

DOI: <https://doi.org/10.35774/econa2025.02.465>

JEL classification: G32, H56, D81, M21, L21, D02

UDC: 658:005.934:336.6:355.02

Віталій МОЖУК

аспірант,

Західноукраїнський національний університет, Україна

Володимир МОЖУК

аспірант,

Західноукраїнський національний університет, Україна

АРХІТЕКТУРА ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА У ВОЄННІЙ ЕКОНОМІЦІ

АНОТАЦІЯ

Вступ. В умовах воєнної економіки фінансова безпека підприємства з «набору статичних коефіцієнтів» трансформується у динамічну систему стійкості, здатну витримувати каскадні енергетичні та логістичні збої, підвищену макрофінансову волатильність і кіберзагрози. Концентрація екзогенних та ендогенних чинників ризику підсилює актуальність подальших теоретичних досліджень архітектури фінансової безпеки та розроблення прикладного інструментарію її оцінювання і управління в галузях із високою воєнною експозицією.

Мета. Розробити концептуальну архітектуру фінансової безпеки підприємства у воєнній економіці, що інтегрує інституційний (зовнішній) і ресурсний (внутрішній) контури, та формалізувати її у вигляді інтегрального індексу FSAI з режимною логікою «мир — війна — відновлення» для управлінської інтерпретації та порівняння профілів безпеки між підприємствами і галузями.

Метод (методологія). Використано структурно-функціональний підхід для виокремлення підсистем і каналів взаємодії; положення інституційної економіки для моделювання «правил гри» та зовнішніх обмежень; засади Enterprise Risk Management для інтегрованого бачення ризиків і визначення апетиту до ризику; індексний підхід із нормуванням показників та вагуванням субіндексів інституційної стабільності та ресурсної стійкості; сценарне теоретичне моделювання ситуацій у логістиці, агросекторі та енергетиці.

Результати. Сформовано двохшарову архітектуру фінансової безпеки підприємства («інституції × ресурси») з описом її функцій, інтерфейсів та механізмів зворотного зв'язку; запропоновано інтегральний індекс FSAI як кількісну репрезентацію архітектури, визначено набір індикаторів для кожного субіндексу та правила їхнього агрегування; уведено режимну логіку адаптивної зміни ваг інституційного і ресурсного компонентів залежно від інтенсивності екзогенних шоків; продемонстровано прикладну придатність підходу для діагностики «вузьких місць» і пріоритезації управлінських інтервенцій (державні гарантії й страхування воєнних ризиків, буфери ліквідності, реструктуризація боргу, хеджування валютних і процентних ризиків, впровадження BCP/DR і підвищення прозорості розкриттів).

Ключові слова: фінансова безпека підприємства; воєнна економіка; архітектура фінансової безпеки; інституційний підхід; ресурсний підхід; інтегральний індекс FSAI; управління ризиками; ліквідність; капітальна структура

© Віталій Можук, Володимир Можук, 2025

Отримано: 11.04.2025 р.

Рекомендовано до друку: 14.05.2025 р.

Опубліковано: 28.05.2025 р.



Ця стаття розповсюджується на умовах ліцензії Creative Commons Attribution-NonCommercial 4.0, яка дозволяє необмежене повторне використання, розповсюдження та відтворення на будь-якому носії, за умови правильного цитування оригінальної роботи.

Як цитувати:

Можук В., Можук В. Архітектура фінансової безпеки підприємства у воєнній економіці. *Економічний аналіз*. 2025. Том 35. № 2. С. 465-484. DOI: <https://doi.org/10.35774/econa2025.02.465>

Вступ

В умовах воєнної економіки фінансова безпека підприємства перетворюється з набору «статичних» контрольних показників на динамічну систему стійкості, яка має витримувати каскадні шоки — перебої енергопостачання і логістики, підвищену макрофінансову волатильність, санкційні обмеження та зростання кіберзагроз. Класичні підходи, що зосереджуються на коефіцієнтному аналізі або локальних ризиках, виявляються методологічно недостатніми, оскільки не враховують водночас і екзогенну інституційну турбулентність (політика, регулювання, ринкова інфраструктура), і ендегенні можливості підприємства (капітал, ліквідність, процеси управління ризиками). Це зумовлює потребу у новій архітектурі фінансової безпеки, здатній інтегрувати зовнішні інституційні механізми та внутрішні ресурсно-функціональні підсистеми фірми в єдине управлінське ціле. Саме таке бачення покладене в основу даного дослідження, де запропоновано двошарову модель «інституції — ресурси» та її формалізацію через узагальнений індекс FSAI (Financial Security Architecture Index).

Наукова проблема полягає у відсутності цілісної теоретичної конструкції, яка б: одночасно описувала зовнішній інституційний контур (монетарна та фіскальна політика, валютно-курсові режими, державні гарантії/страхування воєнних ризиків, логістичні та енергетичні обмеження) і внутрішній ресурсний контур (ліквідність, капітальна структура, ризик-менеджмент, BCP/DR, кіберзахист, прозорість розкриттів); встановлювала між ними причинно-функціональні зв'язки; надавала вимірник інтегрованого стану безпеки, придатний до порівнянь між підприємствами та галузями. На відміну від фрагментарних підходів — наприклад, виключно фінансових коефіцієнтів чи окремих карт ризиків — запропонована архітектура розглядає фінансову безпеку як систему, у якій інституційні рішення детермінують межі можливого для корпоративних політик, а якість внутрішнього фінансового управління визначає, наскільки

фірма здатна монетизувати зовнішні можливості й амортизувати зовнішні загрози.

Мета і завдання статті

Мета статті — розробити теоретичну архітектуру фінансової безпеки підприємства у воєнній економіці, що інтегрує інституційний і ресурсний рівні, та запропонувати її формалізацію через узагальнений індекс FSAI як інструмент концептуальної діагностики стійкості. Для досягнення мети розв'язуються такі завдання:

1. здійснити аналітико-синтетичне узагальнення підходів до економічної/фінансової безпеки та ERM, виокремивши детермінанти стійкості, релевантні воєнній економіці;
2. побудувати структурно-функціональну схему двошарової архітектури «інституції — ресурси» з чітким поділом ролей, функцій та каналів взаємодії;
3. сформулювати методологічні засади інтегрального індексу FSAI (субіндекси інституційної стабільності та ресурсної стійкості, правила нормування і ваголювання);
4. окреслити теоретичні сценарні імплікації (режими «мир — війна — відновлення») та принципи використання архітектури в управлінських рішеннях.

Теоретико-методологічну основу становлять структурно-функціональний підхід (для інвентаризації підсистем і їхніх функцій), засади Enterprise Risk Management (для інтегрованого погляду на ризики та визначення «апетиту до ризику»), а також елементи інституційної економіки (для моделювання «правил гри» і зовнішніх обмежень). Формалізація індексу FSAI пропонується як абстрактна, але операціоналізована конструкція: два субіндекси — інституційний (I_{ext}) та ресурсний (I_{res}) — агрегуються в єдиний показник $FSAI = \alpha \cdot I_{ext} + \beta \cdot I_{res}$, де вагові коефіцієнти відбивають відносну значущість зовнішнього та внутрішнього контурів у конкретному середовищі. Така постановка не претендує на емпіричну ідентифікацію у межах цієї роботи, але задає каркас подальшої валідації на панельних даних або в експертних оцінках.

Наукова новизна полягає у: концептуалізації фінансової безпеки як взаємодії двох взаємодоповнюваних щитів — інституційного

(зовнішнього) та ресурсного (внутрішнього); запропонованні інтегрального індексу FSAI як метрики архітектури безпеки, що дозволяє порівнювати профілі підприємств/галузей та виявляти «вузькі місця»; введенні режимної логіки («мир — війна — відновлення») для теоретичного картування зміни ваг α і β залежно від інтенсивності екзогенних шоків. У площині практичної значущості архітектура задає алгоритм пріоритезації управлінських інтервенцій: коли домінує зовнішній стрес (енергетичні/логістичні обмеження, валютні шоки), фокус зміщується на інституційні механізми (державні гарантії, страхування, регуляторна гнучкість), а в умовно стабільнішому середовищі — на внутрішню фінансову політику (ліквідність, структуру капіталу, ризик-менеджмент, прозорість розкриттів).

Секторний контекст (логістика, агро, енергетика) підкреслює релевантність запропонованої моделі: від мінливості транспортних коридорів і сезонної волатильності цін до ризиків пошкодження критичної інфраструктури — саме конфігурація архітектури визначає межу витривалості підприємств і траєкторію їхнього відновлення. Таким чином, стаття закладає теоретичні засади для побудови узгоджених політик фінансової стійкості на рівні фірм і для дизайну таргетованих інструментів підтримки на рівні держави.

Виклад основного матеріалу дослідження

Фінансова безпека підприємства традиційно розглядається як ключовий компонент економічної безпеки, що відображає здатність підприємства захистити свій фінансовий стан від загроз і забезпечити стійкий розвиток. Більшість науковців визначають фінансову безпеку підприємства як динамічний стан фінансової системи, здатної протистояти внутрішнім і зовнішнім загрозам [1]. Зокрема, наголошується, що фінансова безпека на рівні суб'єкта господарювання є багатограним явищем, стан якого постійно змінюється під впливом факторів середовища. Це означає, що поняття безпеки є не статичним “захищеним” станом, а динамічною характеристикою підприємства, яка вимагає безперервного

моніторингу фінансового стану та адаптації до нових викликів.

Сучасні дослідження фінансової безпеки особливо підкреслюють її еволюцію в умовах зростання нестабільності. За останні роки концепція фінансової безпеки трансформувалась зі стану пасивного захисту до динамічної адаптивної системи, здатної реагувати на турбулентність середовища. Відповідно, управління фінансовою безпекою все більше інтегрується з концепцією управління ризиками підприємства. Як зазначають Задорожний та ін., фінансова та економічна діяльність в умовах соціальної, економічної та військово-політичної нестабільності піддається системним ризикам, що ставить під загрозу як безпеку держави, так і бізнесу. Головна мета управління ризиками — забезпечити фінансову безпеку підприємства в процесі його розвитку та запобігти можливому зниженню ринкової вартості бізнесу через погіршення фінансового стану. Таким чином, ідеї Enterprise Risk Management (ERM) — інтегрованого управління ризиками — все частіше розглядаються як основа для підтримання фінансової стійкості підприємств.

Окремої уваги набувають питання фінансової безпеки підприємств у контексті воєнної економіки. Повномасштабна війна та запровадження воєнного стану в Україні створили безпрецедентні виклики для бізнес-середовища. Дослідження відзначають появу цілком реальних нових ризиків і загроз для ведення підприємницької діяльності на тлі війни. Зовнішні загрози набули вирішального значення, однак наявні методики оцінки рівня фінансово-економічної безпеки часто не враховують ці загрози. Фінансова безпека підприємств в умовах війни розглядається вже не просто як захищеність від традиційних фінансових ризиків, а як здатність адаптуватися до екстремальної турбулентності бізнес-середовища. Ситник Н., Половко Д. виокремлюють основні загрози фінансовій безпеці підприємств у воєнний період, серед яких: макроекономічні шоки, операційні ризики, фінансово-інвестиційні загрози, регуляторні обмеження та інформаційно-кібернетичні ризики [2]. Ці загрози суттєво перевищують типові ризики мирного часу та

потребують нових підходів до забезпечення стійкості бізнесу.

Крім того, вплив воєнних дій істотно диференціюється за секторами економіки. Аналіз показує, що підприємства різних галузей по-різному переживають кризові явища війни. Найбільша воєнна експозиція характерна для галузей логістики, агросектору та енергетики, які зазнали прямих ударів. Зокрема, у логістиці блокада українських морських портів на початку війни спричинила обвал експорту зерна більш ніж на 80% від довоєнного рівня. Підприємства вимушені були терміново переорієнтовувати постачання через альтернативні маршрути, що призвело до збільшення відстаней перевезень у 5 разів і зростання транспортних витрат у 3-4 рази. У сільському господарстві прямі збитки від воєнних дій обчислюються мільярдами доларів; аграрний сектор України зазнав значних втрат продукції та інфраструктури, поставивши під загрозу глобальну продовольчу безпеку. Не менш критично постраждала енергетична галузь: цілеспрямовані атаки на енергетичну інфраструктуру призвели до того, що вже до середини 2024 р. близько половини генеруючих потужностей країни було зруйновано або пошкоджено, залишивши в дії лише третину довоєнного енергетичного потенціалу [7]. Було знищено або виведено з ладу десятки крупних енергооб'єктів (у тому числі не менш ніж 18 великих ТЕЦ і понад 800 котелень) [8], що спричинило масштабні перебої в енергопостачанні. Таким чином, війна оголила вразливість критичних галузей і продемонструвала необхідність нової архітектури фінансової безпеки підприємств, здатної забезпечити стійкість у надзвичайно несприятливих умовах.

У науковій літературі дедалі частіше звучать заклики до системного, комплексного бачення фінансової безпеки бізнесу. Бакинта Г. та Ганущак Т. [6] наголошували на ролі фінансової безпеки підприємств як складової економічної безпеки держави, проте цілісного підходу до багаторівневого управління безпекою досі бракує. Вони запропонували розглядати архітектуру фінансової безпеки підприємства як багаторівневу систему, де на мікрорівні виділяються два основні рівні захисту. Перший – це безпека фінансових ресурсів підприємства

(власних, позикових, залучених коштів), що забезпечує фінансову стійкість базових ресурсів. Другий – це безпека за функціональними напрямками фінансової діяльності: податкова, кредитна, інвестиційна, валютна, розрахункова безпека тощо. Такий підхід фактично поєднує ресурсний вимір (стан і захист капіталу підприємства) з функціонально-інституційним виміром (спроможність підприємства безпечно виконувати фінансові функції в існуючому інституційному середовищі).

Отже, аналіз літератури свідчить про кілька важливих тенденцій. По-перше, фінансова безпека підприємства має розглядатися як *динамічна система*, що постійно адаптується до викликів, особливо за екстремальних умов воєнної економіки. По-друге, забезпечення фінансової безпеки потребує інтегрованого управління ризиками (ERM), яке б охоплювало всі аспекти діяльності підприємства – від репутаційних втрат до перебоїв постачання і кіберзагроз. І по-третє, необхідна чітка архітектура фінансової безпеки, що об'єднає інституційні механізми (регуляторні, ринкові, державні) та ресурсні можливості підприємства в єдину систему протидії загрозам. В існуючих дослідженнях бракує цілісного відображення такої архітектури, особливо з урахуванням реалій воєнної економіки. Це і визначає напрям даного дослідження – формування авторської концепції архітектури фінансової безпеки підприємства, заснованої на взаємодії інституційного та ресурсного рівнів захисту.

Методологічна основа дослідження ґрунтується на аналітико-синтетичному узагальненні теоретичних підходів, структурно-функціональному підході до побудови системи фінансової безпеки, а також на елементах концепції інтегрованого управління ризиками підприємства (Enterprise Risk Management, ERM). Застосовано економіко-математичне формалізування для розробки узагальненого індексу фінансової безпеки – Financial Security Architecture Index (FSAI). Така багатопідходова методологія дозволяє, з одного боку, сформулювати цілісну концептуальну модель архітектури фінансової безпеки, а з іншого – розробити кількісний інструментарій оцінювання рівня безпеки підприємства.

Концептуальна модель архітектури фінансової безпеки підприємства представлена у вигляді двох взаємопов'язаних рівнів (підсистем): інституційного та ресурсного (рис. 1). Інституційний рівень відображає зовнішні умови і механізми, в межах яких

функціонує підприємство, тоді як ресурсний рівень охоплює внутрішній потенціал та процеси, що забезпечують фінансову стійкість фірми. Кожен із цих рівнів, у свою чергу, має свою структуру елементів і функцій.

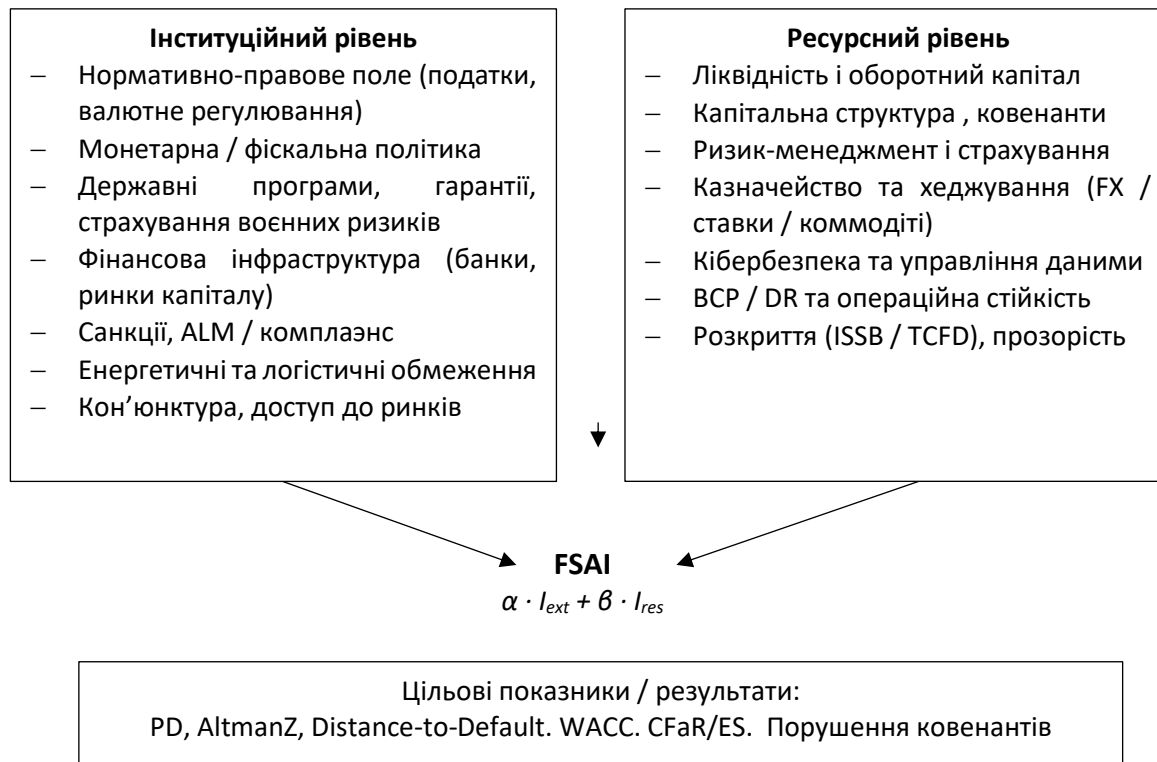


Рис. 1. Архітектура фінансової безпеки підприємства («інституції - ресурси»)

Інституційний рівень архітектури фінансової безпеки охоплює зовнішні *інституції та середовище*, що впливають на безпечну діяльність підприємства. Сюди належать: нормативно-правове забезпечення (закони, регуляції у фінансовій сфері, податкове та валютне регулювання тощо); фінансово-кредитна інфраструктура (стан банківської системи, ринку капіталу, страхового ринку); державна політика і підтримка (програми фінансової стабілізації, гарантії, субсидії в умовах війни); а також ринкові умови (кон'юнктура, доступ до логістики, вплив санкцій та міжнародної ізоляції ринку). Інституційний рівень визначає «правила гри» та загальний рівень зовнішніх ризиків. У воєнній економіці його роль особливо важлива, адже саме на цьому рівні генеруються такі загрози, як різкі зміни курсу валюти, інфляційні скачки, розриви ланцюгів постачань або нормативні обмеження. Аналіз воєнного періоду показав

появу численних нових екзогенних ризиків – від санкцій та торговельних бар'єрів до кібератак і фізичного знищення інфраструктури. Тому інституційна підсистема покликана забезпечити максимально сприятливі умови для виживання підприємств: держава та ринкові регулятори мають мінімізувати дестабілізаційні чинники, надавати підтримку критично важливим галузям, створювати компенсаторні механізми (наприклад, страхування воєнних ризиків, пільгове кредитування для підтримання ліквідності тощо).

Ресурсний рівень архітектури фінансової безпеки охоплює внутрішні фінансові ресурси та процеси управління ними в межах підприємства. Йдеться про капітал підприємства (власний, позиковий, залучений) і ефективність його використання, а також про всі функціональні напрямки фінансової діяльності, що забезпечують стійкість. У

структурі ресурсного рівня можна виділити такі основні компоненти: управління фінансовими ресурсами (формування оптимальної капіталізації та структури капіталу, підтримання достатньої ліквідності та платоспроможності); фінансове планування і контроль (бюджетування, прогнозування грошових потоків, контроль витрат); ризик-менеджмент на рівні підприємства (ідентифікація фінансових ризиків – кредитних, валютних, процентних, цінових; оцінка їх імовірності та впливу; розробка і впровадження заходів мінімізації ризиків); моніторинг та реагування (системи раннього попередження про кризові сигнали, антикризові протоколи дій). Таким чином, ресурсний рівень – це внутрішня підсистема безпеки, яка безперервно працює над підтриманням стійкого фінансового стану підприємства. В умовах воєнних потрясінь ця підсистема набуває проактивного характеру: підприємства змушені оперативно перебудовувати фінансові плани, створювати резерви, шукати альтернативні джерела фінансування та підвищувати гнучкість управління, щоб витримати зовнішні удари.

Структурно-функціональний підхід у даному дослідженні застосовано для чіткого розмежування функцій обох підсистем та встановлення між ними зв'язків. З позицій цього підходу, фінансова безпека постає як цілісна система, що виконує певну інтегральну

функцію (забезпечення стійкого розвитку підприємства), а кожен структурний елемент системи має свою роль. Інституційна підсистема виконує функцію зовнішнього щита – пом'якшення впливу середовища і надання ресурсів або регуляторних умов для стабільності. Ресурсна підсистема – це внутрішній щит, що забезпечує фінансову стійкість за рахунок грамотного управління ресурсами та ризиками всередині фірми. Їх взаємодія носить двосторонній характер: з одного боку, зовнішні інститути створюють рамкові умови і можуть надавати підтримку бізнесу, з іншого – саме стан внутрішніх фінансів визначає, наскільки підприємство здатне скористатися цими умовами або пережити несприятливі зміни. Для наочності було сформовано схему функціонування запропонованої архітектури (рис. 2), яка відображає цикл інформаційно-управлінської взаємодії між рівнями: моніторинг зовнішніх загроз → ідентифікація ризиків на ресурсному рівні → прийняття управлінських рішень (адаптація фінансової стратегії, залучення додаткових ресурсів, використання страхових та хеджувальних інструментів) → реалізація заходів на ресурсному та інституційному рівнях (внутрішні зміни, запит підтримки або реагування з боку державних програм) → оцінка ефективності та стану безпеки → повернення до моніторингу.

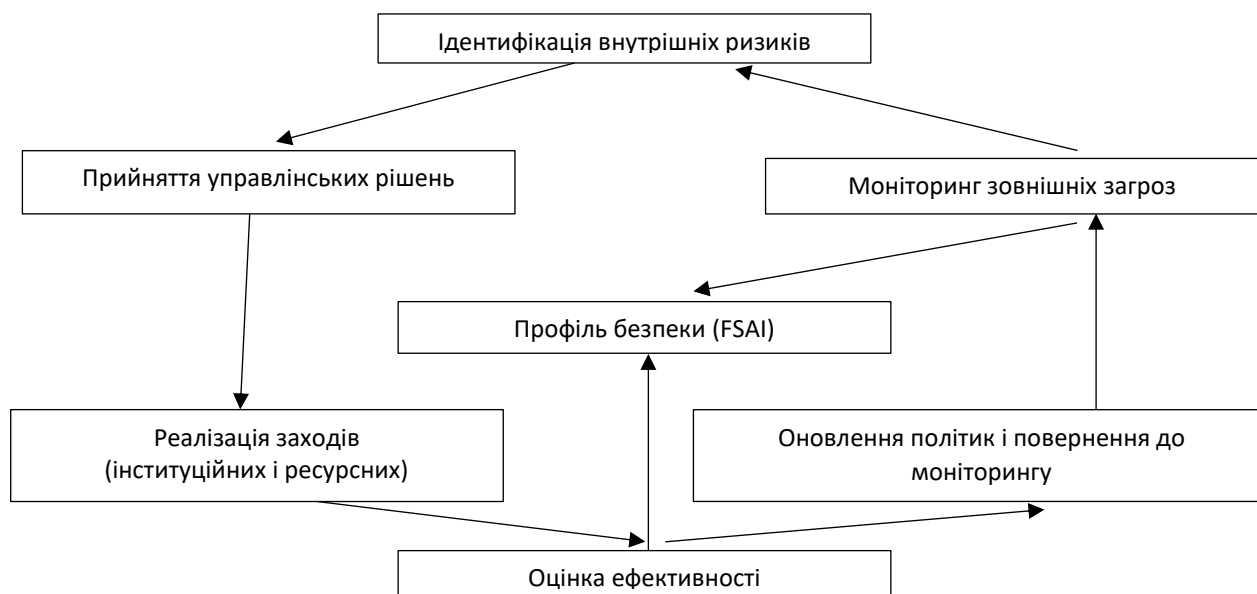


Рис. 2. Схема функціонування архітектури фінансової безпеки

Такий циклічний процес забезпечує динамічну стійкість системи, що відповідає рекомендаціям сучасного антикризового менеджменту: від реактивного “пожежного” гасіння криз перейти до проактивного управління на основі сценаріїв та готовності до турбулентності.

Наступним кроком методології стало економіко-математичне моделювання рівня фінансової безпеки шляхом побудови інтегрального індексу FSAI. Метою розробки індексу Financial Security Architecture Index є кількісна оцінка комплексного стану фінансової безпеки з урахуванням двох розглянутих рівнів. При формуванні FSAI враховано підходи попередніх дослідників до інтегральної оцінки фінансової безпеки. Зокрема, ряд авторів пропонують діагностувати безпеку на основі груп ключових показників фінансового стану – таких як ліквідність, фінансова стійкість, ділова активність, рентабельність – що комплексно відображають здатність підприємства протистояти загрозам. У працях українських вчених зустрічається підхід, де рівень фінансової безпеки визначається через шкали фінансової стабільності, платоспроможності та ризику. В умовах війни дослідники також додають критерії ефективності антикризового управління та якості фінансового менеджменту. Спираючись на ці ідеї, у нашій моделі FSAI передбачено агрегування показників за двома блоками: інституційна стабільність та ресурсна стійкість.

- Блок інституційної стабільності в індексі FSAI покликаний відобразити ступінь сприятливості та передбачуваності зовнішнього середовища для даного підприємства. Його кількісна оцінка може будуватися на індикаторах макро- і мезорівня, релевантних для конкретного бізнесу. Наприклад, індекс інфляції та коливання валютного курсу (як показники макрофінансової стабільності), індекс ділових очікувань або PMI для галузі (як сигнал загальної економічної кон’юнктури), рейтинг ризику країни або регіону, рівень доступності кредитних ресурсів (процентні ставки, обсяги кредитування), ступінь регуляторного навантаження (частота та характер змін податкового і фінансового законодавства), рівень розвитку фінансової

інфраструктури (надійність банків, страхових компаній) тощо. У воєнний час до цього блоку додаються також специфічні воєнні індикатори: наприклад, індекс інтенсивності бойових дій у регіоні присутності підприємства, наявність логістичних коридорів, доступність енергопостачання. Кожен із цих показників потребує нормування (приведення до безрозмірного виду) та вагового коефіцієнта, що відбиває його значущість для фінансової безпеки конкретного підприємства. В результаті агрегування формується субіндекс I_{ext} (умовно – інституційний індекс безпеки).

- Блок ресурсної стійкості відображає безпосередньо фінансовий стан і можливості підприємства протистояти потрясінням. Він розраховується на основі класичних фінансових коефіцієнтів та показників діяльності підприємства, але з акцентом на їх динаміку і здатність витримувати кризові навантаження. До набору таких показників увійшли: ліквідність (коефіцієнт поточної ліквідності, швидкої ліквідності; частка високоліквідних активів у структурі балансу); фінансова стійкість (коефіцієнт автономії – частка власного капіталу; співвідношення позикового і власного капіталу; запас фінансової міцності); рентабельність і ефективність (рентабельність активів, оборотність капіталу, маржа EBITDA – як індикатор здатності генерувати прибуток навіть у кризових умовах); ділова активність (динаміка виторгу, частка ринку, коефіцієнти обіговості коштів); ризиковість (покриття відсотків прибутком, диверсифікація джерел доходу, показники кредитного навантаження та кредитної історії підприємства). Важливо також урахувати якість фінансового менеджменту та ризик-менеджменту: наявність резервного капіталу, використання страхування, хеджування валютних ризиків, системи контролю та аудиту. В інтегральному індексі FSAI ці показники після нормування агрегуються у субіндекс I_{res} (умовно – ресурсний індекс безпеки).

Побудова узагальненого індексу здійснюється шляхом об’єднання двох

субіндексів: $FSAI = \alpha \cdot I_{ext} + \beta \cdot I_{res}$, де α і β – вагові коефіцієнти, що відображають відносну важливість зовнішніх та внутрішніх факторів для даного підприємства. У звичайних умовах, ймовірно, β (вага ресурсного блоку) є більшою, адже фінансовий стан підприємства багато в чому залежить від власного управління. Проте у воєнній економіці значимість зовнішніх факторів різко зростає – нестабільність середовища може переважити зусилля окремого підприємства. Тому при розрахунку FSAI для підприємств, що діють у зоні активних бойових дій або у стратегічно важливих галузях, вагу інституційного компоненту доцільно збільшувати.

Для практичного розрахунку FSAI використано підхід інтегрального оцінювання за допомогою нормування по відхиленню від еталону. Спочатку для кожного показника визначається бажаний напрям (позитивний чи негативний вплив на безпеку) та еталонне значення (наприклад, для коефіцієнта автономії еталон може бути 0,5 або вище; для інфляції – цільовий рівень НБУ тощо). Далі розраховуються нормовані бали показників (0 до 1) залежно від фактичного відхилення від еталону. Ці бали зважуються згідно з експертно визначеними коефіцієнтами важливості і підсумовуються у межах кожного блоку (зовнішнього та внутрішнього). Отримані значення I_{ext} та I_{res} агрегуються у загальний FSAI. Підсумковий індекс можна інтерпретувати за шкалою: чим ближче FSAI до 1 (або 100 %), тим вищий рівень фінансової безпеки підприємства; значення нижче певного порогу свідчать про зону небезпеки, що потребує негайних управлінських дій.

Запропонована концептуальна архітектура та методика індексної оцінки були апробовані шляхом теоретичного моделювання типових ситуацій воєнної економіки. Зокрема, було змодельовано сценарії для підприємств різних галузей (логістика, агро, енергетика) з високою воєнною експозицією. Для кожного сценарію змінювалися значення ключових показників (наприклад, скорочення виручки на 50% через втрату ринку збуту, зростання частки позикових коштів внаслідок кредитів на виплату зарплат, затримки платежів, інфляційний скачок і т. д.), після чого обчислювався FSAI. Це дозволило оцінити чутливість індексу до різних факторів та

перевірити узгодженість результатів із якісними оцінками (експертним очікуванням рівня ризику). Методологія показала адекватність: підприємства з кращими внутрішніми фінансовими показниками і доступом до зовнішньої підтримки мали вищі значення FSAI, що узгоджується з фактичними спостереженнями про їхню більшу стійкість під час війни.

Отже, методологія дослідження поєднує концептуальне моделювання архітектури фінансової безпеки та його кількісну реалізацію через інтегральний індекс. Це дає можливість як теоретично обґрунтувати складові фінансової безпеки підприємства у воєнній економіці, так і практично оцінити її рівень та вразливі місця для подальшого вдосконалення управлінських заходів.

На основі проведеного дослідження сформовано авторську класифікацію підсистем фінансової безпеки підприємства у вигляді дворівневої архітектури, що поєднує інституційний та ресурсний рівні. Основні результати теоретичного моделювання можна підсумувати таким чином:

1. Запропоновано дві головні підсистеми архітектури фінансової безпеки:

- *Інституційна підсистема* – зовнішня щодо підприємства система умов, правил та підтримки, яка визначає межі фінансової стійкості. Вона включає: регуляторно-нормативну компоненту (правове поле фінансової діяльності), інфраструктурну компоненту (фінансові інститути, ринки, логістичні мережі), макроекономічну компоненту (стабільність національної економіки, грошово-кредитну політику) та безпекову компоненту зовнішнього середовища (стан правопорядку, військову ситуацію, рівень загроз для бізнесу на території діяльності). Функція інституційної підсистеми – забезпечувати підприємству сприятливі та передбачувані умови, своєчасно нейтралізувати або компенсувати зовнішні негативні впливи. Як показало моделювання, за наявності сильних інституційних елементів (наприклад, працюючих механізмів страхування ризиків, державних гарантій кредитів, стабільної банківської системи) підприємства отримують “буфер” безпеки,

що значно підвищує їх шанси вистояти в кризу. Навпаки, слабкі чи несприятливі інституції (недосконале регулювання, відсутність підтримки, високі зовнішні ризики) різко знижують граничну стійкість фірми навіть за умови її ефективного менеджменту.

- *Ресурсна підсистема* – внутрішня система фінансових ресурсів, процесів та компетенцій підприємства, спрямована на протидію загрозам і забезпечення безперервності діяльності. Вона охоплює: матеріально-фінансові ресурси (капітал, активи, грошові резерви), управлінські процеси (планування, облік, контроль), систему управління ризиками (політики і процедури оцінки та зниження ризиків) та кадрово-організаційний компонент (професіоналізм фінансового менеджменту, культура ризик-менеджменту). Функція ресурсної підсистеми – підтримувати фінансову рівновагу підприємства шляхом гнучкого і своєчасного управління ресурсами, збереження платоспроможності та рентабельності, навіть коли зовнішнє середовище дестабілізується. Ключовим фактором успіху є адаптивність: результати моделювання підтвердили думку, що відсутність адаптивного підходу і недооцінка фінансових ризиків негативно впливають на ефективність діяльності та фінансовий стан підприємств. Натомість підприємства, які запровадили антикризове планування, диверсифікували джерела фінансування і заздалегідь готували “плани В” на випадок форс-мажорів, демонструють значно вищий рівень фінансової стійкості у критичних ситуаціях.

2. Інституційний та ресурсний рівні мають суттєві відмінності, які було проаналізовано і зіставлено (табл. 1). Основні точки порівняння включають:

- *Джерело загроз*: інституційний рівень має справу переважно з екзогенними загрозами (шоки в економіці, регуляторні зміни, військові дії, ринки, що закриваються), тоді як ресурсний – з ендогенними (внутрішні прорахунки в управлінні, фінансові дисбаланси,

операційні збої) та адаптацією до екзогенних.

- *Суб’єкти управління*: інституційна підсистема формується та контролюється зовнішніми суб’єктами – державними органами, фінансовими регуляторами, міжнародними інституціями та ринковими учасниками (банками, постачальниками, страховиками). Ресурсна підсистема цілком залежить від менеджменту підприємства – фінансових директорів, менеджерів з ризиків, власників, які приймають рішення щодо структури капіталу, інвестицій, витрат тощо. Таким чином, відповідальність за фінансову безпеку розподілена: держава і ринок відповідають за “правила гри” та підтримку, а керівництво компанії – за ефективну гру в межах цих правил.
- *Інформаційна основа і регламенти*: інституційний рівень спирається на стратегії національної безпеки, державні програми, нормативні акти та розпорядження регуляторів. Натомість ресурсний – на корпоративні стратегії, політики фінансової безпеки підприємства, внутрішні інструкції та накази керівництва. Тобто перший рівень діє за допомогою публічних механізмів і законів, другий – за допомогою внутрішніх регламентів і процедур, розроблених під специфіку фірми.
- *Механізми контролю та впливу*: на інституційному рівні вплив реалізується через регулювання, нагляд, моніторинг макропоказників і застосування інструментів економічної політики (податків, ставок, інтервенцій), що впливають на умови функціонування всіх підприємств. На ресурсному рівні механізми – це управлінські рішення підприємства, планові та позапланові заходи, спрямовані на досягнення високого рівня фінансової безпеки фірми та захист інтересів стейкхолдерів навіть за наявності загроз. Іншими словами, держава та ринок можуть “підкривати гвинтики” системи в цілому, тоді як фірма налаштовує власний “внутрішній механізм”, щоб він працював стабільно в умовах, що склалися.
- *Ресурси та інструменти*: інституційна підсистема оперує головним чином

нормативними та фінансовими інструментами макrorівня – законами, стандартами, ліцензуванням, державними фондами, фондами підтримки, центральними банками. Ресурсна – використовує внутрішні фінансові інструменти – резервні фонди, внутрішній контроль, страхування, договори хеджування, диверсифікацію активів,

реінвестування прибутку, оптимізацію витрат та ін. Успішна реалізація архітектури передбачає, що інструменти обох рівнів застосовуються узгоджено: напр., якщо держава пропонує пільгові кредити під гарантії, підприємство має достатньо ліквідності та план розвитку, щоб ними скористатися.

Таблиця 1. Порівняльна характеристика інституційного та ресурсного рівнів фінансової безпеки підприємства

Критерій	Інституційний рівень (зовнішній)	Ресурсний рівень (внутрішній)
1	2	3
Характер загроз	Екзогенні шоки: війна, санкції, регуляторні зміни, курсові/цінові сплески, логістичні та енергетичні обмеження	Ендогенні дисбаланси: ліквідність, боргове навантаження, операційні збої, кіберінциденти; адаптація до зовнішніх шоків
Суб'єкти впливу/контролю	Держава, регулятори (НБУ/НКЦПФР), міжнародні інституції, банки, страховики, біржі, інфраструктурні оператори	Власники/рада директорів, CFO, ризик-менеджер, казначейство, внутрішній аудит
Нормативна база	Законодавчі акти, податкове/валютне регулювання, стандарти звітності (IFRS/ISSB), наглядові вимоги	Корпоративні політики: фінансова стратегія, політика ліквідності, кредитна/податкова/інвестиційна політика, BCP/DR, кіберполітика
Інструменти/політики	Держгарантії, пільгове кредитування, воєнне страхування, валютні режими, фіскальні стимули, регуляторні послаблення	Резерви ліквідності, реструктуризація боргу, хеджування (FX/ставки/коммодіті), страхування, оптимізація запасів/дебіторки
Механізми забезпечення/канали впливу	Економічна політика, пруденційний нагляд, інтервенції на ринках, держзакупівлі/субсидії, регулювання тарифів	Планування/бюджетування, казначейські ліміти, ковенанти, платіжна дисципліна, внутрішній контроль та аудит
Джерела даних/інформації	НБУ/Мінфін/ДССУ, біржові індикатори, PMI/індекси очікувань, дані доходностей ОВДП, енергетичні та логістичні показники	МСФЗ/фінзвітність, управлінський облік, платіжні календарі, реєстри договорів, журнали IT/безпеки
KPI/індикатори оцінки	Інфляція, облікова ставка, волатильність FX/цін, індекси ризику країни/регіону, доступність кредиту	Current/Quick ratio, Net debt/EBITDA, Interest coverage, CFaR/ES, Altman Z, PD, порушення ковенантів

Продовження таблиці 1

1	2	3
Горизонт планування й моніторинг	Квартал–рік; цикли бюджетної/монетарної політики, фази воєнного конфлікту	Тиждень–місяць; щоденні касові позиції, щотижневі стрес-тести, місячні ревізії бюджетів
Основні обмеження	Фіскальні/монетарні рамки, санкційні бар'єри, обмеження енергетики/логістики, регуляторні ризики	Ліміти ліквідності, дефіцит оборотного капіталу, кадрові/технологічні вузькі місця, ІТ-обмеження
Типові збої/ризиків (failure modes)	Різка зміна правил, закриття ринків, блокада портів, перебої енергопостачання, кібератаки/фізичні атаки на інфраструктуру	Касові розриви, дефолт за ковенантами, зрив постачань, помилки у хеджуванні, витік даних/злам фінсистем
Типові управлінські дії у кризі	Податкові канікули, капітальні/кредитні гарантії, надзвичайні тарифи/субсидії, розширення страхових покриттів	«Cut & hold» бюджети, пріоритезація платежів, активація BCP/DR, переговори з кредиторами, консервативні hedge-стратегії
Вартісні наслідки (cost drivers)	Премії ризику в ставках/спредах, податкові навантаження, зовнішні тарифи/логістичні витрати	WACC, вартість хеджів/страхування, утримання резервів, простої/відновлення
Критерії ефективності	Прогнозованість середовища, доступність ресурсів, швидкість/адресність підтримки	Стійка ліквідність, виконання ковенантів, стабільність CFaR/ES, збереження маржинальності
Взаємодія/інтерфейс між рівнями	Комунікація політики, канали доступу до програм, зворотний зв'язок із бізнесом	Подання заявок/звітів, використання інструментів підтримки, сигналізація потреб/ризиків
Роль у фінансовій безпеці	Створює «буфер» та правила гри для стійкості бізнесу	Реалізує безпеку на практиці; забезпечує виживання й адаптацію
Методи оцінювання ризиків	Макро- та секторні стрес-тести, рейтинги країнового ризику, регуляторні сценарії	Сценарний аналіз, VaR/ES, cash-flow stress testing, ковенантний моніторинг, EWS/ML-сигнали

Скорочення: BCP/DR — Business Continuity Planning / Disaster Recovery; FX — валютний ризик; PD — імовірність дефолту; ES — Expected Shortfall; CFaR — Cash-Flow-at-Risk; WACC — середньозважена вартість капіталу; EWS — система раннього попередження; ML — машинне навчання.

На рис. 2 узагальнено схему взаємодії інституційного та ресурсного рівнів у забезпеченні фінансової безпеки підприємства. В нормальних умовах (відносної стабільності) інституційна підсистема забезпечує стале середовище: прогнозовані “правила гри”, доступ до фінансових ресурсів, базову інфраструктуру. Ресурсна підсистема, спираючись на це середовище, здійснює

ефективне управління фінансами: досягає оптимальної структури капіталу, забезпечує прибутковість, формує резерви. Між рівнями існує інформаційний обмін: підприємство відстежує сигнали та зміни зовнішнього середовища, тоді як результати діяльності підприємств (агреговано) впливають на економічну ситуацію, яку моніторять державні інституції.

В умовах кризового впливу (наприклад, воєнного удару по економіці) схема функціонування активізує захисні контури. Припустимо, виникає зовнішній шок: різкий стрибок курсу, втрата доступу до сировини через блокаду, нові податкові обмеження або пряме фізичне пошкодження активів. Інституційний рівень реагує заходами політики: пом'якшення валютного регулювання, надання податкових канікул, компенсацій або субвенцій, запуск державних гарантій для кредитів, контроль цін на критичні ресурси тощо. Ресурсний рівень підприємства одночасно реалізує свій план антикризових дій: задіюються страхові виплати (якщо подія була застрахована), активуються резервні фонди ліквідності, переглядається бюджет (урізання витрат, відкладення інвестицій), можливо, здійснюється реструктуризація боргів чи пошук додаткового фінансування. Важливо підкреслити, що скоординованість реакцій двох рівнів визначає успіх протидії загрозі. Якщо державна програма підтримки працює повільно або не адресна – підприємство може не втриматися, вичерпавши власні ресурси. І навпаки, якщо підприємство не має плану дій і компетенцій, то навіть наявність держпідтримки не врятує його від паніки та помилок. Тому архітектура фінансової безпеки повинна передбачати чіткі канали комунікації та взаємодоповнення: держава (та інші зовнішні суб'єкти) мають оперативно інформувати бізнес про доступні заходи і ризики, бізнес повинен сигналізувати про свої потреби і використовувати зовнішні інструменти грамотно.

Результатом теоретичного моделювання є концепція інтегрального показника FSAI, який кількісно відбиває описану архітектуру. Розрахунок FSAI у тестових сценаріях показав, що він корелює з фактичною стійкістю підприємства. Наприклад, підприємства агросектору, що зазнали катастрофічних втрат інфраструктури і ринків збуту в 2022 р., мали вкрай низькі значення індексу (близькі до порогових), що відповідає їх критичному стану. Натомість компанії у сфері IT-послуг, менш залежні від фізичної інфраструктури і підтримувані державними програмами релокації, отримали значно вищий FSAI – їхня фінансова безпека виявилася надійнішою.

Важливо, що індекс дозволяє порівнювати рівень фінансової безпеки різних підприємств та виявляти “вузькі місця”. Так, в одному із сценаріїв для логістичної компанії інституційний субіндекс I_{ext} був дуже низьким через блокаду портів і зростання цін на паливо, тоді як ресурсний I_{res} залишався відносно прийнятним (компанія мала хороший запас міцності). Це вказує, що основні проблеми – зовнішні, і потрібні рішення саме на інституційному рівні (альтернативні маршрути, державні компенсації). В іншому випадку, виробниче підприємство в глибокому тилу мало досить сприятливе середовище (I_{ext} високий), але слабкий внутрішній менеджмент (I_{res} низький, через високу залежність від кредитів і низьку ліквідність) – відповідно, навіть без зовнішнього тиску воно є уразливим, і пріоритетом мають стати внутрішні реформи і покращення фінансової дисципліни. Таким чином, класифікація підсистем та FSAI працюють у парі: перша концептуально описує що і де слід зміцнювати, другий дає змогу виміряти *наскільки* надійною є кожна складова безпеки.

Узагальнюючи результати, запропонована архітектура фінансової безпеки підприємства у воєнній економіці демонструє наступні переваги: (1) Комплексність: враховано максимальний спектр факторів – від макроекономічних до внутрішньофірмових, що відповідає реальній природі фінансової безпеки як багатоаспектної категорії. (2) Адаптивність: модель опирається на динамічне управління та циклічний процес оновлення рішень, що дозволяє враховувати швидкоплинні зміни воєнного часу. (3) Вимірюваність: індексний підхід (FSAI) переводить якісні міркування у кількісні оцінки, даючи змогу відстежувати прогрес або погіршення стану безпеки підприємства. (4) Прикладна значущість: класифікація підсистем спрощує розробку практичних рекомендацій – зрозуміло, в які “вимикачі” слід втручатися менеджерам чи політикам, щоб посилити фінансову стійкість бізнесу.

Отримані результати формують цілісне бачення архітектури фінансової безпеки підприємства, яке поєднує інституційний та ресурсний рівні в єдину систему протидії кризовим загрозам. Обговорення цих

результатів доцільно провести у двох площинах – науково-концептуальній та прикладній (управлінські висновки).

Авторська концепція підтвердила гіпотезу про необхідність інтегрованого підходу до фінансової безпеки. Традиційно дослідження зосереджувалися або на внутрішніх аспектах (фінансовому стані підприємства, показниках ефективності), або на зовнішніх (економічній безпеці держави, макрофінансовій стабільності). Запропонована архітектура об'єднала ці аспекти, підкресливши їх взаємозалежність. Це узгоджується із сучасними тенденціями менеджменту ризиків, де акцент робиться на enterprise-wide risk management – всеохоплюючому погляді на ризики і безпеку організації. Зокрема, рада директорів і керівництво компанії повинні розглядати ризики не ізольовано (тільки фінансові чи тільки операційні), а у їхньому взаємному переплетенні – репутаційні, санкційні, ланцюжки постачань, кібернетичні тощо утворюють єдиний комплекс ризиків, який потребує єдиної стратегії. Наш підхід до архітектури фінансової безпеки фактично забезпечує такий стратегічний огляд: інституційна підсистема “накриває” стратегічні, зовнішні фактори ризику, а ресурсна – операційні та фінансові аспекти на мікрорівні, при цьому їх інтеграція вказує на каскадні ефекти (наприклад, зовнішня криза породжує внутрішні проблеми з ліквідністю, які, у свою чергу, впливають на ринкову позицію підприємства).

Цікаво відзначити, що отримані результати відображають принцип «antifragility», який набуває популярності в управлінських науках: йдеться про побудову систем, здатних не лише витримувати удари, але й ставати сильнішими, навчаючись на них. У випадку фінансової безпеки підприємства, це означає, що правильна взаємодія інституційних механізмів (наприклад, антикризових програм підтримки) та ресурсних стратегій підприємства (реінвестування у стійкі проекти, підвищення ефективності) може в результаті підвищити конкурентоспроможність і життєздатність бізнесу навіть після кризи. Таким чином, війна, попри всі руйнівні наслідки, здатна стимулювати впровадження кращих практик фінансового менеджменту і державного

регулювання, що в довгостроковій перспективі посилить економічну безпеку країни в цілому. Наше дослідження закладає теоретичне підґрунтя для таких висновків, демонструючи, як взаємодія інституційного та ресурсного рівнів може стати джерелом стійкості.

З практичної точки зору, результати дослідження дозволяють сформулювати низку рекомендацій для менеджерів підприємств та для органів, що формують політику у сфері економічної безпеки:

1. Розробка та впровадження корпоративної фінансової стратегії безпеки. Кожне підприємство, особливо діюче в умовах високих воєнних ризиків, має розробити чітку політику фінансової безпеки. Ця політика повинна включати: визначення прийнятного рівня ризику (risk appetite) і ключових показників FSAI, яких компанія прагне досягти; план дій на випадок різних кризових сценаріїв (від кібератаки до втрати основного ринку збуту); процедури регулярного моніторингу зовнішніх загроз (економічних новин, військової обстановки, регуляторних змін). Відповідальні особи (наприклад, фінансовий директор чи менеджер з ризиків) мають періодично звітувати вищому керівництву про “профіль безпеки” компанії – поточне значення індексу FSAI, динаміку його компонентів, нові виявлені загрози тощо. Такий підхід відповідає кращим світовим практикам: компанії, які перейшли від реактивного кризового управління до проактивного “resilience playbook”, значно легше переносять потрясіння.

2. Оптимізація капітальної структури та підвищення фінансової гнучкості. Одним з пріоритетних напрямів забезпечення фінансової безпеки (відповідно до нашого індексного аналізу) є підтримання збалансованої структури фінансування підприємства. Менеджменту слід прагнути до зниження надмірної залежності від короткострокових позик, забезпечення достатнього рівня власного капіталу та резервів. Наприклад, під час відносного затишшя варто акумулювати фінансові “подушки безпеки” – частину прибутку спрямовувати у резервні фонди або високоліквідні активи, які можна швидко конвертувати у гроші. Це підвищить ліквідність

та стійкість до раптових шоків. Також доцільно диверсифікувати джерела фінансування: використовувати різні банки, інструменти (облігації, акціонерний капітал), а за можливості – страхові механізми, щоб у разі кризи не втратити одразу всі канали ресурсів. Як свідчить досвід 2022–2023 рр., підприємства з більш гнучкою фінансовою моделлю (меншим борговим навантаженням, наявністю альтернативних кредиторів) швидше адаптувалися до нових умов.

3. Реалізація систем раннього виявлення загроз та оперативного реагування. У воєнний час критично важливо не чекати, коли проблеми відобразяться у кварталній звітності, а передбачати їх заздалегідь. Рекомендується впроваджувати системи моніторингу ключових індикаторів: наприклад, відстежувати зміни собівартості через здорожчання ресурсів, рух курсу гривні, динаміку попиту на продукцію, фінансовий стан ключових контрагентів. При виявленні відхилень від норми – негайно скликати внутрішню “фінансову комісію” для аналізу ситуації. Такі практики відповідають рекомендаціям щодо підвищення проактивності: компанії мають запровадити *early warning systems*, які подають сигнал керівництву до того, як ризик переросте в кризу. Одночасно повинен бути готовий набір типових швидких дій: наприклад, у разі валютного сплеску – перегляд цін і контрактів, в разі втрати складу – перерозподіл логістики, при кібератаці – резервні ІТ-канали та офлайн-операції. Регулярні стрес-тести фінансової моделі компанії (з моделюванням воєнних ризиків, падіння виручки, тощо) допоможуть підготувати ці плани.

4. Використання страхових, хеджувальних та інших захисних інструментів. Менеджерам слід активно залучати інструменти зниження фінансових ризиків, які надає ринок. В сучасних умовах набувають актуальності спеціалізовані страхові продукти від воєнних ризиків (*war risk insurance*), страхування перерви діяльності, страхування кредитів. Хоча такі поліси можуть бути дорогими, держава та міжнародні партнери дедалі частіше пропонують механізми розподілу ризику (наприклад, міжнародні страхові фонди для інвестицій в Україні). Крім страхування, варто розглянути

хеджування валютних та процентних ризиків – використання форвардів, ф’ючерсів чи опціонів для фіксації курсу або ставки за кредитами. Особливо це актуально для аграріїв та імпортозалежних підприємств, чия діяльність критично залежить від валютних коливань. Запровадження таких інструментів значно підвищує фінансову безпеку, мінімізуючи потенційні втрати від несприятливих ринкових рухів. Водночас слід подбати про фізичну та кібербезпеку активів: інвестувати в захист виробничих приміщень (укриття, дублювання потужностей), резервні системи електропостачання, кібербезпекові рішення для фінансових систем підприємства. Це пряму пов’язано з фінансовою безпекою, адже атаки на інфраструктуру можуть миттєво паралізувати діяльність і грошові потоки.

5. Співпраця з державою та стейкхолдерами у питаннях фінансової безпеки. Підприємствам варто активно комунікувати свої потреби та проблеми органам влади та галузевим асоціаціям. Воєнна економіка – це час, коли приватний сектор і держава мусять діяти спільно для збереження економіки. Менеджменту доцільно брати участь у програмах обміну інформацією про ризики (наприклад, повідомляти про критичні вузли постачання, які потребують охорони чи альтернативи), лобювати необхідні регуляторні послаблення або підтримку. З боку уряду, зважаючи на наші результати, рекомендація полягає в розробці секторальних програм фінансової безпеки: таргетованих на галузі з високим ризиком (логістика, агро, енергетика). Ці програми можуть включати: фінансову допомогу для відновлення інфраструктури (наприклад, компенсації аграріям за знищену техніку чи посіви), пільгові кредити на поповнення обігових коштів для транспортних компаній, створення державних резервів критичних матеріалів, гарантії для страхових виплат тощо. Попередній аналіз свідчить, що фокусування на вузьких місцях конкретних секторів дає більший ефект, ніж розмиті загальні заходи. Тому бізнесу варто доносити до влади конкретні дані (наприклад, пороги витривалості – скільки місяців фірма протримається без експорту зерна; який обсяг кредитування потрібен енергокомпанії для

ремонту тощо), аби заходи підтримки були обґрунтованими.

6. Формування стратегії післявоєнного фінансового відновлення. Нарешті, управлінським пріоритетом має стати довгострокова стратегія фінансової стабільності, яка виходить за межі поточної кризи. Вже зараз підприємствам слід планувати, як вони відновлюватимуть фінансову позицію у післявоєнний період: реструктуризувати борги, залучати інвестиції для модернізації, повертати втрачені ринки або освоювати нові. Наше дослідження показує, що підприємства, які збережуть “кістяк” фінансової стійкості під час війни, матимуть конкурентну перевагу у відбудові. Державі ж варто готуватися до переходу від режиму виживання до режиму розвитку – вже на етапі мирного відновлення механізми інституційної підтримки мають сприяти притоку капіталу, технологій, інтеграції у світові ринки. Фінансова безпека еволюціонує: з настанням миру акцент зміститься з короткострокового захисту на стратегічне зростання, тому і критерії FSAI для післявоєнного часу слід переглянути (більше важитимуть показники інвестиційної активності, інноваційності, глобальної конкурентоспроможності). Менеджерам необхідно врахувати це у баченнях розвитку бізнесу.

Підсумовуючи, архітектура фінансової безпеки підприємства у воєнній економіці, що була розроблена в цьому дослідженні, не лише описує взаємодію інституційного та ресурсного рівнів, але й пропонує конкретні інструменти для її реалізації на практиці. Використання інтегрованого підходу до управління ризиками та фінансами є життєво необхідним у сучасних умовах. Ігнорування або недооцінка ризиків неминуче призводить до втрат і стагнації бізнесу, тоді як добре організована система фінансової безпеки мінімізує втрати та дозволяє продовжувати діяльність навіть у найскладніших умовах війни. Отримані результати можуть служити дорожньою картою для підприємств у розбудові власної фінансової стійкості. Крім того, вони мають значення і для політиків – при формуванні державної політики економічної безпеки слід враховувати двокомпонентну природу цієї безпеки: жодні інституційні зусилля не будуть

успішними без належного фінансового менеджменту на рівні підприємств, і навпаки, навіть найкращий менеджмент може зазнати невдачі без підтримки здорового економічного середовища. Лише синергія обох рівнів забезпечить справжню фінансову безпеку, що є запорукою виживання і розвитку бізнесу в період воєнних потрясінь і підґрунтям для швидкого економічного відродження в майбутньому

Висновки та перспективи подальших досліджень

У дослідженні обґрунтовано двохарову архітектуру фінансової безпеки підприємства, що концептуально поєднує інституційний і ресурсний рівні як взаємодоповнювані «щити» стійкості. Інституційний рівень формує зовнішні умови та компенсаторні механізми – від регуляторної гнучкості й програм підтримки до функціонування фінансових ринків і логістичної інфраструктури, – тоді як ресурсний рівень репрезентує внутрішні можливості підприємства підтримувати ліквідність, оптимізувати структуру капіталу, управляти ризиками, забезпечувати безперервність бізнес-процесів (BCP/DR) і кіберстійкість. Взаємодія цих рівнів вибудовується як керований цикл із безперервним моніторингом загроз, ідентифікацією ризиків, прийняттям рішень, реалізацією заходів та оцінкою ефективності з подальшим оновленням політик. Запропонований інтегральний індекс $FSAI = \alpha \cdot I_{ext} + \beta \cdot I_{res}$ формалізує цю архітектуру, дозволяючи кількісно відобразити профіль безпеки, порівнювати підприємства та галузі й цілеспрямовано виявляти «вузькі місця» для управлінського втручання. Введення режимної логіки «мир – війна – відновлення» відкриває можливість динамічної калібровки ваг інституційного та ресурсного компонентів: за посилення екзогенних шоків зростає роль зовнішнього контуру ($\alpha \uparrow$), у стабільнішому середовищі переважає внутрішнє фінансове управління ($\beta \uparrow$). Секторні приклади (логістика, агро, енергетика) підтверджують корисність моделі: архітектура дозволяє таргетувати саме ті підсистеми, що визначають граничну витривалість бізнесу, від логістичних коридорів і паливних шоків до резервування генеруючих потужностей та кіберзахисту критичних систем.

Практична цінність підходу полягає у зведенні стратегічних інституційних інструментів (держгарантії, страхування воєнних ризиків, регуляторні послаблення) з тактичними корпоративними рішеннями (касові буфери, реструктуризація боргу, хеджування FX/ставок, впровадження BCP/DR, підвищення прозорості за ISSB/TCFD), що дає керівникам основу для побудови «дорожньої карти» фінансової стійкості. Методологічно робота узгоджує структурно-функціональну схему з кількісною метрикою, підготовленою до емпіричної валідації (визначення ваг через PLS-SEM; стрес-тести та оптимізація політик ліквідності з обмеженням Expected Shortfall). Водночас дослідження має усвідомлені обмеження — теоретичний характер без емпіричної ідентифікації, чутливість FSAI до вибору індикаторів і ваг, потенційну ендегенність (наприклад, між прозорістю та вартістю боргу), а також галузеву й регіональну гетерогенність і можливі структурні зміни у воєнний період, — що окреслює необхідність подальшої перевірки на даних.

Перспективи подальших досліджень впливають із означених обмежень і логіки розвитку запропонованої рамки. По-перше, доцільною є емпірична валідація FSAI на панельних вибірках (2018-2025/2026 pp.) із використанням PLS-SEM/SEM для ідентифікації латентних конструктів і ваг, перевірки надійності (CR, AVE), дискримінантної валідності (HTMT) та стабільності результатів у галузевих і розмірних підвибірках. По-друге, потребує розроблення шкала інтерпретації індексу з порогоми й зонами ризику, узгодженими з класичними бенчмарками (Altman Z-score, структурні PD), включно з ROC-аналізом розпізнавальної здатності. По-третє, варто оцінити режимні моделі (Markov-switching/HMM) для параметрів WACC, PD і Expected Shortfall грошових потоків, ідентифікувати ймовірності переходів між «миром», «війною» та «відновленням» і побудувати карти станів для галузей і регіонів. По-четверте, необхідне системне стрес-тестування та стохастична оптимізація політик ліквідності/хеджування/страхування з

обмеженням CVaR/ES, що дозволить кількісно порівнювати компроміси «вартість—ризик» для управлінських інтервенцій за різних сценаріїв (енергетичні та логістичні перебої, валютні сплески, кіберінциденти). По-п'яте, каузальна ідентифікація ефектів політик (DID/IV/подієві дослідження) допоможе оцінити внесок державних гарантій, податкових відстрочок, страхових схем і валютних регуляцій у зміну вартості боргу, ліквідності та імовірності дефолту. По-шосте, доцільно врахувати просторові та мережеві ефекти через SAR/SEM-моделі регіональної експозиції до бойових дій і пошкодженої інфраструктури та дослідити «зараження» ризиків у ланцюгах постачання. По-сьоме, варто розробити системи раннього попередження на базі explainable-ML (градієнтні бустинги з інтерпретацією SHAP) для прогнозу переходів між зонами FSAI і порівняти їх із традиційними скоринговими підходами. По-восьме, слід операціоналізувати кібер- та ОТ-ризик (CAPEX/OPEX на кіберзахист, RTO/RPO, частота інцидентів) у складі I_{res} і перевірити їхній вплив на вартість капіталу та безперервність процесів. По-дев'яте, перспективним є створення «цифрового двійника» фінансової стійкості (гібрид system dynamics + agent-based), який уможливить експерименти з політиками в «пісочниці» та узгодження з FSAI в реальному часі. По-десяте, міжкраїнні порівняння дадуть змогу оцінити зовнішню валідність підходу і перенесеність ваг/порогів у середовищах із різною якістю інституцій та інтенсивністю воєнних ризиків. Нарешті, необхідно перевірити робастність індексу щодо альтернативних нормувань і вагувань (AHP/FAHP, ентропійні ваги) та врахувати «товсті хвости» розподілів втрат (EVT, copula-моделі), а також узгодити змінні I_{ext} та I_{res} зі стандартами ISSB/TCFD і забезпечити реплікабельність через відкриті словники змінних і код. У сумі ці напрями перетворюють подану архітектуру та FSAI з теоретичної конструкції на стандартизований інструмент діагностики і керованого підвищення фінансової стійкості підприємств у воєнній економіці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Варналій З. С., Бондаренко С. М. Фінансова безпека підприємств України в умовах війни та повоєнного відновлення. Економічний вісник університету. 2023. Вип. 56. С. 106–113. DOI: 10.31470/2306-546X-2023-56-106-113.
2. Ситник Н., Половко Д. Фінансова безпека підприємства в умовах війни: цілі, пріоритети й шляхи забезпечення. Галицький економічний вісник. 2024. Т. 91, № 6. С. 111–122. DOI: 10.33108/galicianvisnyk_tntu2024.06.111.
3. Орлова О., Батюк Р. Управління фінансовою безпекою підприємств: виклики воєнного часу. Економіка та суспільство. 2024. Вип. 62. DOI: 10.32782/2524-0072/2024-62-170.
4. Хома І. Б., Боберський Р. І. Управління фінансовими ризиками в умовах війни. Причорноморські економічні студії. 2023. Вип. 84. С. 47–51.
5. Zadorozhnyi Z.-M., Muravskiy V., Shevchuk O., Bryk M. Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. Marketing and Management of Innovations. 2021. № 4. P. 36–46. DOI: 10.21272/mmi.2021.4-03.
6. Blakyta G., Ganushchak T. Enterprise financial security as a component of the economic security of the state. Investment Management and Financial Innovations. 2018. Vol. 15, № 2. P. 248–256. DOI: 10.21511/imfi.15(2).2018.22.
7. International Energy Agency. Ukraine's Energy Security and the Coming Winter. Paris : IEA, 2024. URL: <https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter>.
8. International Energy Agency. Electricity 2024. Paris : IEA, 2024. URL: <https://www.iea.org/reports/electricity-2024> (дата звернення: 13.09.2025).
9. ACAPS. Ukraine: Energy infrastructure attacks — outlook and impact during 2024–2025 cold season. 13.09.2024. URL: <https://reliefweb.int/report/ukraine/acaps-thematic-report-ukraine-energy-infrastructure-attacks-outlook-and-impact-during-2024-2025-cold-season-13-september-2024>.
10. KSE Institute. Ukraine: Firms through the War (Policy Note). 28.11.2023. URL: <https://kse.ua/wp-content/uploads/2024/03/Ukraine.-Firms-through-the-War-Paper-Nov-2023.pdf>.
11. GMK Center. Challenges for Ukrainian iron and steel industry in 2024. 10.04.2024. URL: <https://gmk.center/en/posts/challenges-for-ukrainian-iron-and-steel-industry-in-2024/>.
12. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management — Integrating with Strategy and Performance. New York : COSO, 2017. URL: <https://www.coso.org/guidance-erm>.
13. COSO. Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples. New York : COSO, 2018. URL: <https://www.coso.org/guidance-erm>.
14. IFRS Foundation (ISSB). IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information. London : IFRS, 2023. URL: <https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s1-general-requirements/>.
15. IFRS Foundation (ISSB). IFRS S2 Climate-related Disclosures. London : IFRS, 2023. URL: <https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/>.
16. Task Force on Climate-related Financial Disclosures (TCFD). Final Report: Recommendations of the Task Force on Climate-related Financial Disclosures. Basel : FSB, 2017. URL: <https://www.fsb-tcfd.org/recommendations/>.

17. ISO 31000:2018 Risk management — Guidelines. Geneva : International Organization for Standardization, 2018. URL: <https://www.iso.org/standard/65694.html>.
18. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Geneva : International Organization for Standardization, 2019. URL: <https://www.iso.org/standard/75106.html>.
19. Modigliani F., Miller M. H. The Cost of Capital, Corporation Finance and the Theory of Investment. The American Economic Review. 1958. Vol. 48, № 3. P. 261–297. URL: <https://www.aeaweb.org/aer/top20/48.3.261-297.pdf>.
20. Myers S. C. The Capital Structure Puzzle. The Journal of Finance. 1984. Vol. 39, № 3. P. 575–592. DOI: 10.2307/2327916.
21. Myers S. C., Majluf N. S. Corporate Financing and Investment Decisions When Firms Have Information That Investors Do Not Have. Journal of Financial Economics. 1984. Vol. 13, № 2. P. 187–221. DOI: 10.1016/0304-405X(84)90023-0.
22. Altman E. I. Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy. The Journal of Finance. 1968. Vol. 23, № 4. P. 589–609. DOI: 10.1111/j.1540-6261.1968.tb00843.x.
23. European Parliamentary Research Service (EPRS). Economic impact of Russia's war on Ukraine and the European Council response. Brussels : European Parliament, 23.02.2024. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757783/EPRS_BRI\(2024\)757783_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757783/EPRS_BRI(2024)757783_EN.pdf).

REFERENCES

1. Varnalii, Z. S., & Bondarenko, S. M. (2023). Financial security of Ukrainian enterprises in wartime and post-war recovery. *Economic Bulletin of the University*, 56, 106–113. <https://doi.org/10.31470/2306-546X-2023-56-106-113>
2. Sytnyk, N., & Polovko, D. (2024). Financial security of enterprises in wartime: Goals, priorities, and ways of ensuring. *Halytskyi Economic Bulletin*, 91(6), 111–122. https://doi.org/10.33108/galicianvisnyk_tntu2024.06.111
3. Orlova, O., & Batiuk, R. (2024). Management of enterprise financial security: Challenges of wartime. *Economy and Society*, 62. <https://doi.org/10.32782/2524-0072/2024-62-170>
4. Khoma, I. B., & Boberskyi, R. I. (2023). Financial risk management in wartime. *Black Sea Economic Studies*, 84, 47–51.
5. Zadorozhnyi, Z.-M., Muravskyi, V., Shevchuk, O., & Bryk, M. (2021). Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. *Marketing and Management of Innovations*, 4, 36–46. <https://doi.org/10.21272/mmi.2021.4-03>
6. Blakyta, G., & Ganushchak, T. (2018). Enterprise financial security as a component of the economic security of the state. *Investment Management and Financial Innovations*, 15(2), 248–256. [https://doi.org/10.21511/imfi.15\(2\).2018.22](https://doi.org/10.21511/imfi.15(2).2018.22)
7. International Energy Agency. (2024). *Ukraine's energy security and the coming winter*. Paris: IEA. <https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter>
8. International Energy Agency. (2024). *Electricity 2024*. Paris: IEA. <https://www.iea.org/reports/electricity-2024>

9. ACAPS. (2024, September 13). *Ukraine: Energy infrastructure attacks — Outlook and impact during 2024–2025 cold season*. <https://reliefweb.int/report/ukraine/acaps-thematic-report-ukraine-energy-infrastructure-attacks-outlook-and-impact-during-2024-2025-cold-season-13-september-2024>
10. KSE Institute. (2023, November 28). *Ukraine: Firms through the war (Policy Note)*. <https://kse.ua/wp-content/uploads/2024/03/Ukraine.-Firms-through-the-War-Paper-Nov-2023.pdf>
11. GMK Center. (2024, April 10). *Challenges for Ukrainian iron and steel industry in 2024*. <https://gmk.center/en/posts/challenges-for-ukrainian-iron-and-steel-industry-in-2024/>
12. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management — Integrating with strategy and performance*. New York: COSO. <https://www.coso.org/guidance-erm>
13. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2018). *Enterprise risk management — Integrating with strategy and performance: Compendium of examples*. New York: COSO. <https://www.coso.org/guidance-erm>
14. IFRS Foundation (ISSB). (2023). *IFRS S1 General requirements for disclosure of sustainability-related financial information*. London: IFRS. <https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s1-general-requirements/>
15. IFRS Foundation (ISSB). (2023). *IFRS S2 Climate-related disclosures*. London: IFRS. <https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/>
16. Task Force on Climate-related Financial Disclosures (TCFD). (2017). *Final report: Recommendations of the Task Force on Climate-related Financial Disclosures*. Basel: Financial Stability Board. <https://www.fsb-tcfd.org/recommendations/>
17. International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk management — Guidelines*. Geneva: ISO. <https://www.iso.org/standard/65694.html>
18. International Organization for Standardization (ISO). (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. Geneva: ISO. <https://www.iso.org/standard/75106.html>
19. Modigliani, F., & Miller, M. H. (1958). The cost of capital, corporation finance and the theory of investment. *The American Economic Review*, 48(3), 261–297. <https://www.aeaweb.org/aer/top20/48.3.261-297.pdf>
20. Myers, S. C. (1984). The capital structure puzzle. *The Journal of Finance*, 39(3), 575–592. <https://doi.org/10.2307/2327916>
21. Myers, S. C., & Majluf, N. S. (1984). Corporate financing and investment decisions when firms have information that investors do not have. *Journal of Financial Economics*, 13(2), 187–221. [https://doi.org/10.1016/0304-405X\(84\)90023-0](https://doi.org/10.1016/0304-405X(84)90023-0)
22. Altman, E. I. (1968). Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *The Journal of Finance*, 23(4), 589–609. <https://doi.org/10.1111/j.1540-6261.1968.tb00843.x>
23. European Parliamentary Research Service (EPRS). (2024, February 23). *Economic impact of Russia's war on Ukraine and the European Council response*. Brussels: European Parliament. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757783/EPRS_BRI\(2024\)757783_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757783/EPRS_BRI(2024)757783_EN.pdf)

Vitalii Mozhuk, PhD student, West Ukrainian National University, Ukraine

Volodymyr Mozhuk, PhD student, West Ukrainian National University, Ukraine

Architecture of enterprise financial security in a wartime economy

Abstract

Introduction. In a wartime economy, enterprise financial security transforms from a “set of static ratios” into a dynamic resilience system capable of withstanding cascading energy and logistics disruptions, heightened macro-financial volatility, and cyber threats. The concentration of exogenous and endogenous risk factors strengthens the relevance of further theoretical inquiry into the architecture of financial security and the development of applied tools for its assessment and management in sectors with high war exposure.

Purpose. To design a conceptual architecture of enterprise financial security in a wartime economy that integrates the institutional (external) and resource (internal) contours, and to formalize it as a composite FSAI index with the regime logic “peace — war — recovery” for managerial interpretation and for comparing security profiles across firms and industries.

Method (methodology). The study applies a structural-functional approach to delineate subsystems and interaction channels; the tenets of institutional economics to model the “rules of the game” and external constraints; the principles of Enterprise Risk Management for an integrated view of risks and the determination of risk appetite; an index-based approach with normalization of indicators and weighting of the sub-indices of institutional stability and resource resilience; and scenario-based theoretical modelling for logistics, agriculture, and energy.

Results. A two-layer architecture of enterprise financial security (“institutions × resources”) is developed with a description of its functions, interfaces, and feedback mechanisms; a composite FSAI index is proposed as a quantitative representation of the architecture, with indicator sets defined for each sub-index and aggregation rules specified; a regime-based logic for adaptively adjusting the weights of institutional and resource components is introduced depending on the intensity of exogenous shocks; and the practical applicability of the approach is demonstrated for diagnosing “bottlenecks” and prioritizing managerial interventions (state guarantees and war-risk insurance, liquidity buffers, debt restructuring, hedging of currency and interest-rate risks, implementation of BCP/DR, and enhanced disclosure transparency).

Keywords: enterprise financial security; wartime economy; financial security architecture; institutional approach; resource-based approach; FSAI composite index; risk management; liquidity; capital structure.

Cite as: Mozhuk, V., & Mozhuk, V. (2025). Architecture of enterprise financial security in a wartime economy. *Economic analysis*, 35 (2), 465-484. DOI: <https://doi.org/10.35774/econa2025.02.465>