УДК 338.242.2:004.056
JEL Classification: M21; L21; D81

КІБЕРСТІЙКІСТЬ ПІДПРИЄМСТВА ЯК СТРАТЕГІЧНИЙ ЧИННИК ФОРМУВАННЯ КОНКУРЕНТОСПРОМОЖНОГО ПОТЕНЦІАЛУ В УМОВАХ РИНКОВОЇ НЕСТАБІЛЬНОСТІ

©2025 **ВАСИЛЬЄВ А. С.**

УДК 338.242.2:004.056
JEL Classification: M21; L21; D81

Васильєв А. С.

Кіберстійкість підприємства як стратегічний чинник формування конкурентоспроможного потенціалу в умовах ринкової нестабільності

У статті досліджено кіберстійкість промислових підприємств як стратегічний чинник формування конкурентоспроможного потенціалу в умовах ринкової нестабільності та цифрової трансформації. Обґрунтовано, що стрімке впровадження цифрових технологій – індустріального Інтернету речей, «розумних» виробничих систем, штучного інтелекту, блокчейну та біометричної аутентифікації – створює нові можливості для підвищення ефективності бізнес-процесів, але водночас супроводжується зростанням кіберризиків, які загрожують економічній безпеці підприємств. Визначено, що кіберстійкість охоплює технічні, організаційні та поведінкові компоненти, які у взаємодії забезпечують здатність підприємства протидіяти кіберінцидентам, підтримувати безперервність діяльності та швидко відновлювати критичні функції. Запропоновано організаційно-економічний механізм забезпечення кіберстійкості, що охоплює технічні, управлінські та поведінкові інструменти. Сформовано модель формування кіберстійкості підприємства та визначено її взаємозв'язок із конкурентоспроможним потенціалом. Доведено, що кіберстійкість виступає не лише елементом цифрової безпеки, а й стратегічним ресурсом, який забезпечує адаптивність, інноваційність і довгострокові конкурентні переваги підприємства в умовах ринкової турбулентності. Показано, що високий рівень кіберстійкості прямо корелює зі зростанням конкурентоспроможного потенціалу підприємства, зокрема через підвищення операційної стабільності, інноваційності, фінансової стійкості та репутаційного капіталу. Практична реалізація запропонованих рішень може здійснюватися на різних рівнях – від упровадження комплексних систем кіберзахисту в межах окремих компаній до розроблення галузевих стандартів і створення спільних центрів моніторингу та реагування на кіберінциденти. Це формує основу для довгострокового розвитку промисловості та забезпечення її конкурентоспроможності в умовах зростаючих ризиків цифрової епохи.

Ключові слова: *кіберстійкість, конкурентоспроможний потенціал, ринкова нестабільність, кіберризики, цифрова трансформація, стратегічне управління, кібербезпека, адаптивність підприємства.*

DOI: *https://doi.org/10.32983/2222-0712-2025-4-190-196*

Рис.: *1.* ***Табл.:*** *1.* ***Бібл.:*** *12.*

Васильєв Антон Сергійович *– здобувач, Харківський національний університет імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*

E-mail: *tolst.top@gmail.com*

ORCID: *https://orcid.org/0009-0002-9605-4574*

UDC 338.242.2:004.056
JEL Classification: M21; L21; D81

Vasyliev A. S. Cyber Resilience of an Enterprise as a Strategic Factor in the Formation of Competitive Potential in Conditions of Market Instability

The article examines the cyber resilience of industrial enterprises as a strategic factor in the formation of competitive potential in conditions of market instability and digital transformation. It is substantiated that the rapid introduction of digital technologies – the industrial Internet of Things, smart production systems, artificial intelligence, blockchain and biometric authentication creates new opportunities for increasing the efficiency of business processes, but at the same time is accompanied by an increase in cyber risks that threaten the economic security of enterprises. It is determined that cyber resilience encompasses technical, organizational and behavioral components that, in interaction, ensure the ability of an enterprise to counteract cyber incidents, maintain business continuity and quickly restore critical functions. An organizational and economic mechanism for ensuring cyber resilience is proposed, which encompasses technical, managerial and behavioral tools. A model for the formation of cyber resilience of an enterprise has been developed and its relationship with competitive potential has been determined. It is proved that that cyber resilience is not only an element of digital security, but also a strategic resource that ensures adaptability, innovativeness and long-term competitive advantages of an enterprise in conditions of market turbulence. It has been shown that a high level of cyber resilience directly correlates with the growth of the competitive potential of an enterprise, in particular through increased operational stability, innovativeness, financial stability and reputational capital. The practical implementation of the proposed solutions can be carried out at different levels – from the implementation of comprehensive cyber protection systems within individual companies to the development of industry standards and the creation of joint monitoring and response centers for cyber incidents. This forms the basis for the long-term development of the industry and ensuring its competitiveness in the face of growing risks of the digital age.

Keywords: *cyber resilience, competitive potential, market instability, cyber risks, digital transformation, strategic management, cybersecurity, enterprise adaptability.*

Fig.: *1.* ***Tabl.:*** *1.* ***Bibl.:*** *12.*

Vasyliev Anton S. *– Applicant, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*

E-mail: *tolst.top@gmail.com*

ORCID: *https://orcid.org/0009-0002-9605-4574*

Вступ. Функціонування підприємств у сучасному економічному середовищі відбувається за умов посиленої ринкової турбулентності, яка формується під впливом взаємодії економічних, політичних, технологічних і соціальних трансформацій. Одним із найбільш загрозливих чинників для стабільного розвитку бізнесу стає інтенсивне зростання кіберризиків, здатних призводити до збоїв у операційних процесах, істотних фінансових втрат, погіршення ділової репутації та послаблення конкурентних позицій підприємства. За таких обставин традиційні інструменти забезпечення інформаційної безпеки виявляються недостатньо ефективними, що обумовлює потребу в переході до більш комплексних підходів, зокрема до формування кіберстійкості як здатності організації протистояти цифровим загрозам, адаптуватися до них і оперативно відновлювати функціональну спроможність після інцидентів.

У сучасній науковій парадигмі кіберстійкість дедалі частіше розглядається як стратегічно значущий актив, що забезпечує стабільність функціонування підприємства та підтримання його конкурентних позицій в умовах цифрової турбулентності й невизначеності. За своїм змістом ця категорія виходить за межі суто технічного захисту інформаційних систем, охоплюючи управлінські, організаційні та поведінкові аспекти, які в сукупності формують цілісну систему управління кіберризиками. Водночас у вітчизняних наукових дослідженнях проблематика інтеграції кіберстійкості в механізми формування конкурентоспроможного потенціалу підприємства залишається недостатньо систематизованою та комплексно опрацьованою. Це актуалізує потребу в поглибленому вивченні кіберстійкості як стратегічного чинника формування конкурентних переваг, що створює можливості для розвитку теоретико-методологічних підходів до стратегічного управління та обґрунтування практичних рекомендацій щодо підвищення стійкості підприємств у нестабільному ринковому середовищі.

Аналіз останніх досліджень і публікацій. Проблематика цифрової трансформації промислових підприємств та її впливу на конкурентоспроможність активно представлена в працях зарубіжних і вітчизняних науковців (зокрема Гринько Т. [1], Зінченко О. [2], Краус К. [4], Прохорової В. [7], Субач І. [10], Яковенко Я. [12]), які акцентують увагу на ролі індустріального Інтернету речей, «розумних» виробничих систем, великих даних та автоматизації у підвищенні ефективності бізнес-процесів і гнучкості підприємств. У межах цього напряму значна увага приділяється питанням інтеграції цифрових технологій у виробничу й управлінську діяльність, формуванню цифрових бізнес-моделей, а також удосконаленню систем управління на основі аналітики даних та штучного інтелекту. Дослідження показують, що цифровізація створює підґрунтя для зміцнення конкурентних позицій підприємств, однак суттєво підвищує їхню залежність від стійкості цифрової інфраструктури.

У сучасній науковій літературі сформувався окремий напрям досліджень, присвячений проблематиці економічної та інформаційної безпеки підприємств у контексті цифрової трансформації. У межах цього напряму особлива увага приділяється аналізу впливу процесів цифровізації на зміну бізнес-моделей, управлінських підходів і механізмів забезпечення стійкості підприємств. Зазначені аспекти отримали відображення у працях вітчизняних і зарубіжних учених, зокрема у дослідженнях Безуглої Ю. Є. [7], Кіндзерського Ю. [3], Краус Н. [4], Юхман Я. В. [8], Чубук Л. [11], Яковенко Я. [12]. Дослідники розглядають кібербезпеку як один із ключових компонентів системи економічної безпеки підприємства, підкреслюють зростання кіберризиків, пов'язаних із використанням хмарних сервісів, розподілених обчислень, відкритих мережевих протоколів та інтелектуальних пристроїв. Значний внесок зроблено у розроблення підходів до класифікації кіберзагроз, побудови систем моніторингу, виявлення аномалій, управління інцидентами та формування політик інформаційної безпеки. Водночас у більшості робіт кібербезпека розглядається переважно як технічна або функціональна підсистема, а не як стратегічний чинник формування конкурентоспроможного потенціалу.

У сучасній літературі набирає обертів концепція кіберстійкості (cyber resilience), яка трактується як здатність організації протидіяти кіберінцидентам, підтримувати критичні функції та оперативно відновлюватися після порушень. Значний внесок у розвиток цієї тематики також зробили вітчизняні дослідники Мазулевський О. [5], Омельченко Н. [6], Каліберда М. [1], Прохорова В. [8], Штепа О. В. [4], Федієнко О. [9], Фесьоха В. [10], Яценко О. [11]. Дослідження у цій сфері зосереджені на розробленні моделей кіберстійкості, побудові систем управління кіберризиками, використанні SIEM-платформ, технологій блокчейну, криптографії, біометричної аутентифікації та рішень на основі штучного інтелекту для моніторингу загроз. Водночас у більшості робіт кіберстійкість аналізується фрагментарно, без глибокого розкриття її впливу на структурні компоненти конкурентоспроможного потенціалу підприємства, такі як інноваційний, кадровий, організаційний та репутаційний.

Вітчизняні науковці роблять вагомий внесок у розроблення теоретико-методичних засад управління конкурентоспроможністю та економічною безпекою підприємств в умовах нестабільності ринку, досліджують інноваційний потенціал, диверсифікацію діяльності, адаптивні стратегії розвитку та механізми протидії ризикам. Однак аспекти інтеграції кіберстійкості в систему стратегічного управління та її осмислення як одного з ядрових елементів конкурентоспроможного потенціалу висвітлені недостатньо. Це зумовлює наукову прогалину, пов'язану з потребою комплексного дослідження кіберстійкості промислових підприємств саме крізь призму формування їхньої довгострокової конкурентоспроможності в умовах ринкової нестабільності, що й обумовлює актуальність обраної тематики статті.

Метою статті є теоретичне та практичне обґрунтування значення кіберстійкості як ключового чинника у процесі формування конкурентоспроможного потенціалу підприємства, а також розроблення методичних засад її оцінювання та забезпечення в умовах ринкової турбулентності та нестабільності зовнішнього середовища.

Опис методики проведення дослідження. Методика проведення дослідження ґрунтується на комплексному поєднанні теоретичних, аналітичних та прикладних під-

ходів, що забезпечують всебічне вивчення кіберстійкості підприємства та її впливу на формування конкурентоспроможного потенціалу. На початковому етапі було здійснено теоретико-методологічне опрацювання проблематики, яке передбачало систематизацію наукових підходів до трактування понять, пов'язаних із кіберстійкістю, кіберризиками та конкурентоспроможним потенціалом підприємства. Подальший аналітичний блок був спрямований на дослідження впливу кіберризиків на діяльність підприємств у період ринкової турбулентності. На основі отриманих результатів було розроблено організаційно-економічний механізм забезпечення кіберстійкості, який розглядається як інтегрована система технічних, управлінських і поведінкових інструментів. Наступним етапом стало створення моделі оцінювання кіберстійкості підприємства, у межах якої визначено систему індикаторів, розроблено підхід до нормалізації даних та сформовано інтегральний показник, що відображає рівень кіберстійкості. Завершальним етапом стало узагальнення результатів, їх інтерпретація та формування практичних рекомендацій щодо підвищення кіберстійкості підприємств у сучасних умовах ринкової нестабільності.

Викладення основного матеріалу дослідження. Сучасні промислові підприємства функціонують у складному та динамічному середовищі, для якого характерними є прискорений технологічний прогрес і посилення глобальної економічної та політичної нестабільності. Всеохопна цифрова трансформація, що проникає в усі сфери діяльності компаній, створює передумови для підвищення операційної результативності, зростання організаційної гнучкості та посилення конкурентних переваг на ринку. Водночас активне впровадження цифрових рішень супроводжується появою якісно нових ризиків і загроз економічній безпеці підприємств, масштаб і складність яких суттєво перевищують традиційні виклики минулих періодів.

Ключовим чинником інтенсифікації цифровізації промислового сектора є прагнення суб'єктів господарювання до раціоналізації виробничих процесів, підвищення їх адаптивності до змін зовнішнього середовища та покращення споживчих характеристик продукції й послуг. У зв'язку з цим все більшого поширення набувають концепції «розумного» виробництва, використання індустріального Інтернету речей, автоматизація й роботизація технологічних операцій, а також застосування інструментів аналізу великих масивів даних і сучасної бізнес-аналітики [3]. Разом із поглибленням цифрової інтеграції виробничих систем суттєво зростає значущість проблем інформаційної та кібербезпеки, які перетворюються на критично важливі чинники забезпечення стійкого функціонування та довгострокової стабільності промислових підприємств.

Промислові підприємства дедалі частіше зазнають впливу зростаючих кіберризиків, що проявляються у формі несанкціонованого доступу до інформаційних ресурсів, витоку конфіденційних даних, дестабілізації роботи критично важливих виробничих та управлінських систем, а також інших проявів кіберагресії. Наслідки таких інцидентів можуть бути вкрай суттєвими, оскільки вони призводять не лише до прямих фінансових втрат, але й до погіршення ділової репутації, порушення безперервності операційної діяльності та зниження загального рівня фінансової стійкості підприємства. За цих обставин забезпечення захисту інформаційних активів, цифрових платформ управління та технологічних процесів набуває статусу одного з ключових пріоритетів у системі економічної безпеки промислового сектора [4].

Водночас сучасні компанії функціонують у середовищі, де цифрова трансформація виступає не лише інструментом підвищення ефективності, а й необхідною умовою збереження життєздатності в умовах ринкової нестабільності. Посилення залежності від цифрових технологій об'єктивно супроводжується зростанням кількості та складності кіберінцидентів, які безпосередньо впливають на ключові параметри діяльності підприємств, зокрема на стабільність бізнес-процесів, фінансові результати та імідж на ринку. У такому контексті кіберстійкість трансформується у стратегічно значущий ресурс, що визначає спроможність підприємства забезпечувати безперервність функціонування, своєчасно адаптуватися до зовнішніх загроз та підтримувати конкурентні позиції в умовах цифрової та економічної турбулентності [5].

Кіберстійкість охоплює не лише технічні аспекти захисту, а й організаційні, управлінські та поведінкові компоненти, що формують цілісну систему реагування на кіберризики. Вона забезпечує здатність підприємства протидіяти атакам, мінімізувати наслідки інцидентів та швидко відновлювати критичні функції. Саме тому рівень кіберстійкості дедалі частіше розглядається як один із ключових індикаторів конкурентоспроможного потенціалу підприємства [6].

Аналіз сучасних тенденцій розвитку цифрових технологій дає змогу виокремити кілька перспективних напрямів [1; 8; 12]. По-перше, це впровадження комплексних систем управління інформаційною безпекою, які інтегрують засоби захисту, моніторингу, аналізу та реагування на кіберзагрози. По-друге, стрімко розвиваються технології індустріального Інтернету речей та промислової робототехніки, у яких підвищені вимоги до кіберзахисту. По-третє, зростає роль аналітичних технологій, зокрема рішень на основі штучного інтелекту, які забезпечують моніторинг та автоматизоване реагування на кіберінциденти в режимі реального часу. По-четверте, активно впроваджуються технології шифрування, ідентифікації та біометричної аутентифікації, що гарантують захист конфіденційних даних, промислових секретів та інших критично важливих активів. По-п'яте, технології розподілених реєстрів (блокчейн) забезпечують незмінність і простежуваність інформації про операції, виробничі процеси та транзакції, що підвищує довіру до цифрових платформ і зменшує ризики фальсифікацій.

Вплив цифрових технологій на кіберстійкість та конкурентоспроможний потенціал підприємства наведено у табл. 1.

Таким чином, сучасний стан і ключові тенденції розвитку цифрових технологій у сфері економічної безпеки промисловості свідчать про зростання потреби у комплексних рішеннях, спрямованих на захист інформаційних систем, даних і виробничих процесів від кіберзагроз. Використання передових цифрових інструментів стає кри-

Таблиця 1

Вплив цифрових технологій на кіберстійкість і конкурентоспроможний потенціал підприємства

Цифрова технологія / інструмент	Вплив на кіберстійкість підприємства	Вплив на конкурентоспроможний потенціал
SIEM-системи (моніторинг та реагування)	Забезпечують централізований контроль, виявлення аномалій, швидке реагування на інциденти	Підвищують стабільність бізнес-процесів, зменшують ризики простоїв та фінансових втрат
Індустріальний інтернет речей (IIoT)	Вимагає підвищеного рівня захисту пристроїв та мереж, впровадження шифрування та аутентифікації	Оптимізує виробництво, підвищує продуктивність, скорочує витрати
Штучний інтелект та машинне навчання	Автоматизують виявлення загроз, прогнозують ризики, забезпечують проактивний захист	Підсилюють інноваційність, прискорюють прийняття рішень, підвищують якість управління
Блокчейн	Гарантує незмінність даних, прозорість транзакцій, захист ланцюгів постачання	Підвищує довіру партнерів, зменшує ризики шахрайства, зміцнює репутацію
Біометрична аутентифікація	Забезпечує високий рівень контролю доступу до критичних систем	Зменшує ризики внутрішніх загроз, підвищує безпеку інтелектуальної власності
Системи резервування та відновлення	Забезпечують безперервність бізнесу у разі інцидентів	Мінімізують втрати, підвищують стійкість до зовнішніх шоків

Джерело: сформовано автором на основі [1–12]

тично важливим чинником формування кіберстійкості та довгострокової конкурентоспроможності промислових компаній.

У відповідь на зростання рівня кіберзагроз підприємства дедалі активніше орієнтуються на впровадження комплексних цифрових рішень у сфері захисту інформаційних ресурсів [2; 10]. Особливе місце серед них посідають інтегровані системи управління інформаційною безпекою, зокрема платформи класу SIEM, які забезпечують централізовану акумуляцію даних, безперервний моніторинг подій та оперативне реагування на ознаки потенційних інцидентів. Використання інструментів інтелектуальної аналітики й алгоритмів машинного навчання в межах таких систем розширює можливості виявлення складних, малопомітних і комбінованих атак, а також сприяє автоматизації процесів запобігання та нейтралізації загроз. У результаті це дозволяє суттєво підвищити результативність управління інформаційною безпекою та зміцнити загальний рівень кіберстійкості підприємства [9].

Значну увагу приділено захисту «розумних» виробничих систем і пристроїв індустріального інтернету речей. З цією метою підприємства впроваджують спеціалізовані програмно-технічні рішення, оснащені вбудованими інструментами криптографічного захисту, багаторівневої аутентифікації та диференційованого контролю доступу до інформаційних і виробничих ресурсів.

Технології блокчейн сприяють підвищенню прозорості та захищеності ланцюгів постачання, виробничих операцій і фінансових транзакцій, що дозволяє ефективно протидіяти шахрайству та несанкціонованим втручанням.

Застосування аналітичних інструментів, побудованих на технологіях штучного інтелекту, створює умови для безперервного контролю кіберзагроз, своєчасного виявлення аномальних подій та автоматизованого реагування на атаки у цифровому середовищі. Такий підхід істотно зміцнює рівень кіберстійкості підприємств, забезпечуючи їхню здатність підтримувати стабільність функціонування та знизити ймовірність виникнення та негативні наслідки інцидентів, пов'язаних із порушенням інформаційної безпеки [12].

Кіберстійкість виступає центральним елементом, який поєднує технічні, організаційні та поведінкові компоненти системи економічної безпеки підприємства (рис. 1). Вона формує основу для забезпечення безперервності бізнес-процесів, підвищення операційної стабільності та мінімізації наслідків кіберінцидентів. У результаті кіберстійкість безпосередньо впливає на ключові складові конкурентоспроможного потенціалу – інноваційність, ефективність, репутацію та адаптивність підприємства в умовах ринкової нестабільності.

Кіберстійкість стає інтегральною характеристикою конкурентоспроможного потенціалу, оскільки визначає здатність підприємства зберігати ефективність, інноваційність та фінансову стабільність у період цифрових загроз. Підприємства, які впроваджують комплексні системи кіберзахисту та цифрової аналітики, демонструють вищий рівень операційної надійності, швидше адаптуються до змін і формують стійкі конкурентні переваги.

Цифрова трансформація виробничих процесів, систем управління та бізнес-моделей суттєво змінює підходи до забезпечення економічної безпеки промислових підприємств. Для ефективного протидіяння новим викликам компаніям необхідно формувати комплексні стратегії впровадження цифрових рішень, у центрі яких має бути побудова всеосяжної системи управління інформаційною безпекою [11]. Інтеграція SIEM-платформ, використання аналітики, машинного навчання, технологій шифрування, багатофакторної аутентифікації та блокчейну створює основу для надійного захисту інформаційних активів і виробничих процесів. Синергія SIEM-платформ, спеціалізованих засобів захисту пристроїв індустріального Інтернету речей, криптографічних технологій та механізмів багатофакторної ав-

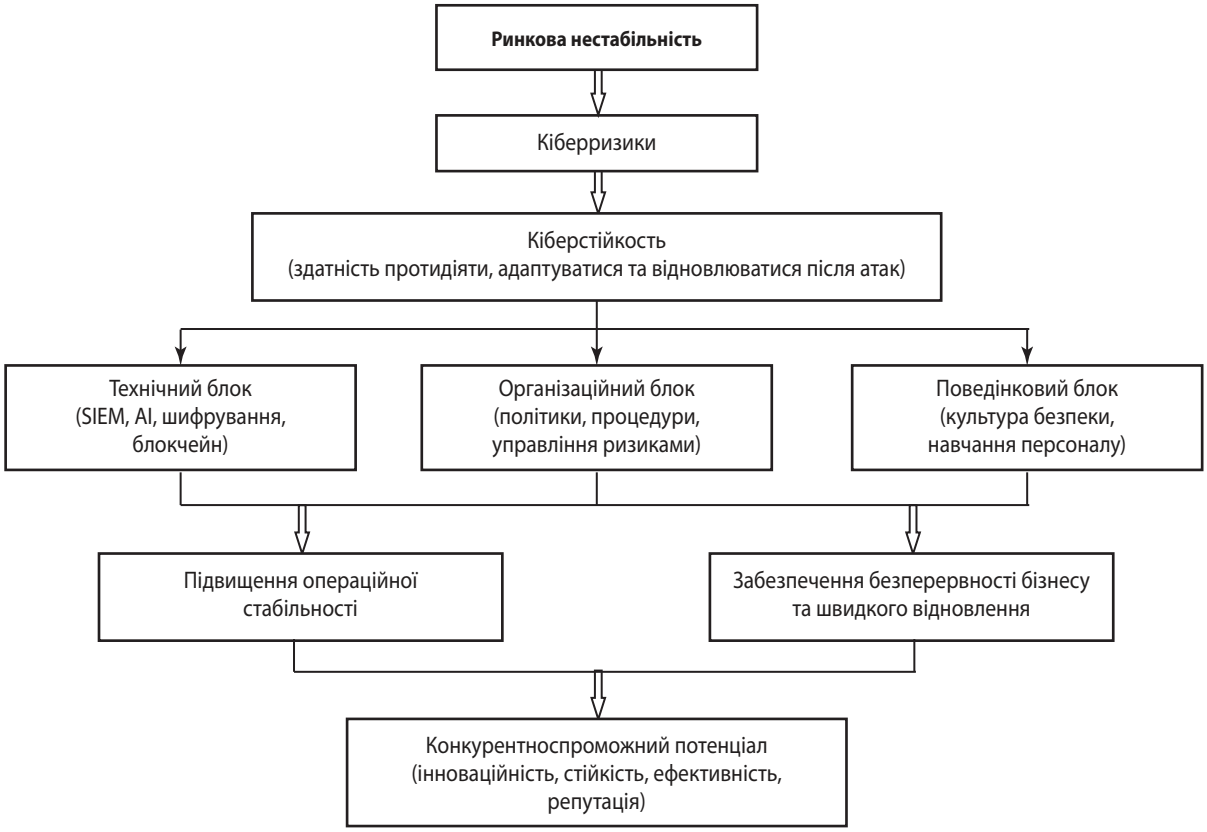

Рис. 1. Модель формування кіберстійкості підприємства

Джерело: сформовано автором на основі [1–12]

тентифікації створює багаторівневу систему кіберзахисту, здатну ефективно протистояти складним і комбінованим загрозам та забезпечувати стабільність і безперервність виробничих процесів. Застосування інструментів штучного інтелекту сприяє переходу від переважно реактивних методів реагування до проактивних моделей управління ризиками, що суттєво підвищує адаптивність підприємств і зміцнює їхню стійкість в умовах динамічної ринкової нестабільності.

Комплексний підхід до управління ризиками, впровадження систем резервування та відновлення, регулярне тестування сценаріїв реагування на надзвичайні ситуації формують фундамент для підвищення економічної стійкості підприємств. Запровадження зазначених рішень сприяє посиленню конкурентних переваг підприємств, зростанню рівня їх фінансової стійкості та забезпеченню довгострокової конкурентоспроможності промислових компаній в умовах посилення цифрових загроз [7].

Запропонований комплекс рекомендацій щодо впровадження і результативного використання сучасних цифрових технологій, спрямованих на посилення економічної безпеки промислових підприємств, характеризується високою практичною значущістю та може бути використаний не лише на рівні окремих суб'єктів господарювання, а й у межах галузевих структур і промислового комплексу в цілому. Для окремих підприємств комплексне впровадження таких підходів створює умови для формування надійної системи захисту критично важливих інформаційних ресурсів, виробничих процесів та фінансово-господарської діяльності. Використання інтегрованих SIEM-платформ, спеціалізованих рішень для «розумних» виробничих систем, технологій шифрування та біометричної ідентифікації персоналу забезпечує належний рівень кіберстійкості підприємства та знижує ймовірність фінансових втрат і репутаційних ризиків [1–4; 8].

Застосування передових аналітичних інструментів на основі штучного інтелекту та машинного навчання дає змогу підприємствам здійснювати комплексний моніторинг ризиків, своєчасно виявляти аномальні події та автоматизувати реагування на інциденти інформаційної безпеки. Це суттєво підвищує ефективність і швидкість управління економічною безпекою в умовах постійного зростання кіберзагроз. Реалізація цілісного підходу до управління ризиками та забезпечення безперервності бізнес-процесів, що включає впровадження систем резервування, відновлення та регулярне тестування сценаріїв реагування, формує міцну основу для довгострокового стабільного розвитку підприємств.

На галузевому рівні запропоновані рішення мають значний потенціал для масштабування та поширення. Розроблення галузевих стандартів і методичних рекомендацій щодо впровадження сучасних цифрових інструментів економічної безпеки сприятиме створенню єдиної системи протидії кіберзагрозам у межах усієї виробничої екосистеми. Крім того, формування спільних центрів моніторингу, аналізу та реагування на інциденти, що об'єднуватимуть

ключових учасників ринку, забезпечить синергетичний ефект і підвищить загальний рівень кіберстійкості промисловості. Це також сприятиме обміну досвідом, поширенню кращих практик і підвищенню професійної компетентності в сфері кіберзахисту.

Отже, практична реалізація комплексного підходу до цифровізації систем економічної безпеки промислових підприємств може здійснюватися на різних рівнях – від упровадження інноваційних рішень у межах окремих компаній до розроблення галузевих стандартів та спільних ініціатив. Такий підхід забезпечує надійний захист ключових активів, виробничих процесів і фінансово-господарської діяльності, створюючи умови для сталого розвитку промисловості в умовах зростаючих ризиків цифрової трансформації.

Висновок. Цифрова трансформація промислових підприємств відкриває широкі можливості для зростання їхньої ефективності та посилення конкурентних позицій, проте водночас породжує новий спектр ризиків, пов'язаних із наростанням кіберзагроз. Це актуалізує потребу у переосмисленні та модернізації системи економічної безпеки підприємств, орієнтованої на формування високого рівня кіберстійкості як визначального стратегічного чинника їхнього сталого розвитку. Кіберстійкість охоплює технічні, організаційні та поведінкові компоненти, які у взаємодії формують здатність підприємства протидіяти кіберінцидентам, підтримувати безперервність бізнес-процесів та оперативно відновлювати критичні функції. Саме інтеграція цих компонентів забезпечує стійкість підприємства до зовнішніх цифрових загроз і визначає його здатність адаптуватися до умов ринкової нестабільності.

Аналіз сучасних цифрових технологій показав, що ключовими чинниками формування кіберстійкості підприємств виступають інтегровані SIEM-платформи, спеціалізовані рішення для захисту індустріального інтернету речей, системи шифрування та біометричної аутентифікації, а також аналітичні інструменти, побудовані на основі штучного інтелекту. Їхнє впровадження забезпечує можливість проактивного управління ризиками, своєчасного виявлення аномальних подій та автоматизації процесів реагування на кіберінциденти. Це, своєю чергою, істотно посилює рівень захищеності виробничих процесів та інформаційних активів, створюючи умови для стабільного функціонування підприємств у цифровому середовищі.

Встановлено, що кіберстійкість має прямий вплив на конкурентоспроможний потенціал підприємства, оскільки забезпечує стабільність операційної діяльності, зменшує ризики фінансових втрат, зміцнює репутацію та підвищує довіру з боку партнерів і споживачів. Підприємства, які впроваджують комплексні системи кіберзахисту, демонструють вищу адаптивність, інноваційність та здатність до довгострокового розвитку в умовах цифрової турбулентності.

Реалізація запропонованих підходів може здійснюватися на різних управлінських рівнях – від упровадження цифрових рішень у діяльність окремих підприємств до розроблення галузевих стандартів і створення координаційних центрів спільного моніторингу та реагування на кіберінциденти. Така багаторівнева модель сприяє виникненню синергетичного ефекту, підвищує сукупний рівень кіберстійкості промислового сектора та створює передумови для його стабільного розвитку в умовах посилення цифрових ризиків.

Отже, кіберстійкість доцільно трактувати не лише як елемент системи інформаційної безпеки, а як стратегічно значущий ресурс, що визначає спроможність підприємства зберігати та зміцнювати конкурентні позиції в умовах ринкової нестабільності. Її цілеспрямований розвиток виступає ключовою передумовою забезпечення економічної безпеки, зростання результативності господарської діяльності та формування довгострокових конкурентних переваг промислових компаній у цифровій економіці.

ЛІТЕРАТУРА

1. Гринько Т., Гвініашвілі Т., Каліберда М. Я. Стратегічне управління підприємством в умовах цифрової економіки. *Економіка та суспільство.* 2023. № 50.
DOI: https://doi.org/10.32782/2524-0072/2023-50-71

2. Зінченко О. Адаптивні стратегії підприємств у цифровому середовищі. *Проблеми економіки.* 2021. № 3 (49). P. 110–116.
DOI: https://doi.org/10.32983/2222-0712-2021-3-110-116

3. Кіндзерський Ю. В. Кібербезпека і становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Національного гірничого університету.* 2020. № 3. P. 18–27.
DOI: https://doi.org/10.33271/ebdut/71.018

4. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability.* 2022. №3. P. 26–37.
DOI: https://doi.org/10.31649/ins.2022.3.26.37

5. Мазулевський О., Назар Ж. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2024. Т. 51. № 3. P. 34–40.

6. Омельченко Н. О. Концептуальні засади та основні характеристики кіберстійкості компаній. *Цифрова економіка та економічна безпека.* 2024. № 6 (15). P. 300–307.

7. Прохорова В. В., Безугла Ю. Є., Грицай О. Ю. Процесний підхід в управлінні цифровими змінами на підприємствах в умовах циркулярної економіки. *Економічний вісник Дніпровської політехніки; Economic Bulletin of Dnipro University of Technology.* 2024.
DOI: https://doi.org/10.33271/ebdut/87.131

8. Прохорова В. В., Юхман Я. В., Янчак Ю. О. Управління трансформацією підприємств на основі цифрової когерентності. *Бізнес Інформ.* 2024. Т. 6. № 557. P. 104–111.
DOI: https://doi.org/10.32983/2222-4459-2024-6-104-111

9. Федієнко О. П. Міжнародні стандарти оцінки кіберстійкості. *Інформація і право.* 2024. № 3 (50). P. 124–135. DOI:
DOI: 10.37750/2616-6798.2024.3(50).311680

10. Фесьоха В., Субач І. Концептуальна основа підвищення кіберстійкості інформаційно-комунікаційних систем в умовах еволюції кіберзагроз. *Кібербезпека: освіта, наука, техніка.* 2025. № 4 (28). P. 511–528.
DOI: https://doi.org/10.28925/2663-4023.2025.28.856

11. Чубук Л. П., Яценко О. В., Овандер Н. Л. Вплив цифрової економіки на зміну моделей бізнесу та фінансового управління: інституціоналізація цифрових трансформацій. *Економіка. Менеджмент. Бізнес.* 2024. № 1. P. 58–64.
DOI: 10.31673/24158089.2024.010008

12. Яковенко Я. Ю., Білик М. Ю., Олійник Є. В. Цифрова трансформація бізнес-структур: стратегічні орієнтири в епоху

інновацій та технологічних змін. *Економічний простір.* 2024. № 190. P. 355–360.
DOI: 10.32782/2224-6282/190-63

REFERENCES

Chubuk L. P., Yatsenko O. V. & Ovander N. L. (2024). Vplyv tsyfrovoi ekonomiky na zminu modelei biznesu ta finansovoho upravlinnia: instytutsionalizatsiia tsyfrovykh transformatsii [Impact of the digital economy on changing business models and financial management: institutionalization of digital transformations]. *Ekonomika. Menedzhment. Biznes*, *1*, 58–64. https://doi.org/10.31673/24158089.2024.010008

Fediienko O. P. (2024). Mizhnarodni standarty otsinky kiberstiikosti [International standards for assessing cyber resilience]. *Informatsiia i pravo*, *3 (50)*, 124–135.

Fesokha V. & Subach I. (2025). Kontseptualna osnova pidvyshchennia kiberstiikosti informatsiino-komunikatsiinykh system v umovakh evoliutsii kiberzahroz [Conceptual framework for improving the cyber resilience of information and communication systems in the context of the evolution of cyber threats]. *Kiberbezpeka: osvita, nauka, tekhnika*, *4 (28)*, 511–528. https://doi.org/10.28925/2663-4023.2025.28.856

Hrynko T., Hviniashvili T. & Kaliberda M. Ya. (2023). Stratehichne upravlinnia pidpryiemstvom v umovakh tsyfrovoi ekonomiky [Strategic management of the enterprise in the conditions of the digital economy]. *Ekonomika ta suspilstvo*, *50*. https://doi.org/10.32782/2524-0072/2023-50-71

Kindzerskyi Yu. V. (2020). Kiberbezpeka i stanovlennia tsyfrovoi ekonomiky: problemy vzaiemozviazku [Cybersecurity and the formation of the digital economy: problems of interconnection]. *Ekonomichnyi visnyk Natsionalnoho hirnychoho universytetu*, *3*, 18–27. https://doi.org/10.33271/ebdut/71.018

Kraus K. M., Kraus N. M. & Shtepa O. V. (2022). Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu [Digital transformation of cybersecurity at the micro level under martial law]. *Innovation and Sustainability*, *3*, 26–37. https://doi.org/10.31649/ins.2022.3.26.37

Mazulevskyi O. & Nazar Zh. (2024). Otsinka potochnoho stanu kiberstiikosti z urakhuvanniam sytuatsii u kiberprostori [Assessment of the current state of cyber resilience taking into account the situation in cyberspace]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, *3*(51), 34–40.

Omelchenko N. O. (2024). Kontseptualni zasady ta osnovni kharakterystyky kiberstiikosti kompanii [Conceptual principles and main characteristics of cyber resilience of companies]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, *6 (15)*, 300–307.

Prokhorova V. V., Bezuhla Yu. Ye. & Hrytsai O. Yu. (2024). Protsesnyi pidkhid v upravlinni tsyfrovymy zminamy na pidpryiemstvakh v umovakh tsyrkuliarnoi ekonomiky [Process approach in managing digital changes at enterprises in the conditions of circular economy]. *Ekonomichnyi visnyk Dniprovskoi politekhniky; Economic Bulletin of Dnipro University of Technology*. https://doi.org/10.33271/ebdut/87.131

Prokhorova V. V., Yukhman Ya. V. & Yanchak Yu. O. (2024). Upravlinnia transformatsiieiu pidpryiemstv na osnovi tsyfrovoi koherentnosti [Management of enterprise transformation based on digital coherence]. *Biznes Inform*, *557*(6), 104–111.

Yakovenko Ya. Yu., Bilyk M. Yu. & Oliinyk Ye. V. (2024). Tsyfrova transformatsiia biznes-struktur: stratehichni oriientyry v epokhu innovatsii ta tekhnolohichnykh zmin [Digital transformation of business structures: strategic orientations in the era of innovation and technological changes]. *Ekonomichnyi prostir*, *190*, 355–360. https://doi.org/10.32782/2224-6282/190-63

Zinchenko O. (2021). Adaptyvni stratehii pidpryiemstv u tsyfrovomu seredovyshchi [Adaptive strategies of enterprises in the digital environment]. *Problemy ekonomiky*, *3 (49)*, 110–116.

Стаття надійшла до редакції 25.10.2025 р.
Статтю прийнято до публікації 11.11.2025 р.
Оприлюднено 01.02.2026 р.