances its importance. An analysis of the changes in the share of enterprises employing ICT specialists and the share of enterprises providing training for ICT specialists in Ukraine has been conducted. Based on this, the general state and trends in the formation of enterprise information security under conditions of "green" development are characterized. There are grounds to assert the absence of an adequate кадрової and educational foundation for information security at domestic enterprises, as well as the presence of a systemic problem in this area. The stages, principles, and tasks of forming an enterprise information security policy under conditions of "green" transformation are systematized. Relevant conclusions are drawn regarding the orientation of the information security policy in the context of "green" transformation, its impact on enhancing information protection and improving efficiency, which is determined by the level of alignment between the strategic objectives of the enterprise, its information infrastructure, and environmental development priorities.

Keywords: information security, information security policy, digitalization, information and communication technologies, "green" transformation, "green" development.

Постановка проблеми. «Зелена» трансформація національної економічної системи зумовила активізацію процесів цифровізації, що формують нові вимоги до функціонування вітчизняних підприємств, в основу яких закладено принципи раціонального використання ресурсного потенціалу. При цьому, особливого значення набуває питання забезпечення належного рівня інформаційної безпеки, адже вона створює передумови для підвищення ефективності господарської діяльності та конкурентоспроможності підприємства.

Інноваційна модернізація низки вітчизняних підприємств передбачає впровадження «зелених» технологій, обладнання, цифрових платформ управління ресурсами, систем екологічного моніторингу та обробки даних, що, в свою чергу, супроводжується підвищенням рівня інформаційних ризиків, пов'язаних, перш за все, з можливими кіберзагрозами й іншими організаційними недоліками тощо. Відповідно, виникає гостра необхідність поглиблення теоретичних засад формування політики інформаційної безпеки сучасного підприємства з урахуванням специфіки «зеленої» трансформації економіки.

Аналіз останніх досліджень і публікацій. Формування політики інформаційної безпеки підприємства в сучасних умовах привертає значну увагу, як вітчизняних, так і зарубіжних науковців, що обумовлено зростанням ролі інформаційних ресурсів у забезпеченні ефективного функціонування економічних систем та посиленням впливу цифрових технологій на всі сфери господарської діяльності.

Загалом у дослідженнях вітчизняних вчених простежується прагнення до поєднання різних підходів, що дозволяє розглядати політику інформаційної безпеки як багатовимірне явище, інтегроване у систему управління підприємством. Зокрема, В. Тітов, Ю. Кльоц, В. Волинець, Н. Петляк Н. та М. Огородник звертають увагу на прикладні аспекти форування політики інформаційної безпеки на рівні приватного підприємства [1]. О.В Курсик [2] розглядав підходи до формування політики інформаційної безпеки підприємства з огляду на сучасні виклики цифровізації, наголошуючи на необхідності переходу від фрагментарних заходів захисту до комплексних систем управління інформаційною безпекою. Т.О. Каменчук [3] обґрунтовано необхідність узгодження державних і корпоративних підходів до забезпечення інформаційної безпеки підприємства. Д.В. Дячковим [4] запропоновано модель політики інформаційної безпеки на основі концепції «глибинного захисту» та обґрунтовано доцільність багаторівневого підходу до забезпечення безпеки.

У працях зарубіжних дослідників наголошується на необхідності розширеного розуміння інформаційної безпеки, що виходить за межі виключно цифрового середовища, оскільки інформація, зафіксована у фізичних документах, може виступати об'єктом загроз нарівні з електронними ресурсами [5]. Такий підхід актуалізує необхідність формування політики інформаційної безпеки як цілісної системи, що враховує всі можливі канали витоку або втрати інформації.

Також, окремі автори розглядають підходи до формування політики інформаційної безпеки, як складової корпоративної стратегії, що забезпечує узгодженість інформаційних процесів із загальними напрямами розвитку підприємства [6].

Однак, все ж відсутній єдиний підхід до формування політики інформаційної безпеки підприємства та її узгодження з екологічними цілями в контексті «зеленої» трансформації, що ускладнює її реалізацію на практиці.

Мета статті полягає в узагальненні теоретичних положень щодо формування політики інформаційної безпеки вітчизняних підприємств, уточнення її змістовних характеристик, функціонального призначення у системі управління інформаційними ризиками в умовах «зеленої» трансформації економіки.

Виклад основного матеріалу дослідження. З метою запобігання втраті інформаційних ресурсів («витоку» інформації), а також забезпечення ефективності «зеленого» розвитку, насамперед з метою підвищення інвестиційної привабливості та конкурентоспроможності, потреба у формуванні чіткої політики інформаційної безпеки вітчизняних підприємств з кожним роком лише зростає.

Варто взяти до уваги, що «на даний момент відсутнє загальноприйняте визначення для терміна «політика інформаційної безпеки» [7], а тому вважаємо за доцільне розглянути різні погляди щодо його тлумачення, адже це дасть змогу не лише більш глибше осягнути зміст цієї політики, а й зрозуміти чому вона відіграє таку важливу роль для підприємства (табл. 1).

Проведений аналіз підходів до трактування категорії «політика інформаційної безпеки» надав підстави стверджувати, що її зміст варіюється залежно від рівня й функціонального призначення, що, в свою чергу, підкреслює її багатогранність. Зокрема, у широкому розу-

Таблиця 1

Визначення терміна «політика інформаційної безпеки»

Визначення терміна «політика інформаційної безпеки»	Джерело (автор)
У широкому контексті (на рівні держави, галузей економіки або суспільства)	
«Набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз» [8]	Положення про систему захищеного доступу державних органів до мережі Інтернет
«Сукупність керівних принципів, правил, процедур фактичних прийомів, якими об'єкт керується у своїй діяльності» [9]	Ю. Хохлачова
«Своєрідна захищеність найважливіших інтересів індивіда, громадськості та держави, яка може завдати найменші збитки, обумовлені неповнотою, затримкою та неправдивістю інформаційних даних, несприятливим інформаційним впливом, негативними результатами використання новітніх інформаційних технологій, а також несанкціонованим розповсюдженням інформаційних даних» [2]	О.В. Курсик
«Важливий складник політики національної безпеки, що передбачає системну діяльність органів державної влади України щодо надання гарантій інформаційної безпеки особі, соціальним групам і суспільству загалом» [3]	Н.С. Орлова
«Набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз» [10]	В.В. Домарєв; О.В. Гордієнко
«Набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист та розподіл критичної інформації в системі» [10]	А.Я. Страхарчук; В.П. Страхарчук
У контексті діяльності підприємства	
«Політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки» [11]	Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури
«Науково обґрунтована система поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань інформаційного захисту організацій та установ від протиправних дій» [10]	Є.М. Бодюл
«Сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів та технічних, програмних і криптографічних засобів, спрямованих на захист інформаційної інфраструктури організації від випадкового і навмисного втручання в процес її функціонування» [10]	М.Ф. Бондаренко; О.В. Потій; Ю.І. Горбенко
«Ключовий елемент загальної бізнес-стратегії корпорації, який включає адекватну підтримку її стратегічного розвитку, згуртованість інформаційних систем і бізнесу та координацію зусиль з інформаційної безпеки» [10]	В.І. Чубаєвський
«Цілісна система положень (правил, інструкцій, вимог тощо), за допомогою яких керівництво підприємства впливає на забезпечення відповідного стану …, інформаційної безпеки… за рахунок прийняття результативних управлінських рішень» [12]	Р.М. Скриньковський, Н.Р. Костюк, Ж.В. Семчук, О.О. Коропецький
«Серія документів, що відображають вимоги до захисту даних і основні напрямки діяльності компанії щодо безпеки» [1]	В. Тітова, Ю. Кльоц, В. Волинець, Н. Петляк, М. Огородник
«Сукупність нормативних документів, які встановлюють порядок забезпечення безпеки інформації на конкретному підприємстві, а також висувають вимоги до підтримки цього порядку» [13]	А.Ю. Нашинець-Наумова

Джерело: сформовано авторами на основі [1–3; 8–13]

мінні політика інформаційної безпеки має інституційний характер і відіграє важливу роль у забезпеченні стабільності функціонування інформаційного середовища на макрорівні. Її реалізація передбачає застосування комплексу законодавчих документів, правил і принципів, спрямованих на регулювання обробки інформації та захист від можливих загроз різного характеру.

У контексті діяльності підприємства, політика інформаційної безпеки інтерпретується як система регламентованих норм, правил, вимог і процедур, що визначають порядок захисту інформаційних ресурсів та організацію безпечного функціонування інформаційної інфраструктури. Однак, вважаємо варто звернути увагу на те, що у деяких, серед розглянутих нами визначень, політика інформаційної безпеки постає як сукупність внутрішніх нормативних актів і інструкцій, що формалізують вимоги до захисту даних і регламентують поведінку персоналу, а в окремих трактуваннях – її розглядають з точки зору елемента стратегічного управління підприємством, що забезпечує узгодження інформаційних процесів із загальною стратегією розвитку.

На дуку М.О. Мельник, Г.Д. Нікітина та К.О. Мезеневої «політику безпеки інформаційної системи необхідно формалізувати з метою опису поглядів керуючої гілки компанії на суть загроз інформаційній безпеці організації, а також на технології, за допомогою яких можна забезпечити безпеку її інформаційних ресурсів» [14]. Вище наведене дозволяє припустити, що формалізація політики інформаційної безпеки підприємства є передумовою ефективного управління інформаційними ризиками, особливо в умовах впровадження «зелених» інновацій, що супроводжуються використанням інформаційно-комунікаційних систем і технологій.

Деякі дослідники наполягають на впровадженні комплексного підходу до формування політики інформаційної безпеки підприємства, що передбачає розробку відповідної документації, методів захисту інформації, перевірку технічного забезпечення, що для цього використовується тощо. «Розробка такої політики включає в себе виявлення поточних недоліків інформаційної безпеки підприємства, визначення типів загроз, які можуть виникнути через недоліки в захисті інформаційних систем підприємства, а також вибір шляхів і засобів для вирішення існуючих проблем» [1].

Слід розуміти, що цифровізація економіки виступає фактором подвійного впливу на «зелену» трансформацію економічних систем на мікрорівні, адже з одного боку, вона забезпечує розвиток підприємства, а з іншого – підвищує його вразливість до інформаційних загроз. Саме для того, щоб подолати зазначені загрози перед вітчизняними підприємствами і виникає необхідність формування політики інформаційної безпеки, що виконуватиме для них важливу роль інструмента системного управління ризиками, а також забезпечуватиме збалансоване поєднання інноваційного розвитку й належного рівня захищеності інформаційних ресурсів (рис. 1).

Інтеграція «зелених» технологій, цифрових платформ управління ресурсами, систем моніторингу сталого розвитку лише надали ваги інформаційній безпеці, після чого її прийнято розглядати не лише як допоміжний елемент господарської діяльності підприємства, а як один із найважливіших факторів забезпечення його економічного процвітання та конкурентоспроможності.

Проведемо аналіз зміни частки кількості підприємств, що мають найманих фахівців та зміни частки кількості підприємств, що проводили навчання для фахівців у сфері інформаційно-комунікаційних технологій (ІКТ), адже вважаємо їх детермінантами формування ефективної політики інформаційної безпеки підприємства, оскільки вони відображають рівень кадрового забезпечення й інтенсивність розвитку компетенцій у сфері ІКТ, що, у свою чергу, визначає здатність суб’єктів господарювання протидіяти сучасним інформаційним загрозам і забезпечувати належний рівень захищеності інформаційних ресурсів.

Проведений аналіз зміни показників частки підприємств, що мають фахівців у сфері ІКТ та частки підприємств, що проводять навчання для фахівців у сфері ІКТ за період 2018-2023 рр. дозволив зробити низку узагальнень щодо стану та тенденцій формування інформаційної безпеки підприємств у контексті «зеленого» розвитку (рис. 2).

Передусім, динаміка частки підприємств, що мають найманих фахівців у сфері ІКТ, свідчить про нестійку та загалом низхідну тенденцію кадрового забезпечення інформаційної безпеки. Водночас показник частки підприємств, що здійснюють навчання для фахівців у сфері ІКТ, хоча й демонструє певне зростання, залишається доволі низьким. Загалом, така картина дає підстави стверджувати, що на більшості вітчизняних підприємств не сформовано належної кадрової та освітньої основи інформаційної безпеки. Вважаємо,

Рис. 1. Роль політики інформаційної безпеки у господарській діяльності підприємства в умовах «зеленої» трансформації

Джерело: сформовано авторами

що це обмежує можливості підприємств щодо впровадження цифрових й «зелених» технологій, знижує їх інвестиційну привабливість, підвищує ризики втрати даних та порушення безперервності бізнес-процесів.

Таким чином, наведені показники свідчать про наявність системної проблеми у сфері забезпечення інформаційної безпеки вітчизняних підприємств, що проявляється у недостатньому рівні кадрового забезпечення та зумовлює необхідність формування ефективної політики інформаційної безпеки, орієнтованої на успішну реалізацію принципів «зеленого» розвитку.

Концептуальна модель формування політики інформаційної безпеки у системі управління інформаційними ризиками підприємства в умовах «зеленої» трансформації, передбачає систематизацію етапів й, відповідно, принципів і завдань, що розкривають її функціональне призначення, як інструмента забезпечення збалансованого поєднання

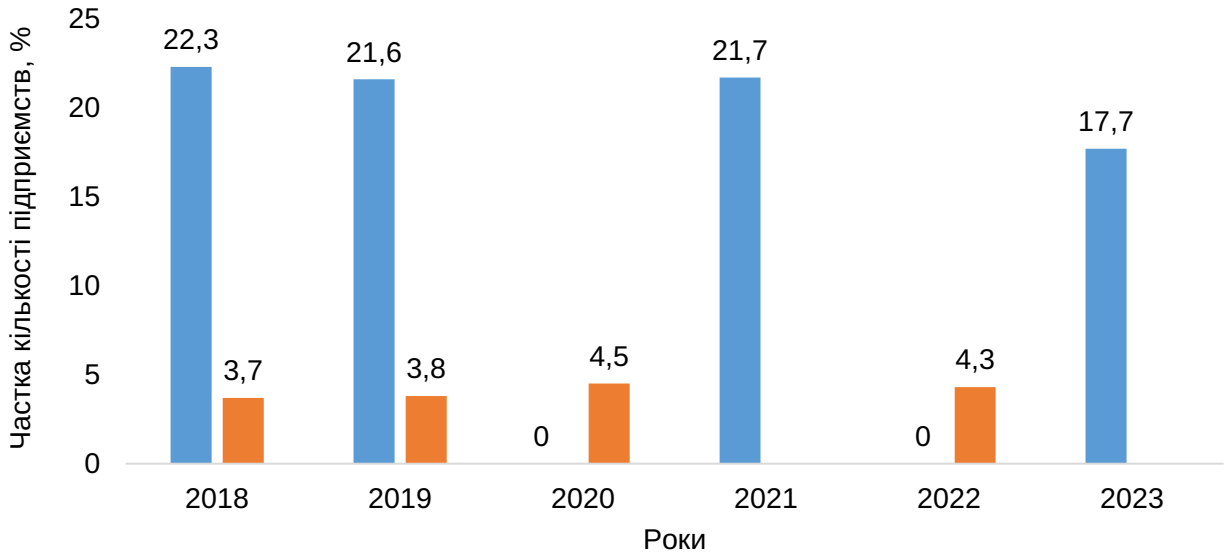

Рис. 2. Аналіз зміни частки підприємств, що мають фахівців у сфері ІКТ та частки підприємств, що проводять навчання для фахівців у сфері ІКТ в Україні за період 2018-2023 рр.

Джерело: сформовано авторами на основі [15]

інформаційного захисту, інноваційного розвитку та подальших напрямків «зеленого» розвитку (табл. 2).

Зазначені в таблиці 2 етапи відображають логічний перехід від фрагментарного забезпечення захисту інформаційних ресурсів до системного управління інформаційними ризиками з урахуванням вимог «зеленої» трансформації економіки, що фактично являє модель структури формування політики інформаційної безпеки підприємства та дозволяє розглядати її не лише як інструмент реагування на загрози, а як інтегрований елемент системи управління підприємством. Такий підхід створює теоретичне підґрунтя для подальшого розвитку методичних засад управління інформаційними ризиками в умовах «зеленої» трансформації економіки.

Висновки. Формування політики інформаційної безпеки підприємства в умовах «зеленої» трансформації слід розглядати як безперервний, багаторівневий процес, спрямований на забезпечення балансу між інноваційним розвитком, екологічною відповідальністю та належним рівнем захищеності інформаційних ресурсів. Встановлено, що її формалізація, інтеграція у систему управління та орієнтація на принципи комплексності, адаптивності й безперервного вдосконалення впливатимуть на підвищення інформаційної захищеності підприємства.

Аналіз показників кадрового забезпечення сфери ІКТ, дозволив виявити недостатній рівень залучення фахівців та їх професійного розвитку, що знижує ефективність реалізації політики інформаційної безпеки й посилює вразливість до сучасних інформаційних загроз на більшості вітчизняних підприємств.

Представлена систематизація основних етапів, принципів і завдань формування політики інформаційної безпеки, розкриває її функціональне призначення як інструмента системного управління інформаційними ризиками. Ефективність такої політики визначається рівнем узгодженості між стратегічними цілями підприємства, його інформаційною інфраструктурою та екологічними пріоритетами розвитку.

Таблиця 2

Етапи, принципи та завдання формування політики інформаційної безпеки підприємства в умовах «зеленої» трансформації

Етапи формування політики	Принципи, яких потрібно дотримуватись	Завдання політики інформаційної безпеки
Ідентифікація інформаційних активів та напрямів «зеленої» трансформації	Комплексне, системне вивчення специфіки функціонування підприємства в умовах «зеленої» трансформації та екологічної релевантності інформаційних потоків	Визначення складу інформаційних ресурсів, що забезпечують функціонування «зелених» технологій; встановлення критичних точок обробки даних; формування реєстру інформаційних активів
Оцінка інформаційних ризиків у контексті «зеленого» розвитку	Дотримання правил превентивності, адаптивності та врахування екологічних факторів ризику	Ідентифікація загроз інформаційній безпеці з урахуванням цифрових та екологічних чинників; оцінювання рівня вразливості інформаційних систем; визначення пріоритетів захисту
Визначення стратегічних напрямів політики інформаційної безпеки	Відповідність загальній стратегії розвитку підприємства, з метою досягнення синергетичного ефекту від впровадження «зелених» технологій	Визначення цілей політики інформаційної безпеки відповідно до стратегії сталого розвитку підприємства; інтеграція безпекових пріоритетів у загальну систему управління
Розробка організаційно-нормативного забезпечення політики	Прозорість, відповідальність та багаторівневий захист, узгодженість дій усіх суб'єктів управління та підвищення надійності захисних механізмів	Формування внутрішніх положень, інструкцій і процедур щодо захисту інформації; розподіл повноважень і відповідальності; встановлення правил доступу до інформаційних ресурсів
Впровадження технічних і управлінських заходів захисту	Багаторівневий захист безперервність та забезпечення ресурсної ефективності	Реалізація засобів технічного захисту інформації; впровадження систем моніторингу та контролю; забезпечення безперервності функціонування інформаційних систем
Підвищення компетентності персоналу	Безперервне навчання, дотримання поведінкової безпеки й відповідальності	Організація навчання працівників у сфері інформаційної безпеки; формування навичок протидії загрозам; тощо
Моніторинг, аудит та адаптація політики інформаційної безпеки	Забезпечення зворотного зв'язку, гнучкості й постійного вдосконалення	Оцінка ефективності політики інформаційної безпеки; проведення аудиту; коригування заходів відповідно до умов «зеленої трансформації

Джерело: сформовано авторами на основі [5; 6]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Тітова В., Кльоц Ю., Волинець В., Петляк Н., Огородник М. Розроблення політики інформаційної безпеки приватного підприємства. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2024. № 3. С. 79–83. DOI: https://doi.org/10.31891/2219-9365-2024-79-10.

2. Курсик О. В. Сучасні підходи до політики інформаційної безпеки. *Регіональні студії.* 2025. № 40. С. 149–153. DOI https://doi.org/10.32782/2663-6170/2025.40.26.

3. Каменчук Т. О. Державна політика України у сфері інформаційної безпеки. *Політикус.* 2025. Вип. 1. С. 46–54. DOI https://doi.org/10.24195/2414-9616.2025-1.7.

4. Дячков, Д. В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захист»". *Підприємництво і торгівля.* 2019. № 25. С. 116–121. DOI: https://doi.org/10.36477/2522-1256-2019-25-17

5. von Solms B., von Solms R. Cybersecurity and information security – what goes where? *Information and Computer Security.* 2018. Vol. 26. № 1. P. 2–9. DOI: https://doi.org/10.1108/ICS-04-2017-0025.

6. Larno S., Seppänen V., Nurmi J. Method framework for developing enterprise architecture security principles. *Complex Systems Informatics and Modeling Quarterly.* 2019. № 20. P. 57–71. DOI: https://doi.org/10.7250/csimq.2019-20.03.

7. Ворохоб М. В., Киричок Р. В., Яскевич В. О., Добришин Ю. Є., Сидоренко С. М. Сучасні перспективи застосування концепції zerotrustпри побудові політики інформаційної безпеки підприємства. *Кібербезпека: освіта, наука, техніка*. 2023. № 1 (21). С. 223–233. DOI: https://doi.org/10.28925/2663-4023.2023.21.223233.

8. Положення про систему захищеного доступу державних органів до мережі Інтернет : Наказ від 15 вересня 2023 р. № 1624/40680 / Міністерство цифрової трансформації України. URL: https://zakon.rada.gov.ua/laws/show/z1624-23/ed20230830#n24 (дата звернення: 17.04.2026).

9. Хохлачова Ю. Політика інформаційної безпеки об'єкта. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2012. № 2 (24). С. 23–29. URL: https://ela.kpi.ua/handle/123456789/8581.

10. Чубаєвський В. І. Стратегічні орієнтири формування корпоративної політики інформаційної безпеки. *Причорноморські економічні студії*. 2021. Вип. 72(2). С. 24–30. DOI: https://doi.org/10.32843/bses.72-28.

11. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 / Кабінет Міністрів України. URL:https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF/ed20190619#n13 (дата звернення: 17.04.2026).

12. Скриньковський Р. М., Костюк Н. Р., Семчук Ж. В., Коропецький О. О. Діагностика політики керівництва у сферах якості, соціальної відповідальності, інформаційної безпеки й охорони праці та механізм забезпечення гідної праці на підприємстві. *Бізнес Інформ*. 2016. № 3. С. 131–137. URL: http://nbuv.gov.ua/UJRN/binf_2016_3_18.

13. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. Київ : Гельветика, 2017. 168 с.

14. Мельник М. О., Нікітин Г. Д., Мезенева К. О. Аналіз побудови моделі політики інформаційної безпеки підприємства. *Системи обробки інформації.* 2017. Вип. 2. С. 126–128. URL: http://nbuv.gov.ua/UJRN/soi_2017_2_26.

15. *Держстат* : офіційний веб-сайт. URL: https://stat.gov.ua/ (дата звернення: 22.04.2026).

REFERENCES:

1. Titova V., Kliots Yu., Volynets V., Petliak N., Ohorodnyk M. (2024) Rozroblennia polityky informatsiinoi bezpeky pryvatnoho pidpryiemstva [Development of information security policy of a private enterprise]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh*, no. 3, pp. 79–83. DOI: https://doi.org/10.31891/2219-9365-2024-79-10. (in Ukrainian)

2. Kursyk O.V. (2025) Suchasni pidkhody do polityky informatsiinoi bezpeky [Modern approaches to information security policy]. *Rehionalni studii*, no. 40, pp. 149–153. DOI: https://doi.org/10.32782/2663-6170/2025.40.26. (in Ukrainian)

3. Kamenchuk T.O. (2025) Derzhavna polityka Ukrainy u sferi informatsiinoi bezpeky [State policy of Ukraine in the field of information security]. *Politykus*, vol. 1, pp. 46–54. DOI: https://doi.org/10.24195/2414-9616.2025-1.7. (in Ukrainian)

4. Diachkov D.V. (2019) Formuvannia modeli polityky informatsiinoi bezpeky na osnovi kontseptsii «hlybynnoho zakhystu» [Formation of an information security policy model based on the "defense in depth" concept]. *Pidpryiemnytstvo i torhivlia*, no. 25, pp. 116–121. DOI: https://doi.org/10.36477/2522-1256-2019-25-17. (in Ukrainian)

5. von Solms B., von Solms R. (2018) Cybersecurity and information security – what goes where? *Information and Computer Security*, vol. 26, no. 1, pp. 2–9. DOI: https://doi.org/10.1108/ICS-04-2017-0025.

6. Larno S., Seppänen V., Nurmi J. (2019) Method framework for developing enterprise architecture security principles. *Complex Systems Informatics and Modeling Quarterly*, no. 20, pp. 57–71. DOI: https://doi.org/10.7250/csimq.2019-20.03.

7. Vorokhob M.V., Kyrychok R.V., Yaskevych V.O., Dobryshyn Yu.Ye., Sydorenko S.M. (2023) Suchasni perspektyvy zastosuvannia kontseptsii zero trust pry pobudovi polityky informatsiinoi bezpeky pidpryiemstva [Modern prospects of applying the zero trust concept in building enterprise information security policy]. *Kiberbezpeka: osvita, nauka, tekhnika*, no. 1 (21), pp. 223–233. DOI: https://doi.org/10.28925/2663-4023.2023.21.223233. (in Ukrainian)

8. Polozhennia pro systemu zakhyshchenoho dostupu derzhavnykh orhaniv do merezhi Internet [Regulation on the system of secure access of public authorities to the Internet]. (2023). Nakaz Ministerstva tsyfrovoi transformatsii

Ukrainy vid 15 veresnia 2023 r. no. 1624/40680. Available at: https://zakon.rada.gov.ua/laws/show/z1624-23/ed20230830#n24 (accessed 17 April 2026). (in Ukrainian)

9. Khokhlachova Yu. (2012) Polityka informatsiinoi bezpeky obiekta [Information security policy of an object]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*, no. 2 (24), pp. 23–29. URL: https://ela.kpi.ua/handle/123456789/8581. (in Ukrainian)

10. Chubaievskyi V.I. (2021) Stratehichni oriientyry formuvannia korporatyvnoi polityky informatsiinoi bezpeky [Strategic guidelines for the formation of corporate information security policy]. *Prychornomorski ekonomichni studii*, vol. 72(2), pp. 24–30. DOI: https://doi.org/10.32843/bses.72-28. (in Ukrainian)

11. Pro zatverdzhennia Zahalnykh vymoh z kiberzakhystu obiektiv krytychnoi infrastruktury [On approval of general requirements for cybersecurity of critical infrastructure facilities]. (2019). Postanova Kabinetu Ministriv Ukrainy vid 19 chervnia 2019 r. no. 518. Available at: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF/ed20190619#n13 (accessed 17 April 2026). (in Ukrainian)

12. Skrynkovskyi R.M., Kostiuk N.R., Semchuk Zh.V., Koropetskyi O.O. (2016) Diahnostyka polityky kerivnytstva u sferakh yakosti, sotsialnoi vidpovidalnosti, informatsiinoi bezpeky y okhorony pratsi ta mekhanizm zabezpechennia hidnoi pratsi na pidpryiemstvi [Diagnostics of management policy in the fields of quality, social responsibility, information security and labor protection and the mechanism for ensuring decent work at the enterprise]. *Biznes Inform*, no. 3, pp. 131–137. URL: http://nbuv.gov.ua/UJRN/binf_2016_3_18. (in Ukrainian)

13. Nashynets-Naumova A.Yu. (2017) Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia [Information security: issues of legal regulation: a monograph]. Kyiv: Helvetyka, 168 p. (in Ukrainian)

14. Melnyk M.O., Nikityn H.D., Mezeneva K.O. (2017) Analiz pobudovy modeli polityky informatsiinoi bezpeky pidpryiemstva [Analysis of building a model of enterprise information security policy]. *Systemy obrobky informatsii*, vol. 2, pp. 126–128. URL: http://nbuv.gov.ua/UJRN/soi_2017_2_26. (in Ukrainian)

15. Derzhavna sluzhba statystyky Ukrainy [State Statistics Service of Ukraine]: ofitsiinyi veb-sait. Available at: https://stat.gov.ua/ (accessed 22 April 2026). (in Ukrainian)

Дата надходження статті: 17.04.2026
Дата прийняття статті: 08.05.2026
Дата публікації статті: 14.05.2026