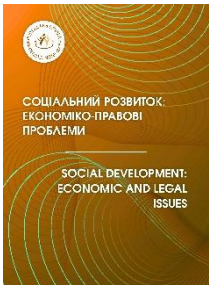
e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

https://www.eu-scientists.com/index.php/sdel



Управління інформаційною безпекою у ланцюгах постачання: ризики цифрової взаємозалежності, моделі довіри та стратегії кіберстійкості

Інна Я. Іпполітова [1]* Марина А. Мащенко [2]
Євгеній М. Іпполітов [3]

[1] *Національний технічний університет «Харківський політехнічний інститут» (Україна). Доцент кафедри підприємництва, торгівлі і логістики, канд. екон. наук, доцент.*

[2] *Національний технічний університет «Харківський політехнічний інститут» (Україна). Завідувачка кафедри підприємництва, торгівлі і логістики, д-р екон. наук, професор.*

[3] *Національний технічний університет «Харківський політехнічний інститут» (Україна). Здобувач третього рівня вищої освіти кафедри підприємництва, торгівлі і логістики.*

*** *Автор-кореспондент,*** e-mail: inna.ippolitova@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3083-6018/2025.7-8.04

АНОТАЦІЯ

Стаття присвячена дослідженню питання управління інформаційною безпекою в ланцюгах постачання. В центрі уваги — аналіз загроз кібербезпеки, оцінка моделей довіри між учасниками ланцюга. Окрема увага приділена стратегіям кіберстійкості, які дозволяють організаціям збільшити здатність до виявлення, стримування, реагування та відновлення після кіберінцидентів, пов'язаних із зовнішніми або внутрішніми контрагентами. Мета дослідження – розробка напрямів щодо створення безпечних та тривких цифрових ланцюгів постачання, з урахуванням сучасних технологічних тенденцій. У ході наукового дослідження застосовувалися загальнонаукові методи пізнання, зокрема аналіз та синтез, індукція й дедукція, порівняльний метод, системний підхід, метод моделювання. Розглянуто дефініцію ланцюга постачання в умовах цифрової трансформації. Впорядковано основні небезпеки цифрової взаємозалежності між суб'єктами ланцюгів постачання, з урахуванням багатошарової структури постачальницьких екосистем. Досліджено моделі довіри як основу інформаційної взаємодії у цифрових ланцюгах. Визначено слабкі місця в ланцюгах постачання, що можуть бути використані як вектори кібератак, враховуючи «вразливі місця» серед надавачів послуг і програмного забезпечення. Для узгоджених дій усіх учасників розглянуто принципи кіберстійкості у ланцюгах постачання. Визначено стратегії кіберстійкості в керуванні ланцюгами постачання, зокрема, концепції та підвалини кіберстійкості у ланцюгах постачання. Проаналізовано стратегії виявлення, реагування та відновлення після кіберінцидентів. Для структурування управлінських та технічних заходів для зменшення кіберзагроз у складних цифрових ланцюгах постачання запропоновано шляхи вдосконалення керування кіберризиками в ланцюгах постачання на основі адаптивних моделей безпеки та стратегій кіберстійкості. Практична цінність даного дослідження дає змогу сформувати цілісне уявлення про сучасні кіберзагрози, побудувати ефективні стратегії захисту в умовах цифрової взаємозалежності та підвищити кіберстійкість постачальницьких екосистем.

КЛЮЧОВІ СЛОВА

ланцюг постачання, цифровізація, інформаційна безпека, модель довіри, аудит кібербезпеки, кіберстійкість, стратегія, кіберризики, інтеграція.

e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

https://www.eu-scientists.com/index.php/sdel

Information Security Management in Supply Chains: Digital Interdependence Risks, Trust Models, and Cyber Resilience Strategies

Inna Ippolitova [1]* ● Maryna Mashchenko [2] ● Yevhenii Ippolitov [3]

[1] *National Technical University "Kharkiv Polytechnic Institute" (Ukraine). Associate Professor at the Business, Trade and Logistics Department, PhD in Economics, Associate Professor.*

[2] *National Technical University "Kharkiv Polytechnic Institute" (Ukraine). Head of Business, Trade and Logistics Department, Doctor of Sciences (Economics), Professor.*

[3] *National Technical University "Kharkiv Polytechnic Institute" (Ukraine). PhD Student at the Business, Trade and Logistics Department.*

*** *Corresponding Author,*** e-mail: inna.ippolitova@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3083-6018/2025.7-8.04

ABSTRACT

This work is devoted to exploring information security management in supply chains. It focuses on assessing cyberthreat risks. Particular stress is given to cyber resilience strategies that enable organizations to enhance their ability to detect, contain, react to, and recover from cyber incidents involving external or internal actors. The study's objective is to create suggestions for building secure and resilient digital supply chains, accounting for current technological advancements. The scientific investigation employed broad scientific methods of cognition, encompassing analysis and synthesis, induction and deduction, comparative approaches, a systems approach, and modeling methods. The findings of the study show that digital interdependence in supply chains substantially elevates cyber risks; thus, effective information security management demands the execution of dynamic trust models, consistent monitoring, and thorough cyber resilience strategies. The idea of supply chains within digital transformation is examined. The central perils to digital interdependence between supply chain entities are structured, considering the multilayered architecture of supply ecosystems. Trust models are examined as the basis for information interaction in digital chains. Vulnerable aspects in supply chains, which may function as cyberattack vectors, are pinpointed, analyzing the "critical areas" amongst service and software vendors. The notions of cyber resilience in supply chains are discussed for shared actions from all stakeholders. Cyber resilience tactics in supply chain management are identified, specifically the concepts and principles of cyber resilience in supply chains. Approaches for identifying, reacting to, and recovering from cyber incidents are explored. To structure managerial and technical responses to reduce cyber threats in complex digital supply chains, recommendations for enhancing cyber risk management in supply chains founded on adaptive security models and cyber resilience plans are proposed. The practical advantage of this research permits us to construct a comprehensive view of current cyber risks, devise effective protection strategies within digital interdependence, and strengthen the cyber resilience of supply ecosystems.

KEYWORDS

supply chain, digitalization, information security, trust model, cybersecurity audit, cyber resilience, strategy, cyber risks, integration.

1. Вступ

В сучасних умовах цифрової трансформації бізнесу ланцюги постачання швидко перетворюються на складні кіберфізичні системи, що охоплюють десятки, а інколи й сотні учасників – від місцевих підрядників до глобальних постачальників хмарних технологій. Взаємодія між ними базується на обміні даними, спільному використанні інформаційних ресурсів та інфраструктури, що суттєво підвищує рівень цифрової взаємозалежності. Разом із новими можливостями це породжує й нові ризики: порушення інформаційної безпеки на будь-якій дільниці ланцюга здатне спричинити масштабні наслідки для всієї мережі — від фінансових втрат до повної зупинки бізнес-процесів.

Збільшення частоти й складності кібератак на ланцюги постачання засвідчує, що звичні підходи до захисту інформації вже не відповідають сучасним викликам. У таких умовах першорядного значення набуває формування нових моделей довіри, що базуються на принципах постійної перевірки (Zero Trust), прозорості дій учасників та багатошарового моніторингу. Окрім того, важливою складовою кібербезпеки стає стратегічна кіберстійкість — здатність організації пристосовуватися до загроз, вчасно виявляти атаки та ефективно відновлюватися після інцидентів.

2. Огляд літературних джерел

Загалом, питання управління інформаційною безпекою в ланцюгах постачання досить вивчено у вітчизняній літературі. Значний вклад у дослідження цієї теми зробив В. Котляров [1, с. 66], котрий у своєму дослідженні зосередив увагу на побудові надійної системи захисту інформації, що має базуватися на своєчасній ідентифікації небезпек інформаційній безпеці. О. В. Бондар-Підгурська, І. І. Хоменко [2, с. 108] наголошували на збільшенні важливості, ролі та значущості кібербезпеки для функціонування та розвитку підприємств малого та середнього бізнесу в умовах нових викликів і загроз. М. А. Мащенко, Є. М. Іпполітов [3] запропонували послідовність імплементації стандарту ISO/IEC 27001 на підприємстві, визначили можливі строки його впровадження та відповідальних. Авторами окреслено ключові щаблі створення стратегії посилення інформаційної безпеки підприємства, що дасть змогу підприємству вибудувати результативну систему управління інформаційною безпекою, звести до мінімуму ризики інформаційних інцидентів. А. Ясінська [4] навела характеристику різновидів захисту інформації на документальному й технічному рівнях. Дослідила різновиди методів та інструментів заради збільшення захисту, які доцільно застосовувати, їх взаємозв’язок з інформаційними джерелами та розпорядниками інформації. Г.В. Осокін [5] довів, що цифрові інструменти забезпечують підвищення ефективності, прозорості та гнучкості ланцюгів постачання, сприяючи адаптації бізнес-моделей до швидко мінливих ринкових умов. В.В. Лісіца, О.М. Михайленко, О.В. Ротенберг [6, с. 99] досліджували ключові аспекти формування цифрових ланцюгів поставок, їх переваг та ймовірних ризиків, а також напрямів використання цифрових технологій у логістиці та управлінні глобальними ланцюгами поставок.

Моделі довіри досліджували О. Б. Придибайло, Р. В. Придибайло, В. О. Яскевич, Ю. В. Яскевич [7, с. 7], котрі детально описали ключові логічні компоненти АНД, зокрема механізм політики та адміністратор політики, та зазначено їхню взаємодію у творенні безпечного середовища. Авторами запропоновано підходи до впровадження АНД для робочих процесів в корпоративних середовищах: покращене керування ідентифікацією, логічну мікросегментацію та сегментацію на основі мережі. Кожен з цих підходів має свої переваги та враховуються залежно від потреб індивідуальної організації. А. В. Куліковський [8, с. 85] розглядав доцільність та перспективи використання технології блокчейн у сфері інформаційної.

Питання кіберстійкості вивчали О. Галушко, Т. Селівьорстова [9, с. 537] проаналізували головні види ризиків та кіберзагроз в ланцюгах постачань, зокрема питання безпеки сторонніх постачальників. Авторами запропоновано заходи щодо усунення кіберризиків та поліпшення кібербезпеки в управлінні ланцюгами постачань. А. Т. Погребняк, Ю. В. Неміш, Г. Павловські, С. Г. Шевченко, Ю. Є. Тиркало [10, с. 10] розкрили ключові теоретичні положення і практичні аспекти, які стосуються питань безпеки та особливостей функціонування ланцюгів поставок в умовах ризику.

Зважаючи на чималу кількість літератури, що висвітлює керування інформаційною безпекою в ланцюгах постачання, відчувається брак систематизованих досліджень. З огляду на це, інформацію з різних джерел було проаналізовано, систематизовано й подано у світлі окресленої теми дослідження.

3. Постановка завдання

Мета дослідження полягає у всебічному обґрунтуванні підходів до ефективного управління інформаційною безпекою в ланцюгах постачання шляхом виявлення небезпек, пов'язаних із цифровою взаємозалежністю, аналізу сучасних моделей довіри та розробки стратегій підвищення кіберстійкості постачальницьких систем.

4. Методи та матеріали

Оцінювати кіберзагрози в умовах децентралізованих цифрових мереж — завдання непросте не тільки технічно, а й концептуально. Жоден із методів, які історично вважалися «науково обґрунтованими», вже не діє відокремлено від інших. У центрі уваги — не одна система, а ціла сукупність взаємопов'язаних компонентів, поведінка яких у кризовій ситуації майже завжди виходить за рамки передбачуваного. Дослідження проблеми управління інформаційною безпекою в ланцюгах постачання виконано з використанням системно-аналітичного підходу, який поєднує теоретичні та прикладні методи аналізу ризиків цифрової взаємозалежності, моделювання довіри й формування стратегій кіберстійкості.

У процесі аналізу довелося поєднувати логічні побудови різної глибини — від дедуктивних гіпотез до індуктивних. Аналітичний метод — використано для критичного опрацювання нормативної, наукової та прикладної літератури з теми. Особливу увагу приділено концепціям zero trust architecture у контексті мережевої взаємодії постачальників. Окрім того, у ході наукового дослідження застосовувалися загальнонаукові методи пізнання, зокрема синтез, індукція й дедукція, порівняльний метод, системний підхід, метод моделювання.

Підсумовуючи, комплексний метод дослідження дав змогу не тільки сформувати цілісне бачення задачі, але й запропонувати способи, здатні зміцнити захист в реальних умовах постійної цифрової взаємозалежності.

5. Результати та обговорення

Стрімке впровадження цифрових технологій та глобалізація виробничо-логістичних процесів потроху формують новий ландшафт взаємозв'язків, де надзвичайно важливі функції — від керування запасами до обробки платіжних відомостей — передаються зовнішнім платформам або хмарним сервісам. У підсумку, замість чітко окресленої ієрархії постає розгалужена цифрова мережа, де кожен учасник виявляється залежним не лише від безпеки власних систем, а й від стабільності та надійності всіх партнерських ланок. Ця зростаюча взаємозалежність, хоч і дає бізнесу гнучкість і масштабованість, водночас докорінно змінює конфігурацію кіберризиків. Якщо раніше центр загроз був сконцентрований всередині компанії — в межах її інфраструктури — сьогодні він розпорошений у десятках точок доступу, які технічно належать зовнішнім партнерам, провайдерам або постачальникам. Атака, що починається з компрометації однієї ланки, здатна миттєво поширитися на всю систему.

На практиці це проявляється в тому, що традиційні способи ізолювання систем, лімітування доступів і тестування на проникнення — хоча й лишаються значущими — уже не надають гарантії результативного захисту в умовах, коли загроза може прийти з неочікуваного напрямку. Саме тому сучасне бачення інформаційної безпеки дедалі більше зосереджується не на побудові "фортеці", а на створенні стійкої, гнучкої архітектури, здатної чинити опір руйнуванню навіть у разі прориву одного з елементів.

Ланцюги постачання в умовах цифрової трансформації — це непрості, динамічні екосистеми, в яких традиційні процеси закупівель, виробництва, логістики та дистрибуції інтегровані з сучасними цифровими технологіями: Інтернетом речей (IoT), хмарними платформами, великими даними (Big Data), штучним інтелектом та автоматизацією [5]. Ця зміна

дає змогу підвищити ефективність, прозорість і гнучкість постачальницьких мереж, але водночас створює нові виклики, пов'язані з інформаційною безпекою. Взаємозалежність систем і процесів, відкритість інтерфейсів для обміну даними та розширення цифрових каналів комунікації збільшують ризики кібератак, витоку інформації та порушення безперервності бізнесу.

Кіберзагрози — це конкретні ризики, щодня визначають стабільність бізнесу. Коли мова заходить про кібернебезпеки в межах логістичних та виробничих ланцюгів, мовиться не лише про атаки на сервери чи витоки паролів. У більшості випадків порушення виникають внаслідок складної сукупності факторів — від слабкого шифрування в системах підрядників до людської необережності в керуванні доступами [11]. Одним із визначальних елементів захищеного середовища є довіра — але не декларативна, а підтверджена технічними і процесними гарантіями. Бізнес не може дозволити собі базувати співпрацю на припущеннях щодо надійності. Замість цього формується культура прозорості: аудит, регулярна перевірка сертифікацій, публічність політик безпеки.

Ще одне поняття, без котрого неможливо говорити про життєздатність цифрової екосистеми, — це кіберстійкість. На відміну від класичної безпеки, котра прагне запобігти інциденту, стійкість передбачає здатність пережити удар і швидко відновитися. Це включає автоматизовані системи виявлення загроз, сценарії реагування у реальному часі та стратегії збереження функціональності навіть під час атаки..

У комплексній екосистемі цифрових ланцюгів постачання небезпеки зрідка з'являються з центру — частіше вони пробиваються через периферію, де нагляд менший, а рівень захисту нижчий. Одним із головних вразливих місць лишаються інформаційні системи контрагентів: саме вони частенько стають «першим вікном» для кіберзлочинців. Насправді не всі партнери дотримуються однаково високих стандартів безпеки, і навіть одиничний збій у невеличкому підряднику може запустити лавину, що зачепить десятки великих учасників.

У низці випадків відмічається звична картина: втрата даних або витік секретної інформації відбувається не через складну атаку, а внаслідок недбалого контролю прав доступу. Відсутність чіткої ролевої моделі, використання спільних облікових записів, неналаштовані журнали доступу — все це відкриває шлях для зловмисників і робить аудит майже неможливим. Окремої уваги заслуговує ще одна масова проблема — використання застарілого програмного забезпечення.

Регулювання інформаційної безпеки в цифрових ланцюгах постачання давно вийшло за межі окремих технічних протоколів — сьогодні це багаторівнева система, в якій переплітаються міжнародне право, галузеві ініціативи та національні режими нагляду. На глобальному рівні стрижнем нормативної архітектури залишаються стандарти ISO/IEC серії 27000, зокрема ISO/IEC 27001, що визначає вимоги до побудови систем управління захистом даних [22, с. 29]. Національні законодавства, незважаючи на різні рівні зрілості, також формують важливий пласт регуляторного тиску. В Україні, наприклад, діє низка нормативних актів щодо захисту критичної інфраструктури, персональних даних та кібербезпеки. Хоча імплементація окремих норм поки нерівномірна, в деяких секторах — насамперед фінансовому — вже простежується рух до інтеграції з європейськими підходами.

Цифрова взаємодія між учасниками ланцюгів постачання створює не тільки вигоди, а й великі зони ризику. Найбільш вразливими виявляються саме ті структури, котрі побудовані каскадно: від виробника сировини до дистриб'ютора, від логістичного оператора до технічного інтегратора. Кожен щабель цієї системи має власну інфраструктуру, політики безпеки (або їх немає), стандарти збереження й обміну даними — і кожний з них може стати слабкою ланкою, що відкриває доступ до всієї мережі.

У багатьох випадках справжня складність полягає не в самих технологіях, а в непрозорості взаємозв'язків. Наприклад, фірма може працювати з офіційним постачальником, який, своєю чергою, доручає частину операцій менш контрольованим субпідрядникам. І якщо на першому рівні діють чіткі вимоги до шифрування, автентифікації та журналювання доступів, то на другому або третьому ці норми вже не виконуються — або взагалі відсутні. У результаті навіть незначна прогалина в безпеці умовного регіонального перевізника може стати воротами для проникнення в корпоративну систему, яка обслуговує тисячі клієнтів.

Можна зауважити, що зростаюча складність цифрових ланцюгів — це не виключення, а нова норма. І в цьому середовищі слабкість одного компонента перетворюється на системну проблему. Без повного розуміння архітектури взаємозв'язків і регулярного огляду партнерських ризиків неможливо гарантувати стійкість. Надійність ланцюга визначається не лише найсильнішими його учасниками, а й тим, наскільки контрольованими залишаються найменш помітні ділянки. По-перше, складність і розгалуженість мережі ускладнюють контроль за безпекою. По-друге, розповсюдження прав доступу без чіткої сегментації ідентифікаційних відомостей збільшує ризик несанкціонованого доступу та витоку конфіденційної інформації. По-третє, відсутність єдиного стандарту безпеки серед учасників ланцюга зумовлює неоднорідність захисних заходів і створює «слабкі ланки», які можуть бути використані зловмисниками. До того ж автоматизація та інтеграція різних ІТ-систем без належної перевірки та контролю відчиняють шлях для складних атак типу ланцюгової компрометації.

Усі ці загрози взаємодіють та посилюють одна одну, підвищуючи загальний рівень небезпеки для інформаційної безпеки у цифрових ланцюгах постачання. У табл. 1. наведено головні загрози цифрової взаємозалежності в багаторівневих ланцюгах постачання.

Таблиця 1. Основні загрози цифрової взаємозалежності в багаторівневих ланцюгах постачання

Загрози	Зміст	Рівень впливу	Наслідки
Проникнення через третіх або четвертих партнерів	Вразливі особи на нижчих щаблях мають слабший захист і стають точками доступу для атак	Третій, четвертий рівні постачальників	Компрометування всієї мережі, масштабні кібератаки
Несегментований доступ	Відсутність ясного розмежування прав доступу між користувачами	Всі рівні	Несанкціонований доступ, витік таємної інформації
Відсутність єдиного стандарту безпеки	Різний рівень безпеки серед партнерів, що спричиняє слабкі місця	Усі учасники	Зростання вразливостей, чутливість до атак
Інтеграція без належного контролю	Автоматизація і з'єднання систем без достатньої перевірки	Всі рівні	Складні ланцюгові напади, розповсюдження шкідливого ПЗ
Помилки в оновленнях і управлінні конфігураціями	Затримки чи негаразди в процесах оновлення створюють вразливості	Всі рівні	Експлуатація слабкостей, несанкціоноване проникнення

Джерело: сформовано автором на основі [12, с. 282; 13, с. 20; 14, с. 78].

Коли системи двох або більше організацій технічно інтегровані, кожний запит на доступ, кожна передача файлу, кожне автоматичне оновлення — це фактично акт довіри. І що складнішою стає архітектура взаємодії, то вищою повинна бути впевненість у тому, що інша сторона не лише дотримується стандартів, а й спроможна оперативно реагувати на загрози, оновлювати свої політики, зберігати прозорість у кризових ситуаціях. На практиці це проявляється в тому, що навіть великі бренди, які ще кілька років тому відкрито передавали дані контрагентам, сьогодні вимагають сертифікатів, журналів подій, наслідків аудитів і чіткої дорожньої карти у разі інциденту.

У цифровій взаємодії довіра — це багатошарова конструкція, кожен елемент якої критично важливий та включає певні рівні. Перший рівень — технічний. Йдеться про те, наскільки впевнено збудована архітектура безпеки: чи застосовуються сучасні алгоритми шифрування, чи є двофакторна аутентифікація, як організовані протоколи передачі даних. У низці ситуацій саме технологічні вади підривають довіру вже спочатку. Другий рівень — організаційний. Це — домовленості, правила, регламенти, механізми контролю. Бренди, що серйозно ставляться до безпеки, не обмежуються словами: вони впроваджують політики нульової довіри, фіксують взаємні зобов'язання в NDA, проводять внутрішні та зовнішні аудити, сертифікують свої процеси за ISO/IEC 27001 або SOC 2. Усе це створює передбачуване середовище, у якому партнери можуть працювати без остраху перед неочікуваними загубленими файлами чи відкритими портами. Це найменш формалізований, але не менш значущий вимір — соціальний. Довіра тут виникає не через протоколи, а через досвід. Партнери, котрі роками виконують зобов'язання, демонструють стабільність у критичних моментах, не приховують негараздів і відкриті до діалогу, поступово стають точками опори для складних екосистем. У низці галузей — приміром,

у фармацевтиці або енергетиці — саме така «людська» довіра визначає, чи буде фірма допущена до стратегічних ланцюгів постачання.

У розгалуженій структурі цифрових ланцюгів постачання класичне уявлення про довіру вже не функціонує. Раніше системи вибудовувалися на припущенні, що внутрішні елементи апріорі безпечні — якщо хтось або щось уже «всередині», йому автоматично дозволяється діяти. Цей підхід виявився помилковим. Зі збільшенням кількості атак, що використовують компрометовані компоненти або доступи низького рівня, стало очевидно: сліпа віра — найкоротший шлях до компрометації всієї інфраструктури.

Сучасна безпекова практика рухається в іншому напрямку. У центрі — концепція Zero Trust, що фактично перевертає сторінку у підходах до контролю доступу. Її сутність — цілковита відмова від припущень. Ні користувач, ні пристрій, ні додаток не здобувають права на дію без попереднього підтвердження. Не важливо, звідки надходить запит — ззовні чи з внутрішньої мережі. Верифікація — завжди. За кожен запит стоїть окреме рішення: перевірка особи, аналіз контексту, оцінка поведінки.

На практиці Zero Trust — це не один засіб, а сукупність технологій та управлінських підходів: багатоетапна аутентифікація, мікросегментація мережі, адаптивна авторизація, поведінковий аналіз. Кожен із цих компонентів — це фільтр, який не допускає жодної операції без пояснення. У низці випадків система навіть перериває сесію, якщо помічає відхилення від звичного патерну дій користувача — скажімо, підозріло швидкий доступ до чутливих документів відразу після входу з нового пристрою.

У теперішніх цифрових ланцюгах постачання захист відомостей потребує не тільки технічних рішень, а комплексного підходу, який поєднує різні моделі довіри. Системи на зразок Zero Trust і технології блокчейн, доповнюють одна одну, утворюючи багаторівневу «броню» проти загроз. Перша зосереджується на безумовній перевірці кожного запиту, незалежно від його джерела, що суттєво знижує ризики внутрішніх порушень, а друга — забезпечує прозорість та незмінність даних через розподілені реєстри, зменшуючи можливості для шахрайських дій і помилок.

У низці випадків ефективне використання моделей довіри перетворює спосіб, у який організації контролюють взаємодію з партнерами та постачальниками, збільшуючи прозорість та знижуючи вразливість перед внутрішніми та зовнішніми загрозами. Це відображається не тільки у технічних параметрах безпеки, а й у формуванні культури відповідального ставлення до керування цифровими активами. На практиці це виявляється в тому, що компанії отримують можливість точніше керувати доступом, а також швидше і гнучкіше відповідати на нові виклики, що виникають у динамічному середовищі сучасних постачальницьких екосистем (табл. 2).

Таблиця 2. Моделі довіри в інформаційній безпеці ланцюгів постачання

Модель довіри	Основний принцип	Ключові характеристики	Застосування у цифрових ланцюгах постачання
Повна довіра (Implicit Trust)	Внутрішні системи та партнери вважаються надійними за замовчуванням	Статична впевненість. Бракує контролю. Великий ризик. Легкість втілення	Локальні мережі без зовнішніх інтеграцій. Ризикована для відкритих чи глобальних ланцюгів постачання
Нульова довіра (Zero Trust)	Довіра не задана, кожен доступ потребує аутентифікації та авторизації, незалежно від місця розташування	Динамічна перевірка доступу Контекстна оцінка (пристрій, місцезнаходження, час) Мікросегментація. Безперервний моніторинг	Захист API, хмарних служб, внутрішніх платформ логістики. Інспекція кожного постачальника/вузла
PKI (ієрархічна довіра)	Довіра виникає через централізований сертифікаційний осередок (CA), котрий засвідчує особу об'єкта.	Сертифікати цифрової автентифікації. ієрархічна структура. Тривала довіра. Просто інтегрується в IoT та мережеві протоколи	Підпис оновлень ПЗ. Перевірка пристроїв у логістичних мережах. Зашифрування комунікацій між вузлами
Поведінкова довіра	Довіра формується на базі аналізу вчинків та історії взаємодії	Самостійна модель. Виявлення незвичної поведінки. Профілювання вузлів та юзерів	Моніторинг діяльності постачальників. Виявлення відхилень у ланцюзі постачання

Модель довіри	Основний принцип	Ключові характеристики	Застосування у цифрових ланцюгах постачання
Транзитивна довіра	Довіра передається через ланцюг: якщо А довіряє В, а В вірить С, то А довіряє С	Ефективна у федеративних мережах. Легка інтеграція сторонніх партнерів. Ризик доміно при зламі вузла	Системи з великою кількістю підрядників. Платформи з численними рівнями постачання

Джерело: сформовано автором на основі [15, с. 236; 16, с. 491; 17, с. 924].

У теперішніх цифрових ланцюгах постачання, де взаємозалежність учасників досягає великого рівня, питання інформаційної безпеки здобуває важливого значення. Збільшена складність і масштабність постачальницьких екосистем, а також широке використання сторонніх постачальників послуг і різноманітного програмного забезпечення утворюють численні ймовірні вразливі місця. Саме ці «слабкі ланки» — постачальники з незадовільним рівнем захисту, неперевірене або застаріле програмне забезпечення, недосконалі процеси оновлення та управління доступом — часто стають векторами кібератак. Зловмисники застосовують ці слабкі місця для проникнення в інформаційні системи, поширення шкідливого коду, викрадення секретних даних чи паралізації операцій. Зневага контролем кіберризиків на рівні окремих ланок ланцюга постачання може спричинити ефект доміно, який зачепить усю партнерську мережу.

Окремої уваги заслуговують так звані «вразливі місця» у ланцюгах постачання. У табл. 3. представлено вразливі місця у ланцюгах постачання, котрі здатні бути векторами кібератак, з акцентом на «слабкі місця» серед постачальників послуг та програмного забезпечення.

Таблиця 3. Вразливі точки у ланцюгах постачання

Вразлива точка	Зміст	Приклади «слабких ланок»	Потенційні вектори кібератак
Постачальники третіх сторін	Партнери з недостатньою кібербезпекою, нерідко з невеликими ресурсами на оборону.	Невеликі постачальники, підрядники	Впровадження зловмисного ПЗ, фішинг, злам через слабкі паролі
Програмне забезпечення і оновлення	Використання застарілого чи піратського ПЗ, брак своєчасних патчів	Неліцензійне програмне забезпечення, неатестовані складові	Використання відомих уразливостей, атаки через бекдори
Віддалений доступ і VPN	Неналежно захищені канали віддаленого доступу, слабкі способи автентифікації	Слабкі шифри, відсутність багатофакторної перевірки автентичності	Перехоплення інформації, атаки типу «Людина посередині», викрадення акаунтів
Інтеграція ІТ-систем партнерів	Відсутність уніфікованих політик безпеки, некеровані API та під'єднання	Неконтрольовані API, застарілі інтерактивні середовища	Ланцюгові напади, розповсюдження шкідливого ПЗ через інтеграції
Людський фактор	Неналежна підготовка персоналу, соціальна інженерія	Помилки співробітників, фішингові атаки	Викрадення облікових даних, несанкціоновані дії
Обладнання та мережеві пристрої	Використання застарілого або незахищеного обладнання	Маршрутизатори, перемикачі без оновлень	Вразливості на рівні мережі, перехоплення трафіку

Джерело: сформовано автором на основі [18-19; 20, С. 142].

Щоб система постачання насправді витримувала удари — як цифрові, так і логістичні, — потрібно навчитися бачити не лише її загальну структуру, а й найтонші місця, де вона найбільш вразлива. У складних, багаторівневих мережах слабкі ланки не завжди очевидні. Їх не знайдеш поверхневим оглядом, бо вони маскуються під стандартні процеси або ховаються на стику кількох операційних вузлів. Саме тому продумана класифікація вразливостей стає не просто технічним завданням, а стратегічним знаряддям управління ризиком. Контроль цифрової безпеки перестав бути другорядним технічним заходом — він перетворився на стратегічну функцію, яка визначає стійкість організації до зовнішніх небезпек та внутрішніх збоїв. У цьому контексті аудити відіграють роль не просто способу перевірки, а складного механізму аналізу,

котрий дає змогу побачити неочевидне: дрібні вразливості в інфраструктурі, розриви у процедурній логіці, помилки в налаштуваннях, про які навіть не здогадувалися.

За останні роки спостерігається швидке зростання зацікавленості бізнесу до таких перевірок — і не тільки серед технологічних фірм. Комунікація тут очевидна: що важча структура взаємодій із зовнішніми партнерами, то більша потреба в перевіреному цифровому просторі, де можна бути певним, що ланцюг не розірветься через найслабшу ланку. І якщо одна зі сторін не проходить аудит — це вже не просто технічний ризик, а пряма небезпека репутації й стабільності всієї екосистеми. Системний підхід до оцінки кіберзахисту дозволяє передовим компаніям не лише тримати руку на пульсі власних процесів, а й чітко розуміти, з ким безпечно мати справи. Превентивний характер таких перевірок особливо важливий: небезпеки постійно змінюються, і те, що вчора виглядало достатнім, сьогодні може виявитися критично вразливим. Саме тому регулярність і прозорість у проведенні аудитів стають фундаментом довіри, без якої неможливо будувати стабільну цифрову взаємодію в умовах швидкої трансформації [21].

Сертифікація постачальників — це формалізоване посвідчення відповідності нормам інформаційної безпеки (таким як ISO/IEC 27001, NIST SP 800-53, SOC 2 тощо), яке демонструє, що постачальник дотримується перевірених практик захисту [22, с. 29]. Сертифікація зменшує інформаційну асиметрію між сторонами та виступає загальним критерієм придатності постачальника з огляду безпеки. Наявність сертифіката також дозволяє спростити процеси оцінювання нових партнерів і скоротити витрати на індивідуальні перевірки. У часи стрімких загроз здатність швидко та адекватно реагувати на інциденти має особливу вагу, адже вона визначає не тільки безпеку, а й конкурентоспроможність фірм у взаємопов'язаному оточенні. На практиці це виявляється у впровадженні багаторівневих заходів моніторингу та контролю, що дають змогу своєчасно локалізувати ризики й запобігти великим збоям через основні принципи кіберстійкості у ланцюгах постачання, які подано на рис. 1.

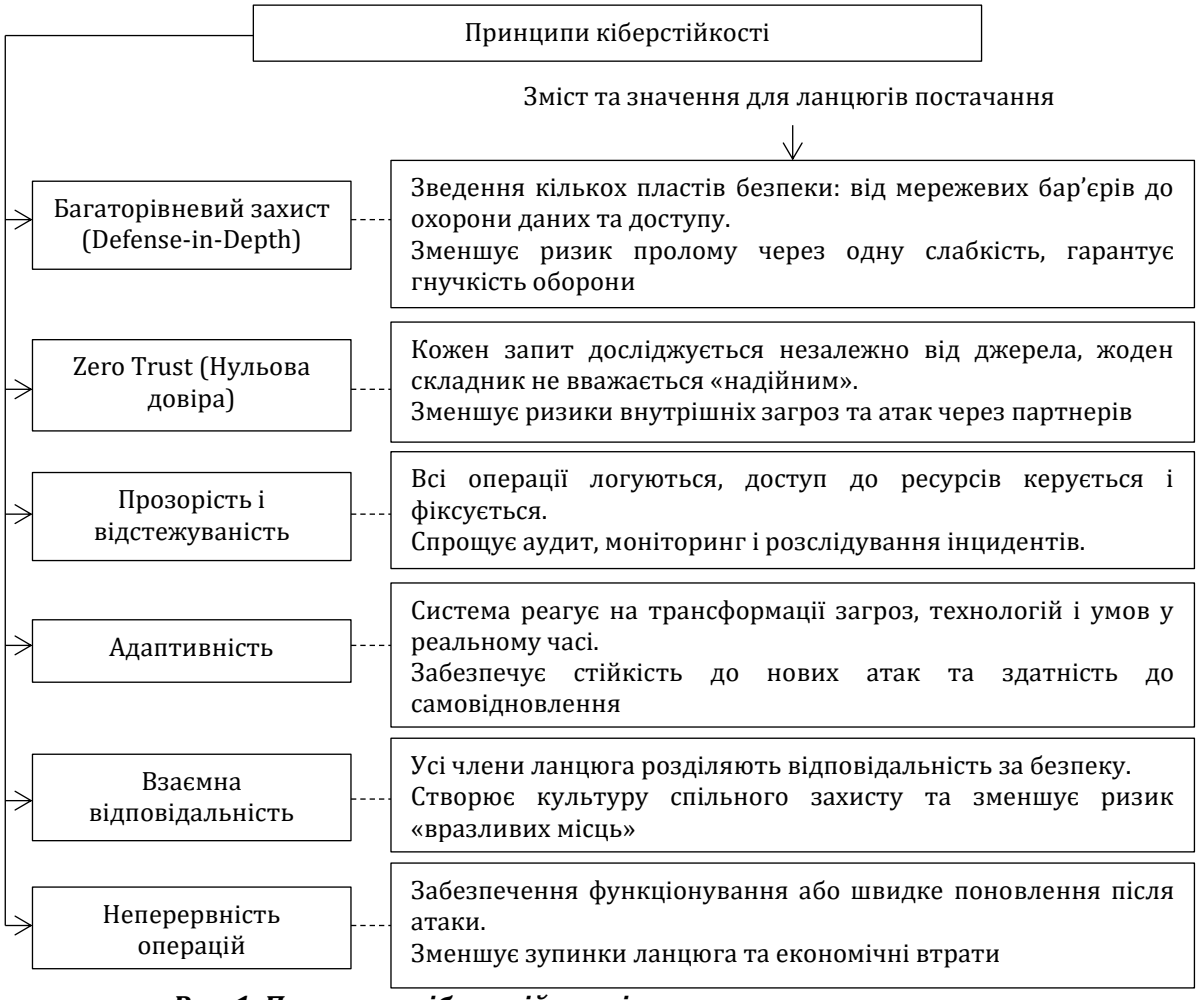


Рис. 1. Принципи кіберстійкості у ланцюгах постачання

Джерело: сформовано автором на основі [23-24; 25, с. 63].

У нинішньому цифровому оточенні ланцюги постачання стали складними, багаторівневими екосистемами, де щільно взаємодіють внутрішні та зовнішні інформаційні системи, підрядники, логістичні провайдери, постачальники програмного забезпечення та інші партнери. Така взаємозалежність, з одного боку, надає високу ефективність та гнучкість постачальницьких процесів, а з іншого — створює нові вектори кібератак, ускладнюючи виявлення загроз і управління ризиками. Вразливість хоча б одного учасника ланцюга може спричинити масштабну компрометацію всієї системи, що підтверджується численними інцидентами останніх років (SolarWinds, MOVEit, Log4j тощо) [26].

У теперішніх умовах, коли цифрові ланцюги постачання стають мішенню для все складніших і координованих кібератак, побудова кіберстійкості перетворюється з технічного завдання на стратегічну потребу. Кіберстійкість у цьому контексті означає здатність постачальницької системи чинити опір кібератакам, вчасно їх виявляти, ефективно реагувати та оперативно відновлювати критичні функції без серйозного порушення операційної діяльності (табл. 4).

Таблиця 4. Стратегії кіберстійкості в управлінні ланцюгами постачання

Стратегії	Зміст	Очікуваний результат
Багаторівнева система захисту (Defense-in-Depth)	Побудова декількох незалежних щаблів безпеки: мережа, програми, дані, юзери	Унеможливлення цілковитого зламу системи через одну вразливість
Zero Trust Architecture	Повна відмова від «довіри за змовчуванням», безупинна перевірка всіх доступів та дій.	Зменшення ризику інсайдерських атак та злому через партнерів
Безперервний моніторинг та виявлення загроз	Впровадження SIEM, IDS/IPS, поведінкового розбору, знаходження аномалій в дійсному часі	Швидке реагування на можливі атаки або порушення.
Сегментація інфраструктури та доступу	Обмеження доступу до систем, інформації та сервісів на основі ролей та рівнів довіри	Локалізація загроз, зменшення зони впливу при інциденті
План безперервності бізнесу (BCP) та відновлення (DRP)	Створення планів заходів у випадку атаки, резервне копіювання, дублювання важливих функцій	Швидке поновлення діяльності, мінімізування збитків
Регулярний аудит і тестування безпеки	Проведення пенетраційних випробувань, імітація атак (червона/синя команди), аудит постачальників.	Виявлення вразливостей перш ніж ними скористаються зловмисники
Навчання персоналу і партнерів	Підвищення свідомості, вивчення сценаріїв нападів, колективні тренування	Зменшення ризику хиб персоналу, покращення культури безпеки
Контроль і сертифікація третіх сторін	Перевірка відповідності постачальників вимогам безпеки (ISO 27001, SOC 2 та інше)	Залучення лише надійних партнерів, зменшення зовнішніх загроз

Джерело: сформовано автором на основі [27, с. 19; 28-29].

Сучасна кіберстійкість у галузі постачань — це вже не комплекс ізольованих інструментів, а гнучка архітектура управління ризиками, що вбудовується в саму структуру корпоративного управління. Вона існує в режимі реального часу, змінюється разом із контекстом, реагує на нові виклики не постфактум, а завчасно. У цій моделі важлива не лише технологія — визначальне значення мають управлінські інструменти, нормативна ясність та навіть поведінкова грамотність персоналу.

На практиці це виглядає як безперервна петля зворотного зв’язку: від миті першого контакту з майбутнім підрядником — до системного моніторингу після підписання контракту. Немає жодного етапу, на якому можна «відпустити нагляд». Навіть ті партнери, з якими співпраця триває роками, потребують регулярної перевірки: не лише сертифікатів, а й цифрової поведінки, налаштувань доступу, способів оновлення програмного забезпечення.

Стратегії виявлення, реагування та відбудови після кіберінцидентів у ланцюгах постачання є вкрай важливою складовою забезпечення кіберстійкості. Саме ці три вектори — діагностика, відповідь, відновлення — стають основою справжньої кіберстійкості. Ці стратегії поділяються на три взаємопов’язані етапи (рис. 2):

Рис. 2. Стратегії виявлення, реагування та відновлення після кіберінцидентів у ланцюгах постачання

Джерело: сформовано автором на основі [30; 31, с. 6; 32].

Коли організація не просто оберігається від загроз, а проактивно будує механізми реагування, вона зміцнює не тільки власну безпеку, але й підвищує стійкість всієї цифрової екосистеми, до якої належить. Інакше й бути не може: ланцюги постачання вже давно стали з лінійних схем на складні, взаємопов'язані мережі, де інформаційні системи, API, хмарні платформи й смарт-пристрої сплітаються в єдине цифрове тіло. У такій конфігурації вразливість одного компонента неминуче стає точкою ризику для решти.

У цій парадигмі мовиться не лише про уникнення. Ключову роль виконує механізм реагування — наскільки швидко система розпізнає порушення, локалізує небезпеку та повертається до стабільної роботи. Це дає змогу не тільки зменшувати втрати, а й утримувати ланцюги постачання в робочому стані навіть під тиском. Ставка не на захист «від усього», а на динамічну здатність тримати контроль під час збоїв — ось на що опираються сучасні моделі кіберстійкості. І якщо раніше ризик-менеджмент мав справу з абстрактними загрозами [33], сьогодні він набуває форми алгоритмів, що функціонують у хмарах, на периферії, у мобільних інтерфейсах. Вони аналізують поведінкові відхилення, зміну доступів, темпи обміну даними — та приймають рішення раніше, ніж небезпека встигає реалізуватися.

Управління кіберзагрозами в цифрових ланцюгах постачання потребує не сталого контролю, а рухомої, гнучкої системи безпеки, що враховує мінливість загроз, технологічну складність екосистеми та глибоку взаємозалежність між учасниками. Нижче наведено ключові поради, які допоможуть організаціям зменшити рівень кіберзагроз і забезпечити стабільність ланцюга (рис. 3):

Рис.3. Напрямки удосконалення управління кіберризиками в ланцюгах постачання на основі адаптивних моделей безпеки та стратегій кіберстійкості

Джерело: сформовано автором на основі [34, с. 187; 35; 36, с. 75; 37, с. 13].

Ці напрямки дозволяють побудувати стійкі до загроз цифрові ланцюги постачання, здатні не тільки захищатися, а й динамічно реагувати на зміни середовища та підтримувати довіру між усіма учасниками.

Інформаційна безпека припиняє бути “супровідною” функцією ІТ-відділу. Вона повинна переходити в стратегічний вимір управління постачанням. Інтеграція кіберризиків у логіку SCM (Supply Chain Management) — це вже не побажання, а потреба сьогодення. Без цього компанія втрачає не тільки оперативну стійкість, але й позиції на ринку: партнери перестають довіряти, клієнти шукають надійніші варіанти, а регулятори — накладають санкції за недотримання стандартів захисту. На практиці це означає: кожен новий технологічний елемент, кожна інтеграція або підключення зовнішнього сервісу мають супроводжуватися оцінкою ризиків — не формальною, а такою, що враховує динаміку загроз, репутацію постачальника, тип доступу до критичних даних і можливі сценарії порушення.

Рис. 4. Ключові напрями інтеграції кіберризик-менеджменту у стратегію управління ланцюгами постачання

Джерело: сформовано автором на основі [38; 39].

Вище вказані напрями інтеграції кіберризик-менеджменту у стратегію управління ланцюгами постачання сприятимуть:

- збільшенню прозорості загроз по всьому ланцюгу постачання;
- скороченню часу виявлення та реагування на випадки;
- формуванню культури проактивного керування безпекою;
- забезпечення узгодженості дій усіх партнерів у кризових обставинах;
- збільшення довіри з боку клієнтів, інвесторів і регуляторів.

Компанії, котрі інтегрують цифрову безпеку на всіх рівнях ланцюгів постачання — від підбору постачальника до контролю за API-доступами — здобувають не тільки захист. Вони вибудовують стійкі ланцюги, що не розпадаються через єдину помилку партнера чи зовнішню атаку, що дозволяє не просто втриматися на плаву, а й швидше відновитися, перехопити клієнтів у менш підготовлених конкурентів і підсилити власну репутацію.

6. Висновки

У реаліях цифрової взаємозалежності ланцюги постачання нині не нагадують класичні моделі. Тепер це складна мережа, що обіймає десятки — а часом і сотні — зовнішніх учасників, кожен з котрих взаємодіє через інтегровані IT-системи, спільні цифрові платформи, автоматизовані процеси та відкриті канали обміну даними. Будь-який із цих елементів може стати точкою прориву, і цього досить, щоб паралізувати критично важливі бізнес-процеси.

За таких обставин традиційні методи все частіше виявляються неефективними. Причина не в тому, що вони застарілі технічно, а в тому, що не беруть до уваги нову конфігурацію загроз. У ряді випадків спостерігається, як компанії, вкладаючи кошти в оборону власної

інфраструктури, нехтують слабкими місцями на стику з підрядниками — і саме там трапляється компрометація.

Цифрова складність ланцюгів постачання — це не просто більша кількість вузлів. Це щільніші з'єднання між ними, вищий ступінь автоматизації, синхронна робота багатьох систем у реальному часі. Те, що раніше було додатковим — зовнішні платформи, віддалені команди, підрядні сервіси, — тепер стало фундаментом щоденної роботи. І саме тому кіберстійкість перестає бути тільки технічною категорією. Вона стає елементом стратегічного управління: передбаченням, хто, як і через що може стати вразливим. У цій динаміці довіра не може бути передумовою. Вона має формуватися через безперервну перевірку, контрольовану прозорість і підтверджену надійність.

Кінцева картина керування інформаційною безпекою в ланцюгах постачання далека від сталої. Це не замкнена система з чіткими кордонами, а скоріше багаторівнева і динамічна екосистема, де один вразливий складник може дати збій усій конструкції. Кожен постачальник, кожна зовнішня інтеграція — це ймовірна точка входу для загроз, які не просто підривають стабільність, а в низці випадків паралізують критичні процеси.

Ланцюги постачання втратили замкненість: між підприємствами більше немає чітких кордонів. Натомість маємо багаторівневу модель, де хмара, API, сторонні платформи та мобільні вузли сплітаються в спільну інфраструктуру. Водночас рівень контролю над цими взаємозв'язками зменшується. У центр виходить довіра — керована, виважена і така, що постійно перевіряється. Сучасна інформаційна архітектура вимагає моделей, здатних реагувати на контекст, адаптуватися до поведінки учасників, оцінювати ризики не лише за принципом «хто», а й «коли», «звідки» та «на яких умовах». Саме тому стрімко зростає роль Zero Trust, поведінкових моделей і механізмів довіри, що формуються не через статус, а через доказову історію взаємодії. Аналіз цифрової довіри виявив ще одну закономірність: найбільш вразливими виявляються саме ті сегменти ланцюга, що мають найбільшу кількість транзитивних довірених зв'язків. Іншими словами, довіра, що передається через посередників, часто стає інструментом компрометації.

У підсумку стає очевидним: інформаційна безпека в постачальницькому середовищі — це не технічне завдання, а стратегічний процес, який потребує синергії інструментів, людського чинника, інституційної довіри та гнучких сценаріїв реагування. Компанії, які зможуть оперативно виявляти цифрові залежності, критично мислити щодо каналів довіри та діяти наперед, здобудуть не просто захист — а конкурентну перевагу.

References

1. Kotliarov, V. (2024). Stratehichne upravlinnia informatsiinoiu bezpekoiu Ukrainy [Strategic management of information security of Ukraine]. *Kyivskyi ekonomichnyi naukovyi zhurnal – Kyiv Economic Scientific Journal*, (6), 66–69. https://doi.org/10.32782/2786-765X/2024-6-9 (in Ukrainian)
2. Bondar-Pidhurska, O. V., & Khomenko, I. I. (2022). Naukovo-metodychni zasady otsinky efektyvnosti protsesu upravlinnia informatsiinoiu bezpekoiu pidpryiemstv maloho ta serednoho biznesu: kiberbezpeka ta intelektualna vlasnist [Scientific and methodological principles for assessing the effectiveness of the information security management process of small and medium-sized businesses: cybersecurity and intellectual property]. *Problemy ekonomiky – Problems of the Economy*, *2*(52), 108–116. https://doi.org/10.32983/2222-0712-2022-2-108-116 (in Ukrainian)
3. Mashchenko, M. A., & Ippolitov, Ye. M. (2024). Formuvannia stratehii posylennia informatsiinoi bezpeky pidpryiemstva [Formation of a strategy to strengthen the enterprise's information security]. *Ekonomika ta suspilstvo – Economy and society*, (70). https://doi.org/10.32782/2524-0072/2024-70-147 (in Ukrainian)
4. Yasinska, A. (2023). Informatsiina bezpeka pidpryiemstva: kontseptualni zasady efektyvnoho zakhystu informatsii [Enterprise information security: conceptual principles of effective information protection]. *Ekonomika ta suspilstvo – Economy and society*, (56). https://doi.org/10.32782/2524-0072/2023-56-118 (in Ukrainian)
5. Osokin, H. V. (2024). Tsyfrovizatsiia lantsiuhiv postachannia yak faktor transformatsii biznes-modelei [Digitalization of supply chains as a factor in transforming business models]. *Ekonomika ta suspilstvo – Economy and society*, (64). https://doi.org/10.32782/2524-0072/2024-64-62 (in Ukrainian)
6. Lisitsa, V. V., Mykhailenko, O. M., & Rotenberh, O. V. (2023). Tsyfrovi lantsiuhy postavok: tekhnolohii, tendentsii ta napriamy rozvytku [Digital supply chains: technologies, trends and development directions].

Ekonomika ta upravlinnia pidpryiemstvamy – Economics and Business Management, (81), 99–106. https://doi.org/10.32782/bses.81-17 (in Ukrainian)

7. Prydybailo, O. B., Prydybailo, R. V., Yaskevych, V. O., & Yaskevych, Yu. V. (2024). Arkhitektura nulovoi doviry: lohichni komponenty ta pidkhody zaprovadzhennia [Zero Trust Architecture: Logical Components and Implementation Approaches]. *Zviazok – Communication*, (3), 7–11. https://doi.org/10.31673/2412-9070.2024.030711 (in Ukrainian)
8. Kulikovskyi, A. V. (2019). Tekhnolohiia blockchain yak skladova informatsiinoi bezpeky [Blockchain technology as a component of information security]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: education, science, technology*, *4*(4), 85–89. https://doi.org/10.28925/2663-4023.2019.4.8589 (in Ukrainian)
9. Halushko, O., & Selivorstova, T. (2022). Kiberbezpeka v upravlinni lantsiuhamy postachan (SCM) [Cybersecurity in Supply Chain Management (SCM)]. *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav – Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, *2*(121), 537–542. https://doi.org/10.31733/2078-3566-2022-6-537-542 (in Ukrainian)
10. Pohrebniak, A. T., Nemish, Yu. V., Pavlovski, H., Shevchenko, S. H., & Tyrkalo, Yu. Ye. (2022). Bezpeka ta osoblyvosti funktsionuvannia lantsiuhiv postavok v umovakh ryzyku [Security and features of supply chains functioning under risk conditions]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava – Scientific Notes of Lviv University of Business and Law*. *Seriia Ekonomichna. Seriia Yurydychna*, (35), 10–18. https://nzlubp.org.ua/index.php/journal/article/download/641/588 (in Ukrainian)
11. Reznikova, N. V., Vovk, V. A., & Ptashchenko, L. V. (2025). Formuvannia mizhnarodnoi konkurentospromozhnosti IT-sektoru: stratehichni chynnyky ta kiberryzyky [Shaping the international competitiveness of the IT sector: Strategic factors and cyber risks]. *European Scientific Journal of Economic and Financial innovation*, *1*(15), 439–449. https://journal.eae.com.ua/index.php/journal/article/view/494 (in Ukrainian)
12. Smerichevska, S. V. (2021). Stratehichni trendy rozvytku lantsiuhiv postavok novoho pokolinnia v epokhu tsyfrovizatsii ekonomiky [Strategic trends in the development of new generation supply chains in the era of digitalization of the economy]. In *Proceedings of the II International Scientific and Practical Conference Business, Innovation, Management: Problems and Prospects* (pp. 282–283). Kyiv: Vydavnytstvo "Politekhnika". https://confmanagement-proc.kpi.ua/article/view/230866 (in Ukrainian)
13. Hirna, O. B. (2025). Tsyfrovi tekhnolohii v upravlinni lantsiuhamy postachannia [Digital technologies in supply chain management]. *Ekonomichnyi prostir – Economic space*, (199), 20–25. https://doi.org/10.30838/EP.199.20-25 (in Ukrainian)
14. Matsyshyna, O. V., & Smerichevska, S. V. (2022). Intehrovanyi pidkhid do stratehichnoho upravlinnia lantsiuhamy postachannia v umovakh tsyfrovoi ekonomiky [An integrated approach to strategic supply chain management in the digital economy]. In *Proceedings of the III International Scientific and Practical Conference Business, Innovation, Management: Problems and Prospects* (pp. 78–79). https://confmanagement-proc.kpi.ua/article/view/271608 (in Ukrainian)
15. Kupershtein, L., & Krentsin, M. (2024). Model nulovoi doviry dlia hibrydnoi pirynhovoi merezhi [Zero Trust Model for Hybrid Peer-to-Peer Network]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh – Measuring and computing equipment in technological processes*, (3), 236–242. https://doi.org/10.31891/2219-9365-2024-79-31 (in Ukrainian)
16. Werbach, K. (2018). Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, *33*(2), 487–550. https://www.jstor.org/stable/26533144
17. Babenko, K. Ye. (2018). Blokchein v ekonomitsi ta biznesi [Blockchain in the economy and business]. *Ekonomika i suspilstvo – Economy and society*, (15), 924–932. https://economyandsociety.in.ua/journals/15_ukr/142.pdf (in Ukrainian)
18. Panchenko, V., & Reznikova, N. (2022). Vid vrazlyvosti lantsiuhiv postavok do yikh hnuchkosti ta stiikosti dlia MSP [From supply chain vulnerability to flexibility and resilience for SMEs]. *INDUSTRY4UKRAINE*. https://www.industry4ukraine.net/publications/vid-vrazlyvosti-lanczyugiv-postavok-do-yih-gnuchkosti-ta-stijkosti-dlya-msp (in Ukrainian)
19. ESET. (2021). *Kilkist atak na lantsiuh postachannia zrostaie: khto pid prytsilom ta yak protystoiaty* [Supply chain attacks are on the rise: Who is being targeted and how to counter them]. https://surl.li/dvzpuy (in Ukrainian)
20. Havrysh, B. M., Tymchenko, O. V., Borzov, Yu. O., & Kobevko, A. T. (2022). Klasyfikatsiia shkidlyvoho prohramnoho zabezpechennia ta osnovni metody zakhystu [Malware classification and basic protection methods]. *Kompiuterni tekhnolohii drukarstva – Computer Printing Technologies*, *2*(48), 142–154. http://doi.org/10.32403/2411-9210-2022-2-48-142-154 (in Ukrainian)

21. ISSP Training Center. (2021). *Shcho potribno znaty pro audyt kiberbezpeky* [What you need to know about cybersecurity auditing]. https://www.issp.training/post/scho-potribno-znaty-pro-audyt-kyberbezpeky (in Ukrainian)
22. Kovalenko, S. V., Smoliev, Ye. S., & Barhylevych, O. A. (2021). Tekhnolohiia audytu kiberbezpeky korporatyvnoi informatsiinoi systemy za metodykoiu ISO/IES: 27001 [Corporate information system cybersecurity audit technology according to ISO/IES: 27001 methodology]. *Suchasnyi zakhyst informatsii – Modern Information Protection*, *3*(47), 29–35. http://doi.org/10.31673/2409-7292.2021.032935 (in Ukrainian)
23. B2B Cyber Security. (2025). *Zakhyst lantsiuzhka postachannia prohramnoho zabezpechennia vidpovidno do zakonu pro kiber-stiikist* [Protecting the Software Supply Chain Under Cyber Resilience Act]. https://b2b-cyber-security.de/uk/software-lieferkette-fuer-den-cyber-resilience-act-absichern (in Ukrainian)
24. Yashchuk, V. I. (2024). Rol ta mistse stratehii kiberbezpeky Ukrainy u zabezpechenni informatsiinoi bezpeky derzhavy [The role and place of Ukraine's cybersecurity strategy in ensuring the state's information security]. In *Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie* (pp. 259–286). Mezinárodní Ekonomický Institut s.r.o. https://sci.ldubgd.edu.ua/jspui/handle/123456789/13824 (in Ukrainian)
25. Tsekhmeister, R. D., Platonenko, A. V., Vorokhob, M. V., & Cherevyk, V. M. (2025). Doslidzhennia metodiv zabezpechennia informatsiinoi bezpeky u virtualnomu seredovyshchi [Research on methods for ensuring information security in a virtual environment]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technology*, *3*(27), 63–71. http://doi.org/10.28925/2663-4023.2025.27.703 (in Ukrainian)
26. Progress Community. (2022). *Is MOVEit vulnerable to CVE-2021-44228 (Log4j)*? https://community.progress.com/s/article/Is-MOVEit-vulnerable-to-CVE-2021-44228-Log4j
27. Koval, M. A., Bobrovskyi, O. V., Herashchenko, I. O., & Nykytiuk, A. P. (2025). Stratehii kiberstiikosti: upravlinnia ryzykamy ta bezperervnist biznesu [Cyber Resilience Strategies: Risk Management and Business Continuity]. In *Materials of the All-Ukrainian Scientific and Practical Internet Conference Cyber Resilience Strategies: Risk Management and Business Continuity* (pp. 19–25). Educational and Scientific Institute of Cybersecurity and Information Protection, State University of Information and Communication Technologies. https://duikt.edu.ua/uploads/p_2779_46212583.pdf (in Ukrainian)
28. ESKA. (2024). *BCP (Business Continuity Plan) ta DRP (Disaster Recovery Plan) – Suchasni pidkhody do Kiberbezpeky ta Biznes-Zakhystu* [BCP (Business Continuity Plan) and DRP (Disaster Recovery Plan) – Modern Approaches to Cybersecurity and Business Protection]. https://eska.global/blog/bcp-business-continuity-plan-ta-drp-disaster-recovery-plan-suchasni-pidhodi-do-kiberbezpeki-ta-biznes-zahistu_1 (in Ukrainian)
29. Vamark. (2025). *Zero Trust Architecture: novyi standart u kiberbezpetsi* [Zero Trust Architecture: a new standard in cybersecurity]. https://vamark.ua/blog/zero-trust-architecture-novyj-standart-u-kiberbezpeczi (in Ukrainian)
30. *Upravlinnia kyberintsydentamy. Versiia 1.1. Posibnyk z dodatkhovykh resursiv CRR* [Cyber Incident Management. Version 1.1. CRR Supplemental Resource Guide]. (2016). Carnegie Mellon University. https://cip.gov.ua/services/cm/api/attachment/download?id=62036 (in Ukrainian)
31. Shulha, V. P., Ivanchenko, Ye. V., Vyshnevska, N. S., & Berber, A. S. (2024). Doslidzhennia metodiv ta modelei otsiniuvannia kiberzakhystu krytychnoi infrastruktury derzhavy [Research into methods and models for assessing cyber defense of critical state infrastructure]. *Suchasnyi zakhyst informatsii – Modern Information Protection*, *3*(59), 6–19. http://doi.org/10.31673/2409-7292.2024.030001 (in Ukrainian)
32. Stratehiia informatsiinoi bezpeky [Information Security Strategy]. Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. https://zakon.rada.gov.ua/laws/show/685/2021#Text (in Ukrainian)
33. Prokopenko, O., Bezliudnyi, O., Omelyanenko, V., Slatvinskyi, M., Biloshkurska, N., & Biloshkurskyi, M. (2021). Patterns identification in the dynamics of countries' technological development in the context of military conflict. *Eastern-European Journal of Enterprise Technologies,* *2*(13(110), 6–15. https://doi.org/10.15587/1729-4061.2021.230236
34. Dovhun, O. S., & Stasiuk, K. Z. (2017). Avtomatyzatsiia lohistyky: suchasni rishennia ta perspektyvy [Logistics automation: modern solutions and prospects]. *Naukovyi visnyk Uzhhorodskoho universytetu*. *Seriia "Ekonomika", 2*(50), 187–191. http://nbuv.gov.ua/UJRN/Nvuuec_2017_2_28 (in Ukrainian)
35. Kudyrko, O. (2022). *Avtomatyzatsiia lohistychnykh protsesiv yak suchasnyi trend [Automation of logistics processes as a modern trend]*. In *Proceedings of the II International Scientific and Practical Internet Conference on Modern Technologies in Commercial Activities and Logistics, November 3, 2022, Kyiv* (pp. 56–59). Kyiv National Economic University named after V. Hetman. https://ir.kneu.edu.ua:443/handle/2010/39284 (in Ukrainian)
36. Lomovatskyi, O. V. (2024). Rol audytu informatsiinoi bezpeky v zabezpechenni stiikosti ta nadiinosti informatsiinykh system [The role of information security auditing in ensuring the stability and reliability of

information systems]. In *Proceedings of the All-Ukrainian Scientific and Practical Conference "Digital Transformation of Cybersecurity"* (pp. 75–77). https://duikt.edu.ua/uploads/n_12581_11703414.pdf (in Ukrainian)

37. Zaverbnyi, A. S. (2024). Osoblyvosti formuvannia systemy upravlinnia kiberbezpekoiu pidpryiemstv u voiennyi period: teoretykoprykladnyi aspect [Peculiarities of forming a cybersecurity management system for enterprises during wartime: theoretical and applied aspects]. *Innovation and Sustainability*, (1), 13–22. https://doi.org/10.31649/ins.2024.1.13.21 (in Ukrainian)
38. National Institute for Strategic Studies. (2022). *Ataky cherez lantsiuzhky postachan: formuiuchy stratehichnu vidpovid* [Supply Chain Attacks: Shaping a Strategic Response]. https://niss.gov.ua/sites/default/files/2022-06/ad_cyberresill_structure_var8_new_ed_01_gotove_0.pdf (in Ukrainian)
39. Shtelmashuk, M. S. (2024). Tsyfrovizatsiia ta avtomatyzatsiia lohistychnykh protsesiv: suchasnyi stan ta perspektyvy [Digitalization and automation of logistics processes: current state and prospects]. *Ekonomika ta suspilstvo – Economy and society*, (68). https://doi.org/10.32782/2524-0072/2024-68-193 (in Ukrainian)