Тимоць Мирослава, кандидат економічних наук, доцент, професор кафедри бізнесу та управління ЗВО «Університет Короля Данила», м. Івано-Франківськ, Україна, ORCID: https://orcid.org/0009-0001-0266-1756

Манько Юрій, аспірант ЗВО «Університет Короля Данила», м. Івано-Франківськ, Україна, ORCID: https://orcid.org/0000-0001-9369-490X

Tymots Myroslava, PhD in Economics, Associate Professor, Professor of the Department of Business and Administration, King Danylo University, Ivano-Frankivsk, Ukraine

Manko Yuriy, postgraduate student King Danylo University, Ivano-Frankivsk, Ukraine

ЦИФРОВІ ІНСТРУМЕНТИ В СИСТЕМІ АНТИКРИЗОВОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ

DIGITAL TOOLS IN THE ANTI-CRISIS MANAGEMENT SYSTEM OF AN ENTERPRISE

Анотація

У статті досліджено механізми забезпечення безперервності бізнес-процесів (BCP) українських підприємств в умовах воєнного стану. Обґрунтовано, що стійкість бізнесу сьогодні залежить від поєднання організаційних рішень та гнучкої технологічної архітектури. Виділено ключову роль хмарних сервісів, систем віддаленого доступу та інструментів командної роботи (Slack, Teams, Zoom) у мінімізації залежності від фізичних локацій. Особливу увагу приділено інноваційним підходам для зміцнення цифрової стійкості: створенню мережі регіональних «континуїтет-хабів», запровадженню стандартів «BCP-in-a-box» для МСП та розвитку «offline-

first» цифрових процесів. Розглянуто необхідність формування інституційних модулів підтримки підприємців із типовими сценаріями відновлення та чек-листами. Доведено, що стратегічний акцент має зміститися з формального опису ризиків на керованість критичних функцій та швидкість повернення до операційної спроможності. Запропоновано інструментарій операційної безперервності, що включає стандартизацію спрощених процедур, взаємозамінність ролей, диверсифікацію логістики та створення фінансових буферів. Окреслено важливість кібербезпеки (Zero Trust, багатофакторна автентифікація) та захисту фізичних IT-активів. Зроблено висновок, що впровадження коротких циклів прийняття рішень («антикризового контуру») та перехід до багаторівневих цифрових екосистем збуту є вирішальними факторами адаптації бізнес-моделей до воєнних викликів.

Ключові слова: цифровізація, суб'єкти господарювання, антикризове управління підприємством

Abstract

The article examines the mechanisms for ensuring business continuity (BCP) of Ukrainian enterprises under martial law. It is substantiated that business resilience today depends on a combination of organizational decisions and flexible technological architecture. The author highlights the key role of cloud services, remote access systems, and teamwork tools (Slack, Teams, Zoom) in minimizing dependence on physical locations. Special attention is paid to innovative approaches for strengthening digital resilience: the creation of a network of regional "continuity hubs," the introduction of "BCP-in-a-box" standards for SMEs, and the development of "offline-first" digital processes. The necessity of forming institutional support modules for entrepreneurs with standard recovery scenarios and checklists is considered. It is proved that the strategic focus should

shift from a formal description of risks to the manageability of critical functions and the speed of return to operational capacity. The paper proposes a toolkit for operational continuity, which includes the standardization of simplified procedures, role interchangeability, logistics diversification, and the creation of financial buffers. The importance of cybersecurity (Zero Trust, multi-factor authentication) and the protection of physical IT assets is outlined. It is concluded that the implementation of short decision-making cycles ("anti-crisis circuit") and the transition to multi-level digital sales ecosystems are decisive factors in adapting business models to wartime challenges.

Key words: digitalization, business entities, enterprise crisis management

Постановка проблеми. Нині підприємства, особливо суб'єкти малого бізнесу, не повністю використовують потенціал цифровізації. Їх рівень впровадження технологій відстає від великого бізнесу. Зокрема, веб-сайт мають близько 70% великих компаній, тоді як серед середніх підприємств лише 47%, а серед малих менш як 30%. Причини включають брак обізнаності, дефіцит цифрових навичок і фінансові обмеження. Тому держава та партнери зосереджуються на програмах розвитку цифрової зрілості бізнесу.

Аналіз останніх досліджень та публікацій. Питання забезпечення життєздатності та цифрової трансформації бізнесу в умовах невизначеності перебувають у центрі уваги провідних вітчизняних та зарубіжних науковців. Теоретичні засади антикризового управління підприємством та його концепції ґрунтовно досліджені у працях таких класиків менеджменту, як І. Ансофф, П. Друкер та С. Фінк. На сучасному етапі ці підходи адаптуються до умов цифрової економіки. Вагомий внесок у дослідження цифровізації як інструменту стійкості підприємства зробили українські вчені, зокрема Левчинський Д.Л., Ступнікер Г.Л., Каширнікова І.О., Зозуля Н.В [1]. У їхніх

роботах акцентується увага на тому, що впровадження ІТ-рішень дозволяє суб'єктам господарювання гнучко реагувати на ринкові шоки. Автори підкреслюють, що наявність цифрових компетенцій та попередній досвід використання хмарних технологій стали вирішальними факторами збереження операційної спроможності.

Водночас, попри наявність значної кількості публікацій щодо загальної цифровізації, механізми їх впровадження для малого та середнього бізнесу в умовах затяжних воєнних ризиків потребують подальшого глибшого опрацювання. Саме ці прикладні аспекти цифровізації антикризового управління складають науковий пошук даної статті.

Постановка завдання. Розкрити роль цифрових технологій в системі антикризового управління підприємства.

Виклад основного матеріалу. В 2024 р. ухвалено Стратегію розвитку малого та середнього бізнесу на період до 2027 р., одним із пріоритетів якої є післявоєнне відновлення та цифровізація економіки. Ціль – знизити витрати підприємців на дотримання регуляцій і звітності щонайменше на 25% завдяки електронним сервісам та автоматизації [2].

Забезпечення безперервності бізнес-процесів у воєнний період набуває характеру управлінської функції, що має підтримуватися не лише організаційними рішеннями, а й технологічною архітектурою підприємства. Досвід українського бізнесу засвідчила результативність перенесення критичних даних і ІТ-систем у хмарні сервіси та використання віддаленого доступу, адже це зменшує залежність від конкретної локації і фізичних носіїв. Для малих та середніх підприємств (МСП) хмарні рішення є економічно доцільними, оскільки забезпечують доступ до обчислювальних ресурсів і сервісів без капітальних витрат на власну інфраструктуру. Великі підприємства, як правило, комбінують хмарні середовища з внутрішніми резервними потужностями. Водночас наявність резервних копій не гарантує

стійкість, якщо не сформовано технологічно підтримуваний план аварійного відновлення із визначеними ролями, строками відновлення і порядком пріоритезації процесів.

З огляду на затяжний характер воєнних ризиків доцільно доповнити вже поширені рішення (хмара, резервне живлення, альтернативні канали зв'язку) новими інноваційними підходами, зокрема:

- по-перше, перспективним є створення мережі регіональних «континуїтет-хабів» для бізнесу (на базі індустріальних парків, бізнес-інкубаторів або центрів підтримки підприємців). Це можуть бути стандартизовані майданчики з автономним енергоживленням, резервним інтернетом, захищеними робочими місцями та базовими хмарними сервісами «під ключ». Для МСП такий хаб знижує вартість готовності до блекаутів і забезпечує можливість тимчасово перенести критичні операції, а для великого бізнесу слугує резервною локацією для окремих команд або функцій;

- по-друге, доцільним є запуск «BCP-in-a-box» (комплектів безперервності) як стандарту для МСП. Наприклад, попередньо налаштований набір з маршрутизатором, UPS/акумулятором, резервним каналом зв'язку, захищеним VPN та інструкціями відновлення, що може закуповуватися підприємствами самостійно або через механізм часткової компенсації;

- по-третє, для бізнесів із високою залежністю від зв'язку варто розвивати «offline-first» цифрові процеси. Зокрема, локальні касові/складські рішення, що працюють без інтернету з подальшою синхронізацією, а також резервні сценарії комунікації на рівні громади (малі mesh-мережі для обміну короткими службовими повідомленнями між точками продажу/складами у разі тривалих збоїв зв'язку).

Окрему увагу доцільно приділити інституційним механізмам цифрової стійкості. Доцільним є формування модуля «безперервність бізнесу» у рамках екосистеми підтримки підприємців (із наборами типових сценаріїв, чек-листами, шаблонами політик доступу, картами критичних процесів, інструментами оцінки готовності та системою сповіщень про ризики на рівні регіону). Для МСП це створює «короткий шлях» до впорядкованих рішень без залучення дорогих консультантів, а для підприємств середнього й великого масштабу може стати базою для уніфікації мінімальних стандартів континуїтету в ланцюгах постачання (коли підрядники/постачальники підтверджують наявність мінімальної готовності).

Також зауважимо, що віддалене управління і робота стали нормою для більшості підприємств у воєнний час. Пандемія COVID-19 ще раніше привчила бізнес до гнучких форматів, і цей досвід став у пригоді з початком війни. Там, де це можливо, компанії перевели співробітників на дистанційний режим або гібридний формат роботи. Цифрові платформи для командної роботи такі як Slack, Microsoft Teams, Zoom, Google Workspace забезпечують постійну координацію та комунікацію розподілених команд.

Важливо, що підприємствам не довелося «винаходити з нуля» нові інструменти взаємодії. Більшість вже використовували їх у тій чи іншій мірі, тож під час війни відбулося швидке нарощення масштабу використання цих рішень. А. Комишева, Х. Роте, Л. Вессель відзначають, що українські МСП, які мали напрацювання у цифрових комунікаціях до війни, змогли просто інтенсифікувати їх застосування, не марнуючи час на навчання з нуля. Наприклад, у згаданій компанії MacPaw для екстреного зв’язку створили резервні канали. Окрім основного корпоративного месенджера, усіх співробітників підключили до групи у захищеному месенджері Signal для оперативних сповіщень у кризових ситуаціях [3].

Подібно й інші підприємства впроваджують декілька каналів зв'язку (електронна пошта, месенджери, телефонія) на випадок, якщо якийсь з них тимчасово недоступний. Для МСП такі рішення часто доступніші (є безкоштовні чи недорогі сервіси), і вони дозволяють навіть маленьким командам, розкиданим по різних містах або країнах, працювати синхронно. Великі корпорації, у свою чергу, інвестують у власні захищені платформи, VPN і інші засоби дистанційного доступу, щоб масштабувати віддалену роботу тисяч співробітників. Тому, вважаємо, що платформи віддаленого управління потрібно розвивати надалі.

Хочемо наголосити також на зміщенні акценту з формального опису ризиків на керованість критичних процесів. Підприємство має чітко знати, які 3-5 функцій забезпечують життєздатність, які ресурси для них потрібні та в який спосіб вони підтримуються за дефіциту часу, персоналу, електроенергії чи зв'язку. Для МСП першочерговим є створення «мінімально достатнього контуру керування» (короткий перелік пріоритетів, відповідальних осіб, контактів, резервних каналів комунікації та фінансових інструментів), тоді як для середніх і великих підприємств доречною є побудова портфеля сценаріїв із визначеними тригерами переходу між ними.

У фокусі управління має бути не прогнозування війни, а швидкість відновлення. Тому базовим показником ефективності антикризової системи доцільно визначати час повернення до операційної спроможності (відновлення продажів, постачань, виробництва, сервісу) та здатність працювати в «режимі деградації», коли частина процесів тимчасово вимикається без зупинки бізнесу [4].

Для цього рекомендовані наступні заходи (рис. 1).

Гнучке управління в умовах війни доцільно підкріпити короткими циклами ухвалення рішень і регулярним переглядом планів. Практично це означає впровадження щотижневого «антикризового контуру»: оцінка

ключових ризиків, уточнення сценарію на найближчі 2-4 тижні, перерозподіл ресурсів і перевірка готовності (зв'язок, доступи, резерви). Для МСП ефективним є формат «15-хвилинного штабу» керівника з відповідальними за фінанси, продажі та операції; для більших компаній (короткі цикли управління в межах підрозділів із централізованою координацією). У результаті антикризове планування перетворюється на механізм стабілізації, що забезпечує керованість рішень і знижує залежність підприємства від випадкових обставин, зберігаючи здатність швидко адаптувати бізнес-модель та канали збуту під зміну ринку.

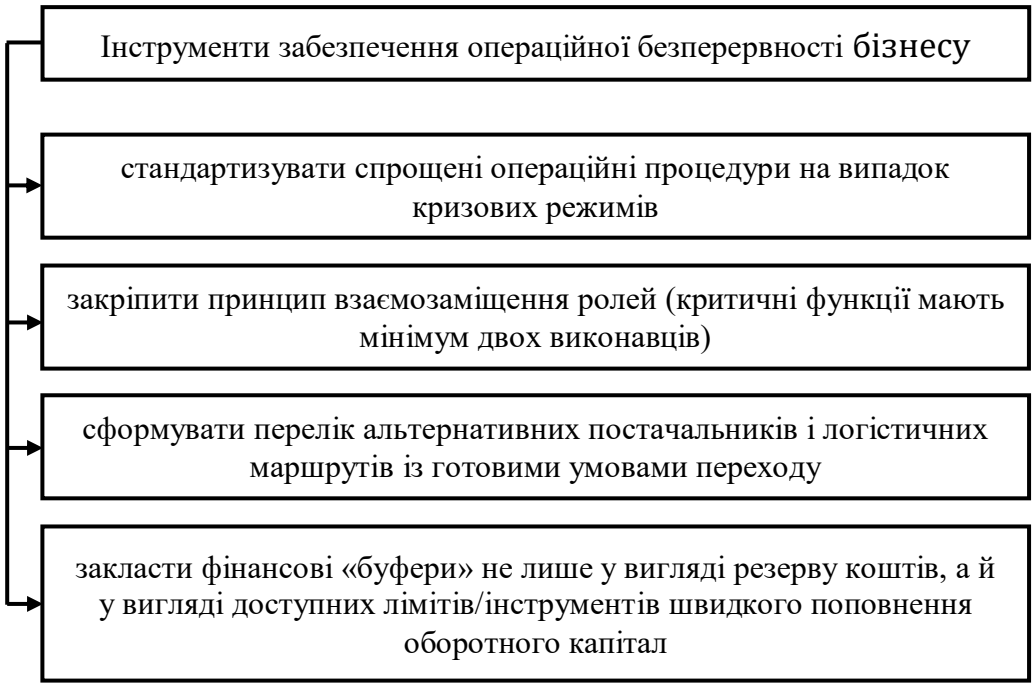


Рис.1. Інструменти забезпечення операційної безперервності бізнесу

Джерело: складено автором

Війна ведеться не лише на фізичному фронті, а й у кіберпросторі, тож кібербезпека бізнесу набула надзвичайної ваги. Підприємництво має інвестувати в сучасні засоби кіберзахисту: шифрування даних, багатофакторну автентифікацію для доступу до корпоративних систем,

брандмауери та системи виявлення вторгнень, регулярне оновлення програмного забезпечення. Не менш значущим є навчання персоналу кібергігієні, працівники повинні вміти розпізнавати підозрілі листи, дотримуватися правил безпеки при роботі з інформацією. Під час війни чимало компаній стикнулися з необхідністю працювати з різних локацій і пристроїв, тож впровадження політики Zero Trust (нульової довіри) стало актуальним навіть для МСП [3]. Тобто, доступ до систем надається мінімально необхідний і постійно перевіряється, незалежно від того, з корпоративної мережі входить користувач чи з домашнього інтернету.

Для малого бізнесу вищезазначене може бути реалізовано через використання хмарних сервісів з вбудованими функціями безпеки та простими у використанні інструментами (менеджери паролів, сервіси резервного копіювання з автоматичним шифруванням, тощо). Великі підприємства, зі свого боку, часто співпрацюють із професійними провайдерами кібербезпеки, впроваджують системи моніторингу мереж у режимі 24/7, створюють окремі кіберцентри.

Не можна залишати поза увагою і захист фізичних ІТ-активів. В умовах ракетних ударів та бойових дій офісна техніка, сервера та обладнання можуть бути знищені або викрадені. Тому підприємці ще з початку війни подбали про евакуацію найціннішого обладнання в безпечніші регіони або країни. Дехто сформував запас критично важливого «заліза» (ноутбуки, жорсткі диски, мережеве обладнання) на випадок, якщо постачання нових буде неможливим. Такі апаратні резерви особливо важливі для середнього бізнесу та виробничих компаній, де вихід з ладу однієї машини може зупинити весь процес. МСП часто не мають великих складів резервного обладнання, але можуть заздалегідь домовитися про лізинг чи оренду техніки, або створити спільні фонди взаємодопомоги з іншими підприємствами на випадок форс-мажору.

Підкреслимо, що кіберзахист і захист даних – це сфера, де рішення для всіх підприємств багато в чому спільні. І малий стартап, і велика корпорація мають робити резервні копії, оновлювати системи, ставити антивіруси та вчити персонал безпеки. Різниця лише в масштаб, адже великі компанії витрачають більше ресурсів і можуть впроваджувати найсучасніші комплекси захисту, тоді як МСП покладаються на більш стандартні, але все одно ефективні засоби.

Цифрові канали збуту та онлайн-експорт уже довели свою ефективність у період воєнних потрясінь, однак подальше підвищення стійкості підприємництва потребує переходу від використання окремих маркетплейсів і рекламних інструментів до побудови нових платформних моделей взаємодії ринку [5]. Виникає необхідність у формуванні багаторівневої цифрової екосистеми збуту, орієнтованої не лише на продаж, а й на стабілізацію попиту, кооперацію виробників та зниження ринкових ризиків. Використання платформ попереднього контрактування попиту та експортних цифрових консорціумів забезпечує прогнозованість замовлень і спрощує вихід на зовнішні ринки, що особливо важливо за умов порушених логістичних ланцюгів і нестабільного внутрішнього попиту.

Підключення аналітичних сервісів прогнозування збуту розширює інформаційну базу управлінських рішень, дозволяє підприємствам оперативно коригувати товарну та цінову політику. Інтеграція збутових платформ із фінансовими інструментами та логістичними модулями формує єдиний цифровий контур операційної підтримки продажів.

Висновки. Таким чином, напрямами підвищення стійкості підприємницької діяльності в умовах війни є формування інфраструктури цифрової безперервності бізнесу через створення регіональних континуїтет-хабів, запровадження стандартизованих комплектів безперервності для підприємств (BCP-in-a-box) та розвиток offline-first операційних процесів із

подальшою синхронізацією даних. Реалізація цих заходів дозволяє знизити залежність бізнесу від локальної інфраструктури, скоротити час відновлення операцій та зробити антикризову готовність доступною для малих підприємств.

Необхідно впровадити управлінські інновації, а саме: моделі «мінімально достатнього контуру керування», системи коротких антикризових циклів прийняття рішень, стандартизованих спрощених процедур роботи в кризових режимах та принципу обов'язкового взаємозаміщення критичних функцій. Окремий інноваційний блок становлять платформні рішення у сфері збуту та експорту, зокрема це кооперативні цифрові маркетплейси МСП, платформи попереднього контрактування попиту, цифрові експортні консорціуми, а також інтегровані моделі «збут + фінансування», що поєднують продажі з інструментами факторингу та гарантування платежів.

Список використаних джерел

1. Левчинський Д.Л., Ступнікер Г.Л., Каширнікова І.О., Зозуля Н.В. Підприємництво України в умовах воєнного стану. *Економічний простір. №181.* 2022. С. 110-114.

2. Про схвалення Стратегії відновлення, сталого розвитку та цифрової трансформації малого і середнього підприємництва на період до 2027 року. Розпорядження Кабінету Міністрів України від 30 серп. 2024 р. № 821-р. URL: https://www.kmu.gov.ua/npas/pro-skhvalennia-stratehii-vidnovlennia-staloho-rozvytku-ta-tsyfrovoi-transformatsii-maloho-i-s821300824

3. Komysheva A., Rothe H., Wessel L. Entrepreneurial digital resilience in war: lessons from Ukrainian SMEs. Proceedings of the 59th Hawaii International Conference on System Science. 2026. URL: https://www.researchgate.net/

publication/395823396_Entrepreneurial_Digital_Resilience_in_War_Lessons_from_Ukrainian_SMEs

4. Harush A. Business resilience during conflict in Israel. Panorays Blog. 2023. URL: https://panorays.com/blog/business-resilience-during-conflict-in-israel

5. Тарасовський Ю. Бізнес не бачить перспектив покращення економічної ситуації найближчим часом – дослідження. Журнал «Forbs». 2023. URL: https://forbes.ua/news/biznes-poki-ne-bachit-perspektiv-pokrashchennya-ekonomichnoi-situatsii-dos-lidzhennya-16022023-11771

References

1. Harush, A. (2023). *Business resilience during conflict in Israel*. Panorays Blog. https://panorays.com/blog/business-resilience-during-conflict-in-israel

2. Komysheva, A., Rothe, H., & Wessel, L. (2026). Entrepreneurial digital resilience in war: lessons from Ukrainian SMEs. *Proceedings of the 59th Hawaii International Conference on System Science*. https://www.researchgate.net/ publication/395823396_Entrepreneurial_Digital_Resilience_in_War_Lessons_from_Ukrainian_SMEs

3. Levchynskyi, D. L., Stupniker, H. L., Kashyrnikova, I. O., & Zozulia, N. V. (2022). Pidpryiemnytstvo Ukrainy v umovakh voiennoho stanu [Entrepreneurship of Ukraine under martial law]. *Ekonomichnyi prostir*, (181), 110–114.

4. Cabinet of Ministers of Ukraine. (2024, August 30). *Pro skhvalennia Stratehii vidnovlennia, staloho rozvytku ta tsyfrovoi transformatsii maloho i serednoho pidpryiemnytstva na period do 2027 roku* [On approval of the Strategy for recovery, sustainable development and digital transformation of small and

medium-sized entrepreneurship for the period until 2027] (Order №. 821-r). https://www.kmu.gov.ua/npas/pro-skhvalennia-stratehii-vidnovlennia-staloho-rozvytku-ta-tsyfrovoi-transformatsii-maloho-i-s821300824

5. Tarasovskyi, Yu. (2023, February 16). Biznes ne bachyt perspektyv pokrashchennia ekonomichnoi sytuatsii naiblyzhchym chasom – doslidzhennia [Business does not see prospects for improving the economic situation in the near future – research]. *Forbes Ukraine*. https://forbes.ua/news/biznes-poki-ne-bachit-perspektiv-pokrashchennya-ekonomichnoi-situatsii-dos-lidzhennya-16022023-11771