19 dicembre, 2025;
Bologna, Repubblica Italiana

SEZIONE 4.
ATTIVITÀ DI MARKETING E LOGISTICA

DOI 10.36074/logos-19.12.2025.008

СТІЙКІСТЬ ЛАНЦЮГІВ ПОСТАЧАННЯ: ПІДХОДИ ДО ПІДВИЩЕННЯ НАДІЙНОСТІ ЛОГІСТИКИ

Становий Олексій Сергійович[1]

1. магістр за спеціальністю «Підприємництво, торгівля та біржова діяльність», асистент кафедри логістики та торговельного бізнесу
Державний торговельно-економічний університет, УКРАЇНА
ORCID ID: 0009-0004-6950-9902

Ланцюги постачання функціонують у середовищі зростаючої турбулентності: геополітичні ризики, обмеження інфраструктури, кібератаки, коливання попиту та дефіцит ресурсів можуть одночасно порушувати транспортні, складські й виробничі операції. Для логістики це проявляється як падіння рівня сервісу (SLA/OTIF), зростання часу виконання замовлень, розриви у забезпеченні запасами та підвищення собівартості. Відтак стійкість ланцюга постачання стає ключовою умовою надійності логістичних процесів і конкурентоспроможності підприємства.

У науковій літературі стійкість (resilience) розглядається як здатність ланцюга постачання підготуватися до збоїв, ефективно відреагувати та відновити працездатність у прийнятні строки, зберігаючи (або підвищуючи) результати діяльності [1;2]. Систематичні огляди підкреслюють, що стійкість є багатовимірним явищем і поєднує готовність, реагування, відновлення та адаптацію до нових умов [3]. У логістиці ці виміри трансформуються у вимоги до надійності перевезень, прозорості руху матеріальних потоків, гнучкості складів і керованості запасів.

Практичним завданням підвищення надійності логістики є збалансування вразливостей і можливостей. Концептуально це можна описати через «зону стійкості», де рівень логістичних вразливостей (залежність від одиничних постачальників, низька видимість 2–3 рівнів постачання, довгі lead time, обмежена пропускна здатність складів/портів) компенсується розвитком відповідних можливостей (гнучкість, резервування, співпраця, швидке переналаштування) [4]. Таким чином, метою є не максимізація запасів чи дублювання потужностей, а раціональна «комбінація»

інструментів, що забезпечує прийнятний ризик-профіль за заданого бюджету.

Перший блок підходів пов'язаний із системним управлінням ризиками. ISO 31000 пропонує логіку ідентифікації, аналізу та оцінки ризиків із подальшим плануванням заходів реагування, моніторингом і комунікацією [8]. Для логістики це означає: (1) формування карти ризиків по вузлах мережі (постачальники, склади, маршрути, IT-сервіси); (2) ранжування за впливом на SLA та фінансовий результат; (3) визначення «критичних» позицій номенклатури та маршрутів; (4) розробку планів безперервності, що узгоджуються з підходами бізнес-континуїті (ISO 22301) [9]. Окремо для логістичних ланок актуальним є впровадження вимог до безпеки та стійкості в ланцюгу постачання згідно ISO 28000 [10].

Другий блок підходів стосується формування портфеля стійкісних стратегій. Класичні рекомендації охоплюють підвищення видимості (end-to-end visibility), розвиток гнучкості та співпраці між учасниками ланцюга [1]. Для зниження ризику «розривів» постачання доцільні диверсифікація постачальників і регіонів, контракти з альтернативними перевізниками, а також модульне проєктування логістичної мережі (можливість швидко перемикатися між вузлами). Важливо, що «робастні» стратегії мають забезпечувати ефективність у звичайних умовах і водночас підвищувати стійкість у кризових ситуаціях (postponement, гнучкі потужності, стандартизація компонентів, risk pooling) [7]. Управління типами ризиків (попит, постачання, процеси, контроль) і відповідними інструментами реагування розглядається як базова компетенція сучасного SCM [6].

Третій блок пов'язаний із цифровими інструментами, що підсилюють керованість і швидкість реакції. Побудова «control tower» та інтеграція даних (TMS/WMS/ERP, телематика, дані перевізників і митниці) дають змогу скорочувати час виявлення відхилень (time-to-detect) і прискорювати ухвалення рішень. Перспективним напрямом є сценарне моделювання та цифрові двійники мережі, які дозволяють оцінювати наслідки шоків і вибирати адаптаційні стратегії. У цьому контексті підхід «viability» акцентує не лише відновлення, а й здатність мережі зберігати життєздатність за тривалих екстремальних порушень [5].

Узагальнення ключових логістичних ризиків та практик підвищення надійності наведено в (табл. 1). Запропонована логіка може використовуватися як «шаблон» для аудитів стійкості: від діагностики вразливостей до вибору інструментів і метрик контролю (OTIF, lead time, TTR/TTS, рівень запасів, частота зривів поставок).

Таблиця 1

Інструменти підвищення стійкості логістики за видами ризиків

Категорія ризику	**Типові прояви в логістиці**	**Підходи/ інструменти**	**Приклади метрик контролю**
Постачання	затримки, недопоставки, банкрутство постачальника, блокування кордонів	мультисорсинг; альтернативні маршрути; резервні перевізники; буфери критичних позицій; аудит 2–3 рівнів постачання	OTIF постачальника; lead time; частка альтернативних поставок
Попит	піки/провали, зміна структури замовлень, нестабільний прогноз	прогнозування та S&OP; сегментація клієнтів; postponement; risk pooling на складах	MAPE; рівень сервісу; оборотність запасів
Процеси/інфраструктура	відмова складу/сортування, дефіцит персоналу, аварії обладнання	резервування потужностей; крос-тренінг; стандарти операцій; план відновлення (BCP); контрактні склади	TTR/TTS; продуктивність, % простоїв, час комплектації
IT та безпека	кібератаки, збій інтеграцій, втрата даних відстеження	контроль доступу; резервне копіювання; вимоги ISO 28000; тестування планів реагування; кібергігієна партнерів	MTTR; частота інцидентів; доступність систем, %

дані сформовано з [1; 4; 6; 7; 8–10]

Висновки. Підвищення надійності логістики в умовах збоїв потребує комплексного підходу: (1) ризик-орієнтованого управління та планів безперервності; (2) розвитку можливостей гнучкості, видимості та співпраці в мережі; (3) застосування робастних стратегій, що не руйнують ефективність у «нормальних» умовах; (4) цифрових інструментів для раннього виявлення відхилень і сценарного планування. З практичної точки зору, ключовим є регулярний аудит вразливостей і метрик (OTIF, lead time, TTR/TTS), що дозволяє обґрунтовано інвестувати в стійкість та підтримувати прийнятний рівень сервісу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Christopher, M., & Peck, H. (2004). Building the resilient supply chain. The International Journal of Logistics Management, 15(2), 1–14. Вилучено з: https://doi.org/10.1108/09574090410700275

[2] Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), 124–143. Вилучено з: https://doi.org/10.1108/09574090910954873
[3] Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: definition, review and theoretical foundations for further study. International Journal of Production Research, 53(18), 5592–5623. Вилучено з: https://doi.org/10.1080/00207543.2015.1037934
[4] Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. Journal of Business Logistics, 31(1), 1–21. Вилучено з: https://doi.org/10.1002/j.2158-1592.2010.tb00125.x
[5] Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. International Journal of Production Research, 58(10), 2904–2915. Вилучено з: https://doi.org/10.1080/00207543.2020.1750727
[6] Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. MIT Sloan Management Review, 46(1), 53–61.
[7] Tang, C. S. (2006). Robust strategies for mitigating supply chain disruptions. International Journal of Logistics: Research and Applications, 9(1), 33–45. Вилучено з: https://doi.org/10.1080/13675560500405584
[8] International Organization for Standardization. (2018). ISO 31000:2018 Risk management — Guidelines. ISO.
[9] International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. ISO.
[10] International Organization for Standardization. (2022). ISO 28000:2022 Security and resilience — Security management systems — Requirements. ISO.