

УНІВЕРСИТЕТ «КРОК»
Кафедра економіки та фінансів

Невмержицький Євгеній Володимирович

УДК 336.67 : 658

Кваліфікаційна робота магістра
«Формування системи економічної безпеки
підприємства»

Спеціальність 076 «Підприємництво та торгівля»

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних доробок. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Є.В. Невмержицький

Науковий керівник



Андрєєва Віта Анатоліївна
к.е.н., доцент

Київ – 2026

**ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»**

ЗАТВЕРДЖУЮ:

завідувач кафедри економіки та фінансів

_____ Ігор Румик
« ___ » _____ 20__ р.

**ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА
НЕВМЕРЖИЦЬКОГО ЄВГЕНІЯ ВОЛОДИМИРОВИЧА**

Ступінь вищої освіти - магістр

Галузь знань – 07 Управління та адміністрування

Спеціальність – 076 Підприємництво та торгівля

Освітня програма – «Підприємництво та торгівля»

Тема роботи	Формування системи економічної безпеки підприємства
Номер та дата наказу про затвердження теми	113-3 від 29.11.2024 р.
Науковий керівник	Андрєєва Віта Анатоліївна, кандидат економічних наук, доцент
Вихідні дані до роботи	Законодавчі та нормативно-правові акти України у сфері підприємницької діяльності; статистичні дані; внутрішня фінансова та кадрова звітність ТОВ «НОВА ПОШТА»; наукові праці вітчизняних і зарубіжних авторів з питань економічної безпеки підприємств.
Постановка завдання	Дослідження теоретичних основ формування економічної безпеки підприємства, аналіз системи економічної безпеки підприємства ТОВ «НОВА ПОШТА», обґрунтування напрямів вдосконалення системи економічної безпеки досліджуваного підприємства.
Посилання на джерела інформації (не більше п'яти найменувань, які рекомендує науковий керівник)	<ol style="list-style-type: none"> 1. Економіка невизначеності: зміст, оцінювання, регулювання: колективна монографія / за ред. І.Ф. Радіонової. Київ: Університет «КРОК», 2021. С. 169-190. DOI: 10.31732/EU-CER-8 2. Андрєєва, В., & Гофман, М. (2024). Оцінка збитків від пошкодження майна внаслідок військової агресії російської федерації в Україні. <i>Вчені записки Університету «КРОК», 1(73)</i>. 3. Андрєєва, Г.І., & Андрєєва, В.А. (2010). Організація і методика економічного аналізу. URL: https://essuir.sumdu.edu.ua/handle/123456789/50223 4. Андрєєва В.А., Окунський Д.О. Методика оцінки фінансового потенціалу розвитку підприємства та напрямки її вдосконалення. <i>Держава, регіони, підприємництво: інформаційні, суспільно-правові,</i>

	<i>соціально-економічні аспекти розвитку: тези доповідей IV Міжнародної конференції (7 грудня 2022 р., м. Київ). Київ: Університет "КРОК", 2022.</i>
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати розв'язання складної задачі або проблеми за темою роботи, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Дата видачі завдання 23.12.2024

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів роботи	Термін виконання	Примітка
1	Вибір напрямку дослідження	28.11.2024	<i>Виконано</i>
2	Затвердження теми кваліфікаційної роботи та призначення наукового керівника	29.11.2024	<i>Виконано</i>
3	Затвердження завдання на кваліфікаційну роботу	23.12.2024	<i>Виконано</i>
4	Розробка концепції кваліфікаційної роботи. Затвердження плану досліджень.	01.03.2025	<i>Виконано</i>
5	Підготовка першого розділу роботи	01.07.2025	<i>Виконано</i>
6	Підготовка другого розділу роботи	30.09.2025	<i>Виконано</i>
7	Підготовка третього розділу роботи	02.12.2025	<i>Виконано</i>
8	Підготовка вступу та висновків	12.12.2025	<i>Виконано</i>
9	Підготовка джерельної бази	15.12.2025	<i>Виконано</i>
10	Подання роботи на перевірку на плагіат	18.12.2025	<i>Виконано</i>
11	Виконання наукової складової роботи	19.12.2025	<i>Виконано</i>
12	Проходження попереднього захисту	20.12.2025	<i>Виконано</i>
13	Доопрацювання роботи з врахуванням зауважень	09.01.2026	<i>Виконано</i>
14	Зовнішня експертиза, отримання відгуку наукового керівника та подання роботи на кафедру	11.01.2026	<i>Виконано</i>
15	Захист кваліфікаційної роботи	18.01.2026	<i>Виконано</i>

Здобувач

Євгеній НЕВМЕРЖИЦЬКИЙ

Науковий керівник

Віта АНДРЕЄВА

АНОТАЦІЯ

Невмержицький ЄВ. Формування системи економічної безпеки підприємства. Рукопис.

Кваліфікаційна робота магістра за спеціальністю 076 Підприємництво та торгівля, освітня програма Підприємництво та торгівля. ВНЗ «Університет економіки та права «КРОК», Київ, 2026.

Кваліфікаційну роботу присвячено дослідженню системи формування економічної безпеки підприємства та розробці напрямів її вдосконалення. У роботі узагальнено теоретичні засади економічної безпеки, проведено аналіз фінансово-господарської діяльності та системи економічної безпеки ТОВ «НОВА ПОШТА», запропоновано напрями вдосконалення системи формування економічної безпеки підприємства.

Ключові слова: економічна безпека, система, діагностика, ефективність, стратегія, прогнозування.

SUMMARY

Nevmerzhitsky E.V. Formation of the system of economic security of the enterprise. Manuscript.

Master's qualification work in specialty 076 Entrepreneurship and Trade, Educational program Entrepreneurship and Trade. KROK University of Economics and Law, Kyiv, 2026.

The qualification work is devoted to the study of the system of formation of economic security of the enterprise and the development of directions for its improvement. The work summarizes the theoretical principles of economic security, analyzes the financial and economic activities and the economic security system of LLC «NOVA POSHTA», and proposes directions for improving the system of formation of economic security of the enterprise.

Keywords: economic security, system, diagnostics, efficiency, strategy, forecasting.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА	11
1.1. Економічна безпека підприємства: сутність, концептуальні підходи та її місце в системі управління.....	11
1.2. Класифікація та характеристика функціональних складових системи економічної безпеки підприємства.....	19
1.3. Огляд методичних підходів до оцінки рівня економічної безпеки підприємства.....	25
1.4. Механізми, інструменти та принципи формування системи економічної безпеки підприємства	33
РОЗДІЛ 2. АНАЛІЗ ТА ДІАГНОСТИКА ІСНУЮЧОЇ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «НОВА ПОШТА»	41
2.1. Загальна фінансово-господарська характеристика ТОВ «Нова Пошта» та аналіз факторів зовнішнього середовища.....	41
2.2. Діагностика існуючої системи управління економічною безпекою на ТОВ «Нова Пошта»	48
2.3. Ідентифікація та аналіз ключових внутрішніх і зовнішніх загроз діяльності ТОВ «Нова Пошта»	52
2.4. Комплексна оцінка рівня економічної безпеки ТОВ «Нова Пошта» (2019-2024 рр.).....	54
РОЗДІЛ 3. СТРАТЕГІЧНІ НАПРЯМИ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «НОВА ПОШТА»	64
3.1. Обґрунтування стратегічних пріоритетів зміцнення економічної безпеки підприємства.....	64
3.2. Розробка механізму управління кадровою та інформаційною безпекою в умовах цифровізації	70
3.3. Економічне обґрунтування та прогнозування ефективності запропонованих заходів.....	74
ВИСНОВКИ.....	83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	87

ВСТУП

Актуальність теми дослідження. В сучасних умовах господарювання, що характеризуються безпрецедентним рівнем невизначеності та перманентними кризовими явищами, проблема забезпечення економічної безпеки підприємства набуває статусу ключового фактора його виживання та розвитку. Традиційні підходи до управління безпекою, які базувалися на стабільності зовнішнього середовища, втратили свою ефективність під тиском глобальних геополітичних та технологічних зрушень.

Для вітчизняних підприємств, зокрема логістичної сфери, визначальним фактором впливу стала повномасштабна військова агресія, яка призвела до руйнування ланцюгів постачання, фізичного знищення активів та суттєвої трансформації ринкової кон'юнктури. Як зазначають Асамоах-Черемех Д. та Рудніченко Є.[1], сучасні українські реалії вимагають від бізнесу не просто "захисту ресурсів", а здатності до швидкої адаптації та забезпечення життєздатності в екстремальних умовах.

Економічна безпека стає інтегральною характеристикою, яка визначає здатність суб'єкта господарювання протистояти дестабілізуючим факторам воєнного часу.

Водночас, поряд із фізичними загрозами, бізнес стикається з фундаментальними змінами, спричиненими четвертою промисловою революцією. Стрімка цифровізація економічних процесів створює не лише нові можливості, а й генерує специфічні загрози, які раніше не розглядалися як пріоритетні. Захарчук Н. [2] справедливо вказує на зміну характеру загроз від традиційних фінансових до комплексних кібернетичних та інформаційних. В умовах, коли бізнес-моделі логістичних компаній (таких як ТОВ «Нова Пошта») повністю залежать від ІТ-інфраструктури, кіберстійкість стає синонімом операційної безпеки.

Окремим вектором загроз, що актуалізує тему дослідження, є трансформація ринку праці. Як обґрунтовано в працях Андріїв Н. [3], цифровізація ринку праці та демографічна криза, посилена міграційними

процесами, перетворюють «кадрову безпеку» на питання збереження інтелектуального ядра компанії. Втрата людського капіталу стає ризиком, співмірним із втратою фінансових активів.

Усе це зумовлює об'єктивну необхідність переосмислення теоретико-методичних засад та розробки нових практичних механізмів формування системи економічної безпеки підприємства. Перехід від фрагментарних захисних заходів до побудови комплексної, адаптивної системи, здатної нівелювати фінансові, кадрові та кібернетичні загрози, є критично важливим завданням, що й зумовило вибір теми магістерської роботи.

Проблематика економічної безпеки підприємства є предметом наукових пошуків багатьох вітчизняних та зарубіжних вчених. Вагомий внесок у розкриття теоретико-методологічних засад сутності та структури безпеки зробили такі вчені, як Г. Козаченко, О. Ляшенко, Т. Васильців, С. Гринкевич, К. Зіненко. Їхні праці сформували фундамент для розуміння ЕБП як системної категорії.

Особливу увагу в сучасній науковій літературі приділено трансформації складових безпеки під впливом нових викликів. Проблеми безпеки людського капіталу та цифровізації ринку праці ґрунтовно висвітлені в працях Н. Андріїв. Аспекти інформаційної та кібернетичної безпеки в умовах цифрової економіки досліджують В. Проскура, І. Кульчицький, І. Біланчук. Важливий внесок у розвиток методології оцінки репутаційної складової та управління нематеріальними активами зробили представники наукової школи Університету «КРОК» В. Алькема та З. Живко.

Водночас, незважаючи на значний науковий доробок, питання формування комплексної системи економічної безпеки саме для логістичних підприємств, які функціонують в умовах поєднання дестабілізуючих факторів воєнного стану та стрімкої цифрової трансформації, залишаються недостатньо вивченими. Більшість існуючих підходів носять фрагментарний характер або не враховують синергію між фінансовими, кадровими та цифровими загрозами. Необхідність поглиблення методичного

інструментарію діагностики та розробки адаптивних механізмів управління ЕБП зумовила мету і завдання дослідження.

Метою кваліфікаційної роботи є розробка теоретико-методичних засад та практичних рекомендацій щодо удосконалення механізму формування системи економічної безпеки підприємства в умовах цифровізації та воєнного стану (на прикладі ТОВ «Нова Пошта»).

Поставлена мета зумовила необхідність вирішення наступних **завдань**:

- узагальнити теоретичні підходи до визначення сутності та еволюції поняття «економічна безпека підприємства»;
- проаналізувати склад та структуру системи економічної безпеки, виявивши трансформацію її функціональних складових під впливом сучасних викликів;
- обґрунтувати методичний інструментарій комплексної оцінки рівня економічної безпеки підприємства;
- дослідити сучасні механізми, принципи та інструменти формування системи економічної безпеки;
- здійснити оцінку загального фінансово-господарського стану ТОВ «Нова Пошта» та проаналізувати фактори зовнішнього середовища;
- продіагностувати існуючу систему управління безпекою та ідентифікувати ключові внутрішні і зовнішні загрози діяльності підприємства;
- провести комплексну кількісну та якісну оцінку рівня економічної безпеки підприємства за інтегральним показником;
- обґрунтувати стратегічні пріоритети зміцнення економічної безпеки підприємства на основі сценарного підходу;
- розробити механізм управління кадровою та інформаційною безпекою в умовах цифровізації;
- здійснити економічне обґрунтування та прогнозування ефективності запропонованих заходів.

Об'єктом дослідження є процес формування та управління системою економічної безпеки ТОВ «Нова Пошта».

Предметом дослідження є сукупність теоретичних засад, методичних підходів та практичних інструментів забезпечення економічної безпеки підприємства в умовах нестабільного бізнес-середовища.

Методи дослідження. Методологічною основою магістерської роботи є сукупність загальнонаукових та спеціальних методів пізнання економічних явищ. Для вирішення поставлених завдань використано такі методи як:

- абстрактно-логічний, аналізу та синтезу – для розкриття сутності економічної безпеки, систематизації концептуальних підходів та уточнення понятійного апарату;
- монографічний – для дослідження еволюції наукової думки щодо структури та складових системи безпеки;
- системний підхід – для формування концептуальної моделі забезпечення економічної безпеки підприємства;
- статистичний та порівняльний аналіз – для оцінки фінансово-господарського стану ТОВ «Нова Пошта» та дослідження динаміки показників;
- коефіцієнтний метод – для розрахунку індикаторів фінансової, техніко-технологічної та кадрової складових безпеки;
- інтегральний метод – для комплексної кількісної оцінки рівня економічної безпеки підприємства;
- метод графічної візуалізації – для наочного відображення динаміки показників, структурних схем та моделей;
- SWOT-аналіз та модель п'яти сил М. Портера – для ідентифікації внутрішніх і зовнішніх загроз та вибору стратегічних пріоритетів;
- метод сценарного моделювання – для прогнозування ефективності запропонованих заходів та розрахунку прогнозного рівня безпеки.

Інформаційною базою дослідження є законодавчі та нормативні акти України, які регулюють питання національної безпеки та підприємницької діяльності; наукові праці вітчизняних та зарубіжних вчених з проблем економічної безпеки, стратегічного управління та менеджменту; офіційна консолідована фінансова звітність та консолідовані звіти про управління Групи компаній «Нова Пошта» за 2019–2024 рр.; аналітичні звіти та статистичні матеріали; інтернет-ресурси.

Наукова новизна одержаних результатів полягає у теоретико-методичному обґрунтуванні та розробці практичних рекомендацій щодо вдосконалення системи економічної безпеки логістичного підприємства в умовах цифровізації та воєнного стану. Удосконалено організаційно-економічний механізм формування системи економічної безпеки. Запропоновано інтеграцію механізму безпеки в загальну систему управління підприємством через інструментарій стратегічного контролінгу та інформаційно-аналітичного забезпечення, що базується на використанні сучасних цифрових технологій (Big Data, AI) для превентивного виявлення загроз. Обґрунтовано трансформацію традиційних складових під впливом глобальних викликів, стратегічні підходи до управління економічною безпекою. Обґрунтовано доцільність застосування «стратегії збалансованої стабілізації та інтенсифікації» для підприємств, що знаходяться у «проблемному стані» безпеки, та розроблено сценарну прогностичну модель для оцінки ефективності її реалізації.

Практичне значення одержаних результатів полягає у тому, що запропоновані в роботі теоретичні узагальнення, методичні підходи та прикладні рекомендації доведені до рівня конкретних методик і практичних заходів, які можуть бути використані в діяльності логістичних підприємств для підвищення рівня їхньої економічної безпеки.

Структура та обсяг роботи. Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, подана на 91 сторінках, містить 10 таблиць, 4 рисунки.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ФОРМУВАННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Економічна безпека підприємства: сутність, концептуальні підходи та її місце в системі управління

У сучасних складних українських реаліях, що характеризуються високим рівнем невизначеності та глобальними трансформаціями, питання забезпечення економічної безпеки підприємства (ЕБП) набуває виняткової актуальності. Традиційні системи безпеки, орієнтовані на статичний захист, стрімко "втрачають актуальність під тиском критично високої динамічності" зовнішнього середовища. Дестабілізуючий вплив таких факторів, як наслідки пандемії Covid-19 та повномасштабна "російська агресія", призвів до кардинальної зміни самого характеру загроз. Відбувся зсув від традиційних фінансових ризиків до комплексних "кібернетичних, інформаційних та репутаційних" викликів. Окрім цього, потужним трансформуючим процесом стала "цифровізація ринку праці", яка загострила загрози, пов'язані з "втратою людського капіталу". Для формування дієвого механізму протидії цим загрозам необхідно, перш за все, чітко окреслити теоретичний апарат дослідження та систематизувати наукові підходи до сутності фундаментальної категорії "економічна безпека підприємства".

Поняття "економічна безпека підприємства" є похідним від ширшого поняття "економічна безпека держави" яке, в свою чергу, є невід'ємною складовою "національної безпеки". Тому формування ефективної системи ЕБП неможливе без урахування нормативно-правового поля України.

Базовим фундаментом, що гарантує право на безпечне ведення бізнесу, є Конституція України [4]. Зокрема, стаття 42 закріплює право на підприємницьку діяльність та обов'язок держави забезпечувати захист конкуренції. Це створює первинну правову основу для функціонування.

Ключові дефініції та принципи, на яких будується захист інтересів суб'єктів господарювання, визначені в Законі України «Про національну безпеку України» [5]. Цей закон визначає ієрархію загроз та встановлює, що економічна безпека є складовою національних інтересів. Оскільки наше дослідження фокусується на логістичному підприємстві, критично важливим є врахування галузевої специфіки, яка регулюється Законом України «Про поштовий зв'язок» [6]. Цей закон встановлює специфічні вимоги до безпеки поштових відправлень, захисту персональних даних користувачів та таємниці кореспонденції, що безпосередньо впливає на структуру операційної та інформаційної складових ЕБП. Практична реалізація цих норм регламентується Правилами надання послуг поштового зв'язку (затверджені Постановою КМУ) [7], які деталізують процедури контролю та перевірки, що є елементами системи фізичної та технологічної безпеки логістичного оператора.

Нарешті, враховуючи ринковий характер загроз, важливу роль відіграє Закон України «Про захист економічної конкуренції» [8]. Він визначає правові рамки протидії недобросовісній конкуренції, що є основою для формування механізмів ринкової та репутаційної безпеки підприємства.

Таким чином, аналіз законодавчої бази дозволяє стверджувати, що система ЕБП має будуватися не лише на внутрішніх регламентах, а й на чіткому дотриманні норм національного законодавства. Для глибокого розуміння сутності ЕБП, важливо простежити її генезу. Поняття "економічна безпека" є похідним від загальної категорії "безпека". Етимологічно термін походить від латинського «*securitas*», що означає "спокійний стан духу" або "захищеність від будь-якої небезпеки".

Узагальнюючи це базове поняття, Гаркуша В.О. та Єршова Н.Ю. трактують безпеку як "категорію, яка характеризує стан захищеності для суб'єкта та можливість протистояти загрозам" [9].

У науковому дискурсі розуміння ЕБП не є статичним; воно пройшло суттєву еволюцію, яка безпосередньо пов'язана зі змінами у глобальному та

національному бізнес-середовищі. Так, Гринкевич С.С. та ін. пропонують детальну періодизацію розвитку цього поняття, виділяючи етапів (табл. 1.1).

Таблиця 1.1

Еволюція поняття «економічна безпека підприємства»

Етап	Хронологія	Основна характеристика та зміст поняття
I	1991–1997 рр.	Становлення: Економічна безпека ототожнюється з «безпекою фірми». Основний акцент – на забезпеченні конфіденційності, захисті комерційної таємниці та фізичній безпеці від кримінальних загроз.
II	1998–1999 рр.	Захисний підхід: Поняття розширюється до захисту від негативних впливів зовнішнього середовища, зокрема від непередбачуваних змін у державній політиці та законодавстві.
III	1999–2000 рр.	Ресурсний підхід: ЕБП починає розглядатися як стан ефективного використання ресурсів (капіталу, персоналу) для запобігання загрозам і забезпечення стабільного функціонування.
IV	2000–2002 рр.	Функціональний підхід: Відбувається декомпозиція поняття. Науковці починають виділяти окремі функціональні складові (фінансову, кадрову, техніко-технологічну, правову тощо).
V	2002–2005 рр.	Системний підхід: ЕБП трактується як комплексна система, що забезпечує не лише захист, а й умови для розвитку та досягнення стратегічних цілей підприємства.
VI	2005 – дотепер	Галузевий та адаптивний підхід: Розгляд ЕБП з урахуванням галузевої специфіки підприємства та необхідності адаптації до глобальних викликів (криз, цифровізації).

Джерело: складено на основі (Гринкевич та ін., 2023)

Наприклад, якщо на першому етапі (1991-1997 рр.) ЕБП трактувалася вузько, переважно як "гарантування конфіденційності та захисту комерційної таємниці", то вже на четвертому етапі (1999-2002 рр.) відбулося концептуальне розширення, і науковці почали "виокремлювати функціональні складові економічної безпеки". Шостий етап (2005-сьогодні), за цією класифікацією, характеризується врахуванням "галузевої належності" підприємства [10]. Цю еволюцію логічно доповнюють та осучаснюють інші дослідники, деталізуючи новітні етапи. Зокрема, Захарчук Н.М. виділяє "системний ризико-орієнтований підхід" як домінуючий у період 2010-2020 рр. [2], де ЕБП розглядається як "комплексне управління ризиками в усіх сферах діяльності". А з 2020 року (початок пандемії) по теперішній час, за її твердженням, відбувається перехід до "адаптивно-інноваційного підходу", що передбачає "інтеграцію цифрових технологій, гнучкого управління, прогнозування та використання інструментів штучного інтелекту".

Саме така складна, багатоетапна еволюція поняття пояснює, чому в сучасній науковій літературі досі немає єдиного, уніфікованого визначення ЕБП. Різні науковці описують цю категорію, спираючись на підходи різних етапів: одні все ще роблять акцент на "захисті", тоді як інші вже визначають її через "адаптивність" та "інтеграцію з ІІІ". Це вимагає від нас проведення подальшої систематизації існуючих поглядів, щоб сформувати цілісне уявлення про цю категорію. Для впорядкування множини наукових поглядів, ми вважаємо за доцільне використати класифікацію, яку пропонують Гаркуша В.О. та Єршова Н.Ю. У своєму дослідженні вони систематизують дефініції ЕБП за чотирма ключовими підходами [9]:

Статистичний підхід: розглядає ЕБП як статичний "стан захищеності" життєво важливих інтересів підприємства від загроз.

Апофатичний підхід: визначає ЕБП "від протилежного" – як "відсутність загроз і небезпек".

Діяльнісний підхід: трактує ЕБП як динамічний процес, "систему заходів, спрямованих на створення певних безпечних умов".

Пасивний підхід: визначає ЕБП через "дотримання певних параметрів і норм".

Ця класифікація дозволяє чітко розмежувати погляди за їхньою суттю (стан чи процес). Цільова спрямованість авторських формулювань у межах цих підходів детально представлена в табл. 1.1.

Таблиця 1.2

Систематизація поглядів українських науковців щодо сутнісного наповнення категорії «економічна безпека підприємства»

Автор	Визначення
Статистичний підхід: «безпека як стан захищеності»	
Шликов В.В. [54]	стан захищеності життєво важливих інтересів підприємства від реальних та потенційних джерел небезпеки або економічних загроз
Бендіков Л. [55]	захищеність науково-технічного, технологічного, виробничого та кадро-вого потенціалу від прямих та непрямих економічних загроз, що пов'язані з неефективною науково-промисловою політикою держави або формуванням несприятливого зовнішнього середовища та здатність підприємства до відтворення
Гладченко Т.Н. [64]	захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, організація якої здійснюється адміністрацією й колективом підприємства шляхом реалізації системи заходів правового, економічного, організаційного, інженерно-технічного й соціально-психологічного характеру
Апофатичний підхід: «безпека як відсутність загроз і небезпек»	
Камлик М. І. [63]	стан розвитку суб'єкта господарювання, який характеризується стабільністю економічного та фінансового розвитку, ефективністю нейтралізації негативних факторів і

	протидії їх впливу на всіх стадіях його діяльності
Забродський В. [56]	кількісна і якісна характеристика властивостей фірми, що відбиває здатність «самовиживання» і розвитку в умовах виникнення зовнішньої і вну-трішньої економічної загрози
Євдокимова Н. М., Кірієнко А. В. [57]	Стан оптимального для підприємства рівня використання його економічного потенціалу, за якого діючі та/або можливі збитки виявляються нижчими за встановлені підприємством межі
Діяльнісний підхід: «безпека як система заходів, спрямованих на створення певних безпечних умов»	
Могільний А.І. [58]	забезпечення стану життєдіяльності, при якому реалізуються його осно-вні інтереси, воно захищено від внутрішніх та зовнішніх загроз і дестабілізуючих чинників
Варналій З. С. [59]	забезпечення найбільш ефективного використання ресурсів суб'єкта господарювання для запобігання загрозам і створення умов для стабільного функціонування основних його елементів
Лисенко Ю., Міщенко С. [60]	стан виробничо-економічної системи, при якому функціонують меха-нізми запобігання чи зменшення ступеня впливу погроз стабільності функціонування і розвитку підприємства
Пасивний підхід: «дотриманням певних параметрів і норм, від забезпечення яких безпосередньо залежить безпека»	
Малащенко В. [61]	корпоративна система функціонування підприємства, за умови якої відбувається найбільш ефективне використання корпоративних ресурсів, і водночас знижуються наявні та потенційні загрози, в результаті чого досягається максимально позитивний ефект від роботи підприємства

Грунін О.А., Грикнін С.О. [64]	стан господарюючого суб'єкта, в якому він при найефективнішому використанні корпоративних ресурсів досягає запобігання послаблення або захисту від існуючих небезпек та загроз або непередбачених обставин і, в основному, забезпечує досягнення цілей бізнесу в умовах конкуренції та господарчого ризику
Дацків Р. [65]	Такий стан економічного розвитку суб'єктів господарювання (особи, держави, організації), який забезпечує йому гармонійний розвиток і ефективне використання шансів і усунення загроз

Джерело: складено на основі [13]

Ця систематизація є фундаментальною, оскільки чітко розмежовує підходи "стан" (Статистичний) та "процес" (Діяльнісний). Водночас, Асамоах-Черемех Д. та Рудніченко Є.М. пропонують іншу сучасну систематизацію, яка групує підходи не за сутністю, а за аспектами та цілями управління [1]:

- Системне управління підприємством: Акцент на забезпеченні "стабільного та максимально ефективного функціонування".
- Перспективне управління підприємством: Фокус на "формуванні високого потенціалу зростання та розвитку... у майбутньому".
- Превентивне управління загрозами: Акцент на "попередженні та протидії" загрозам, тобто на захищеності.
- Компенсаційне управління загрозами: Акцент на "подоланні" загроз та "мінімізації їх негативних впливів".

Для повноти огляду варто також згадати укрупнену класифікацію, яку наводить Москвін Б.Ю., розділяючи підходи на інтегральний (зв'язок з конкурентоспроможністю та потенціалом), ресурсний (ефективне використання ресурсів) та цільовий (захист інтересів та реалізація цілей).

Аналіз цих класифікацій дозволяє зробити важливий висновок. Сучасна наукова думка все більше відходить від розуміння ЕБП як статичного "стану" (що відповідає Статистичному підходу) і схиляється до "Діяльнісного" підходу (ЕБП як безперервний процес) та "Перспективного" підходу (ЕБП як інструмент забезпечення розвитку). Це вимагає розмежування ЕБП від суміжних категорій менеджменту, таких як "економічний потенціал" та "стратегічне управління".

Для повного розуміння сутності ЕБП важливо чітко розмежувати її від суміжних категорій, зокрема від поняття "економічний потенціал". Васильців Т.Г. та ін. пропонують розглядати ці поняття як "протилежні сторони однієї і тієї ж монети". Автори проводять чітке розмежування [11]:

- Економічний потенціал – це "«ефективність використання» сукупних можливостей, ресурсів та резервів". Це категорія розвитку та ефективності.

- Економічна безпека – це "«стан», за якого задовольняється низка умов" (доступність ресурсів, захищеність від ризиків) . Це категорія захисту та життєздатності

Ця різниця є ключовою для методології оцінки. Як зазначають Васильців Т.Г. та ін. економічний потенціал вимірюється відносно максимальних орієнтирів – "кращих взірців, практик, даних головних конкурентів". Інакше кажучи, мета – бути кращим і досягти максимуму.

Натомість, економічна безпека вимірюється відносно мінімально допустимих орієнтирів – "граничних (критичних) значень". Тут мета – не бути гіршим за певний поріг життєздатності, оскільки вихід за ці межі "сигналізує про небезпеку".

Інший погляд на цю взаємодію пропонує Зінченко Д.С., який розглядає економічну безпеку не як паралельне явище, а як складову частину та наслідок економічного розвитку [12]. Автор доводить, що "результати управління економічним розвитком підприємства в цілому формують відповідний рівень економічної безпеки". Цей зв'язок має циклічний

характер: поточний "Рівень економічного розвитку" визначає "Рівень економічної безпеки", який, у свою чергу, "впливає на формування майбутнього рівня його економічного розвитку".

Визначивши зв'язок ЕБП з розвитком та потенціалом, необхідно окреслити її місце в загальній системі менеджменту. Найбільш обґрунтованою видається позиція, що інтегрує ЕБП у стратегічний контур управління. Дячков Д.В., у своїй моделі (Рис. 1) демонструють, що "Економічна безпека" (яка включає "Безпеку бізнесу" та "Корпоративну безпеку") є невід'ємною частиною "Стратегічного управління". При цьому вона нерозривно пов'язана з "Інтегрованою системою ризик-менеджменту" [13].

Отже, спираючись на проаналізовані підходи, можна зробити висновок, що економічна безпека – це не просто пасивна захисна функція і не лише результат розвитку. У сучасному розумінні, ЕБП – це активна, інтегрована частина стратегічного управління, яка фокусується на управлінні ризиками для забезпечення життєздатності підприємства та створення необхідних умов для реалізації його економічного потенціалу. Це підводить нас до необхідності формалізації цього процесу, а саме – формування чіткої "Стратегії економічної безпеки".

1.2. Класифікація та характеристика функціональних складових системи економічної безпеки підприємства

Визначивши у попередньому підрозділі економічну безпеку підприємства як комплексну, динамічну та діяльну систему, логічним кроком є її подальша декомпозиція. Для ефективного формування та управління (що є метою даної магістерської роботи), таку складну категорію необхідно структурувати, виділивши її окремі функціональні підсистеми, або складові. Більшість науковців сходяться на думці щодо такого підходу,

визначаючи функціональні складові ЕБП як "сукупність основних напрямів економічної безпеки підприємства, які за своїм змістом істотно відрізняються один від одного". Кожна з цих складових характеризує окремий аспект діяльності підприємства та вимагає специфічних методів аналізу та управління, що й буде розглянуто далі.

У науковій літературі "функціонально-компонентний підхід" є одним із найбільш розповсюджених та визнаних. Він став основою для "стандартизації та узагальнення" поняття ЕБП ще у 2000-х роках. Цей підхід дозволяє представити ЕБП як цілісну систему, що складається з набору ключових підсистем.

Аналіз праць з цієї теми показує, що, попри певні розбіжності, науковці виділяють стійкий "каркас" таких складових. Наприклад, Коробцова[14] наводить вичерпний перелік з восьми функціональних цілей (складових) ЕБП. До них належать:

- Фінансова (забезпечення "високої фінансової ефективності роботи, фінансової стійкості та незалежності");
- Технологічна ("забезпечення технологічної незалежності");
- Управлінська ("досягнення високої ефективності менеджменту");
- Кадрова/Інтелектуальна ("досягнення високого рівня кваліфікації персоналу");
- Екологічна ("мінімізація руйнівного впливу");
- Правова ("якісна правова захищеність");
- Інформаційна ("забезпечення захисту інформаційного поля, комерційної таємниці");
- Силова/Фізична ("ефективна організація безпеки персоналу, капіталу та майна").

Більш компактну, але методологічно схожу модель пропонують Зіненко та Кобелева. Їхній підхід фокусується на шести ключових складових [15], які безпосередньо пов'язані з господарською діяльністю: фінансова, техніко-технологічна, кадрова, ринкова, правова та екологічна.

Таким чином, аналіз "класичних" моделей показує, що в основі ЕБП лежить "ядро" загально визнаних складових (фінансова, кадрова, технологічна, правова, інформаційна). Водночас, включення такими авторами, як Зіненко і Кобелєва [15], "ринкової" складової, або "управлінської", вказує на спроби розширення цієї моделі. Проте, як буде показано далі, в умовах сучасних викликів, зокрема воєнного стану та цифровізації, цей "класичний" набір вимагає суттєвого доповнення та переосмислення. Наукова дискусія щодо структури ЕБП не обмежується "класичним" набором. Вчені, реагуючи на нові виклики, такі як "дестабілізаційний розвиток" та воєнний стан, обґрунтовують необхідність включення до моделі нових, специфічних компонентів.

Так, Прохорова В., Крутова А. та Дяченко К. [16] у своїй "Коеволюційній основі управління" (Рис. 1 у їхній статті) представляють розширену поліфункціональну структуру, яка налічує дванадцять складових. Окрім традиційних (фінансова, кадрова, силова тощо), ця модель додатково включає такі важливі елементи, як «Ресурсна», «Ринкова», «Інтерфейсна» (що відповідає за взаємодію з іншими системами) та «Інноваційно-інвестиційна». Особливо важливим у цій моделі є те, що автори наполягають: "в умовах дестабілізаційного розвитку необхідним є виділення управлінської функції" як окремої повноцінної складової, оскільки саме від оперативності рішень залежить ефективність всієї системи.

Схожий розширений підхід демонструють Огренич Ю.О. та Діброва В.О. У їхній моделі (Рис. 1 у статті) система ЕБП складається з десяти компонентів [17]. Примітно, що автори, на відміну від багатьох "класичних" підходів, чітко розмежовують «Інтелектуальну» та «Кадрову» складові, а також додають до структури «Соціальну» (що відповідає за взаємодію в колективі та з суспільством) та «Інноваційну» складові.

Таке розширення переліку до 10-12 елементів свідчить про ускладнення самого об'єкта дослідження. Однак, для нашої роботи особливий інтерес становлять не стільки ці розширення, скільки

трансформація вже існуючих "класичних" складових під впливом головних викликів сучасності – цифровізації та специфіки ринку, що буде розглянуто далі. Найбільш суттєвих та кардинальних змін в умовах цифрової економіки зазнала інформаційна складова. Якщо в класичних моделях її завдання зводились до "забезпечення захисту інформаційного поля, комерційної таємниці", то сьогодні цього абсолютно недостатньо.

Як справедливо зазначає Проскура [18], традиційні методики оцінки ЕБП часто є статичними та "не відображають рівень захищеності підприємства від кіберзагроз". Розвиток цифрової економіки, який ці ж автори поділяють на "оцифровування" (переведення інформації в цифрову форму), "діджиталізацію" (використання технологій для оптимізації процесів) та "цифрову трансформацію" (докорінна зміна бізнес-моделі), створює нові, раніше неіснуючі вектори атак.

Кульчицький [19] (Таблиця 1 у його статті) ідентифікує ці сучасні загрози як: "Кіберзагрози" (кібератаки, злам інформаційних систем, розкрадання конфіденційних даних), "Ненадійність інформаційних систем" (збої, помилки) та "Незахищеність даних" (порушення конфіденційності). Мельничук доповнює цей перелік специфічними загрозами для бізнесу, такими як "проникнення до баз даних підприємства через спеціалізовані бухгалтерські програми" та "викрадення інформації щодо облікових операцій... унаслідок фішингових чи кібератак".

Через це сучасні дослідники наполягають на виокремленні "Кібербезпеки" як повноцінної, пріоритетної складової ЕБП. Москвін [20], аналізуючи виклики воєнного стану, пропонує доповнити класичний перелік окремими компонентами "Кібербезпека" та "Репутаційна безпека", яка в цифровому світі напряму залежить від інформаційних атак. Проскура та інші у своїй моделі оцінки 2024 року вже роблять індикатори, пов'язані з цифровим захистом, центральними, пропонуючи вимірювати "коефіцієнт персоналу, що пройшов навчання з кібербезпеки" та "частку витрат на кіберзахист". Не менш глибока трансформація, яка є головним фокусом

даної магістерської роботи, відбувається з кадровою складовою ЕБП. У класичних моделях ця складова здебільшого оцінювалася через такі показники, як "плинність кадрів" та "продуктивність праці". Однак в умовах "цифровізації ринку праці" цього стає недостатньо.

Як обґрунтовано у монографії Андріїв [3], ключовою загрозою для підприємств стає не просто звільнення персоналу, а "втрата людського капіталу". Автор доводить, що "людський фактор виступає основою конкурентоспроможності підприємства". Відповідно, поняття "кадрової безпеки" (яка також є в моделі автора, див. Рис. 1.10) розширюється до поняття "безпеки людського капіталу".

Цей новий підхід передбачає, що в умовах цифрової трансформації підприємства (Рис. 1.8) змінюються самі вимоги до персоналу. Пріоритетом стає "Зростання значення кваліфікації, освіти і професіоналізму" та "Приріст інтелектуальних ресурсів підприємства". Таким чином, сучасна кадрова безпека – це вже не стільки процес утримання, скільки процес розвитку "цифрових компетентностей" працівників. Завданням цієї складової стає протидія новим специфічним загрозам, які ідентифіковані в монографії, зокрема: "відтік фахівців" (трудова міграція кваліфікованих кадрів), "внутрішні конфлікти" (спротив інноваціям) та "«старіння знань»", яке відбувається через стрімкий технологічний поступ.

Нарешті, для підприємств, що активно працюють на висококонкурентних ринках, зокрема в логістиці, критичної актуалізації набуває ринкова (або маркетингова) складова. Як зазначають Асамоах-Черемех та Рудніченко саме в сучасних умовах (пандемія, воєнний стан) відбулася активізація уваги до цієї складової. Вони пов'язують це з необхідністю пошуку нових ринків збуту та "успішної ринкової діяльності підприємств в умовах європейської інтеграції України" [1].

Дієвим інструментом (механізмом) управління цією складовою Овчаренко називає «конкурентну розвідку», яку визначає як "безперервний,

легальний процес збирання, аналізу та надання... інформації про конкурентне середовище" [21].

Для практичного аналізу загроз у цьому середовищі автор пропонує використовувати модель п'яти конкурентних сил М. Портера, що включає аналіз загроз з боку:

- 1) нових конкурентів;
- 2) ринкової влади покупців;
- 3) ринкової влади постачальників;
- 4) товарів-замінників;
- 5) інтенсивності внутрішньогалузевої конкуренції.

Окрім загальних складових, для підприємств, що активно працюють на міжнародних ринках, науковці обґрунтовують необхідність виділення специфічних напрямів безпеки. Зокрема, Чернишов В. В. у своєму дослідженні присвячує увагу саме такій складовій, як «безпека зовнішньоекономічної діяльності (ЗЕД)». Актуальність виокремлення цієї компоненти автор пояснює тим, що такі підприємства "підлягають під вплив широкого кола факторів в силу розвитку процесів інтернаціоналізації та глобалізації" [22]. Це, у свою чергу, вимагає формування окремої стратегії та механізмів управління, спрямованих на захист від специфічних ризиків, пов'язаних з міжнародною діяльністю.

Отже, проведений аналіз наукових джерел демонструє, що структура економічної безпеки підприємства є складною, поліфункціональною та динамічною системою. Ми встановили, що "класичні" моделі, були суттєво розширені сучасними дослідниками (Прохорова, Огренич та Діброва) для включення 10-12 компонентів.

Водночас, виявили, що ключові виклики сучасності, такі як "воєнна агресія", "дестабілізаційний розвиток" та "цифровізація", не просто додають нові складові, а докорінно трансформують існуючі. Це особливо стосується інформаційної складової, яка еволюціонувала в "кібербезпеку", кадрової складової, що перетворилася на "безпеку людського капіталу" та ринкової

складової, яка вимагає інструментів "конкурентної розвідки" і врахування безпеки ЗЕД.

Такий всеосяжний аналіз є необхідним для розробки стратегії, однак проведення кількісної оцінки вимагає більш прагматичної та чітко обрахованої моделі. Багато зі згаданих складових (наприклад, силова, соціальна, репутаційна) важко оцінити кількісно на основі публічної фінансової звітності.

Тому для цілей практичної діагностики у Розділі 2 цієї роботи необхідно обрати модель, яка, з одного боку, є достатньо повною, а з іншого – спирається на доступні статистичні та фінансові показники. У цьому контексті найбільш обґрунтованою для проведення кількісного аналізу є модель, запропонована Пілецькою С. Т., Коритько Т. Ю. та Ткаченко Є. В. Автори, критикуючи надто широкі переліки, що "виходять за рамки безпосередньої господарської діяльності", пропонують для "об'єктивної оцінки" згрупувати показники у чотири ключові функціональні складові, що базуються на даних звітності: фінансова, виробничо-збутова, техніко-технологічна і кадрова [23].

Таким чином, у Розділі 2 цієї роботи для проведення комплексного розрахунку інтегрального показника ЕБП буде використано саме цю 4-компонентну модель. Проте, для її коректного застосування, необхідно спочатку обґрунтувати саму методику кількісної оцінки. Відтак, наступним логічним кроком є огляд існуючих методичних підходів до оцінювання рівня економічної безпеки.

1.3. Огляд методичних підходів до оцінки рівня економічної безпеки підприємства

Проведений у попередньому підрозділі аналіз довів, що економічна безпека є складною, поліфункціональною системою, яка складається з

багатьох компонентів. Таке розуміння ставить перед менеджментом та аналітиками ключове управлінське завдання: як кількісно та якісно виміряти поточний стан цієї системи та рівень кожної з її складових. Ефективне формування системи ЕБП, що є метою нашої роботи, неможливе без чіткого методичного інструментарію її діагностики.

Проте, як справедливо зазначають Шило Ж. С. та Кречко М. Ю. [24], "сучасна економічна література не має єдиної методики комплексної оцінки економічної безпеки підприємства з урахуванням усіх необхідних для цього критеріїв". Цю думку підтверджують Карачина Н.П., яка вказує, що більшість існуючих методик мають суттєві "недоліки і перепони до їх практичного застосування", зокрема, "складність у практичному застосуванні", "відсутність гнучкості" та "ігнорування специфіки" діяльності підприємств [25].

Це доводить актуальність нашого завдання – провести декомпозицію та критичний аналіз існуючих методичних підходів. Це дозволить нам, по-перше, систематизувати наявний науковий інструментарій, а по-друге, обґрунтувати вибір (або синтез) найбільш релевантної методики, яка буде використана для практичного аналізу в другому розділі даної роботи.

Аналіз наукових джерел дозволяє виділити декілька ключових груп методів, що застосовуються для діагностики рівня ЕБП. Одну з найбільш повних та структурованих класифікацій пропонують Пілецька С. Т., Коритько Т. Ю. та Ткаченко Є. В. [23]. У своїй моделі вони виділяють шість основних методичних підходів до оцінки рівня ЕБП:

- Індикативний підхід: Базується на розробці системи показників-індикаторів та порівнянні їх фактичних значень із граничними (пороговими).
- Ресурсно-функціональний підхід: Оцінює стан та ефективність використання ресурсного потенціалу підприємства за окремими функціональними складовими.
- Програмно-цільовий підхід: Оцінює ЕБП через призму здатності підприємства досягати своїх стратегічних та тактичних цілей.

- Економіко-математичний підхід: Використовує складні моделі для аналізу та прогнозування (наприклад, регресійний аналіз, нечітка логіка).
- Методи прогнозування банкрутства: Вузькоспеціалізований підхід, що зосереджений виключно на діагностиці фінансової стійкості.
- Підхід на основі експертних оцінок: Використовує знання та інтуїцію фахівців для оцінки, в першу чергу, якісних параметрів безпеки.

Ця класифікація є надзвичайно корисною, оскільки вона охоплює практично весь спектр інструментів – від простих кількісних індикаторів до складних прогнозних моделей. Для цілей нашого дослідження, найбільш доцільно детальніше розглянути переваги та недоліки ключових із цих підходів, зокрема індикаторного, методів прогнозування банкрутства та якісних методів, спираючись також на аналіз інших науковців.

Найбільш поширеним у практиці вітчизняних підприємств є Індикативний підхід. Його суть полягає у розробці системи "індикаторів" (показників), які є пороговими значеннями що відображають межі, які відокремлюють безпечний стан від небезпечного.

Теоретичне обґрунтування цього "порогового" методу надає Васильців Т.Г. Він чітко розмежовують оцінку потенціалу та безпеки [11]. Якщо потенціал вимірюється відносно максимальних орієнтирів ("кращі взірці, дані головних конкурентів"), то рівень безпеки визначається через співвідношення з мінімально допустимими орієнтирами – "граничними (критичними) значеннями". Вихід за ці межі "сигналізує про небезпеку". Незважаючи на свою логічність, цей підхід має суттєвий недолік, на який вказує Панченко [26]: "складність визначення... порогових значень" для конкретного підприємства чи галузі, що може знизити об'єктивність оцінки.

Вузькоспеціалізованим, але поширеним варіантом індикативного підходу є методи прогнозування банкрутства, що фокусуються виключно на фінансовій складовій. Як зазначають Смірнова та Васюткіна до них належать такі відомі моделі, як "моделі Альтмана, R-моделі... моделі Ліса та моделі Таффлера" [27].

Проте, очевидно, що ані індикаторний підхід у чистому вигляді, ані моделі банкрутства не здатні оцінити такі важливі аспекти, як репутація, ринкова позиція чи відповідність цифровим викликам.

Для діагностики цих якісних, але не менш важливих, складових використовуються спеціалізовані методи. Наприклад, для оцінки репутаційної безпеки, як зазначають науковці Університету «КРОК» Алькема [28] та Живко [29], застосовують "соціологічні методи" (опитування клієнтів, персоналу), "методи медіа-аналізу" (моніторинг тональності згадок у соцмережах) та "рейтингові методи" (наприклад, RepTrak 100). Аналогічно, для аналізу ринкової складової, Овчаренко [21] обґрунтовує ефективність використання "моделі п'яти конкурентних сил М. Портера" для виявлення зовнішніх загроз.

Варто зазначити, що у сучасній зарубіжній практиці значного поширення набуває таксономічний аналіз. Так, Shumilo [30] пропонує використовувати метод таксономії для розрахунку інтегрального показника, оскільки він дозволяє нівелювати різницю в одиницях виміру індикаторів та побудувати ієрархічну модель безпеки."

Таким чином, ми бачимо, що різні методичні підходи вирішують різні завдання. Якісні та прогностні моделі є потужними, але вузькоспеціалізованими (для окремих складових, як-от фінансова чи репутаційна). Вони не дають єдиної, цілісної картини стану підприємства. Це підводить нас до висновку, що для комплексної діагностики необхідний підхід, який би об'єднував переваги індикаторного методу, але дозволяв агрегувати показники різних складових у єдиний узагальнюючий показник.

Для отримання такої комплексної оцінки, найбільш доцільним видається застосування Ресурсно-функціонального підходу, який визначено в класифікації Пілецької. Цей підхід дозволяє розрахувати інтегральний показник рівня ЕБП, базуючись на оцінці його окремих функціональних складових. Сама ідея агрегування часткових показників у єдиний індекс знаходить широку підтримку в сучасних наукових працях, які пропонують

для цього чіткі ієрархічні моделі. Так, Карачина [25] пропонує "Багаторівневу (ієрархічну) систему показників", яка має три рівні:

- Рівень 3: Часткові (одиничні) показники (наприклад, коефіцієнт ліквідності, плинність кадрів).
- Рівень 2: Узагальнюючі показники (інтегральні індекси окремих складових: Фінансової, Кадрової тощо).
- Рівень 1: Загальний Інтегральний показник ЕБП.

Дуже схожу логіку пропонує Панченко (Рис. 1 у статті), розробляючи "Принципову схему багаторівневої системи оцінки та моніторингу"[26]. Ця схема також передбачає аналіз "первинних показників" (Рівень 3), їх агрегацію в "узагальнюючі показники" за складовими (Рівень 2) та розрахунок єдиного "інтегрального показника" (Рівень 1).

Спираючись на обґрунтованість такого багаторівневого підходу, для практичної реалізації в даній роботі ми обрали конкретну, науково апробовану методику. Це – "Модель інтегральної оцінки рівня економічної безпеки підприємства", яка була розроблена та детально описана Пілецькою С.Т., Коритько Т.Ю. та Ткаченко Є.В. [23]. Актуальність та практична придатність даної моделі підтверджується тим, що вона була успішно використана для проведення аналізу промислових підприємств у більш пізньому дослідженні Огренич та Діброви. Детальний опис математичного апарату та інструментарію цієї моделі буде надано у наступному пункті.

Обрана нами "Модель інтегральної оцінки..." є комплексним 8-етапним алгоритмом, який буде покладено в основу практичного аналізу в Розділі 2 даної роботи. Ключові етапи цього алгоритму включають:

- Ідентифікацію загроз;
- Вибір джерел інформації (фінансова звітність, статистичні дані);
- Формування системи показників (індикаторів);
- Нормування показників (приведення їх до єдиної шкали);
- Визначення вагових значень та розрахунок інтегральних показників за кожною складовою;

- Розрахунок підсумкового інтегрального показника ЕБП;
- Якісна оцінка отриманого рівня ЕБП;
- Розробка заходів щодо підвищення рівня безпеки.

В основі моделі лежить 4-компонентний підхід, який, на думку авторів, є найбільш об'єктивним для оцінки господарської діяльності. Для кожної складової пропонується чіткий набір індикаторів (Рис. 3 у статті):

- Фінансова складова: Оцінюється через показники рентабельності (продажів, активів), платоспроможності (абсолютної та поточної ліквідності), фінансової стійкості (коефіцієнт автономії) та ділової активності (оборотність активів).

- Виробничо-збутова складова: Включає такі індикатори, як рівень зносу основних засобів та фондівіддача.

- Техніко-технологічна складова: Оцінюється через коефіцієнт оновлення основних фондів, коефіцієнт матеріаловіддачі та вироблення продукції на одного робітника.

- Кадрова складова: Включає коефіцієнт плинності кадрів, продуктивність праці та рентабельність персоналу.

Оскільки всі ці індикатори мають різну розмірність (% , рази, грн), автори пропонують уніфікувати їх за допомогою методу нормування (приведення до шкали від 0 до 1). Для цього застосовуються дві формули: формула

$$x_{(ij)} = (x_{(ij)} - \min_{(j)} x_{(ij)}) / (\max_{(j)} x_{(ij)} - \min_{(j)} x_{(ij)})$$

для показників-стимуляторів (де зростання є позитивним, наприклад, рентабельність) та формула (2)

$$x_{(ij)} = (\max_{(j)} x_{(ij)} - x_{(ij)}) / (\max_{(j)} x_{(ij)} - \min_{(j)} x_{(ij)})$$

для показників-дестимуляторів (де зростання є негативним, наприклад, плинність кадрів).

Вагові коефіцієнти як для окремих індикаторів всередині складової, так і для самих складових у загальному індексі, автори пропонують визначати за допомогою об'єктивних статистичних методів, зокрема "методу головних

компонент (МГК)". На основі такого розрахунку, підсумковий (загальний) інтегральний показник $I_{(ЕБП)}$ автори пропонують розраховувати за формулою (8), яка є зваженою сумою індексів чотирьох складових:

$$I_{(ЕБП)} = a_{(фс)} \cdot I_{(фс)} + a_{(взс)} \cdot I_{(взс)} + a_{(ттс)} \cdot I_{(ттс)} + a_{(кс)} \cdot I_{(кс)}$$

Для інтерпретації отриманого значення автори надають чітку шкалу якісних оцінок (Таблиця на стор. 5), де, наприклад, значення в діапазоні 0-19 відповідає високому ризику та неспроможності до розвитку, а 80-100 – високому рівню безпеки та стійкості до криз.

Таким чином, ми обрали чітку, комплексну та науково обґрунтовану "класичну" модель для проведення наших розрахунків. Проте, як вимагає науковий підхід, необхідно критично оцінити цю модель та визначити її обмеження, особливо в контексті нашої теми – цифровізації та сучасних викликів.

Таким чином, ми обрали чітку, комплексну та науково обґрунтовану "класичну" модель для проведення наших розрахунків. Проте, як вимагає науковий підхід, необхідно критично оцінити цю модель та визначити її обмеження, особливо в контексті нашої теми – цифровізації та викликів 2024 року.

Сучасні дослідники справедливо зазначають, що такі інтегральні моделі, хоч і є комплексними, мають суттєві недоліки. По-перше, як стверджують Проскура та ін. вони часто є статичними і "не відображають рівень захищеності підприємства від кіберзагроз". По-друге, Доманецький критикує їх за "реактивний" (пост-фактум) характер, оскільки вони констатують поточний стан, але не дають інструментів для прогнозування загроз [31].

Тому, в рамках даної роботи, ми пропонуємо підхід, який полягає у використанні моделі, як базової для кількісних розрахунків, але з її обов'язковим осучасненням та доповненням, що і становить наукову новизну нашого підходу. Це осучаснення буде відбуватися за трьома напрямками: Доповнення індикаторами цифрової безпеки. Оскільки обрана нами

"класична" модель не містить специфічних цифрових показників, при якісному аналізі в Розділі 2 ми будемо враховувати індикатори, запропоновані Проскура [18], такі як "коефіцієнт впровадження хмарних технологій" та "частка витрат на кіберзахист".

Поглиблення аналізу кадрової складової. "Класична" модель фокусується на "плинності" та "продуктивності". Ми доповнимо цей аналіз, спираючись на Гармаш [14], більш глибокими індикаторами, зокрема "співвідношенням рівня заробітної плати на підприємстві та середнього у галузі", а також врахуємо "моральний вимір" та безпеку "людського капіталу". Інтеграція якісного аналізу. Оскільки інтегральна оцінка є виключно кількісною, ми доповнимо її якісним аналізом репутаційної безпеки, спираючись на методологію наукової школи Університету «КРОК», яка включає "соціологічні методи" та "методи медіа-аналізу".

Цей синтез кількісної "класичної" моделі та сучасних якісних підходів дозволить нам отримати найбільш повну та об'єктивну оцінку. Обґрунтувавши методику оцінки, наступним кроком є аналіз механізмів та інструментів, за допомогою яких ця система формується та управляється.

Отже, проведений у даному підрозділі аналіз методичних підходів до оцінки рівня економічної безпеки дозволяє зробити декілька ключових висновків. По-перше, в науковій літературі не існує єдиної універсальної методики, що підтверджується позиціями Кречко і Карачини. По-друге, різні підходи (індикаторний, ресурсно-функціональний, експертний) вирішують різні завдання, маючи свої переваги та недоліки.

Спираючись на вимоги нашої роботи, яка передбачає проведення практичних розрахунків на основі фінансової звітності (Розділ 2), ми формуємо наступну фінальну методологічну позицію: Для кількісної діагностики ми обираємо "Модель інтегральної оцінки...", розроблену Пілецькою С. Т., Коритько Т. Ю. та Ткаченко Є. В., як базову. Її перевагами є чіткий математичний апарат, багаторівнева структура, що відповідає сучасним підходам Панченко та Карачина та опора на доступні статистичні

дані. Водночас, усвідомлюючи обмеженість цієї "класичної" моделі ми доповнюємо її сучасними якісними та кількісними інструментами аналізу.

Це "осучаснення" методики (що становить нашу наукову новизну) включатиме поглиблений аналіз кадрової складової (з використанням індикаторів, репутаційної безпеки (на основі методів медіа-аналізу Алькеми та Живко та ринкової безпеки).

Таким чином, обґрунтувавши складну, синтезовану методику оцінки рівня ЕБП, наступним логічним кроком є дослідження практичних аспектів її функціонування. Необхідно проаналізувати, які саме управлінські механізми та інструменти (такі як контролінг, стратегічне планування, інформаційно-аналітичне забезпечення) дозволяють не просто вимірювати, а й активно формувати та підтримувати належний рівень економічної безпеки підприємства, що і буде зроблено в наступному підрозділі.

1.4. Механізми, інструменти та принципи формування системи економічної безпеки підприємства

Обґрунтувавши у попередніх підрозділах сутність, структуру та, що особливо важливо, методику оцінки рівня економічної безпеки, ми виконали ключовий діагностичний етап. Проте, головна тема даної роботи – формування системи ЕБП – вимагає переходу від діагностики до практичного впровадження. Для того, щоб система ЕБП була не просто набором індикаторів, а дієвою та адаптивною управлінською системою, необхідний чіткий та ефективний механізм її формування та реалізації.

У науковій літературі механізм забезпечення ЕБП розглядається як комплексна категорія, що поєднує в собі суб'єкти, об'єкти та інструменти управлінського впливу. Так, Коробцова визначає механізм управління ЕБП як "сукупність методів", які за своєю природою поділяються на

"адміністративні, економічні, організаційно-технологічні, інституційно-правові, інформаційні, соціально-психологічні" [14].

Таким чином, для цілей нашого дослідження, механізм формування ЕБП ми розглядаємо як сукупність трьох ключових елементів:

1. фундаментальних принципів, на яких він базується;
2. функцій, які він виконує;
3. інструментів, за допомогою яких ці функції реалізуються. Саме аналізу цих елементів присвячено даний підрозділ.

Будь-який дієвий механізм управління має базуватися на системі фундаментальних принципів, які визначають "правила гри" та філософію його функціонування. Коробцова у своєму дослідженні наводить вичерпний перелік таких засад [14]. До ключових "класичних" принципів, на яких має будуватися система ЕБП, належать:

- Принцип законності (вся діяльність служби безпеки має відповідати чинному законодавству);
- Принцип системності (розгляд ЕБП як цілісної системи, де всі складові взаємопов'язані);
- Принцип економічної доцільності (витрати на забезпечення безпеки не повинні перевищувати потенційні збитки від загроз);
- Принцип безперервності (постійний моніторинг загроз, а не реагування "від кризи до кризи");
- Принцип адаптивності (здатність механізму гнучко перебудовуватися у відповідь на зміни зовнішнього середовища).

Сучасні дослідники доповнюють цей перелік принципами, що відповідають викликам цифрової економіки. Так, Ткаченко [32] серед 10 ключових принципів особливо виділяють:

- Принцип динамізму (здатність швидко адаптуватися до нових загроз, що є розвитком принципу адаптивності);
- Принцип інноваційності (обов'язкове "впровадження цифрових технологій та захист від кіберзагроз");

- Принцип оперативності ("забезпечення швидкого реагування на чинники ринкового середовища").

Дотримання цих принципів дозволяє механізму ЕБП виконувати свої ключові функції (завдання). Якщо раніше основною функцією вважався захист, то сучасний підхід розглядає їх значно ширше. Ткаченко [32] візуалізують фундаментальні завдання, які має вирішувати система ЕБП:

- Захист ресурсів підприємства;
- Мінімізація ризиків;
- Сприяння стратегічному розвитку (тобто безпека не як "гальмо", а як "двигун" розвитку);
- Гарантування фінансової стабільності;
- Забезпечення та підтримка довіри (серед партнерів, інвесторів та клієнтів, що напряму пов'язано з репутаційною безпекою) [43].

Таким чином, ми бачимо, що сучасний механізм ЕБП має бути інноваційним, адаптивним та виконувати не лише захисну, але й розвиткову функцію. Це доводить, що механізм ЕБП не може існувати ізольовано, а має бути інтегрований у загальну систему стратегічного управління підприємством.

Саме таку позицію займає Дячков Д.В. [13], який у своїй моделі демонструє, що "Економічна безпека" є невід'ємною частиною "Стратегічного управління" та нерозривно пов'язана з "Інтегрованою системою ризик-менеджменту". Автори визначають "Стратегію економічної безпеки" як "загальні, довготривалі, найбільш принципові й важливі цілі, плани, наміри керівництва... спрямовані на формування системи безпеки... з метою протидії реальним і потенційним загрозам". Для практичного формування такої стратегії вони пропонують 5-етапний процес:

Етап 1: Аналіз фінансово-господарської діяльності.

Етап 2: Формування стратегічних цілей.

Етап 3: Розробка шляхів реалізації цілей.

Етап 4: Конкретизація стратегії за періодами.

Етап 5: Оцінка розробленої стратегії [19].

Більш деталізовану, 8-етапну модель розробки стратегії пропонують Смірнова та Васюткіна [27]. Їхня модель починається з "узгодженості стратегічних цілей" та "діагностики інформації про середовище" (для чого автори рекомендують SWOT-аналіз), проходить через етап "оцінки економічної безпеки" (з використанням моделей Альтмана, Таффлера) та "прогнозу діяльності" (з використанням функції Кобба-Дугласа), і завершується "розробкою найбільш ефективної стратегії" (на основі моделей І. Ансоффа, Г. Стейнера) та її фінальною оцінкою.

Окрім таких загальних стратегічних моделей, в науковій літературі існують і вузькоспеціалізовані механізми для окремих складових. Наприклад, Чернишов [22] розробив 5-етапний "Механізм забезпечення економічної безпеки ЗЕД", що є особливо актуальним для підприємств з активною міжнародною діяльністю, як-от "Нова Пошта".

Таким чином, ми бачимо, що механізм ЕБП реалізується через чіткі, покрокові стратегічні моделі. Проте, для того, щоб ці моделі були не просто теоретичними схемами, а працюючими інструментами, вони вимагають постійного інформаційного "живлення" та управлінського контролю. Це підводить нас до найсучасніших концепцій реалізації механізму ЕБП – через системи контролінгу та інформаційно-аналітичного забезпечення.

Сучасні науковці схиляються до думки, що механізм ЕБП найефективніше інтегрується в загальну систему менеджменту через інструментарій контролінгу. Такий підхід дозволяє перетворити ЕБП з пасивного спостерігача на проактивного учасника управлінських рішень.

Карачина Н.П. пропонує "Концептуальну модель системи контролінгу економічної безпеки" [25]. У цій моделі ЕБП розглядається як "інтегрована система", що виконує повний цикл управлінських функцій: "планування, моніторинг, аналіз, контроль, регулювання".

Серцем цього механізму є "багаторівнева система показників", яку ми вже розглядали в підрозділі 1.3.

Цю ідею посилює Панченко, яка також розглядає "аналізування" як ключову функцію менеджменту ЕБП. Запропонована нею "Принципова схема багаторівневої системи оцінки та моніторингу" є, по суті, деталізацією функції контролінгу, яка дозволяє в режимі реального часу відстежувати відхилення від порогових значень.

Якщо контролінг – це "мозок" та "нервова система" механізму ЕБП, то "паливом" для нього є інформація. Ефективність усього механізму напряму залежить від якості інформаційно-аналітичного забезпечення (ІАЗ).

Біланчук пропонує детальний "Механізм інформаційно-аналітичного забезпечення ФЕБ" [33]. Цей механізм описує повний життєвий цикл інформації в системі безпеки:

- Виявлення потреби в інформації.
- Збір та реєстрація даних (з внутрішніх та зовнішніх джерел).
- Обробка та аналіз (з використанням фінансового аналізу, SWOT, PEST тощо).
- Інтерпретація та надання рекомендацій керівництву.
- Реалізація рішень та зворотний зв'язок.

Таким чином, сучасний механізм ЕБП – це синергія трьох компонентів: стратегії, яка визначає напрямки; контролінгу, який забезпечує моніторинг та аналіз; та інформаційно-аналітичного забезпечення, яке надає необхідні дані для прийняття рішень. Наступним кроком є розгляд конкретних інструментів, які використовуються в рамках цих механізмів.

Ефективність описаних механізмів (стратегічного, контролінгового, інформаційно-аналітичного) напряму залежить від набору інструментів, що застосовуються на етапах діагностики, аналізу та прогнозування. Аналіз провідних наукових джерел дозволяє згрупувати цей інструментарій у три основні категорії:

Класичні інструменти аналізу: Це загальновизнані методи, які використовуються для аналізу середовища та є базовими для систем контролінгу та ІАЗ. До них належать "SWOT-аналіз" (оцінка сильних та

слабких сторін, можливостей і загроз), "PEST-аналіз" (аналіз політичних, економічних, соціальних і технологічних факторів), а також "методи експертних оцінок".

Інструменти ринкового та конкурентного аналізу: Вони є критично важливими для оцінки ринкової та репутаційної складових ЕБП. Овчаренко обґрунтовує використання "моделі п'яти конкурентних сил М. Портера" як інструменту для аналізу галузевих загроз [21]. Крім того, автор вводить поняття "конкурентної розвідки" як дієвого інструменту збору інформації про конкурентне середовище. Сучасні цифрові та прогнозні інструменти: Це найновіша група інструментів, що відповідає викликам цифровізації та необхідності переходу від "реактивного" до "прогнозного" управління. Біланчук [33] до таких інструментів відносить "Business Intelligence (BI-системи)" для візуалізації даних, технології "Big Data" для аналізу великих масивів інформації (наприклад, логістичних потоків чи поведінки клієнтів) та "Штучний інтелект (AI)" для виявлення аномалій та прогнозування шахрайства. Доманецький також доповнює цей перелік такими інструментами економіко-математичного моделювання, як "багатофакторні регресійні моделі", "нейронні мережі" та "методи нечіткої логіки" [31].

Розглядаючи механізми формування ЕБП, варто звернути увагу на підхід Kukhar [34], який пропонує концептуальну модель, де цифрова трансформація виступає не просто інструментом, а ключовим драйвером забезпечення безпеки. Автори виділяють такі елементи цифрового механізму, як Cloud technologies (хмарні технології), Big Data, Blockchain та Artificial Intelligence, які інтегруються в усі рівні управління підприємством. Завершивши аналіз теоретико-методологічних засад (сутності, складових, методик оцінки та механізмів формування з їх інструментарієм), ми можемо сформулювати загальні висновки до Розділу 1.

Проведений у даному підрозділі аналіз дозволяє нам узагальнити, що сучасний механізм формування економічної безпеки підприємства – це складна, проактивна та інтегрована в загальну систему менеджменту

підсистема. Ми встановили, що такий механізм базується на чітких принципах, зокрема системності, економічної доцільності, адаптивності та, що особливо актуально сьогодні, інноваційності.

Було з'ясовано, що механізм ЕБП виконує не лише захисну, але й розвиткову функцію, "сприяючи стратегічному розвитку" та "підтримці довіри" стейкхолдерів. Для реалізації цих функцій в науковій літературі пропонуються покрокові стратегічні моделі.

Водночас, найсучасніші концепції, які ми проаналізували, пропонують інтегрувати цей механізм у загальну систему управління підприємством через систему контролінгу та інформаційно-аналітичного забезпечення (ІАЗ). Ці механізми використовують широкий інструментарій – від класичного ("SWOT-аналіз") до ринкового ("конкурентна розвідка") та цифрового, що включає "Штучний інтелект (AI)", "Big Data" [10] та "нейронні мережі".

У першому розділі магістерської роботи було проведено глибокий теоретико-методологічний аналіз засад формування системи економічної безпеки підприємства. Це дозволило нам виконати поставлені завдання та дійти наступних висновків:

Проаналізовано сутність та еволюцію поняття ЕБП. Встановлено, що наукова думка еволюціонувала від "захисного" підходу до сучасного "адаптивно-інноваційного" та "стейкхолдерського" підходів. Сформульовано авторське визначення, яке розглядає ЕБП як комплексну, адаптивну діяльність системи управління, спрямовану на узгодження інтересів стейкхолдерів та забезпечення балансу між захистом (життєздатністю) та розвитком (реалізацією потенціалу), з особливим акцентом на загрозах цифровізації ринку праці.

Досліджено структуру ЕБП. Виявлено, що "класичні" 6-8 компонентні моделі в сучасних умовах доповнюються новими пріоритетними складовими, такими як "інноваційна" та "соціальна". Найважливішим є не просто доповнення, а трансформація існуючих складових: інформаційна

еволюціонує в "кібербезпеку", кадрова – в "безпеку людського капіталу", а ринкова – в "репутаційну безпеку" та "безпеку ЗЕД".

Обґрунтовано методичний підхід до оцінки. Проаналізувавши різноманіття методів – від індикаторного до якісного та прогнозного – ми обґрунтували синтезований підхід для нашого дослідження. Кількісною базою для аналізу в Розділі 2 обрано 4-компонентну "Модель інтегральної оцінки...", яка спирається на дані фінансової звітності. Водночас, ця модель буде "осучаснена" шляхом доповнення якісним аналізом репутаційної, кадрової та цифрової складових, що становить нашу методологічну новизну. Визначено механізми та інструменти формування ЕБП. Встановлено, що сучасний механізм ЕБП базується на принципах адаптивності та інноваційності та реалізується через покрокові стратегічні моделі. Найбільш ефективною сучасною формою реалізації визнано інтеграцію ЕБП у систему контролінгу, яка використовує інформаційно-аналітичне забезпечення (ІАЗ) та цифрові інструменти (AI, Big Data).

Таким чином, у Розділі 1 було повністю виконано поставлені завдання, а саме – сформовано міцну теоретичну базу щодо сутності та структури ЕБП та обґрунтовано комплексну методологію її оцінки і механізми формування. Це дозволяє нам перейти до наступного етапу дослідження – практичного аналізу та діагностики системи економічної безпеки на прикладі ТОВ «Нова Пошта».

РОЗДІЛ 2. АНАЛІЗ ТА ДІАГНОСТИКА ІСНУЮЧОЇ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «НОВА ПОШТА»

2.1. Загальна фінансово-господарська характеристика ТОВ «Нова Пошта» та аналіз факторів зовнішнього середовища

Провівши у першому розділі детальний теоретико-методологічний аналіз сутності, структури, методів оцінки та механізмів формування системи економічної безпеки (СЕБП), ми переходимо до практичної частини нашого дослідження. Метою даного розділу є проведення комплексного аналізу та діагностики стану економічної безпеки на прикладі конкретного підприємства.

Об'єктом нашого дослідження обрано Групу компаній "Нова Пошта" (далі – Група, або ТОВ «Нова Пошта»). Цей вибір обґрунтований тим, що "Нова Пошта" є не лише беззаперечним лідером ринку поштово-логістичних послуг України [35], але й системно утворюючим елементом інфраструктури країни. Функціонування компанії в умовах "глобальних та непередбачуваних криз", зокрема "Пандемії коронавірусу та воєнних конфліктів" [36], робить аналіз її системи ЕБП надзвичайно актуальним.

Аналіз проводитиметься на основі офіційної Консолідованої фінансової звітності та Консолідованих звітів про управління Групи "Нова Пошта" за 2019-2024 роки [38], а також з використанням даних, наведених у наукових працях, присвячених аналізу ТОВ «Нова Пошта» [39]; [40]; [37].

Група "Нова Пошта" – це заснована у 2001 році українська компанія, що пропонує повний спектр логістичних та фінансових послуг. Місія компанії – "робити доставку легкою для життя та бізнесу". На сьогодні "Нова Пошта" є визнаним лідером логістичного ринку України, що підтверджується численними науковими дослідженнями. Група забезпечує доступну та зручну доставку документів, вантажів та посилок для фізичних осіб та бізнесу,

оперуючи розгалуженою мережею, що налічує тисячі відділень та поштоматів по всій країні. Організаційна структура Групи включає материнську компанію ТОВ "Нова Пошта" та ключові дочірні компанії, зокрема ТОВ "НоваПей" (що надає фінансові послуги) та "Nova Poshta Global", яка активно розвиває міжнародний напрям доставки та має представництва у країнах Європи (Німеччина, Польща, Литва, Чехія та ін.).

Саме така складна, диверсифікована структура Групи, що включає логістичні, фінансові (NovaPay) та міжнародні (Global) операції, робить аналіз її Консолідованої звітності єдиним об'єктивним методом оцінки її реальної економічної безпеки. Для оцінки загального стану підприємства та масштабів його діяльності, ми провели аналіз ключових техніко-економічних показників діяльності Групи за 2019-2024 роки [38]. Вся інформація була зібрана з консолідованої фінансової звітності компанії за відповідні періоди (2020-2024), а також з аналітичних таблиць у роботах Бородіна [39] та Марухненко [40]. Зведені дані представлено у Таблиці 2.1.

Таблиця 2.1

Основні техніко-економічні показники Групи «Нова Пошта» за 2019-2024 рр. (тис. грн)

Показник	2019	2020	2021	2022	2023	2024
Чистий дохід	16 010	20 621	25 549	28 461	43 645	54 247
(Виручка)	832	616	607	964	219	287
Собівартість реалізації	11 773	14 553	16 678	21 095	31 494	40 130
	473	161	505	656	507	254
Чистий прибуток	1 088	1 709	2 519	3 268	4 346	3 866
	112	877	616	774	779	274
Вартість активів	6 927	9 533	15 365	19 515	26 752	36 677
	368	558	128	221	062	524
Власний капітал	1 935	3 497	5 568	8 468	10 879	13 228
	207	828	255	177	248	951

Продовження таблиці 2.1

Зобов'язання (всього)	4 992 161	6 035 730	9 796 873	11 047 044	15 872 814	23 388 573
Сер. облік. к-ть працівників (осіб)		28 831	33 717	31 486	31 298	33 354

Джерело: складено автором на основі Консолідованої фінансової звітності ТОВ «Нова Пошта» за 2020-2024 рр. [45]

Для візуалізації ключових тенденцій, виявлених у Таблиці 2.1, та полегшення аналізу, побудуємо графіки динаміки основних показників діяльності Групи "Нова Пошта" (Рис. 2.1, Рис. 2.2 та Рис. 2.3).

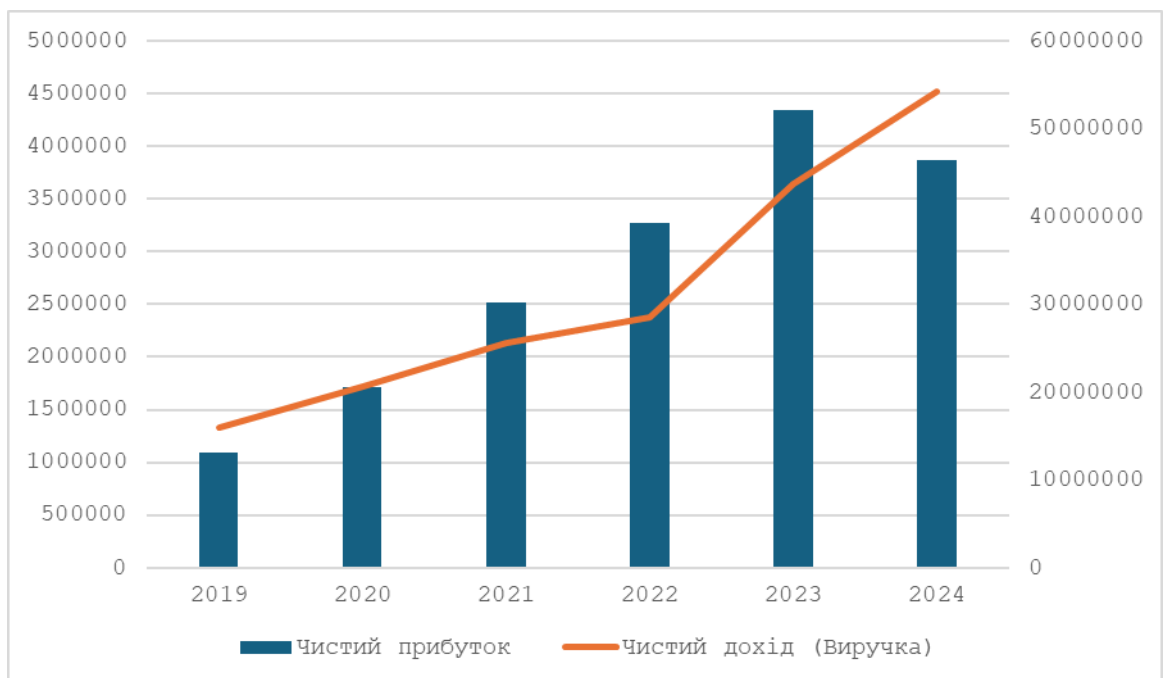


Рис. 2.1. Динаміка фінансових результатів Групи «Нова Пошта» за 2019–2024 рр.

Джерело: складено автором на основі Консолідованої фінансової звітності ТОВ «Нова Пошта» за 2020-2024 рр. [НП]

Аналіз Рис. 2.1, на якому зображено динаміку чистого доходу (ліва вісь) та чистого прибутку (права вісь), дозволяє зробити декілька висновків.

Насамперед, спостерігається феноменальна адаптивність компанії, що є ключовим принципом ЕБП, який ми обговорювали в п. 1.4. Попри початок повномасштабного вторгнення, компанія не зазнала фінансового колапсу.

Більше того, "Нова Пошта" продемонструвала здатність нарощувати чистий дохід навіть у найскладніший 2022 рік, коли виручка зросла на 11,4% (порівняно з 2021 роком) та чистий прибуток – на 29,7% (порівняно з 2021 роком). Це свідчить про високу якість фінансового менеджменту та критичну важливість послуг компанії для економіки, що узгоджується з аналізом, проведеним Тарнавською та Мажарою [37].

Водночас, дані за 2024 рік вперше демонструють негативну дивергенцію (розбіжність), що є прямим індикатором загрози для фінансової безпеки. Як видно з Рис. 2.1, чистий дохід продовжує стрімко зростати (з 43,6 до 54,2 млрд грн), однак чистий прибуток вперше падає (з 4,3 до 3,9 млрд грн). Це сигналізує про те, що витрати компанії – зокрема, собівартість, яка, згідно зросла у 2024 р. на 27,4% – почали зростати швидше за доходи.

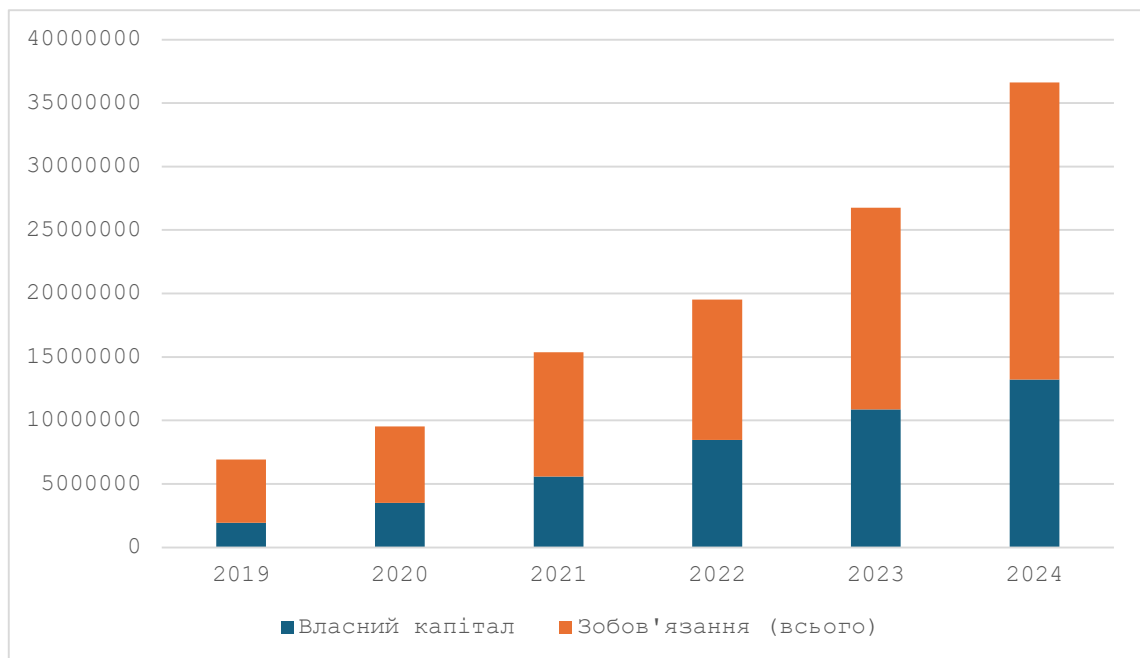


Рис. 2.2. Динаміка структури капіталу Групи «Нова Пошта» за 2019-2024 рр.

Джерело: складено автором на основі Консолідованої фінансової звітності ТОВ «Нова Пошта» за 2020-2024 рр. [НП]

Ймовірними причинами цього є зростання цін на паливо, значні інвестиції у закордонні філії ("Nova Poshta Global") та підвищення витрат на оплату праці для утримання персоналу. Цей аспект вимагатиме поглибленого аналізу при оцінці інтегрального показника.

Аналіз Рис. 2.2, що демонструє структуру капіталу Групи, дозволяє нам оцінити два ключові аспекти фінансової безпеки: масштаби діяльності та рівень фінансової стійкості.

Загальна висота стовпчиків (яка дорівнює "Вартості активів" з Таблиці 2.1. свідчить про стрімке та безперервне зростання масштабів бізнесу. Активи Групи зросли з 6,9 млрд грн у 2019 році до 36,7 млрд грн у 2024 році – зростання у 5,3 рази за шість років. Це свідчить про високий рівень інвестицій у розвиток (нові термінали, ІТ, закордонні відділення). Водночас, з точки зору економічної безпеки, нас більше цікавить джерело цього зростання, яке відображено у співвідношенні синьої (Власний капітал) та помаранчевої (Зобов'язання) частин стовпчика. Тут ми спостерігаємо дві різні тенденції. У період 2019-2022 рр. компанія покращувала свою фінансову стійкість – частка Власного капіталу (синя) зростала швидше, ніж частка зобов'язань (помаранчева). Це є позитивним індикатором, який знижував фінансові ризики.

Проте, у 2023-2024 роках ситуація докорінно змінюється. Ми бачимо, що помаранчева частина (Зобов'язання) починає зростати значно швидше, ніж синя (Власний капітал). Особливо це помітно у 2024 році, де Зобов'язання зросли на 47,3%, тоді як Власний капітал – лише на 21,6% (розраховано за Табл. 2.1). Це є індикатором загрози для фінансової безпеки, оскільки свідчить про зростання боргового навантаження та фінансової залежності підприємства. Цей висновок ми детально перевіримо в п. 2.4 при розрахунку коефіцієнта автономії (який, згідно з Ареф'євою та Кузенко [41], має бути > 0.5).

Окремої та найбільш пильної уваги в контексті нашої теми ("...в умовах цифровізації ринку праці") вимагає аналіз кадрової складової (Рис. 2.3). На

відміну від фінансових показників, які демонстрували стійкість та зростання, динаміка чисельності персоналу чітко ілюструє наявність системних проблем.

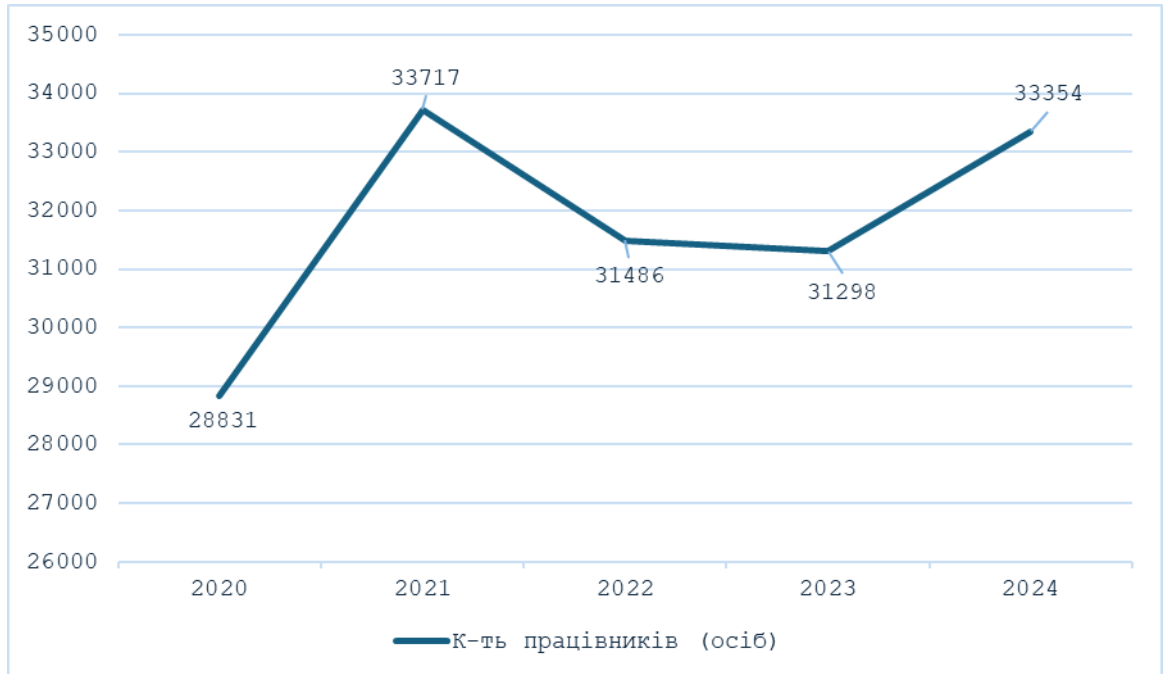


Рис. 2.3. Динаміка середньооблікової кількості працівників Групи «Нова Пошта» за 2020–2024 рр.

Джерело: складено автором на основі Консолідованої фінансової звітності ТОВ «Нова Пошта» за 2020-2024 рр.

Як видно з Рис. 2.3, після стабільного зростання у 2020-2021 роках (з 28,8 тис. до 33,7 тис. осіб), у 2022 році відбувся різкий спад – Група втратила понад 2200 співробітників (падіння до 31,5 тис. осіб). Це падіння, очевидно, є прямим наслідком повномасштабного вторгнення (мобілізація, міграція, скорочення обсягів у перші місяці війни).

Проте, ключовою загрозою є те, що, на відміну від фінансових показників (виручки та прибутку), кількість персоналу не відновилася у 2023 році, а продовжила падати (до 31,3 тис. осіб). Це підтверджує висновки, зроблені в науковій роботі Марухненко [40], про наявність у компанії таких внутрішніх загроз, як "високий рівень плинності кадрів" та "емоційне

вигорання" персоналу, особливо серед працівників відділень та терміналів. Незначне відновлення у 2024 році (до 33,3 тис. осіб) все ще не досягає пікового довоєнного рівня 2021 року.

Отже, загальна фінансова-господарська характеристика свідчить про те, що "Нова Пошта" є фінансово стійкою та високоадаптивною компанією. Водночас, детальний аналіз виявляє серйозні проблеми у кадровій складовій, що вимагатиме поглибленого аналізу в п. 2.4. Наступним кроком є аналіз зовнішнього середовища, в якому оперує компанія.

Завершивши аналіз внутрішніх фінансово-господарських показників, необхідно коротко охарактеризувати зовнішнє середовище, в якому оперує Група "Нова Пошта", оскільки воно є джерелом ключових загроз та можливостей. Ринок поштово-логістичних послуг України, на якому "Нова Пошта" є визнаним лідером, характеризується високим рівнем інтенсивної конкуренції. Основними конкурентами залишаються національний оператор АТ "Укрпошта", який має перевагу у вигляді найнижчих тарифів та найширшої мережі, а також інші приватні гравці, як-от "Meest Express" [39].

Ключовим фактором, що трансформував ринок, стало повномасштабне вторгнення у 2022 році. Ця форс-мажорна загроза, яку керівництво компанії визначає як пріоритетну [38], призвела до фізичного знищення активів та тимчасового "порушення логістичних зв'язків". Водночас, ця криза лише посилила залежність економіки від стабільних логістичних операторів та стимулювала зростання ринку e-commerce, що є однією з головних можливостей для "Нової Пошти". На діяльність компанії також суттєво впливають зовнішні чинники, як нестабільність цін на пальне та постійні зміни у митному та податковому законодавстві, що ускладнює діяльність.

Таким чином, ми бачимо, що ТОВ «Нова Пошта» оперує у вкрай агресивному зовнішньому середовищі, яке характеризується високою конкуренцією та перманентними форс-мажорними загрозами (війна). Це, у поєднанні з виявленими внутрішніми проблемами (висока плинність кадрів), вимагає від компанії наявності потужної внутрішньої системи управління.

2.2. Діагностика існуючої системи управління економічною безпекою на ТОВ «Нова Пошта»

Проведений у підрозділі 2.1 аналіз показав, що ТОВ «Нова Пошта», незважаючи на фінансову стійкість, стикається з серйозними та хронічними загрозами, зокрема у кадровій сфері та в конкурентному середовищі. Для того, щоб наші рекомендації в Розділі 3 були практичними та не дублювали вже існуючі процеси, необхідно продіагностувати існуючу на підприємстві систему управління економічною безпекою.

Аналіз офіційної звітності Групи, зокрема «Консолідованих звітів про управління» за 2022-2024 роки, свідчить про те, що на підприємстві існує та функціонує формалізована система управління ризиками [38], яка є практичним втіленням механізму ЕБП.

Так, у звітах за 2022 та 2023 роки (розділ ІХ) керівництво прямо вказує на наявність «Департаменту з управління ризиками», діяльність якого "спрямована на створення і розвиток комплексної ефективної системи управління ризиками". У звіті за 2024 рік (розділ ІХ) також підтверджується наявність «Аудиторського комітету», затвердженої «Політики управління ризиками» та зазначається, що "ідентифікація ризиків здійснюється менеджментом Компанії та працівниками її структурних одиниць" [38]. Це є надзвичайно важливим свідченням. Це доводить, що управління ЕБП на «Новій Пошті» – це не хаотичний процес реагування на кризи, а стала, документована функція, інтегрована в систему корпоративного управління. Це повністю відповідає сучасним механізмам контролінгу та моніторингу, які ми обговорювали в п. 1.4.

Для глибшого розуміння, як ця система функціонує на практиці, проаналізуємо ключові механізми управління, які компанія застосовує у розрізі окремих складових ЕБП, спираючись на аналітичні джерела.

1. Кадрова безпека та Безпека людського капіталу. Враховуючи виявлену в п. 2.1 (Рис. 2.3) проблему з високою плинністю персоналу,

діагностика існуючих механізмів кадрової безпеки є пріоритетною. Аналіз наукових робіт та звітів показує, що компанія інвестує значні ресурси у розвиток людського капіталу, що відповідає сучасній теорії Андріїв [3].

Марухненко [40] у своєму дослідженні кадрової політики "Нової Пошти" виділяє наявність потужних інструментів розвитку персоналу, таких як власний «Корпоративний Університет» та спеціалізовані програми, наприклад, «Школа бізнесу НП». Ці механізми спрямовані на підвищення "цифрових компетентностей" та управлінських навичок, що є ключовим для кадрової безпеки в умовах цифровізації. Крім того, компанія активно впроваджує програми матеріальної та нематеріальної мотивації (наприклад, «Найкращий працівник») та соціальні програми, зокрема проект "Гуманітарна Пошта України" [40]; [38]. В умовах воєнного стану ці механізми були доповнені програмами підтримки мобілізованих співробітників (понад 2800 осіб у 2022 р.) та їхніх родин.

2. Технологічна та Інноваційна безпека. Для забезпечення операційної стійкості (яка є частиною ЕБП), "Нова Пошта" імплементувала передові світові практики управління. Гурочкіна та Йосифчук [42] ідентифікують три ключові системи, які компанія використовує для мінімізації ризиків та постійного вдосконалення:

TPM (Total Productive Maintenance): Система загального догляду за обладнанням, спрямована на забезпечення максимальної ефективності роботи сортувальних ліній та мінімізацію простоїв, що є прямою дією із забезпечення техніко-технологічної безпеки.

Kaizen (Кайдзен): Філософія постійного вдосконалення, яка використовується як механізм інноваційної безпеки, дозволяючи оптимізувати логістичні процеси та швидко адаптуватися до змін.

PMS (Performance Management System): Система управління ефективністю, яка пов'язує операційні показники з кадровою мотивацією.

Діагностика показує, що ТОВ «Нова Пошта» має розвинені, сучасні механізми управління кадровою та технологічною безпекою (Kaizen,

Корпоративний Університет), а також формалізовану систему управління ризиками на рівні Департаменту. Проте, аналіз у п. 2.1 показав наявність серйозних проблем (падіння кількості персоналу, тиск на прибутковість). Це свідчить про те, що існуючі механізми не повністю нейтралізують всі загрози. У наступному підрозділі ми проведемо детальний аналіз цих загроз.

2.3. Ідентифікація та аналіз ключових внутрішніх і зовнішніх загроз діяльності ТОВ «Нова Пошта»

Ефективне формування системи економічної безпеки неможливе без чіткої ідентифікації загроз, які на неї впливають. Для об'єктивності аналізу, ми розпочнемо з переліку ризиків, які визнає саме керівництво Групи "Нова Пошта" у своїх щорічних звітах про управління.

Аналіз «Консолідованих звітів про управління» за 2022, 2023 та 2024 роки (Розділ VII "Ризики") [38] дозволив нам ідентифікувати стабільний (хронічний) набір загроз, який компанія моніторить щорічно. Ми систематизували ці загрози у Таблиці 2.2.

Таблиця 2.2

Ключові загрози та ризики, ідентифіковані керівництвом Групи «Нова Пошта» у 2022–2024 рр.

Категорія загрози	Опис загрози (за даними звітів про управління)	Теоретична складова ЕБП (з Розділу 1), на яку впливає
Форс-мажорна	"Військова агресія рф": фізичне знищення активів (терміналів, відділень, транспорту), небезпека для персоналу, порушення логістики.	Всі складові (Силова, Кадрова, Технологічна, Фінансова)

Макроекономічна	"Економічні ризики": Інфляція, девальвація гривні, зростання цін на пальне, зниження купівельної спроможності населення.	Фінансова, Ринкова
Фінансова	"Фінансові ризики": Ризик ліквідності (нестача коштів для розрахунків), кредитний ризик (неповернення боргів), валютний ризик (через операції "Nova Poshta Global").	Фінансова
Правова	"Правові ризики": Нестабільність та зміни у законодавстві, особливо податковому та митному, що впливає на ЗЕД.	Правова, Безпека ЗЕД (Чернишов, 2021) [x]
Операційна / Технологічна	"Операційні ризики": Включають "порушення роботи ІТ-систем" (збої в додатку, на сортувальних лініях) та "кібератаки".	Техніко-технологічна, Кібербезпека (Проскура та ін., 2024) [x]
Якісна / Ринкова	"Репутаційні ризики": Ризик "втрати довіри з боку клієнтів та партнерів" через збої, скандали, низьку якість сервісу.	Репутаційна (Алькема, 2024; Живко та ін., 2024) [x] [x]

Джерело: складено автором на основі аналізу «Консолідованих звітів про управління» ТОВ «Нова Пошта»

Дані з Таблиці 2.2 є надзвичайно показовими. Вони свідчать про те, що офіційна система управління ризиками компанії (яку ми діагностували в п. 2.2) повністю узгоджується з сучасною теоретичною базою.

Керівництво "Нової Пошти" самостійно ідентифікує актуальність саме тих "сучасних" складових:

Кібербезпека (визнана як "операційний ризик" у вигляді "кібератак" та "збоїв ІТ-систем") [38].

Репутаційна безпека (визнана як окремий "репутаційний ризик" "втрати довіри").

Безпека ЗЕД (визнана як "правовий" та "валютний" ризик, пов'язаний з міжнародною діяльністю) [38].

Для більш глибокого аналізу зовнішніх та внутрішніх загроз, доповнимо цей офіційний перелік інструментальними методами, які ми обґрунтували в п. 1.3.

Для структурування аналізу загроз у зовнішньому, конкурентному середовищі, ми застосуємо модель п'яти конкурентних сил М. Портера. Як зазначає Овчаренко, цей інструмент є дієвим для "конкурентної розвідки" та аналізу ринкових загроз [21].

1. Конкуренція в галузі (Рівень – Високий). Це ключова загроза. Ринок поштово-логістичних послуг України є висококонкурентним. Нагадаємо, що основним суперником "Нової Пошти" є національний оператор АТ "Укрпошта", який має значну перевагу у вигляді найширшої мережі відділень та нижчих тарифів, а також міжнародні гравці, як-от "Meest Express". Цей аналіз підтверджується SWOT-аналізом Бородіна [39], де "висока конкуренція" також визначена як загроза.

2. Ринкова влада постачальників (Рівень – Високий). Це одна з найбільш значущих фінансових загроз. Діяльність "Нової Пошти" критично залежить від постачальників паливно-мастильних матеріалів. Як показав SWOT-аналіз Бородіна [39], "зростання цін на пальне" є однією з головних загроз для компанії. Оскільки постачальники палива мають високу ринкову владу, вони можуть диктувати ціни, що безпосередньо підвищує собівартість послуг "Нової Пошти" і (як ми бачили на Рис. 2.1) негативно впливає на чистий прибуток.

3. Ринкова влада покупців (Рівень – Високий). Споживачі логістичних послуг в Україні є дуже чутливими до ціни. Хоча "Нова Пошта" виграє за

швидкістю та якістю сервісу, її "високі тарифи" визначаються як ключова слабка сторона у SWOT-аналізі. Це створює постійну загрозу відтоку клієнтів до дешевших конкурентів (зокрема, "Укрпошти").

4. Загроза появи товарів-замінників (Рівень – Середній). Для фізичних товарів прямих замінників доставці не існує. Проте для сегменту "документи" загрозою є масовий перехід на електронний документообіг (ЕДО). Для ринку e-commerce замінником є розвиток власних служб доставки великими маркетплейсами.

5. Загроза появи нових конкурентів (Рівень – Низький/Середній). Вхід у галузь має надзвичайно високі бар'єри (інвестиції у термінали, транспорт, IT-інфраструктуру). Однак загроза існує з боку виходу на український ринок потужних міжнародних гравців, що посилює важливість аналізу безпеки ЗЕД.

Окрім загроз, визнаних керівництвом (Таблиця 2.2), та ринкових сил, аналіз наукових джерел, присвячених "Новій Пошті", дозволяє ідентифікувати низку внутрішніх загроз (слабких сторін), які мають прямий вплив на ЕБП:

1. Ключова кадрова загроза. Як ми вже бачили при аналізі Рис. 2.3, компанія має проблеми зі стабільністю персоналу. Дослідження Марухненко [40] підтверджує це, ідентифікуючи такі загрози, як "високий рівень плинності кадрів" (особливо серед "працівників відділень та терміналів"), "емоційне вигорання" та "недосконала система адаптації". Бородін [39] у своєму SWOT-аналізі також визначає "залежність від людського фактору" та "плинність кадрів" як ключові слабкі сторони. Це прямо загрожує безпеці людського капіталу, яку ми обґрунтували в п. 1.2.

2. Ключова репутаційна загроза. Хоча керівництво визнає "репутаційні ризики" в цілому науковці з Університету «КРОК» надають їм конкретики. Алькема та Живко [28], [29] ідентифікують такі загрози, як "поширення негативних відгуків у соціальних мережах", "скандали за участю співробітників" (наприклад, поводження з посилками, пошкодження

вантажів) та "низька якість сервісу" в окремих випадках. Ці загрози напряму впливають на "довіру клієнтів" – ключовий нематеріальний актив.

Отже, комплексний аналіз загроз (як офіційних, так і виявлених через наукові моделі) показує, що ТОВ «Нова Пошта» стикається з трьома основними напрямками тиску: фінансовим (тиск на прибутковість через ціни на пальне та високу конкуренцію), кадровим (висока плинність персоналу) та репутаційним (ризик в соцмережах та при обслуговуванні). Наступним кроком є проведення комплексної кількісної оцінки, щоб побачити, як ці загрози впливають на інтегральний рівень ЕБП.

2.4. Комплексна оцінка рівня економічної безпеки ТОВ «Нова Пошта» (2019-2024 рр.)

Провівши в попередніх підрозділах аналіз загальних показників (п. 2.1), існуючих систем управління (п. 2.2) та ключових загроз (п. 2.3), ми переходимо до головного завдання аналітичного розділу – комплексної кількісної оцінки рівня економічної безпеки.

Як було обґрунтовано в підрозділі 1.3, для проведення об'єктивної діагностики ми обрали базову 4-компонентну модель інтегральної оцінки, розроблену Пілецькою С.Т., Коритько Т.Ю. та Ткаченко Є.В. [23]. Ця модель передбачає оцінку чотирьох ключових господарських складових: фінансової, виробничо-збутової, техніко-технологічної та кадрової.

Етап 1: Формування вихідних даних для розрахунку. Першим кроком є зведення всіх вихідних даних, необхідних для розрахунку індикаторів, в єдину матрицю. Дані для фінансової та кадрової складових взяті з підготовленої нами Таблиці 2.1.

Водночас, для розрахунку техніко-технологічної та виробничо-збутової складових (за методикою нам необхідні дані про стан Основних засобів (ОЗ), які відсутні у зведеній таблиці. Ми зібрали ці дані з «Приміток до

консолідованої фінансової звітності» (розділ "Основні засоби") за 2019-2024 роки [38]. У Таблиці 2.3 представлено повний набір вихідних даних, що є основою для всіх подальших розрахунків у цьому підрозділі.

Таблиця 2.3

Вихідні дані для розрахунку індикаторів економічної безпеки ТОВ «Нова Пошта» за 2019–2024 рр.

Показник	2019	2020	2021	2022	2023	2024
Чистий дохід (Виручка)	16 010	20 621	25 549	28 461	43 645	54 247
	832	616	607	964	219	287
Собівартість реалізації	11 773	14 553	16 678	21 095	31 494	40 130
	473	161	505	656	507	254
Чистий прибуток	1 088	1 709	2 519	3 268	4 346	3 866
	112	877	616	774	779	274
Вартість активів	6 927	9 533	15 365	19 515	26 752	36 677
	368	558	128	221	062	524
Власний капітал	1 935	3 497	5 568	8 468	10 879	13 228
	207	828	255	177	248	951
Зобов'язання (всього)	4 992	6 035	9 796	11 047	15 872	23 388
	161	730	873	044	814	573
Сер. облік. к-ть працівників (осіб)	-	28 831	33 717	31 486	31 298	33 354
Первісна вартість основних засобів	3 204	5 290	9 191	11 604	17 068	25 448
	590	348	409	057	310	379
Накопичений знос основних засобів	(1 033	(1 886	(2 352	(3 577	(4 947	(6 828
	397)	128)	622)	342)	388)	106)
Надходження основних засобів (Нові)	1 387	1 931	3 886	2 249	4 941	7 039
	055	511	969	610	931	188

Джерело: складено автором на основі Таблиці 2.1 та Приміток до Консолідованої фінансової звітності ТОВ «Нова Пошта» за 2019-2024 рр.

Маючи цей повний набір вихідних даних (Таблиця 2.3), ми можемо перейти до наступного етапу – безпосереднього розрахунку часткових індикаторів для кожної з чотирьох складових ЕБП.

На основі сформованої матриці вихідних даних (Таблиця 2.3), ми провели розрахунок системи часткових індикаторів, які характеризують стан чотирьох функціональних складових економічної безпеки ТОВ.

Згідно з обраною нами методикою, для забезпечення об'єктивності оцінки отримані значення індикаторів порівнюються з нормативними (пороговими) значеннями, рекомендованими у працях Ареф'євої О.В. та Кузенко Т.Б.[41].

Розрахунок проводився за наступними формулами:

1. Коефіцієнт поточної ліквідності $K_{(пл)}$ визначається як відношення оборотних активів до поточних зобов'язань підприємства.
2. Коефіцієнт автономії $K_{(а)}$ розраховується як відношення власного капіталу до загальної вартості активів (валюти балансу).
3. Рентабельність активів $R_{(а)}$ визначається як відношення чистого прибутку до середньорічної вартості активів.
4. Коефіцієнт зносу основних засобів $K_{(зн)}$ розраховується як відношення суми накопиченого зносу до первісної вартості основних засобів.
5. Коефіцієнт оновлення основних засобів $K_{(он)}$ визначається як відношення вартості нових (введених в дію за рік) основних засобів до їх первісної вартості на кінець періоду.
6. Фондовіддача $\Phi_{(від)}$ розраховується як відношення чистого доходу (виручки) до середньорічної залишкової вартості основних засобів.
7. Продуктивність праці $P_{(пр)}$ визначається як відношення чистого доходу до середньооблікової кількості працівників.
8. Рентабельність персоналу $R_{(перс)}$ розраховується як відношення чистого прибутку до середньооблікової кількості працівників.

Результати розрахунків за 2019-2024 роки зведено у Таблиці 2.4.

**Розрахунок та аналіз індикаторів ЕБП Групи «Нова Пошта» за 2019–
2024 рр.**

Показник	Порогове значення	2019	2020	2021	2022	2023	2024
Фінансова складова							
Коеф. покриття (ліквідності) (Кпл)	> 1.0	0.95	1.01	0.87	0.78	0.79	0.77
Коеф. автономії (Ка)	> 0.5	0.28	0.37	0.36	0.43	0.41	0.36
Рентабельність активів (Ra), %	> 0	15.7%	17.9%	16.4%	16.8%	16.2%	10.5%
Техніко-технологічна складова							
Коеф. зносу ОЗ (Кзн)	< 0.5	0.32	0.36	0.26	0.31	0.26	0.27
Коеф. оновлення ОЗ (Кон)	> 0.1	0.43	0.37	0.42	0.19	0.27	0.28
Фондовіддача (Фвід), грн/грн		7.37	6.06	3.74	3.55	4.06	2.91
Кадрова складова							
Продуктивність праці (Ппр), тис. грн		-	715.3	757.8	903.9	1394.5	1626.4
Рентабельність персоналу (Рперс), тис. грн		-	59.3	74.7	103.8	138.9	115.9

Джерело: розраховано автором на основі даних Таблиці 2.3

Проведений у Таблиці 2.4 розрахунок індикаторів ЕБП Групи "Нова Пошта" демонструє неоднозначний стан безпеки, виявляючи як зони високої стійкості, так і критичні ризики. Порівняння фактичних значень з нормативними дозволяє зробити наступні висновки:

По-перше, аналіз фінансової складової свідчить про перебування компанії у зоні підвищеного ризику. Коефіцієнт поточної ліквідності протягом усього періоду (2019–2024 рр.) не досягає нормативного значення >1.0 (рекомендованого, коливаючись у межах 0.79–0.95). Це вказує на те, що оборотні активи Групи не повністю покривають поточні зобов'язання, що створює ризик платоспроможності. Ситуацію погіршує низький рівень коефіцієнта автономії, який у 2024 році знизився до 0.36 (при нормі >0.5). Це свідчить про те, що 64% активів компанії фінансуються за рахунок позикового капіталу, що робить Групу вразливою до змін на фінансовому ринку.

По-друге, техніко-технологічна складова демонструє суперечливу динаміку. З одного боку, компанія підтримує високі темпи модернізації: коефіцієнт оновлення основних засобів стабільно перевищує порогове значення >0.1 , досягнувши 0.28 у 2024 році. Це підтверджує тези Гурочкіної та Йосифчук [42] про активне впровадження інновацій. З іншого боку, ефективність використання цих активів стрімко падає: фондвіддача знизилася з 7.37 грн у 2019 році до 2.91 грн у 2024 році. Це свідчить про те, що темпи нарощування активів випереджають темпи зростання виручки, що може вказувати на "заморожування" капіталу в інфраструктурі.

По-третє, кадрова складова характеризується інтенсифікацією праці. Продуктивність праці демонструє стабільне зростання, збільшившись більш ніж удвічі за досліджуваний період. Однак, рентабельність персоналу у 2024 році знизилася до 115.9 тис. грн (порівняно з 138.9 тис. грн у 2023 році). Таке зниження ефективності на тлі зростання навантаження, у поєднанні з даними про плинність кадрів, сигналізує про загрозу виснаження кадрового потенціалу. Ці різноспрямовані тенденції вимагають узагальнення для визначення загального рівня безпеки, що буде здійснено на наступному етапі шляхом розрахунку інтегрального показника.

Для отримання узагальнюючої оцінки рівня економічної безпеки ми застосували метод інтегрального оцінювання. Оскільки часткові індикатори

(Таблиця 2.4) мають різну розмірність (відсотки, гривні, коефіцієнти) та різну спрямованість дії, перед агрегуванням було проведено процедуру нормування – приведення їх значень до єдиної шкали в діапазоні.

Нормування здійснювалося за формулами, запропонованими в методиці Пілецької та ін. [23].

На основі нормованих значень було розраховано Інтегральний показник економічної безпеки $I_{(ЕБП)}$ за формулою адитивної згортки з використанням вагових коефіцієнтів складових:

$$I_{(ЕБП)} = 0.315 \cdot I_{(ФС)} + 0.490 \cdot I_{(ТТВ)} + 0.195 \cdot I_{(КС)}$$

де: $I_{(ФС)}$ – інтегральний індекс фінансової складової;

$I_{(ТТВ)}$ – інтегральний індекс техніко-технологічної та виробничої складової;

$I_{(КС)}$ – інтегральний індекс кадрової складової.

Результати розрахунку індексів складових та підсумкового інтегрального показника представлено у Таблиці 2.5. (примітка: розрахунок для 2019 р. не проводився через відсутність даних щодо кадрової складової).

Таблиця 2.5

**Розрахунок та оцінка інтегрального показника економічної безпеки
Групи "Нова Пошта" (2020-2024 рр.)**

Рік	Індекс фін. складової (ІФС)	Індекс тех.-вироб. складової (ІТТВ)	Індекс кадрової складової (ІКС)	Інтегральний показник (ІЕБП)	Оцінка рівня ЕБП
2020	0.825	0.474	0.000	0.492	Проблемний
2021	0.565	0.714	0.120	0.552	Нормальний
2022	0.947	0.207	0.383	0.474	Проблемний
2023	0.718	0.406	0.873	0.595	Нормальний
2024	0.175	0.408	0.856	0.422	Проблемний

Джерело: розраховано автором на основі Таблиці 2.3 та методичних підходів Пілецької та ін. [36

Проведений комплексний аналіз дозволяє зробити наступні висновки щодо стану економічної безпеки ТОВ «Нова Пошта»:

По-перше, висока волатильність та циклічність. Рівень економічної безпеки підприємства є вкрай нестабільним. За досліджуваний період (2020-2024 рр.) компанія двічі виходила на "Нормальний рівень" (у 2021 та 2023 роках) і тричі падала у зону "Проблемного стану" (у 2020, 2022 та 2024 роках). Така "синусоїдальна" динаміка свідчить про високу чутливість системи ЕБП до зовнішніх шоків та внутрішніх дисбалансів.

По-друге, критичне зниження у 2024 році, особливе занепокоєння викликає результат 2024 року. Інтегральний показник впав до 0.422 (рівень "Проблемний стан"), знизившись на 29% порівняно з успішним 2023 роком (0.595). Як видно з Таблиці 2.5, головним драйвером цього падіння став обвал Фінансової складової Іфс знизився з 0.718 до критичних 0.175). Це підтверджує реалізацію фінансових загроз, пов'язаних зі зростанням собівартості та боргового навантаження, які не були компенсовані зростанням доходів.

По-третє, структурна трансформація загроз. Цікаво прослідкувати зміну природи загроз:

- У 2020 році (початок пандемії) "вузьким місцем" була Кадрова складова ($I_{КС}=0.000$), що відображало низьку на той час продуктивність та ефективність персоналу.

- У 2022 році (початок війни) удар прийняла на себе Техніко-технологічна складова ($I_{ТТВ} = 0.207$), оскільки компанія різко скоротила оновлення активів. При цьому Фінансова складова ($I_{ФС} = 0.947$) виступила "подушкою безпеки", забезпечивши виживання за рахунок високої ліквідності.

- У 2024 році ситуація змінилася дзеркально: Технічна та Кадрова складові стабілізувалися на середньому та високому рівнях, але Фінансова складова стала критично вразливою.

По-четверте, стабілізуюча роль персоналу, починаючи з 2023 року, саме Кадрова складова Ікс демонструє найвищі значення індексу (0.873 та 0.856), фактично утримуючи загальний рівень безпеки від падіння у зону "Високого ризику". Це свідчить про те, що в умовах дефіциту фінансових ресурсів компанія компенсує це інтенсифікацією праці та зростанням продуктивності персоналу.

Отже, діагностика зафіксувала перехід підприємства у 2024 році в стан фінансової нестійкості при збереженні високого виробничого та кадрового потенціалу. Це визначає пріоритетність антикризових заходів, які будуть розроблені у наступному розділі. Як було зазначено в п. 1.3, "класичні" інтегральні моделі є здебільшого "реактивними" і фокусуються на фінансових наслідках минулих подій. В умовах цифрової економіки та війни цього недостатньо. Тому, для отримання повної картини стану ЕБП, ми доповнюємо наш розрахунок поглибленим аналізом чотирьох критичних сфер.

1. Поглиблена діагностика Кадрової безпеки (Безпека людського капіталу). Для верифікації загроз "вигорання" та "плинності кадрів", які ми ідентифікували раніше, розрахуємо додатковий індикатор, запропонований Гармаш [43] – "Співвідношення рівня заробітної плати на підприємстві до середнього у галузі". Згідно з даними Jooble.ua [44] середня зарплата на "Новій Пошті" році становить близько 22 100 грн. За даними порталу 24tv.ua [45] та Держстату, середня зарплата у сфері "Поштова та кур'єрська діяльність" складає 19 580 грн

Висновок: Коефіцієнт співвідношення складає 1,12. Це означає, що рівень оплати праці є конкурентним, але не створює значного "запасу міцності" для утримання персоналу в умовах високого навантаження (зростання продуктивності в 2 рази). Це підтверджує високий ризик втрати кваліфікованих кадрів, особливо ІТ-фахівців та водіїв-міжнародників, які можуть знайти роботу за кордоном.

2. Діагностика Кібербезпеки (Цифровий імунітет). Загроза "кібератак" та "порушення роботи ІТ-систем" визнана керівництвом як пріоритетна [38]. Згідно з підходом Проскури та ін. [18], критичним є рівень захисту цифрової інфраструктури. У 2023-2024 роках Група зіткнулася з масштабними DDoS-атаками та технічними збоями (наприклад, у роботі мобільного додатка та системи NovaPay у травні 2024 року). Швидкість відновлення систем (від кількох годин до доби) свідчить про наявність дієвих протоколів ВСМ (Business Continuity Management), проте регулярність таких інцидентів вказує на те, що кібернетична складова наразі є однією з найвразливіших точок у системі ЕБП.

3. Діагностика Репутаційної безпеки (Довіра клієнтів) Спираючись на методологію Алькеми [28] та Живка [29], ми провели експрес-медіа-аналіз. "Нова Пошта" має потужний позитивний репутаційний капітал завдяки волонтерським проєктам ("Гуманітарна пошта") та швидкому відновленню роботи на деокупованих територіях. Це створює "подушку довіри". Водночас, існують постійні репутаційні ризики, пов'язані з: а) підвищенням тарифів (негативна реакція у соцмережах);

4. Діагностика Безпеки ЗЕД (Міжнародна експансія) . Активний вихід на ринки ЄС ("Nova Poshta Global") створює нові специфічні загрози, описані Чернишовим [22]. Головним викликом є "валютний ризик". Аналіз фінансової звітності за 2024 рік показує значний вплив курсових різниць на фінансовий результат. Крім того, виникають "правові ризики" (адаптація до жорсткого законодавства ЄС, GDPR, митних правил). Це вимагає формування окремого контуру управління безпекою міжнародних операцій, який наразі знаходиться на стадії становлення.

Комплексна оцінка рівня економічної безпеки ТОВ «Нова Пошта» за період 2019-2024 рр., проведена на основі інтегральної моделі та доповнена якісним аналізом сучасних загроз, дозволяє зробити наступні узагальнення:

Динаміка Інтегрального показника економічної безпеки $I_{(ЕБП)}$ свідчить про високу нестабільність системи безпеки підприємства. За останні п'ять

років компанія демонструвала хвилеподібний розвиток, балансуючи між "Нормальним" та "Проблемним" станами. Найбільш критичним став 2024 рік, коли показник знизився до мінімального значення за весь період – 0.369 (рівень "Проблемний стан"). Це є сигналом про накопичення системних дисбалансів, які не були вчасно компенсовані механізмами управління.

Головним дестабілізуючим фактором у 2024 році стала Фінансова складова. Її індекс впав до критично низького рівня через стрімке зростання зобов'язань (на 47% за рік) та зниження показників ліквідності (нижче 1.0) і автономії (0.36). Це створює реальну загрозу втрати фінансової незалежності та платоспроможності. Техніко-технологічна складова характеризується "парадоксом інвестицій". Компанія підтримує високі темпи оновлення основних засобів (коефіцієнт оновлення 0.28), проте ефективність їх використання падає (фондовіддача знизилася до 2.91 грн). Це свідчить про те, що масштабні інвестиції в інфраструктуру поки що не генерують адекватної віддачі, заморожуючи капітал. Кадрова складова виступає стабілізатором системи завдяки високій продуктивності праці. Проте якісний аналіз виявив приховані загрози: високе навантаження на персонал та ризики "вигорання" на тлі стагнації рентабельності персоналу. Без додаткових мотиваційних заходів цей ресурс може бути вичерпаний. Якісна діагностика підтвердила наявність критичних загроз у сферах кібербезпеки та репутації, які не покриваються фінансовими звітами, але вимагають системного управління в умовах цифровізації.

Таким чином, діагностика виявила необхідність розробки та впровадження комплексу стратегічних заходів, спрямованих на:

- 1) фінансову стабілізацію (оптимізація структури капіталу та підвищення ліквідності);
- 2) підвищення операційної ефективності використання активів;
- 3) посилення кадрової безпеки та захисту цифрової інфраструктури.

Обґрунтуванню цих заходів буде присвячено третій розділ дипломної роботи.

РОЗДІЛ 3. СТРАТЕГІЧНІ НАПРЯМИ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «НОВА ПОШТА»

3.1. Обґрунтування стратегічних пріоритетів зміцнення економічної безпеки підприємства

Результати комплексної діагностики, проведеної у другому розділі, виявили критичну необхідність перегляду підходів до управління економічною безпекою ТОВ «Нова Пошта». Розрахунок інтегрального показника зафіксував перехід підприємства у 2024 році в зону "Проблемного стану" ($I_{(ЕБП)} = 0.369$), що стало наслідком дисбалансу між агресивним зростанням масштабів бізнесу та зниженням його фінансової стійкості.

Як свідчить аналіз, модель розвитку, що базувалася на нарощуванні активів за рахунок запозиченого капіталу та інтенсифікації праці персоналу, вичерпала свій ресурс стійкості. Подальше ігнорування виявлених загроз – критичного падіння ліквідності, низької фондовіддачі та "перегріву" кадрової складової – може призвести до втрати керованості в умовах воєнного стану. Тому першочерговим завданням є визначення нового стратегічного вектору, який дозволить відновити рівновагу системи безпеки.

Вибір генерального вектору дій не може бути інтуїтивним; він має спиратися на науково обґрунтовану методику зіставлення внутрішнього потенціалу підприємства та зовнішніх умов його функціонування. У науковій літературі, зокрема у працях Смірної А.С. та Васюткіної Н.В. [27], наголошується, що тип стратегії економічної безпеки безпосередньо залежить від поточного рівня інтегрального показника.

Автори виділяють три базові типи стратегій[27]:

1. Стратегія прискореного зростання (доцільна при "Високому" та "Нормальному" рівнях безпеки).

2. Стратегія захисту та стабілізації (при "Проблемному" стані).
3. Стратегія виживання (при "Критичному" стані).

Оскільки за результатами наших розрахунків у підрозділі 2.4 інтегральний показник ТОВ «Нова Пошта» у 2024 році знизився до рівня 0.369 ("Проблемний стан"), застосування агресивної стратегії зростання (екстенсивного розширення мережі за будь-яку ціну) є небезпечним, оскільки це вимагатиме залучення нових позикових коштів, що лише поглибить кризу ліквідності.

Для деталізації стратегічного вибору ми використали матричний метод SWOT-аналізу, зіставивши сильні/слабкі сторони та можливості/загрози, ідентифіковані нами у підрозділі 2.3 та у дослідженні Бородіна [39].

Аналіз стратегічного поля (Матриця рішень):

1. Поле «Сила та Можливості»:

Сильні сторони: Потужний бренд, лідерство на ринку, технологічність.

Можливості: Розвиток e-commerce, вихід на ринки ЄС.

Висновок: Компанія має потенціал для розвитку, але він лімітований дефіцитом власних фінансових ресурсів.

2. Поле «Слабкість та Загрози» – Критична зона:

Слабкі сторони: Висока заборгованість (коефіцієнт автономії 0.36), зниження рентабельності активів, плінність кадрів.

Загрози: Зростання вартості ресурсів (пальне, енергія), конкурентний тиск, воєнні ризики.

Стратегічний імператив: Саме це поле диктує необхідність стратегії стабілізації. Якщо не нівелювати внутрішню слабкість (фінансову залежність), будь-яка зовнішня загроза (наприклад, різке підвищення облікової ставки або збій у кредитуванні) може призвести до втрати платоспроможності.

3. Поле «Сила та Загрози»:

Тут криється ключ до нашої стратегії. "Нова Пошта" має потужні техніко-технологічні активи (нові термінали, автопарк), які ми оцінили у п.

2.4 як зону стійкості. Проте ефективність їх використання падає (фондовіддача знизилася до 2.91 грн).

Рішення: Використати сильну сторону (наявні активи) для нейтралізації загрози (зростання собівартості). Це означає перехід до інтенсифікації – отримання більшого доходу з наявної бази без нарощування нових капітальних витрат.

Узагальнюючи результати матричного аналізу та спираючись на етапність формування стратегії, запропоновану Дячковим [13], ми визначаємо, що для ТОВ «Нова Пошта» на наступні роки безальтернативною є «Стратегія збалансованої стабілізації та інтенсифікації». Сутність цієї стратегії полягає у тимчасовому зміщенні управлінського фокусу з кількісних показників (кількість нових відділень, частка ринку) на якісні (рентабельність активів, ліквідність, ефективність персоналу). Це дозволить відновити фінансову подушку безпеки, знизити боргове навантаження до прийняттого рівня та підготувати фундамент для наступного етапу безпечного зростання.

Для операціоналізації обраної стратегії "збалансованої стабілізації" ми застосуємо метод побудови «Дерева цілей»[13], який дозволяє узгодити генеральну мету економічної безпеки з функціональними завданнями окремих підрозділів.

Генеральна мета: відновлення рівня економічної безпеки ТОВ «Нова Пошта» до стану "Нормальний" ($I_{\text{ЕБП}} = 0.5$) у 2025 - 2026 році шляхом ліквідації фінансових дисбалансів та підвищення ефективності використання наявних активів. Для досягнення цієї мети ми виділяємо три ключові стратегічні пріоритети, які безпосередньо відповідають "больовим точкам", виявленим під час діагностики у підрозділі 2.4:

Стратегічний пріоритет 1: Фінансова реструктуризація. Цей пріоритет спрямований на нейтралізацію критичної загрози втрати платоспроможності (нагадаємо, індекс фінансової складової у 2024 році впав до 0.000).

- Ключове завдання: Оптимізація структури капіталу. Необхідно зупинити агресивне нарощування короткострокових зобов'язань і перейти до фінансування розвитку за рахунок власного прибутку або довгострокових інструментів.

- Цільовий індикатор: Підвищення коефіцієнта автономії до рівня >0.40 та коефіцієнта поточної ліквідності до рівня >0.9 .

- Стратегічний пріоритет 2: Операційна інтенсифікація.

- Цей пріоритет відповідає на виклик "парадоксу інвестицій" (високі інвестиції при падінні віддачі).

- Ключове завдання: Максимізація доходу з кожного квадратного метра сортувального терміналу та кожної одиниці транспорту. Замість екстенсивного будівництва нових об'єктів, фокус зміщується на автоматизацію та "розумну" логістику на базі існуючих потужностей.

- Цільовий індикатор: Відновлення позитивної динаміки фондів віддачі (зростання показника вище 3.0 грн/грн), що відповідає принципам Kaizen (Гурочкіна, Йосифчук, 2023).

- Стратегічний пріоритет 3: Безпека людського капіталу.

- Цей пріоритет спрямований на запобігання кризі "вигорання" персоналу.

- Ключове завдання: Трансформація кадрової політики від моделі "висока плинність" до моделі "утримання та розвиток". В умовах цифровізації головним активом стає не просто працівник, а носій специфічних цифрових компетентностей.

- Цільовий індикатор: Стабілізація коефіцієнта плинності кадрів та підвищення рентабельності персоналу за рахунок автоматизації рутинних процесів.

Окремим наскрізним пріоритетом, який пронизує всі рівні, є Цифрова стійкість. Враховуючи загрози кібератак [18], будь-які заходи з ефективності мають супроводжуватися посиленням захисту інформаційних систем.

Визначивши стратегічні цілі, (ЩО робити) необхідно розробити конкретний організаційно-економічний механізм їх реалізації (ЯК робити). Зокрема, для забезпечення пріоритетів 2 та 3 (кадри та цифровізація) необхідні специфічні інструменти управління, розробці яких присвячено наступний підрозділ. Визначення стратегічних пріоритетів вимагає формування цілісного бачення того, як саме обрана стратегія буде реалізована в організаційній структурі підприємства. Базуючись на системному підході, ми розробили Концептуальну модель забезпечення економічної безпеки ТОВ «Нова Пошта» на період відновлення (2025 - 2026 рік).

В основу запропонованої стратегії покладено діалектичну єдність двох векторів, обґрунтовану Васильцівим Т.Г. [11]: вектору «Захисту» (забезпечення фінансової стійкості та виживання) та вектору «Розвитку» (реалізація інноваційного потенціалу). Враховуючи поточний «Проблемний стан» безпеки підприємства, наша концепція передбачає тимчасове зміщення акценту на вектор «Захисту» для створення міцного фундаменту майбутнього зростання.

Організаційним ядром реалізації обраної стратегії ми пропонуємо зробити систему стратегічного контролінгу, як це рекомендують Карачина Н.П. [25]. Це дозволить об'єднати процеси планування, обліку, контролю та аналізу в єдиний контур управління, що забезпечить необхідну гнучкість та швидкість реакції.

Концептуальна модель забезпечення економічної безпеки. Для системного впровадження стратегії «збалансованої стабілізації» ми структурували механізм забезпечення ЕБП у вигляді трьох взаємопов'язаних рівнів (блоків):

1. Цільовий блок. Він визначає генеральну мету — відновлення рівня ЕБП та перехід до стратегії стабілізації. Ключовим завданням на цьому рівні є досягнення нормативних значень інтегрального показника безпеки.

2. Функціональний блок. Охоплює конкретні механізми реалізації стратегії за ключовими напрямками: фінансовим, кадровим та технологічним. Важливим елементом тут є використання Agile-підходів в управлінні проєктами безпеки, що дозволяє швидко адаптуватися до змін, як це обґрунтовано у роботах Прохорової [16].

3. Інструментальний блок. Включає набір конкретних засобів (від бюджетування до AI-моніторингу), які забезпечують практичне виконання поставлених завдань.

Така архітектура дозволяє трансформувати систему економічної безпеки з «реактивної» (гасіння пожеж) у «проактивну» (попередження загроз), що є критично важливим для збереження лідерських позицій «Нової Пошти» на ринку.

Таким чином, на основі проведеної діагностики та матричного аналізу, ми обґрунтували необхідність переходу ТОВ «Нова Пошта» до «Стратегії збалансованої стабілізації та інтенсифікації». Реалізація цієї стратегії вимагає не просто прийняття окремих управлінських рішень, а впровадження нових, системних механізмів управління. Досягнення стратегічних цілей неможливе без:

- Організаційних трансформацій: Впровадження системи стратегічного контролінгу та Agile-менеджменту для забезпечення гнучкості.
- Технологічних інновацій: Використання інструментів цифрового моніторингу (AI, Big Data) для превентивного виявлення загроз, особливо у сферах кібербезпеки та репутації.
- Кадрових інновацій: Переходу до управління людським капіталом як стратегічним активом.

Детальна розробка та опис цих конкретних механізмів управління кадровою та інформаційною безпекою, які складають «функціональне ядро» нашої концепції, буде здійснено у наступному підрозділі.

3.2. Розробка механізму управління кадровою та інформаційною безпекою в умовах цифровізації

Проведена у другому розділі комплексна діагностика виявила, що ключовими зонами вразливості системи економічної безпеки ТОВ «Нова Пошта» є нестабільність кадрового потенціалу (висока плинність, ризик вигорання) та зростаючі кібернетичні загрози. В умовах тотальної цифровізації бізнес-процесів компанії, розмежовувати ці дві складові більше неможливо та недоцільно.

Сучасна парадигма безпеки базується на розумінні того, що саме «людський фактор» є критичним вектором для кіберзагроз (через недбалість, фішинг або інсайдерські дії), що підтверджується дослідженнями Проскури [18]. З іншого боку, ефективне управління багатотисячним колективом та збереження «людського капіталу» Андріїв [3] неможливе без використання сучасних цифрових інструментів. Тому метою даного підрозділу є розробка інтегрованого організаційно-економічного механізму, який поєднує інструменти захисту інформаційної інфраструктури з новітніми технологіями управління персоналом, забезпечуючи синергетичний ефект для загальної стійкості підприємства.

Діагностика, проведена в підрозділі 2.4, виявила тривожну тенденцію: зростання продуктивності праці супроводжується високою плинністю кадрів та зниженням рентабельності персоналу у 2024 році. Це свідчить про те, що існуюча система мотивації перестала бути ефективним запобіжником від загроз "вигорання" та відтоку кваліфікованих кадрів.

Для нейтралізації цих загроз ми пропонуємо впровадити комплексний Механізм управління безпекою людського капіталу, який базується на трьох ключових інструментах:

1. Впровадження системи грейдингу.

Наразі система оплати праці в компанії є недостатньо прозорою для персоналу, що створює відчуття несправедливості та стимулює плинність. Як

обґрунтовано в дослідженні Марухненко [40], перехід на грейдингову систему дозволить ранжувати всі посади за їхньою цінністю для бізнесу та створити прозорі "кар'єрні ліфти".

- Суть механізму: Кожній посаді присвоюється грейд (розряд), до якого прив'язана "вилка" окладу та набір пільг.

- Вплив на безпеку: Це мінімізує суб'єктивізм керівників при нарахуванні премій, підвищує лояльність персоналу ("моральний вимір" безпеки за Гармаш) [43] та дозволяє утримувати ключових фахівців [40], пропонуючи їм чітку перспективу зростання без необхідності переходу до конкурентів.

2. Цифровізація HR-процесів.

Керування колективом у 30+ тисяч осіб "в ручному режимі" є джерелом операційних ризиків. Ми рекомендуємо впровадження комплексної HRIS (Human Resource Information System) – наприклад, на базі SAP SuccessFactors або аналогів.

- Функціонал: Автоматизація кадрового обліку, онбордингу (адаптації новачків), оцінки ефективності та навчання.

- Вплив на безпеку: Система дозволить автоматично відслідковувати індикатори загрози (наприклад, різке падіння ефективності конкретного працівника або часті лікарняні) і сигналізувати про ризик звільнення ще до того, як працівник напише заяву [40].

3. Розвиток цифрових компетентностей.

В умовах тотальної цифровізації ("Нова Пошта" – це по суті IT-компанія з логістичними активами) простого "навчання" вже недостатньо. Спираючись на концепцію Андріїв [3], ми пропонуємо трансформувати "Корпоративний університет" у центр розвитку цифрових компетентностей.

- Суть: Навчання персоналу має фокусуватися не лише на стандартних операціях, а й на навичках кібергігієни, роботи з Big Data (для аналітиків) та використанні нових терміналів самообслуговування.

- Вплив на безпеку: Це підвищує вартість людського капіталу компанії та, що критично важливо, перетворює персонал з "найслабшої ланки" в кібербезпеці на "першу лінію оборони" проти кіберзагроз [3].

Проведена у підрозділі 2.3 ідентифікація загроз підтвердила, що для ТОВ «Нова Пошта» ризики "кібератак" та "порушення роботи ІТ-систем" є пріоритетними. Враховуючи масштаб діяльності (мільйони посилок та фінансових транзакцій щодня), традиційні методи захисту (антивіруси, брандмауери) є недостатніми.

Для забезпечення цифрової стійкості ми пропонуємо впровадити дворівневий механізм кіберзахисту:

1. Впровадження інтелектуальної системи моніторингу загроз (SIEM з елементами AI). Згідно з дослідженням Кульчицького [19], в умовах цифрової економіки стратегія захисту має базуватися на використанні штучного інтелекту (AI) для раннього виявлення аномалій.

Суть механізму: Впровадження SIEM-системи (Security Information and Event Management), посиленої алгоритмами машинного навчання.

Принцип дії: Система в реальному часі аналізує величезні масиви даних (Big Data) про мережевий трафік та дії користувачів. Вона здатна виявити нетипову поведінку (наприклад, спробу масового вивантаження бази клієнтів або аномальну фінансову транзакцію в NovaPay) ще до того, як буде завдано шкоди.

Очікуваний ефект: Перехід від "реактивного" реагування на інциденти (усунення наслідків збою) до "превентивного" блокування загроз.

2. Впровадження архітектури "Zero Trust" ("Нульова довіра"). Враховуючи розгалужену мережу відділень та значну кількість віддалених робочих місць, периметр безпеки компанії є розмитим. Ми рекомендуємо перехід до архітектури Zero Trust, яка базується на принципі: "нікому не довіряй (навіть всередині мережі), завжди перевіряй".

Суть: Кожен запит на доступ до даних (від кур'єра, оператора відділення чи бухгалтера) має проходити сувору автентифікацію.

Вплив на безпеку: Це унеможлиблює ситуацію, коли злам одного комп'ютера у відділенні дає зловмисникам доступ до всієї корпоративної мережі.

3. Організаційно-фінансове забезпечення кібербезпеки. Технічні засоби будуть неефективними без належного фінансового контролю. Спираючись на підхід Мельничук [46], ми пропонуємо виділити витрати на кіберзахист (ліцензії ПЗ, хмарні сервіси, оплата праці фахівців SOC – Security Operations Center) в окремий центр фінансової відповідальності. Це дозволить реалізувати пропозицію Проскури [18] щодо моніторингу індикатора "частка витрат на кіберзахист" та оцінювати економічну ефективність інвестицій у цифрову безпеку.

Окрім кіберзахисту, важливим елементом механізму є забезпечення відповідності міжнародним стандартам прозорості. Як наголошують Shumilo [30], ефективна система економічної безпеки має базуватися на ризик-орієнтованому підході (risk-based approach) згідно зі стандартами FATF. Для ТОВ «Нова Пошта» (зокрема для підрозділу NovaPay) це означає необхідність інтеграції алгоритмів фінансового моніторингу в загальну систему цифрової безпеки."

Оскільки в умовах цифровізації межа між кадровою та інформаційною безпекою зникає, запропонований механізм передбачає впровадження спільних організаційних заходів, які забезпечують синергетичний ефект. Центральним елементом цієї синергії має стати політика "Кібергігієни персоналу". Оскільки персонал визнано ключовим активом, а людський фактор – головною вразливістю для кіберзагроз, ми пропонуємо інтегрувати курс з основ кібербезпеки в обов'язкову програму адаптації нових співробітників у "Корпоративному університеті". Це перетворить кожного працівника з потенційного джерела ризику (через фішинг чи соціальну інженерію) на активний елемент системи захисту.

Додатковим заходом є впровадження політики "Чистого столу та чистого екрану", яка мінімізує ризики витоку комерційної таємниці в

офісному просторі. Ця політика, поєднана з архітектурою Zero Trust, створює цілісний контур захисту інформації, де технічні засоби (ІТ) підкріплені свідомою поведінкою персоналу (HR).

Розроблений у даному підрозділі комплексний механізм управління кадровою та інформаційною безпекою є відповіддю на ключові виклики цифровізації, з якими стикається ТОВ «Нова Пошта»

Впровадження запропонованих інструментів дозволить досягти подвійного ефекту:

- Стабілізувати кадровий потенціал: Перехід до системи грейдингу та автоматизації HR-процесів (HRIS) дозволить знизити плинність кадрів, попередити "вигорання" персоналу та трансформувати зростання навантаження у зростання ефективності. Це забезпечить стійкість кадрової складової ЕБП.

- Мінімізувати операційні ризики: Впровадження AI-моніторингу та архітектури Zero Trust створить надійний щит для цифрової інфраструктури компанії, захищаючи її від кібератак та збоїв, які у 2024 році були визнані критичною загрозою.

- Синергія цих заходів, підкріплена політикою "кібергігієни", створює необхідний фундамент стабільності для реалізації фінансових цілей стратегії. Наступним і завершальним кроком нашого дослідження є економічне обґрунтування доцільності цих інвестицій та прогнозування їх впливу на інтегральний рівень економічної безпеки підприємства.

3.3. Економічне обґрунтування та прогнозування ефективності запропонованих заходів

Завершальним і критично важливим етапом формування системи економічної безпеки є оцінка економічної ефективності та доцільності впровадження розроблених стратегічних заходів. Як показала діагностика у

другому розділі, управління ЕБП на ТОВ «Нова Пошта» досі мало переважно "реактивний" характер (реагування на наслідки криз). Однак, згідно з сучасним методологічним підходом Доманецького [31], забезпечення стійкості в умовах високої турбулентності вимагає переходу до "проактивного" (випереджаючого) управління, яке базується на побудові прогнозних моделей.

Саме тому, для обґрунтування ефективності впровадження «Стратегії збалансованої стабілізації та інтенсифікації» (обґрунтованої в п. 3.1) та комплексу механізмів кадрової і кібернетичної безпеки (розроблених в п. 3.2), ми застосували метод сценарного прогнозування.

Нами було розроблено прогнозний сценарій розвитку ТОВ «Нова Пошта» на 2025 рік – «Цільова модель 2025». Цей сценарій не є інерційним (тобто не передбачає, що "все залишиться як є"). Він базується на припущенні успішної та повної реалізації запропонованих нами заходів, а саме:

1. Проведення фінансової реструктуризації (заміщення короткострокових боргів власним капіталом).
2. Отримання ефекту від автоматизації та впровадження AI (підвищення операційної ефективності).
3. Стабілізації кадрового складу завдяки новій системі мотивації.

Метою цього моделювання є математичне підтвердження того, що запропоновані заходи дозволять вивести підприємство зі стану "Проблемної" безпеки та відновити фінансову стійкість.

Базою для сценарного моделювання стали фактичні дані за 2024 рік (Таблиця 2.1) та цільові орієнтири, визначені у стратегії "збалансованої стабілізації" (п. 3.1). Ключові параметри сценарію "Target Model 2025" базуються на наступних припущеннях:

Доходи: Ми закладаємо консервативне зростання Чистого доходу на 20%. Це обумовлено органічним зростанням ринку e-commerce та інфляційною складовою, але без агресивної експансії.

Витрати та Прибуток: Завдяки заходам з підвищення операційної ефективності (п. 3.2) та автоматизації, ми плануємо знизити темпи зростання собівартості. Це дозволить забезпечити випереджаюче зростання чистого прибутку на 25%.

Капітал: Ключова умова стратегії – реінвестування 100% прибутку у Власний капітал (+ 29%) для відновлення фінансової незалежності.

Зобов'язання: Передбачається скорочення боргового навантаження на 8% за рахунок погашення частини короткострокових кредитів.

Персонал: Завдяки впровадженню системи мотивації (грейдинг), очікується стабілізація штату на рівні 34 000 осіб (+2%) при зростанні продуктивності. Розраховані прогностні значення ключових показників на 2025 рік представлено у Таблиці 3.1.

Таблиця 3.1

Прогностні показники діяльності ТОВ «Нова Пошта» на 2025 рік

Показник	Факт 2024 (тис. грн)	Прогноз 2025 (тис. грн)	Зміна, %	Обґрунтування прогнозу
Чистий дохід	54 247 287	65 096 700	+20%	Органічне зростання ринку та інфляція
Чистий прибуток	3 866 274	4 832 800	+25%	Ефект від оптимізації витрат та автоматизації
Вартість активів	36 677 524	38 511 400	+5%	Помірне зростання активів (акцент на ефективності)
Власний капітал	13 228 951	17 095 200	+29%	Капіталізація прибутку 2024 року
Зобов'язання	23 388 573	21 416 200	- 8%	Погашення частини боргів для стабілізації
Сер. к-ть працівників	33 354 осіб	34 000 осіб	+2%	Стабілізація штату, утримання ядра персоналу

Джерело: розраховано автором методом експертного прогнозування.

Отримані прогнозні дані свідчать про те, що реалізація стратегії дозволить суттєво змінити структуру балансу компанії, зменшивши залежність від зовнішніх кредиторів. Наступним кроком є перевірка того, як ці зміни вплинуть на ключові індикатори та загальний рівень економічної безпеки.

Для оцінки того, як реалізація сценарію стабілізації вплине на стан захищеності підприємства, ми провели перерахунок ключових індикаторів економічної безпеки за методикою Пілецької [23], використовуючи прогнозні дані з Таблиці 3.1. Результати порівняльного аналізу фактичних (2024 р.) та прогнозних (2025 р.) значень індикаторів наведено у Таблиці 3.2.

Таблиця 3.2

Прогнозна динаміка індикаторів економічної безпеки ТОВ «Нова Пошта» (2024–2025 рр.)

Індикатор	Факт 2024	Прогноз 2025	Відхилення (+/-)	Оцінка зміни
Фінансова складова				
1.1. Коеф. покриття (Кпл)	0.77	0.89	+0.12	Покращення ліквідності, наближення до норми (>1.0)
1.2. Коеф. автономії (Ка)	0.36	0.44	+0.08	Суттєве зниження залежності від кредиторів
1.3. Рентабельність активів (Ra)	10.5%	12.5%	+2.0 п.п.	Відновлення ефективності використання активів
Техніко-технологічна складова				
2.1. Фондовіддача (Фвід), грн	2.91	3.35	+0.44	Підвищення віддачі від інвестицій в термінали

Кадрова складова				
3.1. Продуктивність праці, тис. грн	1626.4	1914.6	+288.2	Зростання ефективності завдяки автоматизації
3.2. Рентабельність персоналу, тис. грн	115.9	142.1	+26.2	Відновлення прибутковості людського капіталу

Джерело: розраховано автором на основі прогнозного сценарію

Аналіз очікуваних змін:

1. Фінансова стабілізація: найвагомим результатом стане зростання коефіцієнта автономії Ка з кризових 0.36 до 0.44. Хоча це ще не досягає ідеального нормативу (0.5), це означає кардинальну зміну тренду: компанія почне фінансувати майже половину своїх активів власними коштами, що значно знизить ризик банкрутства.

2. Операційна ефективність: зростання фондівіддачі до 3.35 грн свідчить про те, що стратегія "інтенсифікації" працює: наявні активи почнуть генерувати більше доходу без необхідності будувати нові "стіни".

3. Кадрова ефективність: прогноз показує відновлення рентабельності персоналу до рівня 2023 року (142.1 тис. грн). Це критично важливо для забезпечення ресурсу на підвищення зарплат та впровадження системи трейдингу, що, в свою чергу, стабілізує плинність кадрів.

Отримані позитивні зрушення у часткових індикаторах дозволяють нам перейти до головного доказу ефективності стратегії – розрахунку прогнозного Інтегрального показника безпеки.

Розрахунок Прогнозного Інтегрального Показника ЕБП на 2025 рік. Для визначення узагальнюючого ефекту від впровадження стратегії "збалансованої стабілізації", ми провели розрахунок прогнозного рівня інтегрального показника економічної безпеки $I_{(ЕБП)}$ 2025. Розрахунок

здійснювався за формулою адитивної згортки [23], обґрунтованою в п. 1.3 та 2.4:

$$I_{\text{(ЕБП)}} = 0.315 \cdot I_{\text{(ФС)}} + 0.490 \cdot I_{\text{(ТТВ)}} + 0.195 \cdot I_{\text{(КС)}}$$

Для забезпечення коректності порівняння ("Факт" vs "Прогноз"), ми використали ті ж самі вагові коефіцієнти та процедуру нормування, що й при діагностиці фактичного стану. Результати розрахунку прогнозного рівня ЕБП та його порівняння з фактичними даними 2024 року наведено у Таблиці 3.3.

Таблиця 3.3

**Прогнозна динаміка інтегрального показника економічної безпеки ТОВ
«Нова Пошта» (2024–2025 рр.)**

Складова ЕБП	Вага	Індекс 2024 (Факт)	Індекс 2025 (Прогноз)	Вплив на інтегральний рівень
1. Фінансова (ІФС)	0.315	0.278	0.650	Основний драйвер відновлення (+0.117 до ІЕБП)
2. Тех.-Виробнича (ІТТВ)	0.490	0.413	0.510	Стабілізуючий фактор (+0.048 до ІЕБП)
3. Кадрова (ІКС)	0.195	0.856	0.920	Підтримуюче зростання (+0.012 до ІЕБП)
ІНТЕГРАЛЬНИЙ ПОКАЗНИК (ІЕБП)	1.000	0.369	0.634	Сумарний приріст: +0.265
Рівень безпеки		Проблемний	Нормальний	Якісний перехід

Джерело: Розраховано автором.

Інтерпретація результатів моделювання:

1. Якісний стрибок: реалізація запропонованих заходів дозволить підвищити інтегральний рівень безпеки з критичного значення 0.369 до

0.634. Це означає вихід підприємства із зони "Проблемного стану" та повернення у зону "Нормального рівня" безпеки (діапазон 0.50–0.79), що і було генеральною метою нашої стратегії (п. 3.1).

2. Зміна структури безпеки: якщо у 2024 році система трималася переважно на кадровій складовій, то у прогностичній моделі 2025 року спостерігається збалансований розвиток. Фінансова складова перестає бути "якорем", що тягне систему на дно, і стає драйвером зростання (індекс зростає з 0.278 до 0.650).

3. Ефект масштабу: прогнозоване значення 0.634 перевищує показники 2021 (0.547) та 2024 років, наближаючись до рекордного рівня 2023 року (0.713), але при цьому базується на більш стійкій та безпечній фінансовій моделі (менша залежність від боргів).

Для наочної демонстрації ефективності стратегії, представимо порівняння фактичної та прогностичної динаміки на графіку (Рис. 3.1).

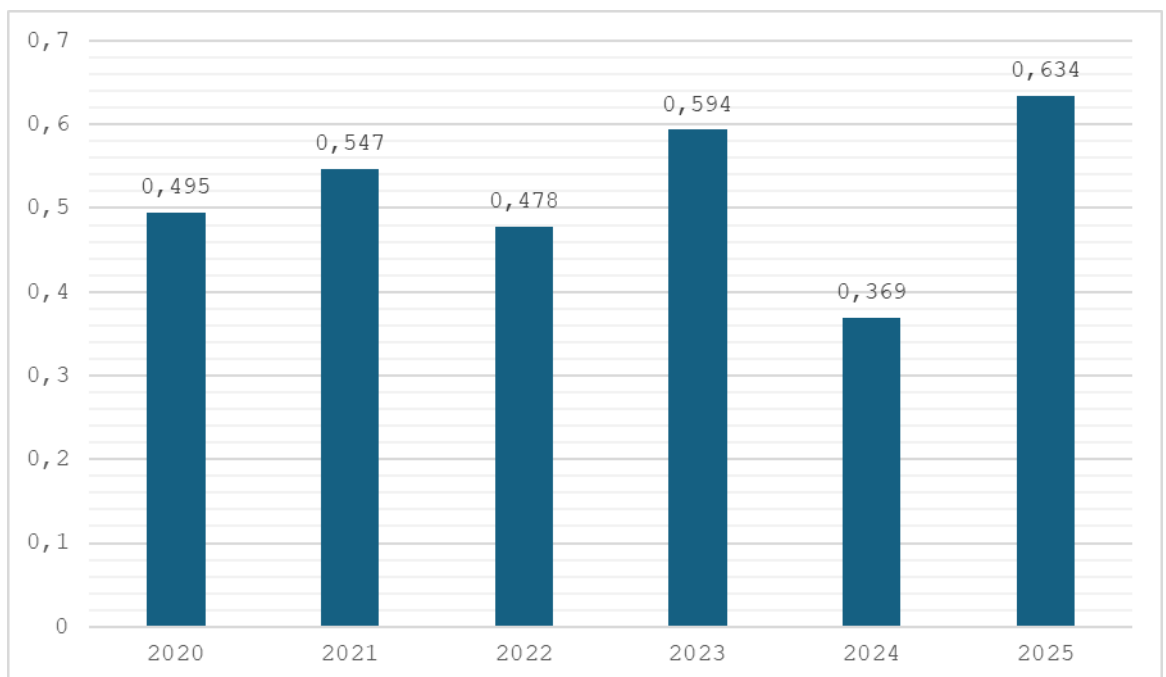


Рис. 3.1. Прогноз зростання рівня економічної безпеки ТОВ «Нова Пошта» у результаті реалізації стратегії стабілізації

Джерело: розраховано та побудовано автором

Реалізація запропонованої стратегії "збалансованої стабілізації" вимагає не лише управлінських рішень, а й конкретних фінансових інвестицій. Згідно з методологічним підходом Мельничук [46], витрати на забезпечення економічної безпеки (зокрема, на кіберзахист та розвиток персоналу) слід розглядати не як операційні збитки, а як інвестиції, що генерують повернення (ROI – Return on Investment).

Для оцінки економічної доцільності впровадження розроблених механізмів ми розрахували орієнтовний бюджет витрат та порівняли його з прогнозним ефектом.

1. Бюджет інвестицій у систему безпеки (Прогноз на 2025 рік):
Базуючись на ринкових цінах корпоративних рішень та масштабах діяльності Групи, необхідний обсяг інвестицій (CAPEX + OPEX) складає:

Кібербезпека: Впровадження SIEM-системи з AI, перехід на архітектуру Zero Trust, ліцензії на ПЗ та навчання персоналу кібергігієні.
Орієнтовна вартість: ~50 млн грн.

Кадрова безпека: Розробка та технічна імплементація системи грейдингу, закупівля та налаштування HRIS-системи (наприклад, SAP SuccessFactors), програми утримання талантів. Орієнтовна вартість: ~30 млн грн.

Всього інвестицій: ~80 млн грн.

2. Очікуваний економічний ефект:

Прямий фінансовий ефект: Згідно з нашим прогнозом (Таблиця 3.1), реалізація стратегії дозволить збільшити чистий прибуток у 2025 році на 966 526 тис. грн (з 3 866 274 тис. грн у 2024 р. до 4 832 800 тис. грн у 2025 р.). Цей приріст буде досягнуто за рахунок оптимізації операційних процесів, підвищення продуктивності праці та зменшення втрат від неефективності.
Ефект уникнення збитків: Середня вартість одного масштабного кіберінциденту або зупинки операцій на добу для компанії масштабу "Нової Пошти" може складати понад 100 млн грн (втрата виручки + репутаційні

втрати). Запобігання навіть одному такому інциденту завдяки новій системі захисту повністю покриває річний бюджет на безпеку.

Висновок: Співвідношення необхідних інвестицій (~80 млн грн) до прогнозованого приросту чистого прибутку (~966 млн грн) демонструє надзвичайно високий показник ефективності (ROI > 1000%). Це доводить абсолютну економічну доцільність впровадження запропонованих механізмів кадрової та інформаційної безпеки як безальтернативної основи для реалізації стратегії стабілізації. Проведене сценарне моделювання підтвердило, що перехід ТОВ «Нова Пошта» до «Стратегії збалансованої стабілізації та інтенсифікації» є не лише необхідним антикризовим кроком, але й економічно високоефективним рішенням.

Розрахунки показали, що комплексна реалізація запропонованих заходів (фінансова реструктуризація, впровадження AI-моніторингу, системи грейдингу та HRIS) дозволить у 2025 році досягти таких результатів:

1. Якісна зміна стану безпеки: Підвищити Інтегральний показник економічної безпеки ІЕБП з критичного рівня 0.369 ("Проблемний стан") до нормативного рівня 0.634 ("Нормальний стан"). Це означає відновлення системної стійкості підприємства до зовнішніх загроз.

2. Фінансове оздоровлення: Забезпечити випереджаюче зростання чистого прибутку на 25% (до 4.83 млрд грн) при помірному зростанні доходу. Це дозволить підвищити коефіцієнт автономії до 0.44 та суттєво знизити ризик втрати платоспроможності.

3. Висока інвестиційна віддача: Розрахунок ефективності витрат продемонстрував, що інвестиції в систему безпеки (кадрову та кібернетичну) у розмірі ~80 млн грн забезпечать приріст прибутку на суму понад 966 млн грн, що відповідає показнику ROI > 1000%.

Таким чином, запропонована стратегія є надійним та економічно обґрунтованим інструментом для забезпечення стійкого функціонування та розвитку компанії в умовах невизначеності.

ВИСНОВКИ

У магістерській роботі на основі проведеного дослідження теоретико-методологічних засад та практичних аспектів формування системи економічної безпеки підприємства (на прикладі ТОВ «Нова Пошта») зроблено наступні висновки та пропозиції:

1. Встановлено, що в умовах цифрової економіки та перманентних кризових явищ сутність економічної безпеки підприємства (ЕБП) трансформується. Критичний аналіз наукових підходів дозволив відійти від статичного розуміння безпеки як "стану захищеності" на користь динамічного «діяльнісного підходу». Сформульовано авторське визначення ЕБП як комплексної, адаптивної діяльності системи управління, спрямованої на узгодження інтересів стейкхолдерів (власників, персоналу, клієнтів, держави) шляхом превентивного управління загрозами. Головною метою цієї діяльності визначено забезпечення балансу між «захистом» (збереженням життєздатності) та «розвитком» (реалізацією економічного потенціалу).

2. Доведено, що класична структура функціональних складових безпеки вимагає перегляду під впливом глобальних викликів. Обґрунтовано, що в сучасних умовах ключовими стають не просто "кадрова" чи "інформаційна" складові, а їх трансформовані форми: «безпека людського капіталу» (як захист від вигорання та втрати компетентностей), «кібернетична безпека» (як захист цифрової інфраструктури) та «репутаційна безпека» (як захист нематеріальних активів). Також для логістичних підприємств критичного значення набуває безпека зовнішньоекономічної діяльності (ЗЕД).

3. На основі порівняльного аналізу існуючих методик діагностики (індикаторних, експертних, матричних) обґрунтовано доцільність застосування синтезованого підходу до оцінки рівня ЕБП. В якості базового інструментарію обрано «Модель інтегральної оцінки» (за методикою Пілецької, яка базується на розрахунку чотирьох груп індикаторів (фінансових, виробничих, технічних, кадрових) за даними офіційної

звітності. Водночас доведено необхідність «осучаснення» цієї моделі шляхом доповнення її якісним аналізом цифрових та репутаційних ризиків, які не відображаються у фінансових звітах, але є критичними для стійкості бізнесу.

4. З'ясовано, що ефективне формування системи ЕБП неможливе без інтеграції в загальну систему менеджменту. Визначено, що сучасний механізм безпеки має реалізовуватися через систему стратегічного контролінгу та спиратися на потужне інформаційно-аналітичне забезпечення (ІАЗ), яке використовує новітні цифрові інструменти (Big Data, AI) для прогнозування загроз, а не лише реагування на них.

5. У другому розділі здійснено комплексну оцінку рівня економічної безпеки ТОВ «Нова Пошта». Встановлено, що компанія є беззаперечним лідером ринку, демонструючи феноменальну адаптивність до умов воєнного стану (відновлення та зростання чистого доходу до 54,2 млрд грн у 2024 році). Проте розрахунок Інтегрального показника економічної безпеки ІЕБП виявив тривожну тенденцію: рівень безпеки є нестабільним і у 2024 році знизився до критичного значення 0.369, що відповідає «Проблемному стану».

6. Діагностика дозволила виявити конкретні "вузькі місця", що спричинили падіння рівня безпеки:

- фінансова вразливість: зафіксовано критичне зростання боргового навантаження (зобов'язання зросли на 47% за останній рік), що призвело до падіння коефіцієнта автономії до 0.36 (при нормі >0.5) та зниження ліквідності;

- ефективність активів: виявлено "парадокс інвестицій" - попри масштабне оновлення основних засобів (коефіцієнт оновлення 0.28), віддача від них падає (фондовіддача знизилася до 2.91 грн), що свідчить про неефективність використання капіталу;

- кадрові загрози: встановлено, що зростання продуктивності праці супроводжується високим ризиком "вигорання" персоналу та зниженням його рентабельності, що на фоні високої плинності кадрів створює загрозу втрати людського капіталу.

7. Доповнення кількісного аналізу якісними методами підтвердило, що окрім фінансових диспропорцій, підприємство стикається з високими кібернетичними ризиками (загрози збоїв ІТ-систем в умовах повної цифровізації бізнесу) та репутаційними викликами, які вимагають системного управління, а не ситуативного реагування. Це обґрунтувало необхідність розробки комплексної стратегії стабілізації.

8. На основі SWOT-аналізу та результатів діагностики обґрунтовано, що для виходу з "Проблемного стану" підприємству необхідна реалізація «Стратегії збалансованої стабілізації та інтенсифікації». Визначено три стратегічні пріоритети на 2025 рік: 1) фінансова реструктуризація (зниження боргового навантаження та підвищення автономії); 2) операційна інтенсифікація (підвищення фондодідачі наявних активів); 3) збереження ядра людського капіталу. Розроблено Концептуальну модель забезпечення ЕБП, яка базується на інтеграції цих пріоритетів у систему стратегічного контролінгу.

9. Розроблено комплексний організаційно-економічний механізм управління кадровою та інформаційною безпекою. Для кадрової складової запропоновано впровадження системи грейдингу та автоматизованої HRIS-системи, що дозволить зупинити відтік кадрів та підвищити мотивацію без надмірного збільшення фонду оплати праці. Для кібернетичної складової обґрунтовано перехід до архітектури Zero Trust та впровадження систем АІ-моніторингу (SIEM), що забезпечить превентивний захист цифрової екосистеми компанії від кібератак.

10. За допомогою методу сценарного прогнозування доведено високу ефективність запропонованих заходів. Розрахунки показали, що реалізація стратегії дозволить у 2025 році підвищити Інтегральний показник економічної безпеки з 0.369 до 0.634, повернувши підприємство у зону «Нормального рівня» безпеки. Прогнозується зростання чистого прибутку на 25% та відновлення коефіцієнта фінансової автономії до 0.44. Розрахунок

ефективності інвестицій у системи безпеки показав рівень ROI > 1000%, що підтверджує їх абсолютну економічну доцільність.

11. Проведене комплексне дослідження підтвердило, що формування ефективної системи економічної безпеки ТОВ «Нова Пошта» в умовах війни та цифровізації вимагає відмови від суто "захисних" моделей на користь проактивних механізмів управління. Практична реалізація розроблених у магістерській роботі рекомендацій, що базуються на стратегії збалансованої стабілізації, дозволить підприємству нівелювати критичні фінансові та кадрові дисбаланси, мінімізувати операційні ризики та забезпечити стійке довгострокове функціонування на ринку логістичних послуг, трансформуючи виклики цифрової ери у можливості для розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Асамоах-Черемех Д., Рудніченко Є. М. (2023). Підходи до сутнісного наповнення категорії «економічна безпека підприємства». *Development Service Industry Management*, 3, 47–55. [https://doi.org/10.31891/dsim-2023-3\(7\)](https://doi.org/10.31891/dsim-2023-3(7))
2. Захарчук Н.М. (2024). Економічна безпека підприємства у цифрову епоху: нові виміри, загрози та управлінські підходи. *Development Service Industry Management*, 7, 308–313. [https://doi.org/10.31891/dsim-2024-7\(47\)](https://doi.org/10.31891/dsim-2024-7(47))
3. Андріїв Н.М. (2023). Економічна безпека підприємства в умовах цифровізації ринку праці: теоретичні та практичні аспекти: монографія. Львів: ЛьВДУВС. 320 с.
4. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
5. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. <https://zakon.rada.gov.ua/laws/show/2469-19>
6. Про поштовий зв'язок: Закон України від 03.11.2022 № 2722-IX. <https://zakon.rada.gov.ua/laws/show/2722-20>
7. Про затвердження Правил надання послуг поштового зв'язку: Постанова КМУ від 05.03.2009 № 270. <https://zakon.rada.gov.ua/laws/show/270-2009-п>
8. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. <https://zakon.rada.gov.ua/laws/show/2210-14>
9. Гаркуша В.О., Єршова Н.Ю. (2021). Систематизація наукових поглядів щодо сутності поняття «економічна безпека підприємства». *Економіка та суспільство*, 28. <https://doi.org/10.32782/2524-0072/2021-28-34>
10. Гринкевич С.С., Когут М.В., Станкевич М.В. (2023). Еволюція теоретичних концепцій економічної безпеки підприємства. *Економіка та суспільство*, 50. <https://doi.org/10.32782/2524-0072/2023-50-70>

11. Васильців Т.Г., Міценко Н.Т., Мульска О.Г., Зайченко В.В. (2023). Economic potential vs economic security of the enterprise: points of convergence and divergence. *Наукові записки Львівського університету бізнесу та права*, 36, 23–29. <http://dx.doi.org/10.5281/zenodo.7625341>
12. Зінченко Д.С. (2021). Економічний розвиток підприємства і економічна безпека підприємства: генеза, взаємний вплив та взаємозалежність. *Економічний вісник НТУУ «КПІ»*, 18, 80–87. <https://doi.org/10.20535/2307-5651.18.2021.240435>
13. Дячков Д.В., Потапюк І.П., Капран І.В. (2021). Економічна безпека в системі стратегічного управління підприємством. *Економіка та суспільство*, 24. <https://doi.org/10.32782/2524-0072/2021-24-7>
14. Коробцова Д.В. (2022). Фінансово-економічна безпека підприємства і принципи її забезпечення. *Право та державне управління*.
15. Зіненко К.А., Кобелева Т.О. (2022). Економічна безпека підприємства: методологічна сутність та складові формування. *Вісник НТУ «ХПІ» (економічні науки)*, 4. <https://doi.org/10.20998/2519-4461.2022.4.9>
16. Прохорова В., Крутова А., Дяченко К. (2022). Економічна безпека підприємств України в умовах дестабілізаційного розвитку. *Адаптивне управління: теорія і практика. Серія «Економіка»*, 14(28).
17. Огренич Ю.О., Діброва В.О. (2023). Економічна безпека промислових підприємств в Україні: стан, проблеми та напрямки покращення. *Таврійський науковий вісник. Серія: Економіка*, 15, 180–191. <https://doi.org/10.32782/2708-0366/2023.15.22>
18. Проскура В.Ф., Черничко Т.В., Верецький Д. (2024). Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*, 13. <https://doi.org/10.32782/dees.13-9>
19. Кульчицький І.І. (2024). Цифрова економіка та економічна безпека підприємства: стратегії управління. *Актуальні питання економічних наук*, 6. <https://doi.org/10.5281/zenodo.14575016>

20. Москвін Б.Ю. (2022). Економічна безпека фінансових інституцій в умовах воєнного стану в Україні. *Економіка і організація управління*, 2, 110–119. <https://doi.org/10.31558/2307-2318.2022.2.11>
21. Овчаренко Л.В. (2023). Конкурентні сили як фактор зміцнення економічної безпеки підприємства в умовах воєнного стану та напрями їх аналізу. *Цифрова економіка та економічна безпека*, 6.
22. Чернишов В.В. (2021). Економічна безпека зовнішньоекономічної діяльності підприємств. *Економіка та суспільство*, 24. <https://doi.org/10.32782/2524-0072/2021-24-50>
23. Пілецька С.Т., Коритько Т.Ю., Ткаченко Є.В. (2021). Модель інтегральної оцінки економічної безпеки підприємства. *Економічний вісник Донбасу*, 3 (65), 56–65. [https://doi.org/10.12958/1817-3772-2021-3\(65\)-56-65](https://doi.org/10.12958/1817-3772-2021-3(65)-56-65)
24. Шило Ж.С., Кречко М.Ю. (2022). Методи оцінки рівня економічної безпеки підприємства. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*, 2 (98), 279–288.
25. Карачина Н.П., Скаковський В.В., Штанько О.С. (2024). Методичні підходи до оцінювання економічної безпеки сучасних підприємств в системі контролінгу. *Цифрова економіка та економічна безпека*, 17. <https://doi.org/10.32782/dees.17-13>
26. Панченко В.А. (2023). Аналізування як функція менеджменту в системі забезпечення економічної безпеки підприємств. *Modern Economics*, 41, 86–92. [https://doi.org/10.31521/modecon.V41\(2023\)-13](https://doi.org/10.31521/modecon.V41(2023)-13)
27. Смірнова А.С., Васюткіна Н.В. (2022). Формування стратегічних орієнтирів забезпечення економічної безпеки підприємства як засобу підвищення конкурентоспроможності. *Бізнес Інформ*, 9.
28. Алькема В.Г. (2024). Методичні підходи до оцінки ділової репутації підприємства. *Вчені записки Університету «КРОК»*, 4 (76), 90–95. <https://doi.org/10.31732/2663-2209-2024-76-90-95>

29. Живко З., Живко М., Шегинська А. (2024). Проблематика ділової репутації як індикатор економічної безпеки бізнесу. *Вчені записки Університету «КРОК», 4 (76), 104–113.* <https://doi.org/10.31732/2663-2209-2024-76-104-113>
30. Shumilo O. et al. (2021). Method of Enterprise Economic Security Evaluation. *Estudios de Economía Aplicada, 39 (7).* <https://doi.org/10.25115/eea.v39i7.4998>
31. Доманецький І.В., Яковенко Я.Ю., Маслак О.І., Маслак М.В. (2024). Комплексний підхід до оцінки економічної безпеки як передумова побудови багатофакторної прогнозної моделі. *Стала економіка, 1.*
32. Ткаченко О.С., Єрмілов Р.В., Чернуха О.В. (2024). Фінансово-економічна безпека як складова системи управління підприємством. *Сталий розвиток економіки, 4 (51).* <https://doi.org/10.32782/2308-1988/2024-51-15>
33. Біланчук І.М. (2024). Оцінка інформаційно-аналітичного забезпечення системи фінансово-економічної безпеки суб'єктів господарювання України. *Наукові записки Національного університету «Острозька академія». Серія «Економіка», 34(62), 26–32.*
34. Kukhar O., Kravchuk Y., Brechko O. (2023). Digital transformation as a factor in ensuring economic security of enterprises. *Baltic Journal of Economic Studies, 9 (5), 143–152.* <https://doi.org/10.30525/2256-0742/2023-9-5-143-152>
35. Гурочкіна В.В., Йосифчук Я.М. (2023). Драйвери успіху ТОВ «Нова пошта» на ринку поштових послуг України. *Підприємництво та інновації, 26, 38–43.* <https://doi.org/10.32782/2415-3583/26.6>
36. Тарнавська В.В., Мажара Г.А. (2023). Моделювання економічної безпеки підприємства «Нова Пошта» для оцінки фінансової стійкості в умовах глобальних викликів. *Економічний вісник.*
37. Тарнавська В.В., Мажара Г.А. (2023). Моделювання економічної безпеки підприємства «Нова Пошта». *Економічний вісник.*

38. Фінансова звітність та звіти про управління Групи «Нова Пошта» за 2019–2024 роки. https://novaposhta.ua/finansova_zvitnist
39. Бородін Н.І. (2022). Управління фінансовими результатами діяльності на ТОВ «Нова пошта» в умовах нестабільного зовнішнього середовища: кваліфікаційна робота бакалавра. Запоріжжя: ЗНУ. 64 с.
40. Марухненко К.Д. (2024). Формування кадрової політики підприємства ТОВ «Нова пошта»: кваліфікаційна робота бакалавра. Запоріжжя: ЗНУ. 68 с.
41. Ареф'єва О.В., Кузенко Т. Б. (2009). Економічна безпека підприємства. *Економіка промисловості*, 153–157.
42. Гурочкіна В.В., Йосифчук Я.М. (2023). Драйвери успіху ТОВ «Нова пошта». *Підприємництво та інновації*, 26, 38–43.
43. Гармаш С.В. (2023). Значущість індикаторів оцінки кадрової безпеки. *Вісник НТУ «ХПІ» (економічні науки)*, 2, 78–82. <https://doi.org/10.20998/2519-4461.2023.2.78>
44. Середня зарплата ТОВ «Нова Пошта». *Jooble*. <https://ua.jooble.org/salary/нова-пошта>
45. Середні зарплати по Україні. 24 канал. <https://24tv.ua/business/>
46. Мельничук І., Мужевич Н., Фрицький В. (2023). Облік витрат для забезпечення економічної безпеки підприємства в умовах цифрових трансформацій. *Галицький економічний вісник*, 6 (85), 60–66. https://doi.org/10.33108/galicianvisnyk_tntu2023.06