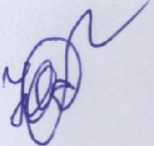


18.12.2025

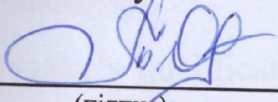
**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»**  
**ФАКУЛЬТЕТ БІЗНЕСУ ТА СФЕРИ ОБСЛУГОВУВАННЯ**  
**КАФЕДРА МЕНЕДЖМЕНТУ, БІЗНЕСУ ТА МАРКЕТИНГОВИХ**  
**ТЕХНОЛОГІЙ**

  
**ШЕЛЯГІН Ігор Валерійовича**  
(здобувач вищої освіти групи МОМ-25)

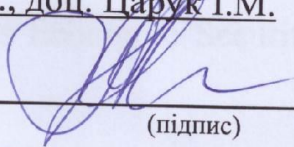
**МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА**  
**ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ**  
**БЕЗПЕКОЮ ПІДПРИЄМСТВА**

(представлена на здобуття ступеня вищої освіти «магістр»  
галузі знань 07 «Управління та адміністрування»  
спеціальності 073 «Менеджмент»)

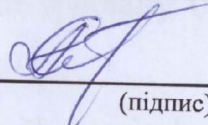
Допущено до захисту  
Зав. кафедри менеджменту, бізнесу  
та маркетингових технологій  
д.е.н., проф. Остапчук Т.П.

  
(підпис)

Керівник роботи:  
к.е.н., доц. Царук І.М.

  
(підпис)

Рецензент:  
к.е.н., доц. Сотник А.А.

  
(підпис)

Житомир, 2025

## **Анотація**

Шелягін І.В. Формування системи управління економічною безпекою підприємства. Рукопис.

Магістерська кваліфікаційна робота представлена на здобуття ступеня вищої освіти «магістр», галузі знань 07 «Управління та адміністрування» спеціальності 073 «Менеджмент». Державний університет «Житомирська політехніка», Житомир, 2025.

У магістерській кваліфікаційній роботі розглянуто теоретико-методичні засади та діючий механізм управління економічною безпекою державного підприємства ІТ-сфери та визначено організаційно-економічні напрями удосконалення відповідної системи на засадах ризик-менеджменту.

**Ключові слова:** економічна безпека підприємства, система управління, ризик-менеджмент, інформаційна безпека, кіберзахист, ДП «ДІА».

## **Annotation**

Sheliakin I. V. Formation of the Enterprise's Economic Security Management System. Manuscript.

The master's qualification work is submitted for the Master's degree, field of knowledge 07 «Management and administration» of specialty 073 «Management». Zhytomyr Polytechnic State University, Zhytomyr, 2025.

The master's qualification work examines the theoretical and methodological principles and the current mechanism of economic security management of a state enterprise in the IT sphere, and the organizational and economic directions for improving the corresponding system based on risk management are defined.

**Keywords:** enterprise economic security, management system, risk management, information security, cyber protection, SE «DIIA».

## **ЗМІСТ**

|                                                                                                          |           |
|----------------------------------------------------------------------------------------------------------|-----------|
| <b>ВСТУП .....</b>                                                                                       | <b>4</b>  |
| <b>РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА .....</b>                    | <b>9</b>  |
| 1.1. Економічна безпека підприємства: сутність, складові та роль у сучасних умовах .....                 | 9         |
| 1.2. Система управління економічною безпекою підприємства: структура та механізм функціонування .....    | 16        |
| 1.3. Методичні засади оцінки рівня економічної безпеки підприємства . . .                                | 27        |
| 1.4. Нормативно-правове та інформаційне забезпечення управління економічною безпекою підприємства .....  | 35        |
| Висновки до Розділу 1 .....                                                                              | 42        |
| <b>РОЗДІЛ 2. АНАЛІТИЧНА ОЦІНКА СТАНУ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДЕРЖАВНОГО ПІДПРИЄМСТВА «ДІЯ» .</b> | <b>45</b> |
| 2.1. Аналіз тенденцій розвитку сфери цифровізації та державних електронних послуг в Україні .....        | 45        |
| 2.2. Діагностика фінансово-економічного стану Державного підприємства «ДІЯ» .....                        | 53        |
| 2.3. Оцінка існуючої системи управління економічною безпекою Державного підприємства «ДІЯ» .....         | 58        |
| Висновки до Розділу 2 .....                                                                              | 69        |
| <b>РОЗДІЛ 3. НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДП «ДІЯ» .....</b>            | <b>71</b> |

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| 3.1. Організаційно-методичні засади удосконалення системи управління економічною безпекою підприємства . . . . . | 71  |
| 3.2. Заходи щодо мінімізації загроз та підвищення рівня економічної безпеки ДП «ДІА» . . . . .                   | 78  |
| 3.3. Оцінка економічної ефективності запропонованих заходів . . . . .                                            | 82  |
| Висновки до Розділу 3 . . . . .                                                                                  | 90  |
| <b>ВИСНОВКИ</b> . . . . .                                                                                        | 92  |
| <b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b> . . . . .                                                                      | 94  |
| <b>ДОДАТКИ</b> . . . . .                                                                                         | 109 |

## ВСТУП

**Актуальність теми дослідження.** Сучасний етап розвитку національної економіки України характеризується безпрецедентним рівнем турбулентності та невизначеності, що зумовлено повномасштабною збройною агресією, руйнуванням традиційних економічних зв'язків та перманентними атаками на критичну інфраструктуру. У цих умовах цифрова трансформація, яка ще донедавна розглядалася як інструмент модернізації, набула екзистенційного значення, ставши фундаментом національної стійкості та спроможності держави виконувати свої функції. Концепція «держави у смартфоні» трансформувалася з іміджевого проєкту в інструмент виживання, що забезпечує надання соціальних послуг, функціонування реєстрів та комунікацію влади з громадянами в умовах війни.

Особливої гостроти проблематика економічної безпеки набуває для стратегічно важливих державних підприємств ІТ-сектору, флагманом яких є Державне підприємство «ДІА». Як технічний адміністратор Єдиного державного вебпорталу електронних послуг та оператор державних реєстрів, підприємство функціонує на перетині економічних інтересів, національної безпеки та соціальної відповідальності. Для таких суб'єктів господарювання економічна безпека трансформується з категорії захисту корпоративного прибутку в категорію забезпечення безперервності надання державних сервісів та збереження цифрового суверенітету країни. Ефективність функціонування ДП «ДІА» прямо корелює з рівнем довіри суспільства до держави, що робить питання його безпеки пріоритетом національного рівня.

Аналіз практики функціонування ДП «ДІА» свідчить, що в умовах гібридної війни існуюча система управління економічною безпекою, орієнтована на стандарти мирного часу, потребує суттєвої трансформації. Зростання інтенсивності кібернетичних атак (кількість яких зросла на 70% у 2024 році), ризики кадрового голоду через міграційні процеси, а також необхідність забезпечення фінансової стійкості в умовах дефіциту державного

бюджету вимагають впровадження нових, проактивних механізмів захисту та управління ризиками. Сучасні виклики вимагають переходу від фрагментарних заходів захисту до побудови комплексної системи управління економічною безпекою, що базується на ризик-орієнтованому підході та міжнародних стандартах.

**Вагомий внесок у дослідження** теоретичних та прикладних аспектів економічної безпеки підприємств зробили такі вітчизняні вчені, як Андрієнко В., Богдан Н., Васильців Т., Воронков О., Денисенко М., Донець Л., Дяченко К., Козаченко Г., Молодід О., Пушкар Т., Ткачук Г., Чорна М., Шуміло О. та ін. Водночас, віддаючи належне науковому доробку попередників, слід зазначити, що питання забезпечення економічної безпеки державних ІТ-підприємств, які є носіями критичної інформаційної інфраструктури в умовах воєнного стану, залишаються недостатньо висвітленими. Більшість існуючих методик фокусуються на фінансових показниках промислових підприємств і не враховують специфіку створення вартості в цифровій економіці, де головним активом є інформація та довіра користувачів.

Необхідність розв'язання цих проблем, а також важливість розробки дієвого механізму управління економічною безпекою для ключового підприємства цифрової галузі України зумовили вибір теми кваліфікаційної роботи, її мету та завдання.

**Метою роботи** є узагальнення теоретичних засад та розробка організаційно-методичних рекомендацій щодо удосконалення системи управління економічною безпекою Державного підприємства «ДІЯ» в умовах цифрової трансформації та безпекових викликів воєнного часу.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі **завдання**:

- 1) визначити сутність, складові та роль економічної безпеки підприємства в сучасних умовах, уточнити понятійний апарат стосовно державних підприємств ІТ-сфери;
- 2) дослідити структуру та механізм функціонування системи управління

економічною безпекою підприємства, визначити особливості суб'єктно-об'єктної взаємодії;

3) узагальнити методичні засади оцінки рівня економічної безпеки, обґрунтувати вибір релевантних індикаторів для ІТ-підприємства, що враховують специфіку цифрових активів;

4) проаналізувати тенденції розвитку сфери цифровізації та надання державних електронних послуг в Україні, оцінити вплив зовнішнього середовища (PEST-аналіз);

5) здійснити діагностику фінансово-економічного стану ДП «ДІЯ» за 2022–2024 роки, виявити тенденції зміни майнового стану та фінансових результатів;

6) провести аналітичну оцінку існуючої системи управління економічною безпекою ДП «ДІЯ», ідентифікувати її сильні та слабкі сторони за допомогою SWOT-аналізу та бальної оцінки підсистем;

7) розробити організаційно-методичні засади удосконалення системи управління економічною безпекою шляхом створення спеціалізованого підрозділу та впровадження ризик-менеджменту;

8) обґрунтувати комплекс заходів щодо мінімізації загроз та підвищення рівня економічної безпеки (впровадження DLP-систем, перевірка контрагентів, страхування кіберризиків);

9) здійснити оцінку економічної ефективності запропонованих заходів на основі розрахунку чистого приведенного доходу (NPV) та рентабельності інвестицій у безпеку (ROSI).

**Об'єктом дослідження** є процес управління економічною безпекою Державного підприємства «ДІЯ».

**Предметом дослідження** є теоретичні, методичні та прикладні засади формування та удосконалення системи управління економічною безпекою державних підприємств, що функціонують у сфері інформаційних технологій.

**Методологічну основу роботи** становить діалектичний метод пізнання та системний підхід до вивчення економічних явищ. Для вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів:

– абстрактно-логічний та метод теоретичного узагальнення – для розкриття сутності економічної безпеки, уточнення її складових та принципів управління;

– системно-структурний аналіз – для побудови ієрархічної моделі складових економічної безпеки та архітектури системи управління;

– статистичний та графічний методи – для аналізу динаміки розвитку ІТ-галузі України, експорту послуг та макроекономічних показників;

– PEST-аналіз – для оцінки впливу політичних, економічних, соціальних і технологічних факторів зовнішнього середовища;

– коефіцієнтний фінансовий аналіз – для діагностики ліквідності, платоспроможності, ділової активності та рентабельності ДП «ДІА»;

– SWOT-аналіз – для виявлення внутрішніх резервів та зовнішніх загроз системі безпеки;

– метод таксономічного аналізу – для інтегральної оцінки рівня економічної безпеки підприємства;

– метод експертних оцінок – для ранжування ризиків та побудови карти ризиків;

– економіко-математичне моделювання – для розрахунку економічної ефективності проєктних рішень (NPV, PP, ROI).

**Інформаційним підґрунтям роботи** слугували законодавчі та нормативно-правові акти України (Конституція України, Закони «Про національну безпеку», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», постанови Кабінету Міністрів України), фінансова звітність ДП «ДІА» (Форма №1 «Баланс», Форма №2 «Звіт про фінансові результати») за 2022–2024 роки, статистичні матеріали Державної служби статистики України, аналітичні звіти асоціації «IT Ukraine», Львівського ІТ Кластера, Національного банку України, внутрішня документація підприємства (Статут, політики безпеки), а також наукові праці вітчизняних та зарубіжних вчених.

**Наукова новизна** одержаних результатів полягає в обґрунтуванні

теоретико-методичних положень та розробці практичних рекомендацій щодо зміцнення економічної безпеки державного ІТ-підприємства.

**Практичне значення** одержаних результатів полягає у розробці прикладних інструментів, спрямованих на підвищення рівня захищеності ДП «ДІЯ» та їх впровадженні у діяльність підприємства.

**Апробація результатів дослідження.** Основні положення та результати дослідження доповідалися та обговорювалися на Конференції-форумі «United Perspectives 24/7» в рамках Міжнародного наукового проєкту Ernst Lortikyan International Scientific Project «Global Creative Ideas Forum 3.0».

**Публікації.** За результатами виконаного дослідження опубліковано 1 наукову працю (тези доповідей): Шелягін І.В., Вдосконалення системи управління економічною безпекою державного підприємства в умовах цифровізації. Crosspoint Scientific Almanac. Ernst Lortikyan International Scientific Project «Global Creative Ideas Forum 3.0». Scientific Conference-Forum «United Perspectives 24/7», 2025. С. 117.

**Структура та обсяг роботи.** Магістерська кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 107 сторінок друкованого тексту. Робота містить 27 таблиць, 4 рисунки. Список використаних джерел налічує 127 найменувань.

# РОЗДІЛ 1

## ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

### **1.1. Економічна безпека підприємства: сутність, складові та роль у сучасних умовах**

Сучасний етап розвитку національної економіки України характеризується безпрецедентним рівнем турбулентності, зумовленим повномасштабною збройною агресією, руйнуванням традиційних логістичних та виробничих ланцюгів, а також глибинною трансформацією бізнес-процесів під впливом цифровізації. У цьому контексті проблематика забезпечення економічної безпеки підприємства (ЕБП) виходить за межі класичного корпоративного менеджменту і набуває ознак стратегічного імперативу виживання та резильєнтності. Особливої гостроти це питання набуває для стратегічно важливих державних підприємств, таких як ДП «ДІА», які виконують функції операторів критичної цифрової інфраструктури. Для таких суб'єктів господарювання економічна безпека трансформується з категорії захисту прибутку в категорію забезпечення національної стійкості, де фінансова стабільність стає фундаментом для безперебійного надання державних сервісів мільйонам громадян. Розуміння онтології економічної безпеки, її архітекτονіки та функціональної ролі в умовах воєнного стану та цифрової економіки є необхідною передумовою для побудови ефективної системи управління нею.

Етимологія поняття «безпека» (від гр. security, лат. securitas) традиційно пов'язується зі станом відсутності небезпеки, спокоєм та впевненістю. Однак перенесення цієї категорії в економічну площину, зокрема на мікрорівень підприємства, сформувало складний, полісемантичний конструкт, який пройшов тривалий шлях еволюції. Аналіз наукового доробку вітчизняних та зарубіжних вчених дозволяє стверджувати, що інтерес до цієї проблематики в Україні актуалізувався на початку 1990-х років, з переходом до ринкових

відносин, коли підприємства втратили державний протекторат і опинилися сам на сам із конкурентним та криміногенним середовищем.

У сучасній економічній науці відсутній єдиний уніфікований підхід до трактування сутності ЕБП. Цей феномен пояснюється різноманіттям наукових шкіл, динамікою змін у зовнішньому середовищі та специфікою об'єктів дослідження. На основі систематизації поглядів провідних науковців, можна виокремити декілька концептуальних підходів до розуміння сутності цієї категорії (табл. 1.1).

Таблиця 1.1

Порівняльна характеристика концептуальних підходів до визначення сутності економічної безпеки підприємства

| Назва підходу           | Сутнісна характеристика                                                                                                                             | Представники та інтерпретація                                                                                                                   | Переваги та обмеження в контексті ДП «ДІЯ»                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                       | 2                                                                                                                                                   | 3                                                                                                                                               | 4                                                                                                                                                                                                |
| Ресурсно-функціональний | ЕБП розглядається як стан найефективнішого використання корпоративних ресурсів для запобігання загрозам та забезпечення стабільного функціонування. | Акцент на ефективності використання капіталу, персоналу, інформації. Головна мета – максимізація прибутку через раціоналізацію витрат ресурсів. | Перевага: дозволяє оцінити ефективність використання бюджетних коштів та грантів.<br>Обмеження: звужує безпеку до внутрішньої ефективності, ігноруючи стратегічні ризики зовнішнього середовища. |
| Захисний (Статичний)    | Трактує ЕБП як стан захищеності інтересів підприємства від внутрішніх та зовнішніх загроз, недобросовісної конкуренції та протиправних дій.         | Домінування понять «захист», «охорона», «відсутність небезпеки». Історично перший підхід, що виник як реакція на криміналізацію економіки 90-х. | Перевага: акцент на кіберзахисті та захисті даних, що є критичним для ІТ-підприємства.<br>Обмеження: пасивна позиція (реакція на загрози), не враховує необхідність розвитку.                    |
| Адаптивний              | Здатність підприємства адаптуватися до змін зовнішнього середовища, нівелювати їх негативний вплив та використовувати можливості.                   | Ключові концепти: «рівновага», «гомеостаз», «гнучкість». Безпека досягається не через «стіни», а через швидку реакцію на зміни ринку.           | Перевага: висока релевантність для сфери ІТ, де технології змінюються миттєво.<br>Обмеження: складність формалізації та кількісного вимірювання рівня адаптивності.                              |
| Розвиваючий             | Безпека – це наявність конкурентних переваг та реалізація потенціалу розвитку. Стійкість досягається лише через постійний рух вперед.               | ЕБП визначається як здатність до самовідтворення та прогресу. Стагнація розглядається як головна загроза безпеці.                               | Перевага: відповідає місії ДП «ДІЯ» щодо постійного впровадження інновацій.<br>Обмеження: розвиток потребує значних ресурсів, що може бути ризикованим у кризові періоди.                        |

Продовження табл. 1.1

| 1                      | 2                                                                                                                                                      | 3                                                                                                                              | 4                                                                                                                                                         |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Системно-синергетичний | Інтегрує вищезазначені підходи. ЕБП – це властивість системи зберігати цілісність, структуру та функціональність в умовах стохастичного впливу загроз. | Розглядає підприємство як відкриту систему. Враховує інтереси стейкхолдерів, соціальну відповідальність та синергію складових. | Перевага: найбільш повний підхід, що дозволяє врахувати багатовекторність діяльності державного підприємства. Обмеження: методологічна складність оцінки. |

Джерело: сформовано автором.

Аналіз табл. 1.1 демонструє, що еволюція наукової думки рухається від розуміння безпеки як статичного стану захищеності («фортеця») до динамічної характеристики здатності до розвитку («корабель у морі»). Сучасні дослідники дедалі частіше наголошують на дихотомії понять «стан» і «процес» у визначенні ЕБП.

Трактування ЕБП як стану фокусується на фіксації певних параметрів (фінансових коефіцієнтів, рівня захисту даних) на конкретний момент часу. Натомість, розуміння ЕБП як процесу акцентує увагу на безперервності управлінських дій щодо моніторингу, ідентифікації та нейтралізації загроз. Враховуючи специфіку ДП «ДІЯ», діяльність якого відбувається у високодинамічному цифровому середовищі, доцільно поєднувати ці підходи: ЕБП – це стан захищеності, який досягається через безперервний процес управління ризиками.

Особливої уваги заслуговує підхід, що пов'язує економічну безпеку з цифровою трансформацією. Вчені вказують, що в умовах Індустрії 4.0 економічна безпека перестає бути суто економічною категорією і набуває ознак інформаційно-технологічного феномену. Для ДП «ДІЯ» економічна ефективність прямо корелює з надійністю цифрових платформ: будь-який технічний збій чи кібератака миттєво конвертуються у репутаційні та фінансові втрати.

Також варто врахувати інституційний аспект. ДП «ДІЯ» є державним підприємством, що накладає специфічні відбитки на сутність його безпеки. На відміну від приватного бізнесу, де домінантою є прибуток, для ДП пріоритетом

є виконання соціально значущих функцій та ефективність використання суспільних ресурсів. Тому в визначенні ЕБП для такого об'єкта необхідно відобразити баланс між економічною ефективністю та соціальною відповідальністю.

Враховуючи вищевикладене, а також сучасні виклики воєнного часу (необхідність забезпечення безперервності бізнесу, релокації процесів, захисту персоналу), пропонується наступне авторське визначення: економічна безпека ДП «ДІА» – це інтегральна характеристика стану захищеності його фінансового, кадрового та цифрового потенціалу, яка забезпечується через проактивну систему управління ризиками і дозволяє підприємству гарантувати безперебійність надання державних електронних послуг, зберігати фінансову стійкість та реалізовувати стратегію інноваційного розвитку навіть в умовах критичного впливу дестабілізуючих факторів зовнішнього середовища (зокрема, воєнно-політичних та кібернетичних загроз).

Це визначення підкреслює три ключові аспекти:

- 1) об'єкт захисту (потенціал у тріаді «фінанси-кадри-технології»);
- 2) механізм забезпечення (проактивне управління);
- 3) мету (безперебійність послуг та розвиток).

Системний підхід вимагає розгляду ЕБП не як моноліту, а як складної структури, що складається з функціональних елементів (підсистем). Декомпозиція ЕБП на складові дозволяє деталізувати об'єкти управління та розробити специфічні інструменти захисту для кожного напрямку діяльності. У науковій літературі представлено широкий спектр класифікацій складових ЕБП.

Більшість авторів виокремлюють такі базові складові: фінансова, кадрова, техніко-технологічна, інформаційна, правова, силова, екологічна. Однак проста перелік не розкриває внутрішніх зв'язків. Для ІТ-підприємства державного сектору ієрархія цих складових має свою специфіку. Розглянемо детально змістове наповнення кожної складової в контексті діяльності ДП «ДІА».

В умовах цифровізації інформаційна та кібернетична безпека трансформується з допоміжної у системоутворюючу. Для ДП «ДІА» це

фундамент існування – стан захищеності інформаційних ресурсів, інфраструктури та процесів обробки даних від випадкових або навмисних загроз.

Специфіка для ДП «ДІЯ»: Охоплює захист персональних даних громадян (мільйони записів), забезпечення цілісності державних реєстрів, протидію DDoS-атакам та АPT-загрозам. Порушення цієї безпеки веде до катастрофічних наслідків національного масштабу, втрати довіри до держави («державна у смартфоні») та, як наслідок, до втрати користувачів і доходів.

Фінансова безпека традиційно вважається результуючою складовою. Здатність підприємства генерувати достатній обсяг фінансових ресурсів для покриття поточних витрат, виконання зобов'язань та інвестування у розвиток.

Специфіка для ДП «ДІЯ»: Фінансова модель підприємства є гібридною (поєднання бюджетного фінансування, доходів від господарської діяльності та донорської допомоги). Безпека полягає у забезпеченні ліквідності, недопущенні касових розривів, ефективному управлінні собівартістю розробки ПЗ та прозорому звітуванні перед донорами (USAID, TAPAS тощо). Фінансова стійкість гарантує незалежність від політичної кон'юнктури.

Кадрова (інтелектуальна) безпека в ІТ-сфері є головним носієм вартості, оскільки забезпечує захист інтересів підприємства у сфері управління людськими ресурсами та інтелектуальним капіталом.

Специфіка для ДП «ДІЯ»: Утримання висококласних фахівців в умовах жорсткої конкуренції з приватним ІТ-сектором, де зарплати часто вищі. Запобігання витоку конфіденційної інформації через працівників. Забезпечення безперервного навчання персоналу для відповідності новітнім технологічним стекам. Втрата ключового архітектора системи може зупинити розвиток продукту на місяці.

Техніко-технологічна безпека відображає відповідність матеріально-технічної бази сучасним вимогам, найкращим світовим аналогам, надійність обладнання.

Специфіка для ДП «ДІЯ»: Це не верстати, а серверна інфраструктура,

хмарні сховища, ліцензійне ПЗ. В умовах війни ця складова набула фізичного виміру: забезпечення роботи дата-центрів під час блекаутів (старлінки, генератори), релокація обладнання у безпечні регіони або міграція у хмари (Amazon AWS, Microsoft Azure) для фізичного збереження даних.

Правова безпека – це юридичний захист діяльності, відповідність законодавству.

Специфіка для ДП «ДІЯ»: Легалізація цифрових документів (е-паспорт, е-права), що вимагає постійних змін у нормативному полі. Захист інтелектуальних прав на програмний код та бренд «Дія». Дотримання процедур публічних закупівель, щоб уникнути корупційних звинувачень.

Політико-інституційна та репутаційна безпека для державного підприємства ця складова є критичною. Залежність від політичної волі, змін в уряді може впливати на фінансування та стратегію. Репутаційна безпека (бренд) прямо впливає на кількість користувачів додатку та довіру міжнародних партнерів. На рис. 1.1 запропоновано ієрархічну модель складових ЕБП для ДП «ДІЯ», що відображає їх взаємозалежність.



Рис. 1.1. Ієрархічна модель складових ЕБП для ДП «ДІЯ»

Джерело: сформовано автором.

Варто зазначити, що між складовими існує тісний діалектичний зв'язок: недофінансування (загроза фінансовій безпеці) призводить до використання застарілого ПЗ (загроза технологічній безпеці) та відтоку фахівців (загроза кадровій безпеці), що сумарно відкриває «діри» для кібератак (загроза інформаційній безпеці).

Сучасний контекст функціонування підприємств в Україні визначається накладанням двох потужних трендів: цифрової трансформації економіки та воєнного стану. Це кардинально змінює роль та функціональне навантаження системи економічної безпеки.

У науковій літературі проводиться чітка демаркація між поняттями «ризик» та «загроза». Якщо у мирний час підприємства оперували переважно категорією ризику (ймовірнісна подія, якою можна управляти, страхувати, мінімізувати – наприклад, коливання курсу валют або зміна попиту), то воєнний час актуалізував категорію загрози (безпосередня небезпека, яка має деструктивний характер і часто не піддається імовірнісній оцінці – наприклад, ракетний удар по дата-центру).

Дослідження дозволяють класифікувати сучасні загрози ЕБП на:

- 1) кінетичні (фізичні): руйнування активів, загибель персоналу, окупація;
- 2) економічні: розрив ланцюгів постачання, інфляційний тиск, дефіцит бюджетного фінансування;
- 3) гібридні: поєднання кібератак з інформаційно-психологічними операціями (ІПСО), спрямованими на підрив довіри до державних цифрових сервісів.

У сучасних умовах роль ЕБП зміщується від пасивного захисту периметра до забезпечення резильєнтності (resilience) – здатності системи поглинати шоки, адаптуватися та відновлюватися. Для ДП «ДІЯ» це означає не просто захистити сервер, а мати розподілену хмарну архітектуру, яка дозволить сервісу працювати навіть при фізичному знищенні частини інфраструктури. Так само – не просто найняти охорону, а створити протоколи безпеки для віддаленої роботи співробітників з будь-якої точки світу. Тобто забезпечити цифрову

стійкість держави (наприклад, сервіси «єВорог», виплати ВПО, військові облігації в Дії), що робить підприємство елементом національного спротиву.

Сучасні дослідження підкреслюють інтеграцію ЕБП з концепцією сталого розвитку (ESG). Навіть в умовах війни підприємство повинно дбати про соціальні аспекти (підтримка співробітників, інклюзивність сервісів) та прозорість управління (боротьба з корупцією). Для ДП «ДІЯ» це є критичним, оскільки довіра міжнародних донорів базується саме на прозорості та відповідності стандартам.

Цифрові технології виступають двосічним мечем. З одного боку, вони створюють нові вразливості (кіберзагрози). З іншого – надають потужні інструменти для забезпечення безпеки (Big Data для аналізу ризиків, AI для виявлення аномалій у транзакціях, блокчейн для захисту реєстрів). Роль системи управління ЕБП полягає у максимізації переваг цифровізації при мінімізації її ризиків.

У підсумку, роль економічної безпеки для ДП «ДІЯ» сьогодні є системоутворюючою. Вона виступає гарантом не лише корпоративної ефективності, але й цифрового суверенітету держави. Від здатності підприємства протистояти загрозам залежить функціонування «держави у смартфоні», що в умовах війни є критично важливим елементом управління країною.

## **1.2. Система управління економічною безпекою підприємства: структура та механізм функціонування**

В умовах сучасних глобалізаційних викликів, перманентної турбулентності зовнішнього середовища та безпрецедентних загроз, пов'язаних із введенням воєнного стану в Україні, питання забезпечення економічної безпеки набувають екзистенційного значення для суб'єктів господарювання державного сектору економіки. Для Державного підприємства «ДІЯ», яке є не лише економічним

агентом, але й ключовим елементом цифрової інфраструктури держави, формування стійкої, адаптивної та ефективної системи управління економічною безпекою (СУЕБП) є необхідною передумовою виживання та розвитку. Дослідження теоретичних засад побудови такої системи, її архітекτονіки та механізму функціонування дозволяє сформувати методологічний базис для практичного удосконалення процесів захисту економічних інтересів підприємства.

Перш ніж перейти до детального аналізу структури та механізму, доцільно визначити сутнісне наповнення категорії «система управління економічною безпекою підприємства». Аналіз наукового дискурсу свідчить про відсутність єдиного уніфікованого підходу, що пояснюється складністю та багатогранністю самого об'єкта дослідження. В науковій літературі прослідковується еволюція поглядів від розуміння безпеки як стану захищеності ресурсів до інтерпретації її як здатності до розвитку та самовідтворення в умовах ризику.

Системний підхід, який є методологічною основою даного дослідження, передбачає розгляд управління економічною безпекою не як набору розрізнених заходів, а як цілісного організму, що має емерджентні властивості. Згідно з джерелами, система економічної безпеки підприємства трактується як сукупність взаємопов'язаних елементів (організаційних, технічних, фінансових, правових), дія яких спрямована на виявлення, попередження та нейтралізацію загроз з метою забезпечення стабільного функціонування та реалізації стратегічних цілей підприємства.

Варто зазначити, що для державних підприємств ІТ-сфери, яким є ДП «ДІЯ», класичне визначення потребує уточнення. Тут економічна безпека тісно переплітається з інформаційною та національною безпекою. Тому під СУЕБП досліджуваного підприємства пропонуємо розуміти інтегровану сукупність управлінських рішень, ресурсів та процесів, що забезпечують захист цифрових активів, фінансову стійкість та безперервність надання державних сервісів в умовах динамічних змін внутрішнього та зовнішнього середовища.

Існує кілька наукових підходів до розуміння сутності цієї системи, які

доцільно систематизувати для глибокого розуміння природи об'єкта дослідження (табл. 1.2).

Таблиця 1.2

Порівняльна характеристика наукових підходів до визначення системи  
управління економічною безпекою підприємства

| Підхід               | Сутність підходу                                                                                                                     | Переваги для ДП «ДІА»                                                                                   | Недоліки або обмеження                                                                                 |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Системно-структурний | Система розглядається як сукупність взаємопов'язаних елементів (суб'єктів, об'єктів, засобів), що мають чітку ієрархію та структуру. | Дозволяє чітко розмежувати повноваження, побудувати зрозумілу організаційну структуру служби безпеки.   | Може бути занадто статичним і не встигати за швидкими змінами загроз у цифровому середовищі.           |
| Процесний            | Акцент робиться на безперервному процесі управління (цикл PDCA: планування, виконання, перевірка, дія), а не на статичних елементах. | Забезпечує динамічність, дозволяє інтегрувати безпеку в бізнес-процеси розробки ПЗ (DevSecOps).         | Вимагає високої культури управління процесами та постійного моніторингу.                               |
| Ресурсний            | Система розглядається через призму захисту та ефективного використання корпоративних ресурсів (капіталу, персоналу, інформації).     | Фокусується на ефективності використання бюджетних коштів та інтелектуального капіталу.                 | Може ігнорувати зовнішні інституційні загрози та стратегічні ризики, не пов'язані напряму з ресурсами. |
| Кібернетичний        | Розгляд системи як контуру управління зі зворотним зв'язком, де головним є обмін інформацією та реакція на збурення середовища.      | Ідеально підходить для ІТ-підприємства, де інформація є головним активом і об'єктом управління.         | Складність математичного моделювання всіх соціально-економічних процесів.                              |
| Ризик-орієнтований   | Система будується навколо ідентифікації, оцінки та мінімізації ризиків. Основа – превентивність дій.                                 | Дозволяє пріоритезувати загрози та раціонально розподіляти обмежені ресурси на захист критичних вузлів. | Залежність від якості експертних оцінок та ймовірнісний характер прогнозів.                            |

Джерело: сформовано автором.

Аналіз таблиці 1.2 дозволяє стверджувати, що для ДП «ДІА» найбільш релевантним є синтез системно-структурного та ризик-орієнтованого підходів. Це дозволяє, з одного боку, створити стійку інституційну основу безпеки, а з іншого – гнучко реагувати на зміну ландшафту загроз, що є критично важливим в умовах кібервійни та цифровізації.

Фундаментальною основою формування дієвої системи управління

економічною безпекою є дотримання ряду принципів, які визначають її філософію та правила функціонування. Науковий доробок вітчизняних та зарубіжних вчених дозволяє виокремити базові принципи, адаптувавши їх до специфіки державного підприємства.

Принцип системності та комплексності. Цей принцип, висвітлений у роботах, передбачає, що система безпеки не може бути фрагментарною. Вона повинна охоплювати всі сфери діяльності підприємства (від фінансів до екології), всі структурні підрозділи та рівні управління. Для ДП «ДІА» це означає, що заходи кібербезпеки не можуть існувати окремо від заходів фізичної охорони серверів або юридичного захисту інтелектуальної власності.

Принцип законності (легітимності). Діяльність системи повинна базуватися виключно на нормах чинного законодавства. Це особливо актуально для державного сектору, де будь-яке відхилення від регламенту може розглядатися як корупційне діяння або перевищення повноважень. Система економічної безпеки повинна функціонувати в межах правового поля, визначеного Конституцією України, Законами «Про національну безпеку», «Про захист інформації в інформаційно-телекомунікаційних системах» та іншими нормативними актами.

Принцип пріоритету превентивності. Як зазначається у дослідженнях, економічно вигідніше попередити загрозу, ніж ліквідовувати її наслідки. Система повинна бути налаштована на раннє виявлення слабких сигналів небезпеки (Early Warning System). Це вимагає розвиненої системи моніторингу та бізнес-розвідки.

Принцип безперервності. Процес забезпечення безпеки не може бути дискретним. Загрози діють постійно, тому і механізм захисту повинен працювати в режимі 24/7/365. Для ДП «ДІА» це критично важливо, оскільки простій сервісів навіть на кілька годин може призвести до значних репутаційних та економічних втрат.

Принцип економічної доцільності. Витрати на функціонування системи безпеки не повинні перевищувати розмір можливого збитку від реалізації

загроз, які вона попереджає. Цей принцип вимагає постійного аналізу ефективності витрат (Cost-Benefit Analysis). Однак для державного підприємства, що виконує соціальні функції, цей принцип може коригуватися: соціальний ефект та національна безпека можуть превалювати над суто фінансовою вигодою.

Принцип взаємодії та координації. Передбачає налагодження ефективних комунікацій як між внутрішніми підрозділами підприємства, так і з зовнішніми суб'єктами (СБУ, Кіберполіція, Держспецзв'язку). Ізольованість служби безпеки призводить до інформаційного вакууму та помилкових рішень.

Принцип адаптивності та гнучкості. Згідно з, система повинна мати здатність до швидкої трансформації під впливом змін у зовнішньому середовищі. В умовах війни та стрімкого розвитку технологій, статичні системи стають вразливими. Адаптивність досягається через модульну структуру системи та регулярний перегляд політик безпеки.

Принцип компетентності. Управління безпекою повинно здійснюватися професіоналами, які володіють спеціальними знаннями та навичками. Це вимагає постійного навчання персоналу та підвищення культури безпеки на підприємстві.

Архітектура системи управління економічною безпекою базується на чіткому розмежуванні суб'єктів управління (хто здійснює вплив) та об'єктів управління (на що спрямований вплив). Для ДП «ДІА» ця структура має свої унікальні особливості, зумовлені подвійною природою підприємства (державна форма власності та ІТ-спеціалізація).

Суб'єкти управління доцільно класифікувати на зовнішні та внутрішні, що дозволяє визначити зони відповідальності та механізми взаємодії (табл. 1.3).

Таблиця 1.3

Класифікація та функції суб'єктів управління  
економічною безпекою ДП «ДІА»

| Рівень суб'єктів | Група суб'єктів | Конкретні представники | Функції та роль у забезпеченні безпеки |
|------------------|-----------------|------------------------|----------------------------------------|
| 1                | 2               | 3                      | 4                                      |

|          |                                 |                          |                                                                                                      |
|----------|---------------------------------|--------------------------|------------------------------------------------------------------------------------------------------|
| Зовнішні | Органи<br>законодавчої<br>влади | Верховна Рада<br>України | Формування нормативно-правової бази,<br>прийняття бюджету, визначення засад<br>національної безпеки. |
|----------|---------------------------------|--------------------------|------------------------------------------------------------------------------------------------------|

Продовження табл. 1.3

| 1         | 2                                     | 3                                                                                                       | 4                                                                                                                                                                                         |
|-----------|---------------------------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Зовнішні  | Органи виконавчої влади та управління | Кабінет Міністрів України, Міністерство цифрової трансформації (Орган управління)                       | Визначення стратегії розвитку, затвердження фінансових планів, контроль за ефективністю управління майном. Мінцифра виступає ключовим стейкхолдером, що визначає політику безпеки галузі. |
|           | Правоохоронні та спеціальні органи    | СБУ, Бюро економічної безпеки (БЕБ), Кіберполіція, Держспецзв'язку                                      | Протидія злочинності, розслідування кіберінцидентів, контроль за захистом державної таємниці, технічний захист інформації.                                                                |
|           | Контролюючі органи                    | Державна аудиторська служба, ДПС України                                                                | Контроль за цільовим використанням коштів, дотриманням податкового законодавства.                                                                                                         |
|           | Ринкові суб'єкти                      | Конкуренти, партнери, споживачі, банки                                                                  | Впливають через ринкові механізми, формують вимоги до конкурентоспроможності та фінансової стійкості.                                                                                     |
| Внутрішні | Стратегічний рівень                   | Керівник підприємства (Генеральний директор), Наглядова рада (за наявності)                             | Визначення політики безпеки, прийняття стратегічних рішень, розподіл ресурсів, загальний контроль.                                                                                        |
|           | Тактичний рівень (Спеціалізовані)     | Служба економічної безпеки, Департамент IT-безпеки (CISO), Юридичний відділ, Служба внутрішнього аудиту | Розробка та впровадження заходів безпеки, моніторинг ризиків, розслідування інцидентів, захист активів.                                                                                   |
|           | Операційний рівень                    | Керівники структурних підрозділів, власники бізнес-процесів                                             | Забезпечення безпеки на рівні конкретних процесів, контроль виконання інструкцій підлеглими.                                                                                              |
|           | Персонал                              | Усі працівники підприємства                                                                             | Дотримання режиму безпеки, конфіденційності, повідомлення про інциденти.                                                                                                                  |

Джерело: сформовано автором.

Особливістю ДП «ДІА» є те, що зовнішні суб'єкти (зокрема Мінцифра та Держспецзв'язку) мають прямий директивний вплив на внутрішні процеси безпеки, встановлюючи стандарти захисту інформації, які є обов'язковими до виконання.

Об'єкти безпеки – це все те, на що спрямовані деструктивні впливи загроз і

що потребує захисту для забезпечення нормального функціонування підприємства. До основних об'єктів належать:

1) фінансові ресурси (власний капітал, бюджетні асигнування, доходи від господарської діяльності, платоспроможність та ліквідність активів);

2) інформаційні ресурси та ІТ-інфраструктура (специфічний та найважливіший об'єкт для ДП «ДІЯ» – сюди входять бази даних, програмні коди, серверне обладнання, канали зв'язку, комерційна таємниця та персональні дані користувачів);

3) кадровий потенціал (життя та здоров'я працівників, їх кваліфікація, інтелектуальний потенціал, лояльність до підприємства (захист від інсайдерства));

4) матеріально-технічна база (офісні приміщення, обладнання, транспортні засоби);

5) інтелектуальна власність (авторські права на програмне забезпечення, патенти, торгові марки (бренд «Дія»));

6) ділова репутація та імідж (довіра громадян до державних цифрових послуг; підрив репутації ДП «ДІЯ» автоматично означає кризу довіри до держави).

Комплексний характер економічної безпеки вимагає її декомпозиції на функціональні складові, кожна з яких відповідає за нейтралізацію специфічного спектру загроз. В науковій літературі виділяють наступні базові складові, які в сукупності формують інтегровану систему безпеки (рис. 1.2).

Фінансова складова. Є індикатором загального стану підприємства. Її сутність полягає у забезпеченні фінансової стійкості, платоспроможності, ефективного управління грошовими потоками та мінімізації фінансових ризиків. Для державного підприємства важливим аспектом є ефективність використання бюджетних коштів та недопущення нецільових витрат.

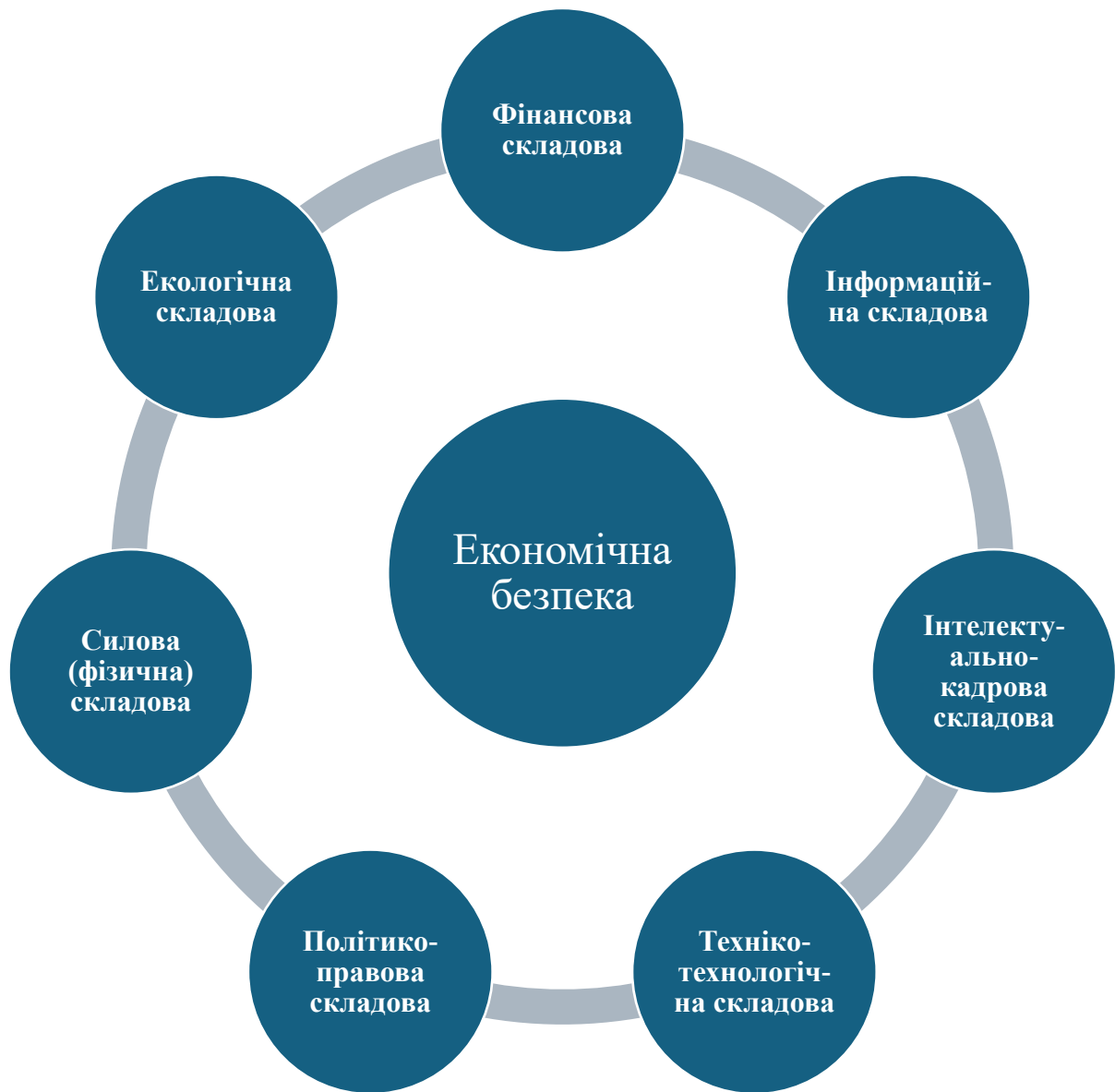


Рис. 1.2. Архітектура системи економічної безпеки ДП «ДІА»

Джерело: сформовано автором.

**Інформаційна складова.** Для ІТ-підприємства ця складова є системоутворюючою. Вона охоплює захист конфіденційності, цілісності та доступності інформації. Включає технічний захист (кібербезпеку), організаційні заходи (політики доступу) та аналітичну роботу (конкурентна розвідка).

**Інтелектуально-кадрова складова.** Спрямована на збереження та розвиток інтелектуального капіталу. Завдання включають: підбір лояльного та кваліфікованого персоналу, мотивацію, запобігання шахрайству з боку працівників, захист від «переманювання» ключових фахівців конкурентами.

Техніко-технологічна складова. Забезпечує відповідність технологічної бази сучасним вимогам, захист від технологічних аварій та збоїв. Для ДП «ДІА» це означає підтримку актуальності стеку технологій, надійність серверного обладнання та захист від залежності від одного постачальника технологій (vendor lock-in).

Політико-правова складова. Полягає у всебічному правовому супроводі діяльності, захисті законних інтересів у судах, моніторингу змін у законодавстві та забезпеченні комплаєнсу. Важливим аспектом є протидія рейдерству та необґрунтованому тиску з боку контролюючих органів.

Силова (фізична) складова. Забезпечення фізичної охорони об'єктів, матеріальних цінностей та персоналу. В умовах воєнного стану актуальність цієї складової зростає (захист від диверсій, ракетних обстрілів, фізичного проникнення).

Екологічна складова. Дотримання екологічних норм та стандартів. Хоча для ІТ-сфери екологічні ризики є менш вираженими, ніж для промисловості, дотримання принципів «зеленого офісу» та енергоефективності серверних є важливим елементом корпоративної соціальної відповідальності.

Взаємозв'язок складових є критичним. Наприклад, недостатнє фінансування (фінансова складова) призводить до неможливості закупівлі сучасного ПЗ захисту (технічна складова), що підвищує ризики витоку даних (інформаційна складова) та завдає шкоди репутації (політико-правова складова).

Якщо структура системи відображає її статику (будову), то механізм управління описує динаміку процесів забезпечення безпеки. Механізм управління економічною безпекою підприємства – це сукупність інструментів, методів, важелів та процесів, за допомогою яких суб'єкт управління впливає на об'єкт з метою забезпечення його захищеності та розвитку.

Аналіз джерел дозволяє представити структуру механізму управління у вигляді взаємодії чотирьох підсистем:

1. Цільова підсистема (Target Subsystem). Визначає вектор розвитку системи. Включає місію, візію, стратегічні цілі та завдання безпеки. Головною

метою є не просто «відсутність загроз», а створення умов для стійкого розвитку підприємства.

2. Забезпечувальна підсистема (Support Subsystem). Створює фундамент для роботи механізму (нормативно-правове забезпечення – закони, постанови, стандарти (ISO 27001), внутрішні регламенти; інформаційно-аналітичне забезпечення – моніторинг ринків, аналіз загроз, управлінський облік; ресурсне забезпечення – бюджет безпеки, технічні засоби, кадри).

3. Функціональна підсистема (Functional Subsystem). Реалізує управлінський цикл. Включає функції планування (розробка стратегії безпеки), організації (створення служби безпеки), мотивації (система KPI для персоналу щодо безпеки), контролю (аудит безпеки) та регулювання.

4. Інструментальна підсистема (Instrumental Subsystem). Являє собою набір конкретних методів впливу, що включають механізми захисту (фізична охорона, криптографія, фаєрволи), механізми регулювання (регламентація бізнес-процесів, дозвільна система доступу), механізми резервування (створення страхових фондів, резервне копіювання даних (бекапи), дублювання каналів зв'язку), механізми компенсації (страхування ризиків, стягнення збитків через суд).

Функціонування механізму відбувається циклічно та описується наступним алгоритмом:

I. Постійний збір інформації про стан зовнішнього та внутрішнього середовища, ідентифікація потенційних та реальних загроз.

II. Визначення ймовірності реалізації загроз та можливих масштабів збитків з паралельним ранжування ризиків за пріоритетністю (наприклад, критичні, суттєві, незначні).

III. Вибір методу реагування (уникнення, мінімізація, передача, прийняття) та розробка плану заходів.

IV. Виконання запланованих дій відповідними підрозділами.

V. Порівняння досягнутого стану безпеки з плановими показниками.

VI. Внесення змін у стратегію та тактику управління на основі отриманого

досвіду.

Сучасний контекст функціонування ДП «ДІА» накладає суттєвий відбиток на роботу механізму економічної безпеки (табл. 1.4).

Таблиця 1.4

Характеристика методів управління  
економічною безпекою в рамках механізму

| Група методів          | Приклади інструментів                                                                  | Застосування на ДП «ДІА»                                                                           |
|------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Адміністративні        | Накази, інструкції, регламенти, дисциплінарні стягнення                                | Затвердження Політики інформаційної безпеки, регламентація доступу до державних реєстрів.          |
| Економічні             | Бюджетування безпеки, страхування, штрафи, преміювання                                 | Формування бюджету на закупівлю ліцензійного ПЗ, страхування кіберризиків (перспективно).          |
| Технічні               | Системи контролю доступу (СКУД), відеоспостереження, DLP-системи, SIEM-системи         | Використання передових засобів моніторингу мережевої активності, захист серверних приміщень.       |
| Соціально-психологічні | Навчання, тренінги, формування корпоративної культури, перевірка лояльності (поліграф) | Проведення регулярних тренінгів з кібергігієни для співробітників, перевірка кандидатів при наймі. |

Джерело: сформовано автором.

По-перше, вплив воєнного стану. Згідно з, війна є потужним деструктивним фактором, що вимагає трансформації системи управління. Механізм стає більш централізованим, скорочується лаг прийняття рішень. Пріоритетом стає фізичне виживання активів (релокація серверів, персоналу) та забезпечення безперервності діяльності (Business Continuity Planning). Зростає роль силової складової (захист від диверсій) та інформаційної (протидія масованим кібератакам ворога).

По-друге, цифрова трансформація. Як зазначається у, в цифровій економіці дані стають головним активом. Це вимагає впровадження принципів Enterprise Architecture в систему безпеки. Безпека повинна бути інтегрована в архітектуру підприємства на етапі проектування (Security by Design). Важливим стає забезпечення інтероперабельності (сумісності) систем безпеки різних державних органів, оскільки «Дія» є платформою взаємодії.

### 1.3. Методичні засади оцінки рівня економічної безпеки підприємства

Проблематика кількісного вимірювання рівня економічної безпеки підприємства належить до найбільш дискусійних питань сучасної економічної науки. Це зумовлено дуалістичною природою самої категорії «безпека», яка, з одного боку, є статичною характеристикою стану захищеності ресурсів та інтересів суб'єкта господарювання, а з іншого – динамічною властивістю системи зберігати гомеостаз в умовах перманентного впливу дестабілізуючих факторів зовнішнього та внутрішнього середовища. Для такого стратегічно важливого об'єкта, як Державне підприємство «ДІА», що функціонує на стику державного управління, надання соціальних послуг та високотехнологічної ІТ-індустрії, вибір методичного інструментарію не може обмежуватися стандартними алгоритмами фінансового аналізу. Необхідним є формування комплексної моделі, яка б враховувала специфіку створення суспільної вартості (public value), нематеріальний характер ключових активів та критичну значущість інформаційної складової.

Ретроспективний аналіз наукового доробку дозволяє стверджувати, що еволюція методичних підходів до оцінки ЕБП відбувалася від простих однокритеріальних методів до складних полікритеріальних моделей, що базуються на теорії нечітких множин та штучному інтелекті. На початкових етапах розвитку теорії безпеки домінував індикаторний підхід, який базувався на порівнянні фактичних значень фінансових коефіцієнтів з нормативними базами. Однак в умовах цифрової економіки, де основна вартість генерується не фізичними активами, а інтелектуальним капіталом та програмним кодом, такий підхід демонструє свою обмеженість. Зокрема, для ДП «ДІА» високий рівень ліквідності може свідчити не про фінансову стійкість, а про неефективне використання бюджетних асигнувань або грантових коштів, які повинні інвестуватися в розвиток цифрової інфраструктури, а не акумулюватися на рахунках.

Сучасна парадигма діагностики економічної безпеки вимагає переходу від

констатації фактів (post-factum аналіз) до предиктивної аналітики, здатної ідентифікувати слабкі сигнали про зародження загроз. У цьому контексті методологія оцінки для досліджуваного підприємства повинна інтегрувати елементи ресурсно-функціонального аналізу, теорії ризиків та кібернетичного підходу, розглядаючи підприємство як відкриту систему, що постійно обмінюється ентропією з навколишнім середовищем. Критичним аспектом стає не стільки наявність ресурсів для покриття збитків, скільки здатність системи до адаптації та швидкого відновлення функціональності після кризових впливів (резильєнтність).

Враховуючи галузеву специфіку ДП «ДІА» як національного розробника цифрових рішень, механічне перенесення методик, розроблених для промислових чи торговельних підприємств, є неприпустимим. Необхідна глибока адаптація існуючих теоретичних конструктів.

Ресурсно-функціональний підхід є найбільш релевантним для комплексного оцінювання, оскільки він дозволяє структурувати систему безпеки на окремі функціональні складові, кожна з яких оцінюється специфічним набором метрик. Для ДП «ДІА» пропонується виділення наступних пріоритетних складових: фінансової, інформаційної, інтелектуально-кадрової, техніко-технологічної та правової. При цьому, на відміну від класичних моделей, де фінансова складова є домінантною, у даному випадку ключову роль відіграє інформаційна та інтелектуальна безпека, оскільки порушення їх цілісності може призвести до втрати функціонального призначення підприємства навіть за умови ідеального фінансового стану.

Оцінка кожної складової повинна базуватися на розрахунку часткових індикаторів, які згодом агрегуються в інтегральний показник. Важливим методичним моментом є визначення вагових коефіцієнтів значущості кожної складової, які не є константами, а динамічно змінюються залежно від фази життєвого циклу підприємства та зовнішніх умов (наприклад, в умовах кібервійни вага інформаційної безпеки прагне до максимуму).

Формування системи індикаторів (табл. 1.5) вимагає дотримання

принципів репрезентативності, вимірності, несуперечливості та чутливості до змін. Нижче наведено обґрунтування вибору ключових метрик для основних складових економічної безпеки ДП «ДІА».

Таблиця 1.5

## Система індикаторів оцінки рівня економічної безпеки ДП «ДІА»

| Функц. складова        | Група показників      | Індикатор (метрика)                                 | Економічний зміст та обґрунтування для ДП «ДІА»                                                                                                   | Джерело даних               |
|------------------------|-----------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 1                      | 2                     | 3                                                   | 4                                                                                                                                                 | 5                           |
| Фінансова              | Бюджетна ефективність | Коефіцієнт виконання фінансового плану ( $K_{fp}$ ) | Відображає дисципліну використання державних коштів; відхилення $>10\%$ свідчить про низьку якість планування або ризики нецільового використання | Звіт про виконання фінплану |
|                        | Фінансова автономія   | Коефіцієнт автономії ( $K_{aut}$ )                  | Частка власного капіталу в балансі; характеризує залежність від зовнішніх запозичень, що для держпідприємства є маркером суверенності             | Баланс (Форма №1)           |
|                        | Ліквідність           | Коефіцієнт покриття ( $K_{cov}$ )                   | Здатність своєчасно розраховуватися з контрагентами (хостинг-провайдери, підрядники з безпеки)                                                    | Баланс (Форма №1)           |
| Інформаційна           | Кіберстійкість        | Кількість успішних кібератак (IR)                   | Прямий індикатор ефективності системи захисту; для «ДІА» будь-яке значення $>0$ є критичним інцидентом                                            | Звіти SOC / CERT-UA         |
|                        | Надійність сервісів   | Час безвідмовної роботи (Up/SLA)                    | Відсоток часу доступності послуг для громадян; норматив: $\geq 99.9\%$ (зниження веде до репутаційних та економічних втрат)                       | Системи моніторингу         |
|                        | Конфіденційність      | Рівень захисту персональних даних                   | Інтегральна оцінка відповідності стандартам КСЗІ (комплексна система захисту інформації)                                                          | Акти аудиту                 |
| Інтелектуально-кадрова | Кадрова стабільність  | Коефіцієнт плинності ІТ-персоналу ( $K_{churn}$ )   | Втрата розробників створює ризики витоку компетенцій та знань про архітектуру систем; критичний поріг: $>15\%$ .                                  | Звітність HR-відділу        |

Продовження табл. 1.5

| 1                      | 2                         | 3                                          | 4                                                                                                          | 5               |
|------------------------|---------------------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------|
| Інтелектуально-кадрова | Лояльність                | Індекс лояльності персоналу (eNPS)         | Характеризує ризик інсайдерських загроз; низька лояльність корелює з ймовірністю саботажу або витоку даних | Опитування      |
| Техніко-технологічна   | Технологічна актуальність | Рівень застарілості ПЗ (Legacy Code Ratio) | Частка коду або систем, що не підтримуються виробником; високий рівень створює вразливості «нульового дня» | Технічний аудит |

Джерело: сформовано автором.

Запропонована система індикаторів є гібридною, поєднуючи класичні фінансові коефіцієнти зі специфічними метриками ІТ-галузі. Це дозволяє уникнути однобокості оцінки. Особливу увагу слід звернути на показник «Legacy Code Ratio», який рідко використовується в економічних дослідженнях, проте для ДП «ДІА» є фундаментальним чинником капіталізації та безпеки: використання застарілих технологій експоненціально збільшує вартість підтримки та ризики збоїв.

Традиційні моделі оцінки ймовірності банкрутства (Альтмана, Таффлера, Ліса) базуються на показниках рентабельності та ринкової капіталізації. Для державного підприємства, основною метою якого є не генерація прибутку, а надання якісних сервісів, ці моделі дають викривлені результати. Висока прибутковість ДП «ДІА» могла б свідчити про завищені тарифи на адміністративні послуги або комерціалізацію даних, що суперечить місії підприємства.

Тому методичний акцент зміщується на аналіз бюджетної ефективності та платоспроможності. Пропонується використовувати модифікований інтегральний показник фінансового стану ( $I_{fin}$ ), який розраховується як середньозважене нормованих значень ключових коефіцієнтів:

$$I_{fin} = \sum_{i=1}^n w_i \cdot \frac{x_i - x_{min}}{x_{max} - x_{min}}, \text{ де} \quad (1.1)$$

$w_i$  – вага  $i$ -го показника (визначається експертно, при цьому найвища вага надається коефіцієнту виконання фінансового плану);

$x_i$  – фактичне значення показника;

$x_{min}, x_{max}$  – порогові значення.

Цей підхід дозволяє нівелювати різницю в одиницях виміру та отримати безрозмірну величину, придатну для динамічного порівняння.

Оскільки економічна безпека є багатовимірною категорією, наявність набору розрізнених показників не дає керівництву цілісної картини. Виникає необхідність агрегації даних. Серед існуючих методів згортки (адитивна, мультиплікативна, метод головних компонент) найбільш обґрунтованим для завдань даного дослідження є метод таксономічного аналізу (метод Пліви або Хелвіга). Цей метод, на відміну від простих рейтингових оцінок, враховує відстань кожного об'єкта від гіпотетичного «еталона розвитку», що дозволяє оцінити не просто місце підприємства в рейтингу, а його реальний відрив від ідеального стану безпеки.

Алгоритм реалізації таксономічного методу для оцінки ЕБП ДП «ДІА» складається з наступних ітерацій:

*Етап 1. Формування матриці спостережень.* Побудова матриці  $X$  розмірністю  $m \times n$ , де  $m$  – кількість періодів (або об'єктів порівняння),  $n$  – кількість індикаторів безпеки.

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \quad (1.2)$$

*Етап 2. Стандартизація показників.* Оскільки показники мають різні одиниці виміру (грн, %, рази), необхідно привести їх до стандартизованого вигляду. Використовується процедура Z-нормалізації:

$$z_{ij} = \frac{x_{ij} - \bar{x}_j}{s_j}, \text{ де} \quad (1.3)$$

$\bar{x}_j$  – середнє арифметичне значення  $j$ -го показника;

$s_j$  – середньоквадратичне відхилення.

*Етап 3. Диференціація ознак та побудова еталона.* Всі показники поділяються на стимулятори (позитивний вплив на безпеку: прибуток, ліквідність, SLA) та дестимулятори (негативний вплив: кредиторська заборгованість, плинність кадрів, кількість атак). Формується вектор-еталон  $P_0(z_{01}, z_{02}, \dots, z_{0n})$ , координати якого визначаються як:

$$z_{0j} = \max_i z_{ij}, \text{ якщо } j \in \text{стимулятори} \quad (1.4)$$

$$z_{0j} = \min_i z_{ij}, \text{ якщо } j \in \text{дестимулятори} \quad (1.5)$$

*Етап 4. Розрахунок відстаней.* Визначається евклідова відстань  $C_{i0}$  між станом підприємства у  $i$ -й період та еталоном  $P_0$ :

$$C_{i0} = \sqrt{\sum_{j=1}^n (z_{ij} - z_{0j})^2} \quad (1.6)$$

*Етап 5. Обчислення таксономічного показника рівня безпеки ( $K_{EBP}$ ).*

$$K_{EBP} = 1 - \frac{C_{i0}}{C_0}, \text{ де} \quad (1.7)$$

$C_0$  – гранична відстань, яка зазвичай розраховується як  $\bar{C}_0 + 2S_0$  (середнє плюс два стандарти).

Значення  $K_{EBP}$  знаходиться в діапазоні  $[0; 1]$ . Наближення до 1 свідчить про високий рівень безпеки та максимальну близькість до еталона; наближення до 0 сигналізує про критичний стан.

Отримане кількісне значення інтегрального показника потребує якісної інтерпретації для прийняття управлінських рішень (табл. 1.6). Для цього пропонується використовувати адаптовану шкалу Харрінгтона, яка дозволяє вербалізувати числові значення рівнів безпеки. Особливістю запропонованої шкали є врахування специфіки ІТ-галузі, де перехід від нормального стану до критичного може відбуватися стрімко (наприклад, внаслідок масштабної кібератаки).

Таблиця 1.6

## Матриця ідентифікації рівня економічної безпеки ДП «ДІЯ»

| К <sub>ЕВР</sub>  | Рівень економічної безпеки | Характеристика стану підприємства                                                                                                                                               | Рекомендована стратегія управління                                                              |
|-------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 0.80<br>–<br>1.00 | Високий<br>(Еталонний)     | Підприємство характеризується абсолютною фінансовою стійкістю, високою захищеністю інформаційних активів, низькою плінністю кадрів. Здатність до протидії загрозам максимальна. | Стратегія розвитку: Інвестування в інновації, масштабування сервісів, експорт технологій.       |
| 0.63<br>–<br>0.79 | Достатній<br>(Нормальний)  | Основні параметри в нормі. Існують локальні проблеми (наприклад, тимчасові касові розриви або окремі інциденти безпеки), які не впливають на загальну функціональність.         | Стратегія підтримки: Моніторинг ключових ризиків, оптимізація бізнес-процесів.                  |
| 0.37<br>–<br>0.62 | Передкризовий<br>(Низький) | Порушення фінансової рівноваги, зростання залежності від зовнішнього фінансування, систематичні збої в роботі сервісів, втрата кваліфікованого персоналу.                       | Антикризова стратегія: Оперативне реагування, секвестр бюджету, аудит безпеки, кадрові ротації. |
| 0.00<br>–<br>0.36 | Критичний<br>(Небезпечний) | Втрата платоспроможності, критичні витоки даних, неможливість виконувати статутні завдання. Загроза ліквідації або реорганізації.                                               | Стратегія виживання: Санація, залучення кризових менеджерів, екстрена державна допомога.        |

Джерело: сформовано автором.

Запропонована градація рівнів дозволяє керівництву ДП «ДІЯ» чітко позиціонувати поточний стан підприємства. Важливо зазначити, що зона «Передкризового» стану (0.37 – 0.62) є найбільш небезпечною через ефект «нормалізації відхилень», коли менеджмент звикає до роботи в умовах постійного стресу і ігнорує накопичення системних проблем. Методика передбачає, що потрапляння в цю зону має автоматично запускати протоколи посиленого контролю.

Методичні засади не будуть дієвими без чітко регламентованої процедури їх застосування. Оцінка рівня ЕБП повинна бути інтегрована в систему стратегічного управління підприємством як безперервний бізнес-процес, а не разова акція.

Процес оцінки пропонується здійснювати за циклом Шухарта-Демінга

(PDCA) з наступною деталізацією етапів:

1. Визначення периметру оцінки (все підприємство чи окремі проєкти «Дія»), формування аналітичної групи. Важливо залучати не лише фінансистів, а й технічних директорів (СТО) та офіцерів безпеки (CISO), оскільки фінансисти не можуть адекватно оцінити технічні ризики.

2. Автоматизований збір даних з ERP-систем, систем моніторингу трафіку, бухгалтерських баз. Верифікація даних на предмет викривлень (window dressing).

3. Розрахунок часткових індикаторів та інтегрального показника за наведеною вище методикою таксономічного аналізу. Виявлення «вузьких місць» – індикаторів, що демонструють найбільше відхилення від еталона.

4. Розробка плану заходів щодо нейтралізації виявлених загроз. Наприклад, якщо виявлено критичне зниження індексу ліквідності, приймається рішення про перегляд графіку платежів; якщо впав показник кіберстійкості – ініціюється позаплановий пен-тест (penetration test).

Враховуючи високу невизначеність зовнішнього середовища (зміни законодавства, технологічні зрушення), кількісні методи доцільно доповнювати якісними. Запропоновано використання методу Delphi для періодичної переоцінки вагових коефіцієнтів індикаторів. Експертна панель повинна складатися як із внутрішніх менеджерів, так і з зовнішніх аудиторів галузі. Крім того, методика передбачає проведення стрес-тестування (stress testing). Це моделювання впливу екстремальних подій на рівень ЕБП. Для ДП «ДІА» типовими сценаріями стрес-тестів мають бути:

- 1) скорочення бюджетного фінансування на 50%;
- 2) масштабна DDoS-атака тривалістю більше 72 годин;
- 3) одночасне звільнення 20% ключових розробників.

Розрахунок прогностного значення  $K_{\text{ЕВР}}$  для кожного сценарію дозволяє оцінити запас міцності системи та розробити превентивні заходи.

#### **1.4. Нормативно-правове та інформаційне забезпечення управління економічною безпекою підприємства**

Функціонування сучасного високотехнологічного підприємства державного сектору, яким є Державне підприємство «ДІА», відбувається в умовах підвищеної турбулентності зовнішнього середовища та перманентних загроз у кіберпросторі. Ефективність системи управління економічною безпекою (далі – СУЕБП) такого суб'єкта господарювання прямо корелює з якістю та повнотою нормативно-правового регулювання його діяльності, а також зі здатністю менеджменту формувати, обробляти та використовувати масиви інформації для прийняття управлінських рішень. Нормативно-правове забезпечення створює легітимний каркас для реалізації захисних механізмів, визначає межі правового поля та встановлює відповідальність, тоді як інформаційне забезпечення виступає ресурсною базою, що живить процеси аналізу ризиків, моніторингу загроз та стратегічного планування. У цьому підрозділі досліджено багаторівневу структуру нормативного регулювання та специфіку інформаційних потоків ДП «ДІА» як критичного елемента цифрової інфраструктури держави.

Система нормативно-правового забезпечення економічної безпеки ДП «ДІА» характеризується складною ієрархічною будовою, що зумовлено подвійною природою підприємства: з одного боку, це суб'єкт господарювання, що підпорядковується загальним економічним законам, а з іншого – оператор критично важливих державних реєстрів та систем, що вимагає дотримання жорстких спеціальних нормативів. Аналіз законодавчого поля дозволяє структурувати нормативну базу за рівнями юридичної сили та сферою впливу на складові економічної безпеки.

Базисом нормативного забезпечення виступають Конституція України, Господарський та Цивільний кодекси України, які регламентують майнові відносини, правовий статус підприємства та загальні засади ведення господарської діяльності. Однак, для формування дієвої СУЕБП ДП «ДІА»

критичне значення має блок спеціалізованого законодавства, що регулює цифрову трансформацію, захист інформації та кібербезпеку. Саме ці норми трансформують абстрактні поняття безпеки у конкретні економічні та організаційні вимоги.

Центральне місце у цій системі посідає Закон України «Про основні засади забезпечення кібербезпеки України». Цей акт не лише вводить понятійний апарат, але й визначає об'єкти критичної інформаційної інфраструктури (ОКІІ). Оскільки ДП «ДІА» адмініструє Єдиний державний веб-портал електронних послуг (Портал Дія), його активи підпадають під визначення ОКІІ. Це накладає на підприємство зобов'язання щодо створення систем виявлення та реагування на кіберінциденти, проведення регулярних аудитів та обміну інформацією про загрози. З економічної точки зору, виконання цих норм вимагає значних капітальних інвестицій, які, однак, є превентивними витратами, що запобігають катастрофічним фінансовим та репутаційним збиткам у майбутньому.

Не менш важливим є Закон України «Про критичну інфраструктуру». Він інтегрує діяльність ДП «ДІА» у національну систему захисту, визначаючи надання електронних публічних послуг як життєво важливу функцію. Закон зобов'язує підприємство розробляти та впроваджувати паспорт безпеки об'єкта, плани локалізації та ліквідації наслідків аварій. Економічний аспект цього закону полягає у можливості отримання державної підтримки для забезпечення стійкості інфраструктури, але водночас встановлює жорстку відповідальність менеджменту за недотримання вимог безпеки, що формує кадрову та адміністративну складові ризиків.

Суттєвим кроком у модернізації нормативного поля стало прийняття Закону України «Про хмарні послуги». Цей документ легалізував використання хмарних технологій у державному секторі та ввів поняття «безпека як послуга» (Security as a Service). Для ДП «ДІА» це відкриває можливості оптимізації витрат на побудову КСЗІ (Комплексних систем захисту інформації) шляхом використання сертифікованих хмарних провайдерів. Це дозволяє трансформувати значні капітальні витрати (CAPEX) на «залізо» в операційні

витрати (ОРЕХ), підвищуючи гнучкість управління фінансовими ресурсами та економічною безпекою.

Регулювання сфери електронної довіри здійснюється через Закон України «Про електронні довірчі послуги». Оскільки ДП «ДІА» виступає Кваліфікованим надавачем електронних довірчих послуг (КНЕДП), воно повинно відповідати суворим вимогам щодо фінансової спроможності та страхування відповідальності. Це безпосередньо впливає на фінансову складову економічної безпеки, вимагаючи створення резервних фондів або придбання страхових полісів для покриття можливих збитків користувачів.

Деталізація законодавчих норм відбувається на рівні постанов Кабінету Міністрів України, які формують «дорожню карту» для операційної діяльності ДП «ДІА». Ключовим документом є Постанова КМУ № 1137 «Питання Єдиного державного веб-порталу електронних послуг...». Цей нормативний акт має фундаментальне значення для економічної безпеки підприємства, оскільки:

1. Закріплює за ДП «ДІА» статус технічного адміністратора Порталу Дія, що фактично надає підприємству монопольне становище у цій ніші. Це гарантує стабільність замовлень від держави та прогнозованість доходів, що є позитивним фактором фінансової безпеки.

2. Покладає на підприємство повну відповідальність за захист персональних даних та інформації від несанкціонованого доступу, модифікації чи знищення. Це генерує високі операційні ризики, адже будь-який технічний збій може трактуватися як порушення умов постанови.

Окремої уваги заслуговує Постанова КМУ № 606, що регламентує функціонування системи електронної взаємодії «Трембіта». Цей документ впроваджує принцип децентралізованого обміну даними, що є критично важливим для архітектури безпеки. Замість створення єдиної вразливої бази даних, норматив зобов'язує налаштовувати захищені шлюзи обміну, що знижує ризики масового витоку інформації та підвищує стійкість системи до атак.

Аналіз нормативного поля дозволяє систематизувати вплив ключових документів на складові економічної безпеки ДП «ДІА» у вигляді аналітичної

таблиці (табл. 1.7).

Таблиця 1.7

**Вплив нормативно-правових актів  
на складові економічної безпеки ДП «ДІА»**

| Нормативно-правовий акт                                           | Сфера регулювання                                                                        | Вплив на складові економічної безпеки                                                                                                                              |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ЗУ «Про основні засади забезпечення кібербезпеки України»         | Визначає правові та організаційні основи кіберзахисту, об'єкти критичної інфраструктури. | Техніко-технологічна: зобов'язує впроваджувати системи моніторингу та аудиту.<br>Кадрова: вимагає наявності фахівців з кіберзахисту відповідної кваліфікації.      |
| ЗУ «Про захист інформації в інформаційно-комунікаційних системах» | Встановлює вимоги до побудови КСЗІ та захисту даних у системах.                          | Фінансова: вимагає значних витрат на сертифікацію та атестацію систем.<br>Правова: визначає відповідальність за порушення режимів захисту.                         |
| Постанова КМУ № 1137                                              | Регламентує роботу Порталу Дія та функції технічного адміністратора.                     | Інституційна: закріплює статус підприємства як оператора національної платформи.<br>Репутаційна: пряма залежність довіри громадян від стабільності роботи Порталу. |
| Постанова КМУ № 1384                                              | Визначає сектори критичної інфраструктури та методику категоризації об'єктів.            | Організаційна: необхідність розробки паспортів безпеки та планів безперервності бізнесу (ВСП).                                                                     |
| Наказ Мінцифри № 173                                              | Встановлює вимоги до якості обслуговування суб'єктів звернення.                          | Клієнтська/Інтерфейсна: впливає на задоволеність користувачів та KPI підприємства.                                                                                 |

Джерело: сформовано автором.

Ефективність імплементації державних вимог залежить від якості внутрішніх регламентів. Локальна нормативна база ДП «ДІА» формує «мікроклімат» безпеки та деталізує процедури для персоналу.

Фундаментом є Статут ДП «ДІА», затверджений наказом Мінцифри. Він чітко окреслює правоздатність підприємства, види діяльності та повноваження органів управління. Це є запобіжником від юридичних ризиків, пов'язаних з перевищенням повноважень (*ultra vires*) та нецільовим використанням державних коштів.

Важливим елементом забезпечення кадрової та фінансової безпеки є Антикорупційна програма ДП «ДІА». Документ декларує принцип «нульової

толерантності» до корупції та встановлює механізми:

1) перевірки ділових партнерів (Due Diligence) перед укладанням договорів, що мінімізує ризики шахрайства та роботи з ненадійними контрагентами;

2) повідомлення про порушення (Whistleblowing) через захищені анонімні канали зв'язку;

3) врегулювання конфлікту інтересів посадових осіб; наявність дієвої антикорупційної програми є не лише вимогою законодавства, але й маркером прозорості для міжнародних донорів та партнерів, що сприяє залученню грантових коштів.

Внутрішні політики інформаційної безпеки розроблені з урахуванням міжнародних стандартів серії ISO/IEC 27000. Зокрема, на підприємстві діють Положення про конфіденційність та класифікацію інформації та Регламент роботи КНЕДП. Ці документи регламентують процеси управління доступом, криптографічного захисту та обробки інцидентів. Впроваджений Кодекс етики та ділової поведінки зобов'язує кожного працівника дбайливо ставитися до активів підприємства та не розголошувати комерційну таємницю, що підкріплюється підписанням угод про нерозголошення (NDA).

Інформаційне забезпечення управління економічною безпекою ДП «ДІЯ» – це не просто набір даних, а динамічна система збору, верифікації, аналізу та зберігання інформації, необхідної для нейтралізації загроз. Специфіка ІТ-підприємства зумовлює те, що інформація тут виступає одночасно і об'єктом захисту, і головним інструментом управління безпекою.

Для побудови адекватної моделі захисту та економічно обґрунтованого розподілу ресурсів на безпеку, ДП «ДІЯ» застосовує класифікацію інформаційних активів (табл. 1.8). Базуючись на міжнародних практиках (NIST, ISO) та внутрішніх потребах, інформацію можна поділити на рівні критичності. Така градація дозволяє застосовувати диференційовані заходи захисту: від базових для публічних даних до максимальних для критичних.

Таблиця 1.8

**Класифікація інформаційних активів ДП «ДІА»  
в системі економічної безпеки**

| Рівень класифікації          | Типи інформації (Приклади)                                                                         | Загрози економічній безпеці                                                                     | Заходи захисту та управління                                                                                           |
|------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Публічна (Public)            | Інформація на порталі diia.gov.ua, фінансова звітність, дані про публічні закупівлі.               | Втрата цілісності (дефейс сайту), дезінформація, репутаційні втрати.                            | Моніторинг контенту, захист від DDoS, контроль версій, резервне копіювання.                                            |
| Внутрішня (Internal)         | Внутрішні накази, листування, проектна документація, навчальні матеріали.                          | Конкурентна розвідка, зниження ефективності управління, операційні збої.                        | Розмежування доступу (IAM), корпоративні політики безпеки, навчання персоналу.                                         |
| Конфіденційна (Confidential) | Персональні дані користувачів, комерційна таємниця, фінансові транзакції, дані партнерів.          | Юридичні позови, штрафи регуляторів (GDPR/національні), відтік клієнтів.                        | Шифрування даних (в спокої та русі), DLP-системи, суворий контроль доступу, NDA.                                       |
| Критична (Restricted)        | Приватні ключі КНЕДП, коди доступу до реєстрів, дані про «Zero-day» вразливості, архітектура КСЗІ. | Повна зупинка діяльності, компрометація національної системи ідентифікації, загроза нацбезпеці. | Ізольовані сегменти мережі, апаратні модулі безпеки (HSM), багатофакторна автентифікація, допуск обмеженого кола осіб. |

Джерело: сформовано автором.

Інформаційна підтримка СУЕБП формується шляхом інтеграції внутрішніх та зовнішніх потоків даних. Система внутрішнього моніторингу генерує масиви даних, що дозволяють оцінювати поточний стан підприємства.

истеми фіксують всі дії в інформаційних системах (хто, коли і до яких даних звертався). Аналіз цих логів через SIEM-системи (Security Information and Event Management) дозволяє виявляти аномальну поведінку, інсайдерські загрози та спроби несанкціонованого доступу в режимі реального часу.

Аналіз балансу, звітів про рух грошових коштів та виконання фінансового плану дає змогу виявляти індикатори фінансової кризи, касові розриви або неефективне використання ресурсів.

Регулярні перевірки на відповідність стандартам ISO 27001 та вимогам КСЗІ надають об'єктивну картину зрілості процесів безпеки та виявляють невідповідності до моменту їх експлуатації зловмисниками.

Динамічний документ, що містить ідентифіковані ризики, оцінку їх впливу на бізнес-процеси та статус заходів з їх мінімізації.

Для адаптації до змін у зовнішньому середовищі ДП «ДІЯ» використовує:

1. Система «Трембіта» – це не лише транспорт для надання послуг, але й джерело верифікованих даних. Через систему електронної взаємодії підприємство отримує актуальну інформацію з базових реєстрів, що дозволяє перевіряти достовірність даних користувачів та контрагентів, мінімізуючи ризики шахрайства.

2. Програми Bug Bounty – унікальним джерелом інформації про вразливості є співпраця з етичними хакерами. Звіти, отримані через платформи Bug Bounty, дозволяють виявляти критичні діри в безпеці до того, як ними скористаються злочинці. Економічний ефект полягає в тому, що виплата винагороди (bounty) завжди значно менша за потенційні збитки від реальної кібератаки.

3. Моніторинг законодавства та загроз – використання правових систем (LIGA:ZAKON) та підписка на фіди кіберзагроз (Threat Intelligence) від CERT-UA та міжнародних партнерів дозволяє превентивно готуватися до нових векторів атак та регуляторних змін.

Для забезпечення оперативності та достовірності інформації ДП «ДІЯ» використовує передові технологічні рішення:

1. Система «Вулик» – програмний комплекс для ЦНАПів, що також слугує джерелом даних про якість надання послуг та навантаження на систему, дозволяючи оптимізувати бізнес-процеси.

2. Технологія Diia.Signature – використання біометричної ідентифікації та кваліфікованого підпису забезпечує неспростовність дій користувачів, що є критичним для доказової бази у разі спірних ситуацій або спроб фроду.

3. SOC (Security Operations Center) – центр оперативного реагування на кіберзагрози забезпечує цілодобовий збір та кореляцію подій безпеки, перетворюючи розрізнені дані на структуровану інформацію для прийняття рішень.

Важливою складовою нормативного забезпечення ДП «ДІЯ» є добровільна сертифікація за міжнародними стандартами, що виступає гарантом надійності для партнерів та користувачів. Підприємство успішно пройшло сертифікацію та підтвердило відповідність стандарту ISO/IEC 27001:2022 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою».

Імплементація цього стандарту в СУЕБП має ряд наслідків, зокрема стандарт вимагає розглядати безпеку як циклічний процес (Plan-Do-Check-Act), а не одноразовий захід. ISO 27001 зобов'язує проводити регулярну оцінку ризиків та впроваджувати адекватні заходи контролю, що забезпечує економічну ефективність витрат на безпеку. Вимоги стандарту щодо Business Continuity Management (BCM) гарантують, що підприємство має плани відновлення після аварій, що мінімізує час простою та фінансові втрати.

Окрім того, відповідність стандартам захисту приватності (ISO 27701) та безпеки розробки (ISA/IEC 62443) свідчить про зрілість процесів та інтеграцію безпеки на всіх етапах життєвого циклу продуктів, що є конкурентною перевагою на ринку GovTech.

## **Висновки до Розділу 1**

Економічна безпека підприємства в сучасних наукових дослідженнях трактується як складна, багаторівнева категорія. Для об'єкта дослідження (ДП «ДІЯ») найбільш релевантним є системно-синергетичний підхід, який розглядає безпеку як динамічний стан захищеності потенціалу та здатність до сталого розвитку в умовах цифрової трансформації та воєнних викликів.

ЕБП складається з ієрархічно пов'язаних елементів. Специфіка діяльності ДП «ДІЯ» зумовлює домінуючу роль інформаційної та кадрової складових, які є базисом для фінансової та репутаційної безпеки.

В умовах війни та глобальної нестабільності (BANI-світ) функція економічної безпеки еволюціонувала від «охоронної» до «стратегічної». Вона

забезпечує резильєнтність бізнес-моделі, безперервність надання послуг та виступає інструментом реалізації національних інтересів у цифровій сфері.

Система управління економічною безпекою ДП «ДІЯ» є складною, поліструктурною системою, що інтегрує фінансові, інформаційні, кадрові та інші аспекти діяльності для забезпечення стійкого розвитку. Її архітектоніка базується на взаємодії зовнішніх та внутрішніх суб'єктів, а механізм функціонування реалізується через циклічний процес моніторингу, аналізу та реагування на ризики. Ефективність цієї системи в сучасних умовах залежить від її здатності адаптуватися до воєнних загроз та інтегрувати передові цифрові технології захисту.

Специфіка ДП «ДІЯ» як об'єкта дослідження вимагає відмови від суто фінансово-орієнтованих методик на користь комплексного ресурсно-функціонального підходу. Критичними детермінантами безпеки визначено не прибуток, а бюджетну ефективність, інформаційну стійкість та збереження інтелектуального капіталу.

Розроблена система індикаторів є збалансованою та охоплює всі ключові сфери життєдіяльності підприємства. Введення специфічних метрик, таких як «Legacy Code Ratio» та «SLA Compliance», дозволяє врахувати технологічну природу загроз, які часто ігноруються в економічних дослідженнях.

Як математичний інструментарій агрегації даних обґрунтовано використання таксономічного методу. Його перевага полягає у здатності синтезувати різномірні показники в єдиний інтегральний індекс, порівнюючи фактичний стан підприємства з ідеалізованим еталоном, що забезпечує об'єктивність оцінки.

Запропонована матриця ідентифікації станів безпеки та відповідних управлінських стратегій перетворює методику з інструменту пасивної констатації на активний інструмент підтримки прийняття управлінських рішень. Це дозволяє керівництву переходити від реактивного реагування на інциденти до проактивного управління ризиками.

Імплементація методики повинна відбуватися за принципом безперервного

циклу з обов'язковим елементом стрес-тестування, що забезпечить адаптивність системи управління економічною безпекою до динамічних змін у цифровому просторі та державному секторі економіки.

Нормативна база підприємства є дворівневою та комплексною. Вона гармонійно поєднує імперативні вимоги національного законодавства (Закони про кібербезпеку, критичну інфраструктуру, хмарні послуги) з гнучкими внутрішніми регламентами, розробленими на основі кращих міжнародних практик (ISO 27001). Це створює міцний правовий фундамент для захисту інтересів підприємства та легітимізації заходів безпеки.

Інформаційне забезпечення побудоване на принципах інтеграції та аналітики. СУЕБП спирається на широке коло джерел: від традиційної фінансової звітності до високотехнологічних даних SIEM-систем, логів «Трембіти» та звітів етичних хакерів. Класифікація інформації дозволяє оптимізувати витрати на захист, концентруючи ресурси на критично важливих активах.

Використання сучасних інструментів (хмарні технології, децентралізований обмін даними, біометрична ідентифікація) не лише підвищує ефективність основної діяльності, але й виступає потужним елементом системи економічної безпеки, знижуючи ризики шахрайства та людського фактора.

Наявність сертифікацій міжнародного рівня та імплементація антикорупційних програм свідчить про перехід ДП «ДІЯ» від реактивної моделі безпеки до проактивної, орієнтованої на управління ризиками та забезпечення стійкості бізнесу в довгостроковій перспективі.

## **РОЗДІЛ 2**

### **АНАЛІТИЧНА ОЦІНКА СТАНУ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДЕРЖАВНОГО ПІДПРИЄМСТВА «ДІЯ»**

#### **2.1. Аналіз тенденцій розвитку сфери цифровізації та державних електронних послуг в Україні**

Сучасна парадигма економічного розвитку України формується під впливом безпрецедентних екзогенних шоків, які зумовили фундаментальну трансформацію ролі цифрових технологій у системі національної безпеки. Якщо у довоєнний період цифровізація розглядалася переважно як інструмент підвищення ефективності державного управління та драйвер економічного зростання через нарощування експортного потенціалу, то в умовах повномасштабної війни вона набула екзистенційного значення, ставши основою стійкості (resilience) держави та суспільства. Для Державного підприємства «ДІЯ», яке виступає ключовим оператором інфраструктури електронного урядування, глибоке розуміння макроекономічних трендів, динаміки ІТ-ринку та специфіки функціонування сфери GovTech є критично необхідним для побудови адаптивної системи управління економічною безпекою. Аналіз тенденцій за період 2019–2024 років (табл. 2.1) дозволяє виявити нелінійні закономірності розвитку галузі, оцінити вплив безпекових факторів на інвестиційну привабливість та визначити стратегічні вектори подальшої еволюції цифрової екосистеми України.

Протягом досліджуваного періоду сектор інформаційно-комунікаційні технології (ІКТ) України продемонстрував феноменальну здатність до адаптації, пройшовши шлях від стабільного екстенсивного зростання до структурної перебудови в умовах воєнного часу. Ретроспективний аналіз даних Асоціації «IT Ukraine» та Національного банку України свідчить, що до 2022 року галузь розвивалася за експоненційною траєкторією. Обсяг експорту комп'ютерних послуг зріс з 4,2 млрд дол. США у 2019 році до рекордних 7,3 млрд дол. США у

2022 році. Цей період характеризувався інтенсивною інтеграцією українських сервісних компаній у глобальні ланцюги доданої вартості, що дозволило ІТ-сектору стати другою за обсягом експортною галуззю України після агропромислового комплексу.

Показовим є те, що навіть у перший рік повномасштабного вторгнення індустрія не лише зберегла, але й наростила обсяги експорту на 5,8% порівняно з 2021 роком, досягнувши частки 44,2% у загальному експорті послуг. Цей феномен, який у фаховій літературі отримав назву «цифрового спротиву», був зумовлений високою мобільністю бізнес-процесів, відсутністю жорсткої прив'язки до фізичних активів та логістичних шляхів, а також ефективною диверсифікацією клієнтського портфеля. Українські компанії змогли забезпечити безперервність надання послуг завдяки швидкій релокації персоналу в безпечні регіони та за кордон, використанню супутникового зв'язку та хмарних технологій.

Однак, починаючи з 2023 року, в галузі сформувався новий тренд на поступове зниження обсягів експортної виручки. За даними Національного банку України, у 2023 році обсяг експорту ІТ-послуг скоротився на 8,5%, склавши 6,7 млрд дол. США. Ця тенденція продовжилася і у 2024 році: за попередніми оцінками Львівського ІТ Кластера та галузевих асоціацій, очікується подальше зниження на рівні 4–5%, до позначки 6,3–6,45 млрд дол. США. Аналіз щомісячної динаміки у 2024 році демонструє волатильність показників: якщо у грудні 2023 року було зафіксовано сплеск до 611 млн дол., то січень 2024 року показав один з найнижчих результатів – 508 млн дол., з подальшим коливанням у межах 520–560 млн дол. щомісяця.

Таблиця 2.1

Динаміка ключових показників розвитку експортоорієнтованого  
ІТ-сектору України (2019-2024 рр.)

| Показник                                | 2019  | 2020  | 2021  | 2022 | 2023 | 2024 |
|-----------------------------------------|-------|-------|-------|------|------|------|
| 1                                       | 2     | 3     | 4     | 5    | 6    | 7    |
| Обсяг експорту ІТ-послуг, млрд дол. США | 4,2   | 5,0   | 6,9   | 7,3  | 6,7  | 6,4  |
| Темп приросту до попереднього року, %   | +30,2 | +19,0 | +38,0 | +5,8 | -8,2 | -4,5 |
| Частка ІТ в експорті послуг України, %  | 23,9  | 32,3  | 37,8  | 44,2 | 40,5 | 37,4 |

Продовження табл. 2.1

| 1                                                     | 2   | 3   | 4   | 5    | 6    | 7    |
|-------------------------------------------------------|-----|-----|-----|------|------|------|
| Частка ІТ в загальному експорті (товари + послуги), % | 6,6 | 8,3 | 8,5 | 12,8 | 13,1 | 11,5 |
| Внесок ІТ-галузі у ВВП України, %                     | 2,0 | 2,5 | 2,7 | 4,5  | 3,7  | 3,4  |

Джерело: сформовано автором.

Зниження показників у 2023-2024 роках зумовлене конвергенцією глобальних макроекономічних факторів та внутрішніх безпекових ризиків. По-перше, світова рецесія технологічного сектору призвела до оптимізації бюджетів ключових замовників у США та Західній Європі, що спричинило скорочення кількості нових контрактів. По-друге, тривалість воєнних дій формує у іноземних партнерів сприйняття України як зони підвищеного ризику, що змушує їх диверсифікувати розробку в інші юрисдикції, такі як Польща, Румунія, Індія та країни Латинської Америки. По-третє, складність процедур бронювання критично важливих фахівців та невизначеність щодо мобілізаційних процесів обмежують можливості компаній щодо довгострокового планування та гарантування виконання зобов'язань перед клієнтами.

Географічна структура експорту залишається орієнтованою на західні ринки. Беззаперечним лідером є Сполучені Штати Америки, на які припадає близько 40% виручки. До топ-5 партнерів також входять Велика Британія, Мальта, Кіпр та Ізраїль. Варто зауважити, що значна частка експорту до Мальти та Кіпру має технічний характер і відображає юридичне структурування бізнесу міжнародних груп, а не кінцеве споживання послуг. Водночас у 2024 році спостерігається посилення співпраці з європейськими країнами, зокрема Німеччиною та Польщею, що корелює з курсом України на євроінтеграцію та приєднанням до Єдиного цифрового ринку ЄС.

Людський капітал залишається головним активом галузі. Станом на 2024 рік загальна кількість ІТ-фахівців, асоційованих з українською індустрією, оцінюється у понад 300 тисяч осіб. Однак структура цієї вибірки суттєво змінилася: близько 20% фахівців (60–65 тис. осіб) перебувають за кордоном.

Хоча більшість з них продовжує працювати в українських компаніях дистанційно, ризик їхньої поступової асиміляції на іноземних ринках праці та зміни податкового резидентства зростає. Крім того, спостерігається суттєве уповільнення темпів приросту нових кадрів: якщо у 2019–2021 роках ринок зростав на 15–20% щорічно, то у 2023 році чистий приріст склав лише близько 3,5 тис. осіб, що свідчить про насичення ринку junior-спеціалістами при збереженні дефіциту фахівців рівня senior.

Особливістю поточного етапу є зміна моделі зайнятості. Традиційна модель співпраці через ФОП (фізичні особи-підприємці), яка домінувала роками, поступово трансформується. У 2024 році частка фахівців, що працюють як ФОП, знизилася до 57% (порівняно з 87% у 2022 році), що пов'язано як з міграцією, так і з переходом компаній на гіг-контракти в рамках правового режиму Дія.City. За 10 місяців 2024 року кількість ФОП у сфері комп'ютерного програмування скоротилася на 7,5 тис. осіб, що є тривожним сигналом для малого бізнесу в секторі.

Паралельно з трансформацією комерційного сектору, в Україні відбувається стрімкий розвиток сфери державних технологій (GovTech), який став драйвером цифровізації суспільних відносин. Реалізація концепції «Держава у смартфоні» через екосистему «Дія» дозволила Україні увійти до світових лідерів за рівнем розвитку цифрових державних послуг. Аналіз динаміки користувацької бази свідчить про глибоке проникнення цифрових інструментів у повсякденне життя громадян. Якщо на етапі запуску у 2020 році кількість користувачів застосунку «Дія» становила близько 6 млн, то станом на початок 2025 року цей показник перевищив 23 млн унікальних користувачів. Це означає, що понад половина всього населення України (включно з дітьми та особами похилого віку) активно взаємодіє з державою у цифровому форматі.

Функціональність екосистеми «Дія» постійно розширюється. Станом на 2024 рік громадянам доступно понад 30 цифрових документів та більше 130 онлайн-послуг на порталі та в застосунку. Важливим етапом розвитку стало впровадження у 2024 році послуги «Шлюб онлайн», яка є унікальним світовим

кейсом повного циклу реєстрації актів цивільного стану через відеозв'язок, що підтверджує технологічне лідерство України у сфері GovTech. Крім того, відкриття програмного коду «Дії» у 2024 році для інших країн свідчить про трансформацію українського GovTech з локального продукту в експортно-орієнтовану технологію, що має значний потенціал для монетизації та посилення «м'якої сили» України на міжнародній арені.

Інституційним фундаментом розвитку цифрової економіки став запуск спеціального правового режиму Дія.City. Ця ініціатива, спрямована на створення сприятливих податкових та регуляторних умов для IT-бізнесу, продемонструвала високу ефективність. Попри війну, кількість резидентів Дія.City демонструє стійке зростання: якщо у 2023 році їх кількість становила близько 800, то на початок 2025 року простір об'єднує понад 1522 компанії. Серед резидентів представлені як глобальні аутсорсингові гіганти (GlobalLogic, EPAM, SoftServe, Ciklum), так і продуктові компанії (Monobank, Ajax Systems) та стартапи у сфері DefenseTech.

Фіскальна ефективність режиму Дія.City також підтверджується статистичними даними. У 2024 році резиденти сплатили до зведеного бюджету понад 18 млрд грн податків, що є рекордним показником за весь час існування режиму. Структура надходжень свідчить, що більше половини (51%) складає податок на доходи фізичних осіб та військовий збір, що підкреслює роль високих заробітних плат в IT-секторі як джерела наповнення бюджету. Запровадження спеціальних умов оподаткування (податок на виведений капітал, знижені ставки ПДФО) дозволило значною мірою детінізувати доходи в галузі та забезпечити стабільність податкових надходжень навіть в умовах скорочення експортної виручки.

Аналіз фінансування процесів цифровізації виявляє змішану модель, що поєднує бюджетні асигнування та значні обсяги міжнародної технічної та фінансової допомоги. Видатки Державного бюджету України за бюджетною програмою КПКВК 2901030 «Електронне урядування» є індикатором державних пріоритетів. У 2024 році на цифрову трансформацію було виділено

2,5 млрд грн, що дозволило забезпечити функціонування базових реєстрів, розвиток порталу «Дія» та системи «Трембіта». На 2025 рік заплановано збільшення бюджету Міністерства цифрової трансформації на понад 60%, що відображає розширення повноважень відомства, зокрема у сферах інновацій, освіти та оборонних технологій.

Водночас, лєвова частка інвестицій у розвиток нових сервісів та інфраструктури надходить від міжнародних партнерів. Проєкти USAID / UK aid «Прозорість та підзвітність у державному управлінні та послугах» (TAPAS) та «Підтримка цифрової трансформації» (DTA), програма «EGOV4UKRAINE» (U-LEAD with Europe) та проєкт «DIA Support» (Швеція, ПРООН) забезпечують фінансування розробки програмного забезпечення, закупівлі обладнання та експертної підтримки.

Стратегічно важливим кроком стало приєднання України до програми Європейського Союзу «Цифрова Європа» (Digital Europe) у 2022 році із загальним бюджетом 6 млрд євро. У 2024 році Верховна Рада ратифікувала угоду, яка звільняє Україну від сплати членських внесків, що відкриває українським підприємствам та державним установам безбар'єрний доступ до грантового фінансування проєктів у сферах високопродуктивних обчислень, штучного інтелекту та цифрових навичок. Це створює унікальні можливості для ДП «ДІЯ» щодо залучення ресурсів ЄС для модернізації власної інфраструктури та інтеграції в європейський цифровий простір.

Загальний обсяг міжнародної допомоги Україні у 2024 році перевищив 41 млрд дол. США. Хоча більша частина цих коштів спрямовується на макрофінансову стабільність та оборону, значні суми (через механізми Світового банку, такі як проєкт PEACE) використовуються для виплати заробітних плат працівникам державного сектору, включаючи фахівців, задіяних у цифровізації.

Повномасштабна війна докорінно змінила пріоритети розвитку цифрової сфери, вивівши на перший план питання безпеки та стійкості (resilience). Кількість кібератак на інформаційну інфраструктуру України зростає з кожним

роком. За даними урядової команди реагування CERT-UA, у 2024 році кількість зареєстрованих кіберінцидентів зростає на 70% порівняно з попереднім роком, перевищивши 4300 випадків. Основними цілями ворожих хакерських угруповань є державні органи, об'єкти енергетики, телекомунікації та логістика. Характер атак еволюціонував від масових DDoS-атак до складних цільових операцій (APT), спрямованих на шпигунство, знищення даних та дестабілізацію критичної інфраструктури.

Відповіддю на ці загрози стала побудова ешелонованої системи кіберзахисту. Критично важливим рішенням, прийнятим у перші дні вторгнення, стала легалізація використання хмарних технологій для розміщення державних інформаційних ресурсів. Зміни до Закону України «Про хмарні послуги» дозволили провести безпрецедентну за масштабами міграцію державних реєстрів у закордонні хмарні сховища (AWS, Microsoft Azure, Google Cloud), що убезпечило дані від фізичного знищення внаслідок ракетних обстрілів дата-центрів на території України.

Іншим аспектом стійкості стало забезпечення зв'язку. Розгортання мережі супутникового інтернету Starlink, яка налічує понад 47 тисяч терміналів (значна частина з яких використовується для потреб критичної інфраструктури та відновлення зв'язку на деокупованих територіях), створило резервний канал комунікації, незалежний від наземних мереж. Цей фактор є критичним для забезпечення безперервності надання державних послуг ДП «ДІА» в умовах блекаутів та пошкодження телекомунікаційних мереж.

Війна також стимулювала виникнення нового сегменту IT-ринку – DefenseTech (військові технології). Створення кластеру Brave1 дозволило консолідувати зусилля держави, бізнесу та волонтерів для розробки інноваційних рішень для фронту. У 2024 році оборонні компанії увійшли до лідерів за доходами серед резидентів Дія.City, що свідчить про переорієнтацію частини технологічного сектору на потреби оборони.

Для систематизації факторів зовнішнього середовища, що впливають на формування системи економічної безпеки ДП «ДІА», проведено PEST-аналіз,

результати якого узагальнено в табл. 2.2.

Таблиця 2.2

**PEST-аналіз розвитку сфери цифровізації та державних електронних послуг в Україні (станом на 2024-2025 рр.)**

| Фактори                             | Фактори впливу                                                                                                                                                                                                                                                                                                                                                                                                                                        | Характер впливу на ДП «ДІЯ»                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P – Political<br>(Політичні)        | <p>1. Гармонізація законодавства з нормами ЄС (Digital Services Act, eIDAS, GDPR). Визнання українських цифрових підписів та документів у ЄС.</p> <p>2. Реалізація стратегії інновацій WINWIN 2030, пріоритетність цифровізації (Мінцифра).</p> <p>3. Обмеження доступу до публічних реєстрів, особливий режим регулювання інформаційної безпеки.</p> <p>4. Політична воля країн-партнерів (G7, ЄС) продовжувати фінансування цифрової стійкості.</p> | <p>Позитивний: Розширення ринків збуту послуг (експорт «Дії»), доступ до європейських програм фінансування.</p> <p>Негативний: Ризики зміни політичних пріоритетів, залежність від зовнішньої політичної кон'юнктури.</p> <p>Висновок: Політичне середовище сприяє розвитку, але вимагає суворого дотримання безпекових протоколів.</p>                                  |
| E – Economic<br>(Економічні)        | <p>1. Дефіцит держбюджету, інфляція, ризики девальвації гривні.</p> <p>2. Реалізація Національної стратегії доходів до 2030 р., потенційне підвищення податків для ФОП (ризик тінізації ІТ).</p> <p>3. Доступність грантів Digital Europe, Horizon Europe. Зменшення валютної виручки від ІТ-експорту.</p> <p>4. Функціонування режиму Дія.City як гарантії стабільності для інвесторів.</p>                                                          | <p>Позитивний: Можливість залучення донорських коштів для капітальних інвестицій.</p> <p>Негативний: Зростання вартості обладнання та ліцензій (валютна складова), ризик скорочення бюджетного фінансування програми «Електронне урядування».</p> <p>Висновок: Висока залежність від зовнішнього фінансування створює загрози для фінансової автономії підприємства.</p> |
| S – Social<br>(Соціальні)           | <p>1. Відтік кваліфікованих кадрів за кордон, мобілізація фахівців, дефіцит senior-розробників.</p> <p>2. Високий рівень адаптації населення до цифрових послуг (23 млн користувачів), попит на онлайн-сервіси.</p> <p>3. Скорочення населення, старіння нації, необхідність інклюзивності сервісів.</p> <p>4. Довіра до цифрових документів як безальтернативного інструменту в умовах війни (єВідновлення, ВПО).</p>                                | <p>Позитивний: Стабільний попит на послуги підприємства, лояльність користувачів.</p> <p>Негативний: Критичний ризик кадрового голоду, необхідність інвестицій у навчання персоналу та утримання талантів.</p> <p>Висновок: Соціальний запит є драйвером розвитку, але демографічна криза загрожує кадровому потенціалу.</p>                                             |
| T – Technological<br>(Технологічні) | <p>1. Впровадження AI в держпослуги, необхідність регулювання (Біла книга AI), автоматизація процесів.</p> <p>2. Еволюція методів атак (APT, фішинг, атаки на ланцюги постачання), зростання інтенсивності атак (+70%).</p> <p>3. Міграція у хмари, розвиток 5G, використання Starlink.</p> <p>4. Інтеграція військових та цивільних технологій, розвиток дронів та систем ситуаційної обізнаності.</p>                                               | <p>Позитивний: Технологічна модернізація, підвищення ефективності, нові продукти.</p> <p>Негативний: Висока вартість кіберзахисту, постійна гонка озброєнь у кіберпросторі, технологічна залежність від глобальних вендорів.</p> <p>Висновок: Технології є джерелом конкурентних переваг, але вимагають постійних капіталовкладень у безпеку.</p>                        |

Джерело: сформовано автором.

Результати аналізу свідчать, що ключовими викликами для економічної безпеки ДП «ДІА» у найближчій перспективі будуть: необхідність утримання кваліфікованого персоналу в умовах глобальної конкуренції та мобілізації; забезпечення фінансової стійкості при потенційному скороченні донорської підтримки; а також протидія кіберзагрозам, що постійно еволюціонують. Водночас, євроінтеграційний вектор та розвиток режиму Дія.City створюють сприятливе підґрунтя для подальшого зростання. Національна стратегія інновацій WINWIN 2030, затверджена урядом, визначає GovTech та DefenseTech як пріоритетні напрями, що гарантує збереження державної підтримки сектору.

## 2.2. Діагностика фінансово-економічного стану Державного підприємства «ДІА»

Фундаментом системи управління економічною безпекою будь-якого суб'єкта господарювання є його фінансовий стан, оскільки саме фінансова стійкість визначає здатність підприємства протистояти внутрішнім та зовнішнім загрозам. Для об'єктивної оцінки поточного рівня фінансової безпеки ДП «ДІА» доцільно провести комплексний аналіз динаміки основних економічних показників, структури майна та ефективності діяльності за період 2022–2024 років.

Аналіз ключових індикаторів господарської діяльності (табл. 2.3) свідчить про стрімке масштабування діяльності підприємства, що є характерним для ІТ-сектору державного управління в умовах цифровізації економіки.

Таблиця 2.3

### Основні економічні показники діяльності підприємства

| № з/П | Показник                             | 2022 р. | 2023 р. | 2024 р. | Відх. 24 до 23 (+/-) | Відх. 24 до 23 (%) |
|-------|--------------------------------------|---------|---------|---------|----------------------|--------------------|
| 1     | 2                                    | 3       | 4       | 5       | 6                    | 7                  |
| 1     | Чистий дохід, тис. грн.              | 43 584  | 65 102  | 110 737 | +45 635              | +70,1%             |
| 2     | Валовий прибуток (збиток), тис. грн. | (5 300) | 22 355  | 28 309  | +5 954               | +26,6%             |
| 3     | Чистий прибуток, тис. грн.           | (590)   | 9 364   | 7 263   | -2 101               | -22,4%             |

Продовження табл. 2.3

| 1  | 2                                                     | 3       | 4       | 5       | 6        | 7      |
|----|-------------------------------------------------------|---------|---------|---------|----------|--------|
| 4  | Середньорічна вартість активів, тис. грн.             | 311 275 | 479 534 | 650 028 | +170 494 | +35,6% |
| 5  | Середньорічна вартість необоротних активів, тис. грн. | 283 098 | 427 905 | 557 038 | +129 133 | +30,2% |
| 6  | Середньорічна вартість оборотних активів, тис. грн.   | 28 177  | 51 628  | 92 990  | +41 362  | +80,1% |
| 7  | Середньооблікова чисельність працівників, осіб        | 285     | 292     | 346     | +54      | +18,5% |
| 8  | Фондовіддача                                          | 0,44    | 0,40    | 0,45    | +0,05    | +12,5% |
| 9  | Фондомісткість                                        | 2,26    | 2,51    | 2,21    | -0,30    | -11,9% |
| 10 | Фондоозброєність, тис. грн /ос.                       | 345,9   | 561,1   | 707,0   | +145,9   | +26,0% |
| 11 | Продуктивність праці, тис. грн./ос.                   | 152,9   | 222,9   | 320,0   | +97,1    | +43,6% |
| 12 | Коефіцієнт оборотності оборотних активів              | 1,55    | 1,26    | 1,19    | -0,07    | -5,6%  |

Джерело: сформовано автором.

За даними таблиці спостерігається суттєва позитивна динаміка чистого доходу, який у 2024 році зріс на 70,1% порівняно з 2023 роком, досягнувши 110,7 млн грн. Це корелює зі збільшенням середньооблікової чисельності працівників на 18,5% (до 346 осіб) та зростанням продуктивності праці на 43,6%. Такий випереджаючий темп росту продуктивності праці над темпом зростання персоналу є позитивним сигналом з точки зору кадрової безпеки та ефективності використання трудових ресурсів.

Водночас, попри зростання валового прибутку на 26,6%, чистий прибуток підприємства у 2024 році скоротився на 22,4% і склав 7,26 млн грн. Це свідчить про зростання операційних та інших витрат, що потребує детальнішого контролю в системі економічної безпеки. Показники ефективності використання основних засобів демонструють покращення: фондівіддача зросла на 12,5%, а фондомісткість знизилася, що вказує на підвищення ефективності експлуатації необоротних активів, які складають лівову частку майна підприємства.

Наступним етапом є аналіз майнового стану підприємства та джерел його фінансування (табл. 2.4).

Таблиця 2.4

## Характеристика майна підприємства та джерел його формування за балансом

| Показники                            | На<br>31.12.22<br>(тис.<br>грн) | Питома<br>вага<br>(%) | На<br>31.12.23<br>(тис.<br>грн) | Питома<br>вага<br>(%) | На<br>31.12.24<br>(тис.<br>грн) | Питома<br>вага<br>(%) | Відхилення<br>2024 до<br>2023 (+/-) | Відхилення<br>(п.п.) |
|--------------------------------------|---------------------------------|-----------------------|---------------------------------|-----------------------|---------------------------------|-----------------------|-------------------------------------|----------------------|
| <b>АКТИВИ</b>                        | <b>410 126</b>                  | <b>100%</b>           | <b>548 942</b>                  | <b>100%</b>           | <b>751 115</b>                  | <b>100%</b>           | <b>+202 173</b>                     | <b>-</b>             |
| 1. Необоротні активи                 | 376 468                         | 91,8%                 | 479 343                         | 87,3%                 | 634 734                         | 84,5%                 | +155 391                            | -2,8                 |
| <i>в т.ч. основні засоби</i>         | 156 846                         | 38,2%                 | 170 882                         | 31,1%                 | 148 670                         | 19,8%                 | -8 176                              | -11,3                |
| 2. Оборотні активи                   | 33 658                          | 8,2%                  | 69 599                          | 12,7%                 | 116 381                         | 15,5%                 | +46 782                             | +2,8                 |
| <i>в т.ч. запаси</i>                 | 92                              | 0,02%                 | 971                             | 0,2%                  | 763                             | 0,1%                  | -208                                | -0,1                 |
| <i>дебіторська заборгованість</i>    | 1 688                           | 0,4%                  | 1 688                           | 0,3%                  | 5 867                           | 0,8%                  | +4 179                              | +0,5                 |
| <i>грошові кошти</i>                 | 13 901                          | 3,4%                  | 20 642                          | 3,8%                  | 26 078                          | 3,5%                  | +5 436                              | -0,3                 |
| <b>ПАСИВИ</b>                        | <b>410 126</b>                  | <b>100%</b>           | <b>548 942</b>                  | <b>100%</b>           | <b>751 115</b>                  | <b>100%</b>           | <b>+202 173</b>                     | <b>-</b>             |
| 1. Власний капітал                   | 143 073                         | 34,9%                 | 268 463                         | 48,9%                 | 428 759                         | 57,1%                 | +160 296                            | +8,2                 |
| <i>в т.ч. зареєстрований капітал</i> | 25 580                          | 6,2%                  | 25 580                          | 4,7%                  | 25 580                          | 3,4%                  | 0                                   | -1,3                 |
| <i>нерозподілений прибуток</i>       | (10 575)                        | -2,6%                 | (8 708)                         | -1,6%                 | (7 256)                         | -1,0%                 | +1 452                              | +0,6                 |
| 2. Довгострокові зобов'язання        | 1 532                           | 0,4%                  | 1 449                           | 0,3%                  | 1 231                           | 0,2%                  | -218                                | -0,1                 |
| 3. Поточні зобов'язання              | 265 521                         | 64,7%                 | 279 030                         | 50,8%                 | 321 125                         | 42,7%                 | +42 095                             | -8,1                 |

Джерело: сформовано автором.

Структурний аналіз активів (табл. 2.4) виявив домінування необоротних активів, частка яких на кінець 2024 року становила 84,5%. Абсолютне зростання валюти балансу на 202 млн грн у 2024 році відбулося переважно за рахунок збільшення вартості основних засобів та нематеріальних активів, що є логічним для технологічного підприємства, яке нарощує цифрову інфраструктуру.

У структурі пасивів позитивною тенденцією є зростання частки власного капіталу з 34,9% у 2022 році до 57,1% у 2024 році, що значно підвищує фінансову автономність ДП «ДІЯ». Варто зауважити, що левову частку поточних зобов'язань (які складають 42,7% пасивів) становлять «Доходи майбутніх періодів» (рядок 1665 балансу). Ця стаття відображає цільове фінансування, яке поступово визнається доходом, а не класичну кредиторську заборгованість, що суттєво знижує реальні ризики втрати платоспроможності,

попри формально високий рівень короткострокових зобов'язань.

Деталізація формування фінансового результату (табл. 2.5) дозволяє виявити слабкі місця в управлінні прибутковістю.

Таблиця 2.5

Механізм формування фінансових результатів діяльності підприємства

| Показники                             | 2022 р.   | 2023 р.   | 2024 р.   | Відхилення<br>2024 до 2023<br>(+/-) | Відхилення<br>2024 до 2023<br>(%) |
|---------------------------------------|-----------|-----------|-----------|-------------------------------------|-----------------------------------|
| Чистий дохід від реалізації продукції | 43 584    | 65 102    | 110 737   | +45 635                             | +70,1%                            |
| Собівартість реалізованої продукції   | (48 884)  | (42 747)  | (82 428)  | -39 681                             | +92,8%                            |
| Валовий: прибуток (збиток)            | (5 300)   | 22 355    | 28 309    | +5 954                              | +26,6%                            |
| Інші операційні доходи                | 276 854   | 365 599   | 587 667   | +222 068                            | +60,7%                            |
| Адміністративні витрати               | (44 429)  | (50 294)  | (67 371)  | -17 077                             | +33,9%                            |
| Витрати на збут                       | (81)      | (103)     | (82)      | +21                                 | -20,4%                            |
| Інші операційні витрати               | (259 077) | (402 615) | (662 359) | -259 744                            | +64,5%                            |
| Фін. результат від опер. діяльності   | (32 033)  | (65 058)  | (113 836) | -48 778                             | +75,0%                            |
| Фін. результат до оподаткування       | (590)     | 11 173    | 9 141     | -2 032                              | -18,2%                            |
| Чистий фінансовий результат           | (590)     | 9 364     | 7 263     | -2 101                              | -22,4%                            |

Джерело: сформовано автором.

Аналіз табл. 2.5 показує, що темпи зростання собівартості (+92,8%) суттєво перевищують темпи зростання чистого доходу (+70,1%), що є тривожним сигналом для економічної безпеки в аспекті управління витратами. Специфіка діяльності ДП «ДІЯ» передбачає значний обсяг «Інших операційних доходів» (587,6 млн грн у 2024 році) та кореспондуючих з ними «Інших операційних витрат» (662,3 млн грн), що пов'язано з освоєнням бюджетного фінансування та грантових коштів. Від'ємний операційний результат (-113,8 млн грн) перекривається за рахунок інших доходів, що дозволяє підприємству генерувати чистий прибуток, однак така структура доходів створює залежність від зовнішнього фінансування.

Інтегральна оцінка фінансового стану наведена у табл. 2.6.

Таблиця 2.6

## Механізм формування фінансових результатів діяльності підприємства

| Показники                                      | 2022 р.  | 2023 р.  | 2024 р.  | Відхилення 2024 до 2023 (+/-) |
|------------------------------------------------|----------|----------|----------|-------------------------------|
| 1. Коефіцієнт загальної ліквідності            | 0,13     | 0,25     | 0,36     | +0,11                         |
| 2. Коефіцієнт абсолютної ліквідності           | 0,05     | 0,07     | 0,08     | +0,01                         |
| 3. Чистий оборотний капітал, тис. грн          | -231 863 | -209 431 | -204 744 | +4 687                        |
| 4. Коефіцієнт автономії                        | 0,35     | 0,49     | 0,57     | +0,08                         |
| 5. Коефіцієнт фінансової стабільності          | 0,54     | 0,96     | 1,33     | +0,37                         |
| 6. Коефіцієнт забезпеченості власними засобами | -5,89    | -2,01    | -0,76    | +1,25                         |
| 7. Коефіцієнт оборотності активів              | 0,14     | 0,14     | 0,17     | +0,03                         |
| 8. Коефіцієнт оборотності власного капіталу    | 0,35     | 0,32     | 0,32     | 0,00                          |
| 9. Рентабельність госп. діяльності, %          | -1,35%   | 14,38%   | 6,56%    | -7,82 п.п.                    |
| 10. Рентабельність власного капіталу, %        | -0,48%   | 4,55%    | 2,08%    | -2,47 п.п.                    |
| 11. Рентабельність продукції, %                | -10,84%  | 52,30%   | 34,34%   | -17,96 п.п.                   |

Джерело: сформовано автором.

Показники ліквідності ДП «ДІЯ» формально знаходяться значно нижче нормативних значень (коефіцієнт загальної ліквідності у 2024 році склав 0,36 при нормі  $>1$ ). Однак, в контексті економічної безпеки це не слід трактувати як критичну загрозу банкрутства. Як було зазначено при аналізі балансу, значна частина поточних зобов'язань – це доходи майбутніх періодів, які не вимагають погашення грошовими коштами. Динаміка показників ліквідності є позитивною (+0,11 п.п.), що свідчить про поступове зміцнення платіжної дисципліни.

Коефіцієнт автономії досяг рівня 0,57, що відповідає оптимальним значенням ( $>0,5$ ) і підтверджує, що підприємство більше ніж на половину фінансується за рахунок власних джерел. Це є ключовим фактором фінансової стійкості. Водночас спостерігається зниження показників рентабельності у 2024 році порівняно з піковим 2023 роком (рентабельність продукції знизилася на 17,96 в.п.), що актуалізує необхідність впровадження заходів з оптимізації

собівартості та підвищення операційної ефективності в системі управління економічною безпекою ДП «ДІА».

Таким чином, діагностика виявила, що фінансово-економічний стан підприємства є стабільним та характеризується розширенням діяльності, проте існують латентні загрози, пов'язані з ефективністю витрат та специфікою структури зобов'язань.

### **2.3. Оцінка існуючої системи управління економічною безпекою Державного підприємства «ДІА»**

Проведення аналітичної оцінки стану управління економічною безпекою Державного підприємства «ДІА» вимагає застосування комплексного, системного підходу, що зумовлено специфікою діяльності об'єкта дослідження. Як адміністратор Єдиного державного веб-порталу електронних послуг та ключовий елемент цифрової інфраструктури держави, ДП «ДІА» функціонує в умовах підвищених ризиків, де межі між економічною, інформаційною та національною безпекою є максимально розмитими. Відповідно до методичних рекомендацій щодо написання магістерських кваліфікаційних робіт, даний підрозділ магістерського дослідження присвячений глибокому аналізу наявних механізмів, інструментів та процедур, за допомогою яких підприємство забезпечує захист своїх економічних інтересів та сталість розвитку.

Метою цього етапу дослідження є не лише констатація наявного стану справ, але й ідентифікація глибинних причинно-наслідкових зв'язків, що формують архітектуру безпеки підприємства. Ми виходимо з гіпотези, що економічна безпека ДП «ДІА» є похідною від ефективності його управлінських бізнес-процесів, здатності адаптуватися до турбулентного зовнішнього середовища та рівня захищеності його ключового активу – інформаційних ресурсів та довіри користувачів.

У процесі оцінювання існуючої системи управління економічною безпекою

(СУЕБ) нами було виокремлено та проаналізовано наступні структурні елементи, які в сукупності формують контур безпеки підприємства:

- 1) організаційно-функціональна структура управління – аналіз суб'єктів управління, розподілу повноважень, відповідальності та каналів комунікації;
- 2) нормативно-регламентне забезпечення – оцінка якості та актуальності внутрішньої документарної бази, що регулює процеси безпеки;
- 3) ресурсне забезпечення – діагностика достатності фінансових, кадрових, технологічних та інформаційних ресурсів для підтримання належного рівня безпеки;
- 4) процесний ландшафт – аудит ключових процесів ідентифікації, оцінки, моніторингу та нейтралізації загроз.

Ефективність будь-якої системи управління першочергово залежить від чіткості побудови її організаційної структури. Аналіз штатного розпису та положень про структурні підрозділи ДП «ДІА» дозволяє класифікувати існуючу систему управління економічною безпекою як ієрархічну, функціонально-орієнтовану модель з елементами матричного управління в частині проектної діяльності.

Суб'єктна структура управління економічною безпекою ДП «ДІА» може бути декомпозована на три рівні, кожен з яких виконує специфічні функції та несе відповідну частку відповідальності.

Стратегічний рівень (вище керівництво). На цьому рівні знаходяться Генеральний директор підприємства та його заступники. Їхня роль у системі економічної безпеки є визначальною, оскільки саме тут формується «ідеологія» безпеки та задаються вектори розвитку.

Функціонал передбачає затвердження Стратегії розвитку підприємства, яка включає безпековий компонент; прийняття рішень щодо алокації значних обсягів ресурсів на модернізацію інфраструктури; координація взаємодії з Міністерством цифрової трансформації України та іншими органами державної влади; кризовий менеджмент у випадку загроз національного масштабу.

Сильною стороною управління на цьому рівні є висока залученість

керівництва у питання цифрової трансформації, що автоматично піднімає питання безпеки на найвищий пріоритет. Однак, існує ризик перевантаження стратегічного менеджменту операційними питаннями, особливо в умовах воєнного стану, що може призводити до ситуативних, реактивних рішень замість системних проактивних дій.

Тактичний рівень (функціональні департаменти та служби). Ядром системи управління економічною безпекою виступають профільні підрозділи, які забезпечують реалізацію політики безпеки у повсякденній діяльності. До ключових суб'єктів цього рівня віднесено:

1. Фінансовий департамент, який виступає гарантом фінансової складової безпеки. Його завданням є бюджетування, контроль витрат, управління ліквідністю, моніторинг дебіторської заборгованості, взаємодія з Державною казначейською службою. Система управління фінансами побудована за жорсткою централізованою моделлю, характерною для державного сектору. Це забезпечує високий рівень контролю за цільовим використанням коштів (що є позитивним для безпеки), але суттєво знижує гнучкість та оперативність фінансування невідкладних потреб, що є критичним недоліком в умовах кібервійни.

2. Юридичний департамент, який забезпечує правову безпеку. Перед ним ставлять завдання з договірної роботи, претензійно-позовної діяльності, моніторингу законодавчих змін, захисту інтелектуальної власності. Юридична служба ДП «ДІА» функціонує в умовах надзвичайної динаміки нормативного поля. Висока ефективність цього підрозділу є критичною умовою легітимності функціонування цифрових сервісів. Аналіз показує високий рівень компетенції юристів, проте навантаження на підрозділ є надмірним, що створює ризики пропуску окремих правових нюансів у договорах з численними контрагентами.

3. Служба інформаційної безпеки. Головна роль – технічний захист інформації, управління доступами, моніторинг інцидентів (SOC), відповідність стандартам КСЗІ (комплексна система захисту інформації). Даний підрозділ фактично виконує левову частку роботи із забезпечення економічної безпеки,

оскільки для ІТ-підприємства втрата даних дорівнює втраті активів. Спостерігається високий рівень технічного оснащення та професіоналізму. Втім, інтеграція технічних метрик безпеки в загальноекономічні показники підприємства залишається недостатньою. Часто витрати на кібербезпеку розглядаються як «технічна необхідність», а не як інвестиція в капіталізацію бренду.

4. HR-департамент. Займається підбором персоналу, перевіркою кандидатів (background checks), адаптацією, мотивації, управлінням плинністю кадрів. В умовах дефіциту кваліфікованих ІТ-фахівців та конкуренції з приватним сектором, роль HR у кадровій безпеці є критичною. Існуюча система перевірки кандидатів є надійною, але система утримання талантів (retention) обмежена рамками фонду оплати праці державного підприємства, що створює постійну загрозу «відтоку мізків».

Операційний рівень (лінійні виконавці). До цього рівня відносяться всі співробітники підприємства, які у своїй щоденній роботі повинні дотримуватися правил та політик безпеки. Тут криється найбільший ризик «людського фактору» – незважаючи на регулярні інструктажі та тренінги, ймовірність ненавмисних помилок (фішинг, слабкі паролі, порушення регламентів обробки даних) залишається актуальною.

Аналіз комунікаційних зв'язків між суб'єктами управління свідчить про наявність певних розривів. Часто фінансова логіка (економія коштів) вступає в конфлікт з логікою інформаційної безпеки (необхідність закупівлі дороговартісного ПЗ). Відсутність єдиного координаційного центру, який би балансував ці інтереси саме з точки зору економічної ефективності безпеки, призводить до затягування процесів прийняття рішень.

В табл. 2.7 наведено матрицю розподілу відповідальності за ключові складові економічної безпеки, що дозволяє візуалізувати зони перетину та потенційні конфлікти інтересів.

Таблиця 2.7

Матриця розподілу відповідальності за складові  
економічної безпеки ДП «ДІЯ»\*

| Складова безпеки     | Генеральний директор | Фін. директор | Керівник з ІТ | Головний юрисконсульт | HR-директор | Служба безпеки |
|----------------------|----------------------|---------------|---------------|-----------------------|-------------|----------------|
| Фінансова            | <b>З</b>             | <b>В</b>      | <b>У</b>      | <b>К</b>              | <b>І</b>    | <b>К</b>       |
| Інформаційна         | <b>З</b>             | <b>П</b>      | <b>В</b>      | <b>П</b>              | <b>І</b>    | <b>К</b>       |
| Кадрова              | <b>З</b>             | <b>П</b>      | <b>У</b>      | <b>П</b>              | <b>В</b>    | <b>К</b>       |
| Правова              | <b>З</b>             | <b>У</b>      | <b>У</b>      | <b>В</b>              | <b>У</b>    | <b>У</b>       |
| Техніко-технологічна | <b>З</b>             | <b>П</b>      | <b>В</b>      | <b>У</b>              | <b>-</b>    | <b>К</b>       |
| Інтелектуальна       | <b>З</b>             | <b>У</b>      | <b>В</b>      | <b>П</b>              | <b>П</b>    | <b>К</b>       |

\***В** – виконавець (несе основну відповідальність); **З** – затверджує рішення; **П** – погоджує; **У** – бере участь; **К** – контролює; **І** – інформується.

Джерело: сформовано автором.

Як видно з таблиці, існує чіткий розподіл виконавців, проте функція контролю (К) часто розпорошена між різними підрозділами або дублюється, що може призводити до розмивання відповідальності за кінцевий результат.

Фундаментом системи управління економічною безпекою є нормативна база. Для ДП «ДІЯ» вона має дворівневу структуру: зовнішню (законодавство України) та внутрішню (локальні акти).

Діяльність підприємства жорстко регламентована Законами України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про публічні електронні реєстри», «Про захист персональних даних», а також постановами Кабінету Міністрів України, що регулюють функціонування порталу «Дія». Жорстка регламентація створює правову визначеність, але водночас робить систему інертною. Будь-яка зміна в бізнес-процесах вимагає внесення змін до нормативних актів, що займає час. Це створює загрозу відставання від темпів розвитку технологічних загроз.

На підприємстві розроблено та впроваджено пакет внутрішніх документів, що регулюють питання безпеки:

1. Політика інформаційної безпеки – базовий документ, що визначає цілі та принципи захисту даних. Аналіз тексту документа свідчить про його

відповідність стандартам серії ISO/IEC 27000.

2. Положення про комерційну таємницю та конфіденційну інформацію – визначає перелік відомостей, що не підлягають розголошенню. Враховуючи статус державного підприємства, значна частина інформації є публічною, проте технологічні ноу-хау та архітектура систем надійно захищені.

3. Регламенти бізнес-процесів (SOPs) – описують алгоритми дій співробітників у стандартних та аварійних ситуаціях.

4. Антикорупційна програма – обов’язковий елемент для державного підприємства, спрямований на мінімізацію ризиків внутрішнього шахрайства та корупції.

Аналіз показав, що частина внутрішніх інструкцій носить формальний характер або перевантажена технічними деталями, що ускладнює їх сприйняття нетехнічним персоналом. Крім того, процедури оновлення регламентів іноді не встигають за змінами в організаційній структурі або впровадженням нових програмних продуктів.

Для глибокого розуміння стану управління доцільно провести декомпозицію системи на окремі функціональні складові та оцінити стан кожної з них.

Фінансова безпека ДП «ДІА» має специфічний характер, відмінний від класичних комерційних підприємств. Основною метою тут є не максимізація прибутку, а забезпечення безперебійного фінансування статутної діяльності та ефективне використання ресурсів.

Основним джерелом надходжень є державний бюджет (через програми інформатизації) та кошти міжнародної технічної допомоги (гранти). Висока частка бюджетного фінансування (понад 70-80% у структурі надходжень) робить підприємство вразливим до макроекономічних шоків та політичних рішень щодо секвестру бюджету. Будь-яка затримка казначейських платежів автоматично створює касові розриви, що загрожує своєчасній виплаті заробітної плати та оплаті послуг хостингу/хмарних сервісів.

Підприємство успішно диверсифікує джерела за рахунок проектів донорів

(USAID, TAPAS тощо). Це підвищує фінансову стійкість, але вимагає складних процедур звітності та комплаєнсу, що створює додаткове навантаження на адміністративний персонал.

Дослідження фінансової звітності за останні три роки (пункт 2.2 дипломної роботи) демонструє наступні тенденції, важливі для безпеки:

1) показники поточної ліквідності знаходяться в межах норми, але мають тенденцію до зниження в кінці бюджетних періодів;

2) коефіцієнт автономії є високим, оскільки підприємство не залучає банківські кредити, фінансуючи капітальні інвестиції за рахунок цільових внесків, що мінімізує ризики банкрутства, але обмежує можливості швидкого масштабування;

3) планово-збиткова або низькорентабельна діяльність (характерна для держсектору) не дозволяє формувати значні власні резервні фонди безпеки.

Стан управління оцінюється як задовільний. Головною проблемою є відсутність фінансової гнучкості та залежність від зовнішніх факторів, на які менеджмент підприємства має обмежений вплив.

Інформаційна та кібернетична складова – найбільш розвинена та критично важлива частина системи економічної безпеки ДП «ДІА». Будь-який інцидент тут (витік даних, недоступність сервісу) має миттєві катастрофічні наслідки для репутації та економіки. Управління цією складовою базується на ешелонованому захисті (Defense in Depth) (табл. 2.8).

Таблиця 2.8

#### Управління інформаційною та кібернетичною складовою

| Складова системи захисту | Завдання складової                                                                                                                                                                   |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Захист периметру         | Використання промислових рішень для захисту від DDoS-атак, міжмережевих екранів (WAF), систем виявлення вторгнень (IDS/IPS).                                                         |
| Безпека додатків         | Впровадження методології DevSecOps, де безпека інтегрована в процес розробки (CI/CD pipeline). Регулярне проведення статичного (SAST) та динамічного (DAST) аналізу коду.            |
| Моніторинг               | Функціонування ситуаційного центру (SOC), що забезпечує цілодобовий моніторинг подій безпеки та реагування на інциденти.                                                             |
| Bug Bounty               | Унікальною практикою для держпідприємства є залучення спільноти етичних хакерів для пошуку вразливостей за винагороду. Це свідчить про високу зрілість процесів управління безпекою. |

Джерело: сформовано автором.

Незважаючи на постійні кібератаки з боку ворожих країн (що особливо актуалізувалося з 2022 року), система демонструє високу стійкість. Портал «Дія» витримує навантаження, які вивели б з ладу більшість комерційних систем. Це свідчить про високий рівень управління цією складовою.

Але лишаються й проблемні аспекти. «Дія» інтегрується з десятками державних реєстрів, рівень захисту яких може бути нижчим. Злам будь-якого підключеного реєстру створює ризики для екосистеми в цілому. Ліцензії на провідні світові рішення безпеки номіновані у валюті, що створює валютні ризики для бюджету підприємства.

Інтелектуальний капітал є основним активом ДП «ДІА». Економічна безпека прямо залежить від здатності залучати та утримувати висококласних фахівців. Процедури рекрутингу включають перевірку доброчесності, що відсіює потенційних інсайдерів. Система оплати праці на ДП «ДІА» є конкурентною порівняно з держслужбою, але все ще відстає від топових позицій в аутсорсингових ІТ-компаніях, що створює ризик переманювання ключових архітекторів та розробників. Інвестування в навчання персоналу є частиною стратегії, але водночас підвищує вартість фахівця на ринку, збільшуючи ризик його втрати.

Висока ідейна мотивація («цифровізація країни») є потужним фактором утримання персоналу. Однак емоційне вигорання через надвисокий темп роботи та відповідальність є серйозною загрозою кадрової безпеки. Втрата ключового розробника може загальмувати проект на місяці, що має прямий економічний вимір збитків. Стан управління оцінюється як достатній, але з тенденцією до погіршення ризиків через дисбаланс ринку праці та бюджетні обмеження.

Техніко-технологічна складова охоплює матеріально-технічну базу (сервери, робочі станції, мережеве обладнання) та технологічні платформи. ДП «ДІА» оперує сучасною інфраструктурою, значна частина якої мігрувала в хмарні середовища (Cloud) для забезпечення відмовостійкості під час війни. Це стратегічно вірне рішення з точки зору безпеки (фізичне знищення дата-центру

в Україні не зупинить роботу системи).

Серед існуючих ризиків – залежність від конкретних постачальників хмарних послуг та обладнання. Якщо інфраструктура серверів оновлюється, то робочі станції співробітників можуть застарівати швидше, що створює технічні незручності та ризики безпеки (непідтримувані ОС).

Для формалізації оцінки рівня економічної безпеки (табл. 2.9) використаємо методику бального оцінювання за ключовими параметрами системи управління. Оцінка проводиться за 5-бальною шкалою, де:

- 1 – критичний рівень (управління відсутнє або неефективне);
- 2 – низький рівень (фрагментарне управління);
- 3 – середній рівень (базові процеси налагоджені, але є збої);
- 4 – високий рівень (системне управління, дрібні недоліки);
- 5 – відмінний рівень (еталонне управління, постійне вдосконалення).

Таблиця 2.9

Оцінка ефективності підсистем  
управління економічною безпекою ДП «ДІА»

| Підсистема безпеки | Критерії оцінювання                                                    | Оцінка | Обґрунтування                                                                        |
|--------------------|------------------------------------------------------------------------|--------|--------------------------------------------------------------------------------------|
| 1                  | 2                                                                      | 3      | 4                                                                                    |
| Фінансова          | Гнучкість бюджетування, ліквідність, диверсифікація джерел             | 3.5    | Жорсткі бюджетні рамки, залежність від держзамовлення, складні процедури закупівель. |
| Інформаційна       | Захищеність периметру, моніторинг інцидентів, відповідність стандартам | 4.8    | Впровадження передових технологій, ефективний SOC, успішна протидія атакам.          |
| Кадрова            | Плинність кадрів, рівень компетенцій, лояльність                       | 4.0    | Високий професіоналізм, але високі ризики вигорання та переманювання.                |
| Правова            | Якість договорів, претензійна робота, комплаєнс                        | 4.5    | Сильна юридична команда, високий рівень правового захисту інтересів.                 |
| Інтерфейсна        | Задоволеність користувачів, стабільність роботи сервісів, Support      | 4.2    | Висока орієнтація на клієнта, якісний UX/UI, швидка реакція підтримки.               |

Продовження табл. 2.9

| 1                         | 2                                                           | 3           | 4                                                                    |
|---------------------------|-------------------------------------------------------------|-------------|----------------------------------------------------------------------|
| Організаційна             | Чіткість структури, швидкість прийняття рішень, координація | 3.8         | Іноді спостерігається бюрократизація процесів та дублювання функцій. |
| <b>Інтегральна оцінка</b> | <b>(Середнє арифметичне)</b>                                | <b>4.13</b> | <b>Високий рівень</b>                                                |

Джерело: сформовано автором.

Інтегральний показник 4.13 свідчить про те, що система управління економічною безпекою ДП «ДІА» знаходиться на високому рівні розвитку. Вона є зрілою, технологічною та адаптивною. Однак, існує дисбаланс між високорозвиненою технічною/інформаційною складовою та більш консервативною фінансово-організаційною складовою, що характерно для державних підприємств. Для систематизації виявлених факторів внутрішнього та зовнішнього середовища, що впливають на стан економічної безпеки, проведено SWOT-аналіз (табл. 2.10).

Таблиця 2.10

### SWOT-аналіз

існуючої системи управління економічною безпекою ДП «ДІА»

| <i>Сильні сторони (Strengths)</i>                                                                                                                                                                                                                                                                                                                     | <i>Слабкі сторони (Weaknesses)</i>                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Потужна технологічна інфраструктура та використання хмарних рішень.<br>2. Висококваліфікована команда та сильний HR-бренд.<br>3. Ефективна система моніторингу кіберзагроз (SOC).<br>4. Підтримка на рівні вищого керівництва держави.<br>5. Успішний досвід залучення міжнародних донорів.<br>6. Високий рівень цифровізації внутрішніх процесів. | 1. Залежність від державного фінансування та бюджетних циклів.<br>2. Бюрократизовані процедури прийняття рішень (порівняно з приватним ІТ).<br>3. Обмежені можливості фінансової мотивації персоналу.<br>4. Складність інтеграції з застарілими системами інших відомств.<br>5. Відсутність сформованих резервних фінансових фондів. |
| 1. Комерціалізація сервісів для бізнесу (API, валідація) для генерації власного доходу.<br>2. Експорт продукту «Дія» в інші країни (посилення бренду та доходів).<br>3. Поглиблення співпраці з світовими технологічними гігантами (Microsoft, Amazon, Google).<br>4. Автоматизація процесів комплаєнсу та аудиту.                                    | 1. Цілеспрямовані кібератаки та фізичне знищення інфраструктури ворогом.<br>2. Зменшення бюджетного фінансування через економічну кризу.<br>3. Відтік кадрів за кордон або в приватний сектор.<br>4. Зміни в законодавстві, що можуть ускладнити діяльність.<br>5. Репутаційні атаки та дезінформаційні кампанії.                    |

Джерело: сформовано автором.

Стратегія SO (сила-можливості) – використання технологічної експертизи (S1) та підтримки держави (S4) для експорту рішень (O2), що дозволить отримати додаткові ресурси для фінансування безпеки.

Стратегія WT (слабкість-загрози) – найбільш небезпечним є поєднання залежності від бюджету (W1) та загрози його скорочення (T2). Для нейтралізації цього ризику необхідно терміново розвивати напрямок комерціалізації послуг (O1) для створення «подушки безпеки».

На основі проведеного аналізу можна виокремити ключові проблеми існуючої системи управління економічною безпекою ДП «ДІЯ», які потребують вирішення. По-перше, система орієнтована на обслуговування поточних потреб («освоєння бюджету»), а не на стратегічне інвестування в безпеку з розрахунком ROI (повернення інвестицій). Відсутні механізми швидкого реагування на фінансові форс-мажори без проходження тривалих бюрократичних процедур погодження змін до фінплану. По-друге, ДП «ДІЯ» має високий рівень захисту, але інтегрується з реєстрами, власники яких (інші ДП, міністерства) часто не мають ресурсів для забезпечення аналогічного рівня. Це створює вразливості, якими ДП «ДІЯ» не може керувати напряму, але несе відповідальність за наслідки.

Крім того, висока інтенсивність праці, характерна для стартап-культури, в умовах довготривалого стресу війни стає фактором ризику. Система управління безпекою праці та психологічним станом співробітників потребує вдосконалення. Також на підприємстві чудово працює управління ІТ-ризиками, але управління сукупним економічним ризиком (де поєднані фінанси, кадри, право, технології) часто здійснюється інтуїтивно на рівні топ-менеджменту, а не як системний регулярний процес.

Встановлені проблеми свідчать про те, що незважаючи на високий технологічний рівень, організаційно-економічний механізм управління безпекою потребує трансформації. Перехід від моделі «Захист інформації» до моделі «Комплексна економічна стійкість» має стати вектором подальшого розвитку системи.

## Висновки до Розділу 2

Проведений аналіз дозволяє зробити висновок, що сфера цифровізації та державних електронних послуг в Україні досягла високого рівня інституційної зрілості та технологічної стійкості. Вона трансформувалася з допоміжної функції у стратегічний ресурс держави, здатний забезпечувати функціонування державних інституцій в екстремальних умовах. Для ДП «ДІА» це означає перехід до нової моделі управління економічною безпекою, яка базується не лише на захисті активів, але й на проактивному управлінні ризиками, інтеграції в європейську екосистему та постійному інноваційному розвитку.

Проведена діагностика фінансово-економічного стану ДП «ДІА» за 2022–2024 роки дозволяє констатувати, що підприємство перебуває на стадії активного масштабування, про що свідчить стрімке зростання валюти балансу, чистого доходу та кадрового потенціалу. Попри позитивну динаміку показників ділової активності та досягнення високого рівня фінансової автономії, аналіз виявив низку структурних диспропорцій, які формують латентні загрози економічній безпеці. Ключовим ризиком є випереджаюче зростання собівартості та інших операційних витрат порівняно з темпами збільшення доходів, що призвело до зниження рентабельності у звітному періоді та вказує на необхідність оптимізації видаткової частини. Низькі нормативні значення коефіцієнтів ліквідності компенсуються специфікою фінансування через механізм доходів майбутніх періодів, що нівелює ризики реального банкрутства, проте висока залежність від зовнішніх цільових надходжень вимагає впровадження механізмів стратегічного контролінгу. Таким чином, поточний стан підприємства можна охарактеризувати як фінансово стійкий, але такий, що потребує переходу від екстенсивного нарощування ресурсів до інтенсивного управління ефективністю для зміцнення фінансової складової економічної безпеки.

Проведена аналітична оцінка дозволяє стверджувати, що система управління економічною безпекою ДП «ДІА» є сучасною, технологічною та

такою, що відповідає викликам часу. Вона базується на пріоритеті інформаційної безпеки, що є цілком виправданим для ІТ-підприємства. Інтегральний показник ефективності системи складає 4.13 бала за 5-бальною шкалою.

Водночас, виявлено ряд системних недоліків, що криються переважно в площині фінансової залежності від державного бюджету, бюрократичної інерції та кадрових ризиків. Існуюча архітектура безпеки ефективно протидіє зовнішнім технічним загрозам, але є менш стійкою до внутрішніх ресурсних дефіцитів та організаційних дисбалансів.

Результати оцінки, отримані в цьому розділі, формують емпіричне підґрунтя для розробки рекомендацій у третьому розділі магістерської роботи, які мають бути спрямовані на диверсифікацію джерел фінансування безпеки, впровадження системного ризик-менеджменту та удосконалення механізмів мотивації персоналу як головного носія інтелектуального капіталу підприємства.

Проведена аналітична оцінка дозволяє стверджувати, що система управління економічною безпекою ДП «ДІА» є сучасною, технологічною та такою, що відповідає викликам часу. Вона базується на пріоритеті інформаційної безпеки, що є цілком виправданим для ІТ-підприємства. Інтегральний показник ефективності системи складає 4.13 бала за 5-бальною шкалою.

Водночас, виявлено ряд системних недоліків, що криються переважно в площині фінансової залежності від державного бюджету, бюрократичної інерції та кадрових ризиків. Існуюча архітектура безпеки ефективно протидіє зовнішнім технічним загрозам, але є менш стійкою до внутрішніх ресурсних дефіцитів та організаційних дисбалансів.

Результати оцінки, отримані в цьому розділі, формують емпіричне підґрунтя для розробки рекомендацій у третьому розділі магістерської роботи, які мають бути спрямовані на диверсифікацію джерел фінансування безпеки, впровадження системного ризик-менеджменту та удосконалення механізмів

мотивації персоналу як головного носія інтелектуального капіталу підприємства.

## **РОЗДІЛ 3**

### **НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ДП «ДІЯ»**

#### **3.1. Організаційно-методичні засади удосконалення системи управління економічною безпекою підприємства**

У сучасних умовах цифрової трансформації національної економіки, забезпечення стійкого розвитку стратегічних державних підприємств, до яких належить Державне підприємство «ДІЯ», вимагає докорінного перегляду підходів до управління економічною безпекою. Як засвідчили результати аналізу, проведеного у другому розділі магістерської кваліфікаційної роботи, існуюча система захисту економічних інтересів підприємства характеризується фрагментарністю, відсутністю єдиного центру прийняття рішень та переважанням реактивної моделі поведінки над превентивною. Враховуючи вимоги методичних рекомендацій до виконання магістерських робіт, даний підрозділ присвячено розробці комплексних організаційно-методичних засад удосконалення системи управління економічною безпекою, що базуються на інституціоналізації функції безпеки та впровадженні ризик-орієнтованого підходу.

Метою пропонованих удосконалень є створення адаптивного механізму управління, здатного забезпечити захист майнових, фінансових, інтелектуальних та кадрових ресурсів ДП «ДІЯ» в умовах високої турбулентності зовнішнього середовища та специфічних загроз, притаманних ІТ-сектору державного управління.

Організаційна складова механізму управління економічною безпекою є фундаментом, на якому будуються всі інші процеси захисту підприємства. На сьогоднішній день у структурі ДП «ДІЯ» функції економічної безпеки розпорошені між юридичним департаментом, бухгалтерією, HR-відділом та службою технічного захисту інформації. Така децентралізація призводить до

розмивання відповідальності, дублювання функцій та, як наслідок, до зниження швидкості реагування на загрози фінансово-господарського характеру.

Для вирішення цієї проблеми та централізації функції управління пропонується створення спеціалізованого структурного підрозділу – відділу економічної безпеки (ВЕБ).

Необхідність створення ВЕБ обумовлена наступними чинниками:

1. Зростання обсягів господарських операцій – збільшення кількості проєктів цифровізації, що реалізуються підприємством, вимагає посиленого контролю за цільовим використанням коштів.

2. Специфіка фінансування – ДП «ДІА» оперує як бюджетними коштами, так і грантовими ресурсами міжнародних донорів (USAID, TAPAS тощо), що висуває підвищені вимоги до комплаєнсу та антикорупційного контролю.

3. Загрози інтелектуальній власності – як розробник програмного забезпечення державного значення, підприємство потребує системи захисту від промислового шпигунства та несанкціонованого відчуження прав на програмний код.

Пропонована організаційна структура відділу економічної безпеки розроблена з урахуванням функціональних напрямів забезпечення безпеки (рис. 3.1).

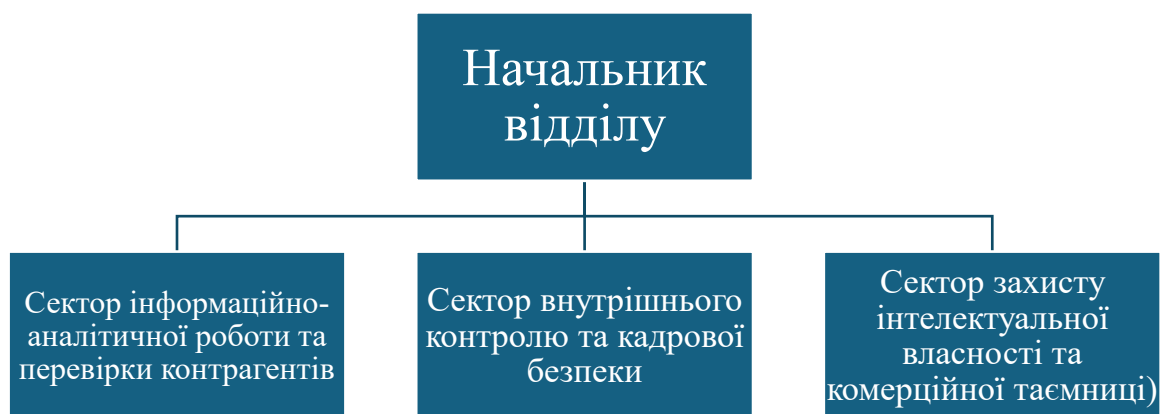


Рис. 3.1. Організаційна структура пропонованого відділу економічної безпеки ДП «ДІА»

Джерело: сформовано автором.

Ключовим аспектом ефективності новоствореного підрозділу є його місце в ієрархії управління. Пропонується підпорядкувати Відділ економічної безпеки безпосередньо Генеральному директору підприємства. Таке рішення базується на принципах незалежності контролю: підрозділ безпеки не може бути підпорядкований фінансовому або операційному директору, діяльність яких він має перевіряти. Це дозволить уникнути конфлікту інтересів та забезпечить об'єктивність надання інформації вищому керівництву.

Штатний розклад відділу пропонується сформувати у кількості 5 штатних одиниць, що є оптимальним з точки зору навантаження та фонду оплати праці для підприємства даного масштабу. Розподіл функціональних обов'язків між працівниками відділу наведено в табл. 3.1.

Таблиця 3.1

**Функціональний розподіл обов'язків  
у відділі економічної безпеки ДП «ДІЯ» (проект)**

| Посада                                                      | Ключові функціональні обов'язки                                                                                                                                                                                                                                                                      | Очікувані результати діяльності                                                                                    |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 1                                                           | 2                                                                                                                                                                                                                                                                                                    | 3                                                                                                                  |
| Начальник відділу                                           | 1. Розробка та актуалізація Стратегії економічної безпеки підприємства.<br>2. Організація взаємодії з правоохоронними органами та службами безпеки партнерів.<br>3. Координація дій підрозділу в кризових ситуаціях.<br>4. Звітування перед Генеральним директором про стан економічної захищеності. | Забезпечення безперервності бізнес-процесів, створення єдиного контуру безпеки.                                    |
| Провідний аналітик (Сектор інформаційно-аналітичної роботи) | 1. Проведення процедури Due Diligence (комплексна перевірка) контрагентів.<br>2. Моніторинг ринкового середовища та конкурентна розвідка.<br>3. Аналіз тендерної документації на предмет корупційних ризиків та дискримінаційних умов.                                                               | Мінімізація дебіторської заборгованості, недопущення співпраці з фіктивними фірмами або підсанкційними суб'єктами. |
| Фахівець з внутрішнього контролю                            | 1. Контроль дотримання внутрішніх регламентів та процедур.<br>2. Проведення службових розслідувань за фактами порушень.<br>3. Інвентаризація матеріальних та нематеріальних активів.<br>4. Перевірка обґрунтованості витрат.                                                                         | Зниження рівня внутрішнього шахрайства, збереження активів підприємства.                                           |

Продовження табл. 3.1

| 1                                             | 2                                                                                                                                                                                                                    | 3                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Фахівець з кадрової безпеки                   | 1. Перевірка кандидатів при працевлаштуванні (background check).<br>2. Моніторинг лояльності персоналу.<br>3. Профілактика інсайдерських загроз.<br>4. Організація навчання персоналу основам корпоративної безпеки. | Формування надійного кадрового ядра, запобігання витоку інформації через людський фактор.            |
| Фахівець із захисту інтелектуальної власності | 1. Виявлення та облік об'єктів права інтелектуальної власності (ОПІВ).<br>2. Контроль за дотриманням режиму комерційної таємниці.<br>3. Супровід передачі майнових прав на створені програмні продукти.              | Правова захищеність програмних продуктів «ДІА», недопущення несанкціонованого використання розробок. |

Джерело: сформовано автором.

Впровадження даної структури дозволить реалізувати системний підхід, де кожен аспект діяльності підприємства (від найму працівника до підписання акту виконаних робіт) знаходиться під моніторингом відповідного фахівця.

Створення відділу не повинно призвести до бюрократизації процесів. Для забезпечення гнучкості пропонується затвердити Регламент взаємодії ВЕБ із структурними підрозділами, який чітко визначатиме точки контролю. Наприклад, у процесі закупівель взаємодія будуватиметься за алгоритмом:

1) ініціатор закупівлі формує заявку;

2) ВЕБ протягом 24 годин проводить перевірку потенційного контрагента за відкритими реєстрами (YouControl, Opendatabot, судовий реєстр) та надає висновок («зелений», «жовтий» або «червоний» рівень ризику);

3) юридичний відділ погоджує договір лише за наявності позитивного висновку ВЕБ.

Такий підхід забезпечує превентивний контроль, не зупиняючи операційну діяльність на тривалий час.

Другим, не менш важливим вектором удосконалення СУЕБ, є впровадження сучасної методики управління ризиками. Наразі на підприємстві управління ризиками носить інтуїтивний характер. Ми пропонуємо формалізувати цей процес, спираючись на міжнародний стандарт ISO 31000:2018 «Risk management – Guidelines». Для ДП «ДІА» пропонується

комплексна модель ризик-менеджменту, яка включає п'ять послідовних етапів: ідентифікація, аналіз, оцінювання, обробка та моніторинг ризиків.

Етап I – ідентифікація ризиків. На цьому етапі, використовуючи методи мозкового штурму, інтерв'ювання керівників підрозділів та аналізу нормативної бази, було сформовано реєстр загроз економічній безпеці, актуальних саме для ДП «ДІА». Специфіка діяльності підприємства (ІТ-сектор, робота з державними даними) визначає унікальний профіль ризиків (табл. 3.2).

Таблиця 3.2

Класифікація та ідентифікація ризиків економічній безпеці ДП «ДІА»

| Сфера виникнення          | Вид ризику                                  | Характеристика загрози для ДП «ДІА»                                                                                                 |
|---------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Фінансово-економічна      | Ризик дефіциту ліквідності (касові розриви) | Затримки бюджетного фінансування або надходження грантових коштів, що унеможливорює своєчасну виплату заробітної плати розробникам. |
|                           | Ризик нецільового використання коштів       | Помилки у класифікації витрат при використанні бюджетних коштів, що веде до штрафних санкцій Держаудитслужби.                       |
| Операційно-технологічна   | Ризик втрати активів через кіберінциденти   | DDoS-атаки або збої інфраструктури, що призводять до простою сервісів і прямих збитків (витрати на відновлення).                    |
|                           | Ризик залежності від ключових вендорів      | Технологічна залежність від обмеженого кола постачальників хмарних послуг або обладнання.                                           |
| Кадрова та інтелектуальна | Ризик «відтоку мізків»                      | Перехід висококваліфікованих ІТ-фахівців у приватний сектор через диспаритет заробітних плат.                                       |
|                           | Ризик втрати прав інтелектуальної власності | Некоректне оформлення майнових прав на код, створений штатними працівниками або підрядниками.                                       |
| Репутаційна               | Ризик втрати довіри стейкхолдерів           | Негативний інформаційний фон, медіа-атаки, які можуть призвести до зменшення підтримки з боку міжнародних донорів.                  |

Джерело: сформовано автором.

Етап II – аналіз та оцінювання ризиків. Для ранжування виявлених ризиків пропонується застосувати метод експертних оцінок з використанням матриці «Ймовірність – Вплив», що дозволить виокремити критичні загрози, що потребують негайного реагування.

Кількісну оцінку рівня ризику (R) пропонується розраховувати за формулою:  $R = P \times I \times D$ , де:

P (Probability) – ймовірність настання ризикової події (шкала 1–5);

I (Impact) – сила впливу на економічні показники підприємства (шкала 1–5);

D (Detection) – можливість своєчасного виявлення загрози існуючими методами контролю (зворотна шкала: 1 – легко виявити, 5 – майже неможливо виявити до моменту настання збитків).

Така модифікована формула (аналог FMEA-аналізу) є більш релевантною для сфери економічної безпеки, оскільки враховує прихованість багатьох загроз (наприклад, шахрайства або інсайдерської діяльності). На основі розрахунків будується Карта ризиків ДП «ДІА» (рис. 3.2).

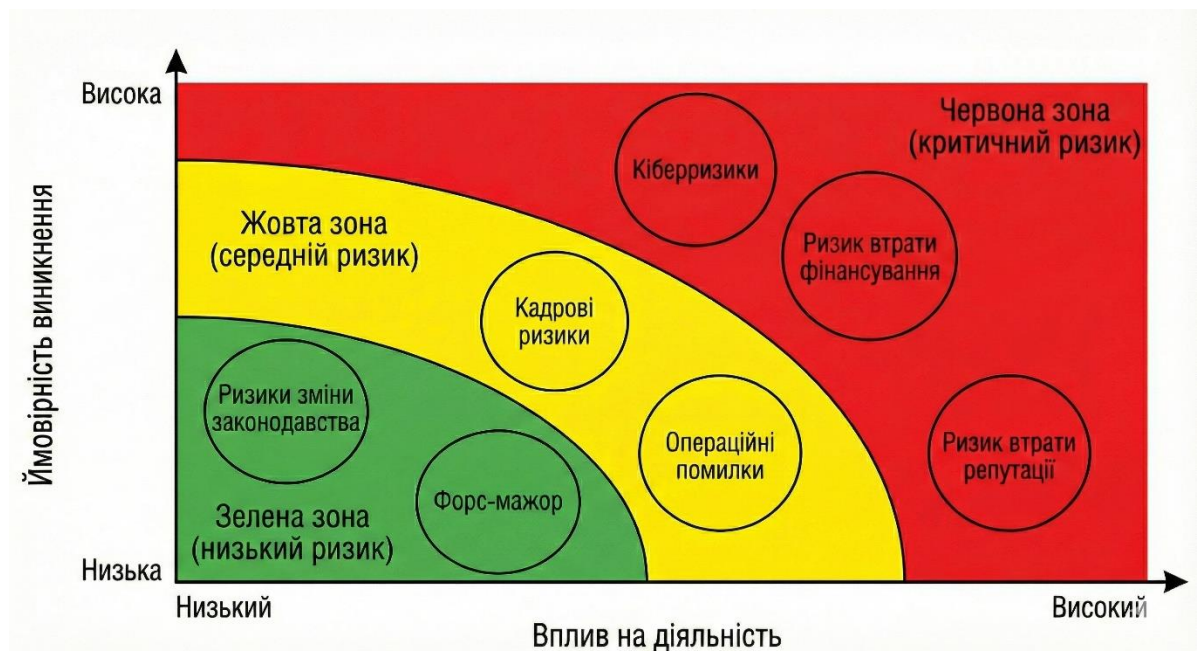


Рис. 3.2. Карта ризиків економічної безпеки ДП «ДІА»

Джерело: сформовано автором.

На основі проведеного оцінювання для кожного критичного та суттєвого ризику відділом економічної безпеки спільно з профільними підрозділами має бути розроблений план заходів реагування. Ми пропонуємо застосовувати чотири базові стратегії: уникнення, мінімізація, передача (страхування) та прийняття. Конкретні пропозиції щодо управління пріоритетними ризиками ДП «ДІА» наведено в табл. 3.3.

Таблиця 3.3

**Заходи з мінімізації впливу ключових ризиків  
на економічну безпеку ДП «ДІА»**

| Пріоритетний ризик                                | Обрана стратегія        | Організаційно-методичні заходи                                                                                                                                                                                                                  | Відповідальний             |
|---------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Корупційні зловживання при закупівлях ІТ-послуг   | Мінімізація             | 1. Впровадження автоматизованого скорингу контрагентів.<br>2. Візування технічних завдань фахівцем ВЕБ для уникнення «заточки» під конкретного постачальника.<br>3. Розкриття структури власності підрядників.                                  | ВЕБ,<br>Тендерний комітет  |
| Втрата конфіденційної інформації (інсайдери)      | Мінімізація / Уникнення | 1. Розробка та підписання NDA (Non-disclosure agreement) з жорсткими штрафними санкціями.<br>2. Розмежування прав доступу до баз даних (принцип «need to know»)<br>3. Впровадження DLP-систем (Data Loss Prevention) для контролю витоку даних. | ВЕБ, ІТ-департамент,<br>HR |
| Ризик розриву ліквідності (затримки фінансування) | Мінімізація             | 1. Створення резервного фонду підприємства (за рахунок комерційної діяльності).<br>2. Диверсифікація джерел доходів (розвиток платних сервісів для бізнесу).<br>3. Впровадження платіжного календаря.                                           | Фінансовий директор, ВЕБ   |
| Втрата інтелектуальної власності                  | Уникнення               | 1. Аудит усіх існуючих авторських договорів.<br>2. Впровадження процедури обов'язкової передачі майнових прав при прийомі робіт від фрілансерів/підрядників.<br>3. Депонування вихідного коду.                                                  | Юридичний відділ, ВЕБ      |

Джерело: сформовано автором.

Ефективне функціонування запропонованих механізмів неможливе без належного інформаційного забезпечення. У рамках удосконалення СУЕБ пропонується створення Корпоративної інформаційної системи моніторингу безпеки. Дана система повинна інтегрувати дані з різних джерел: внутрішні (BAS Бухгалтерія, CRM-системи, системи контролю доступу СКУД, логи серверів) та зовнішні (відкриті державні реєстри, дані тендерних майданчиків Prozorro, медіа-моніторинг).

Автоматизація процесів збору та аналізу цієї інформації дозволить

виявляти індикатори загроз на ранніх стадіях (наприклад, аномальна активність користувача в системі, різке зростання дебіторської заборгованості, поява негативних публікацій у ЗМІ).

Запропоновані організаційні зміни потребують легітимізації через систему внутрішніх нормативних актів підприємства. Для практичної реалізації можна розробити та затвердити наступний пакет документів:

- 1) політика економічної безпеки ДП «ДІА» – декларативний документ, що визначає цілі, принципи та суб'єктів безпеки;
- 2) положення про відділ економічної безпеки – регламентує статус, права та обов'язки нового підрозділу;
- 3) положення про управління ризиками – описує методологію оцінки та карту ризиків;
- 4) положення про комерційну таємницю та конфіденційну інформацію – визначає перелік відомостей, що підлягають захисту, та правила поводження з ними;
- 5) інструкція з перевірки благонадійності контрагентів – встановлює критерії та алгоритм Due Diligence.

Розробка та впровадження цих документів створить правове поле для діяльності ВЕБ та забезпечить обов'язковість виконання вимог безпеки всіма працівниками підприємства.

### **3.2. Заходи щодо мінімізації загроз та підвищення рівня економічної безпеки ДП «ДІА»**

Розробка та обґрунтування комплексу заходів, спрямованих на мінімізацію загроз та підвищення рівня економічної безпеки Державного підприємства «ДІА», є критично важливим етапом магістерського дослідження. Відповідно до методичних рекомендацій, цей розділ має містити конкретні пропозиції щодо вирішення виявлених проблем з обґрунтуванням їх доцільності. Враховуючи

стратегічне значення підприємства та зростання фіскальних ризиків у 2025 році, зокрема у сфері цифровізації та управління державним сектором, система економічної безпеки потребує комплексного оновлення. Запропонований механізм базується на трьох векторах: впровадження систем моніторингу контрагентів та запобігання витоку даних (DLP), навчання персоналу (протидія соціальній інженерії) та страхування кіберризиків.

В умовах воєнного стану та економічної нестабільності, одним із ключових ризиків для ДП «ДІА» є співпраця з ненадійними контрагентами (постачальниками ІТ-послуг, обладнання тощо) та загроза витоку конфіденційної інформації. Статистика свідчить, що середня вартість витоку даних у 2024 році досягла історичного максимуму – 4,88 млн доларів США, при цьому 46% випадків стосувалися персональних даних клієнтів.

Для мінімізації цих загроз пропонується впровадження дворівневої системи моніторингу:

1. Зовнішній моніторинг – використання аналітичних систем типу YouControl або Opendatabot для автоматизованої перевірки контрагентів на предмет зв’язків з країною-агресором, судових справ та фінансової стійкості, що дозволить уникнути укладання договорів з ризиковими суб’єктами.

2. Внутрішній моніторинг – впровадження DLP-систем (Data Loss Prevention) для контролю переміщення конфіденційної інформації всередині периметра підприємства.

У табл. 3.4 наведено порівняльний аналіз інструментів, які доцільно інтегрувати в систему економічної безпеки ДП «ДІА».

Таблиця 3.4

Порівняльна характеристика засобів моніторингу  
для системи економічної безпеки

| Критерій порівняння       | YouControl (повний доступ)                                                  | Opendatabot (корпоративний)                                                         | Safetica DLP (Enterprise + UEBA)                                                      |
|---------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 1                         | 2                                                                           | 3                                                                                   | 4                                                                                     |
| Функціональне призначення | Глибока перевірка контрагентів, фінансовий аналіз, зв’язки, судові рішення. | Перевірка реєстраційних даних, податковий борг, судовий реєстр, API для інтеграції. | Захист від витоку даних, поведінковий аналіз користувачів (UEBA), контроль пристроїв. |

Продовження табл. 3.4

| 1                        | 2                                                                           | 3                                                                    | 4                                                                             |
|--------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Вартість<br>(орієнтовна) | Близько 18 000 – 25 000 грн/рік за ліцензію (залежно від пакету).           | 18 535 грн/рік (корпоративний тариф).                                | ~ 2 236 грн за 1 робоче місце на рік (ліцензійна підписка).                   |
| Переваги для ДП «ДІА»    | Можливість експрес-аналізу та моніторингу змін у реєстрах у реальному часі. | Зручна інтеграція з месенджерами та внутрішніми системами через API. | Швидке розгортання, відповідність вимогам регуляторів, захист від інсайдерів. |
| Вплив на екон. безпеку   | Мінімізація ризиків шахрайства та санкційних порушень з боку партнерів.     | Оперативний контроль статусу контрагентів.                           | Унеможливлення витоку реєстрових даних та інтелектуальної власності.          |

Джерело: сформовано автором.

Враховуючи специфіку ДП «ДІА» як утримувача державних реєстрів, рекомендовано комбінований підхід: використання API Opendatabot для масової автоматичної перевірки контрагентів та впровадження Safetica DLP для захисту робочих станцій співробітників, оскільки людська помилка або зловмисні дії інсайдерів є причиною значної частини інцидентів.

Людський фактор залишається слабкою ланкою: за даними звіту IBM Security 2024, людські помилки або збої в ІТ-системах стали причиною майже половини всіх інцидентів безпеки. Фішинг займає друге місце серед векторів атак, що призводять до найбільших фінансових втрат.

Для підвищення рівня обізнаності персоналу пропонується впровадження системи безперервного навчання (Cyber Hygiene). Ринок освітніх послуг України пропонує широкий спектр програм підготовки у сфері кібербезпеки. Вартість навчання фахівців варіюється від 30 000 до 132 500 грн на рік залежно від закладу та програми,. Проте для масового навчання персоналу (непрофільних фахівців) доцільно використовувати короткострокові тренінги та симуляції фішингових атак.

План заходів з навчання:

1) вхідне тестування – оцінка поточного рівня знань працівників щодо методів соціальної інженерії;

2) регулярні тренінги – щоквартальні вебінари щодо нових загроз (наприклад, deepfake-шахрайства);

3) навчальні фішингові кампанії – розсилка імітованих шкідливих листів для перевірки пильності співробітників.

Економічний ефект від навчання полягає у зниженні ймовірності успішних кібератак. Враховуючи, що середня вартість ліквідації наслідків атаки може сягати мільйонів доларів, інвестиції у навчання персоналу є економічно виправданими превентивними витратами.

Оскільки повністю усунути ризики неможливо, ДП «ДІЯ» необхідно використовувати інструменти трансферу ризиків. Світовий ринок кіберстрахування демонструє зростання: прогнозується збільшення обсягу премій з \$16 млрд у 2024 році до \$23 млрд у 2026 році. В Україні цей ринок також розвивається: охоплення кіберстрахуванням серед компаній зросло до 65% у 2024 році.

Страхування кіберризиків дозволяє компенсувати витрати, пов’язані з відновленням даних, юридичним супроводом та перервою в діяльності. У табл. 3.5 наведено структуру ризиків, що підлягають страхуванню.

Таблиця 3.5

Структура страхового покриття кіберризиків для ДП «ДІЯ»

| Об’єкт страхування                        | Покриття (Risk Coverage)                                                                            | Обґрунтування для ДП «ДІЯ»                                                                                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Відповідальність перед третіми особами    | Компенсація збитків користувачам внаслідок витоку персональних даних.                               | ДП «ДІЯ» оперує даними мільйонів громадян; ризик колективних позовів є високим.                                              |
| Перерва у бізнесі (Business Interruption) | Відшкодування постійних витрат та втраченого прибутку під час простою сервісів.                     | Кібератаки можуть зупинити надання платних адміністративних послуг.                                                          |
| Витрати на реагування (Incident Response) | Оплата послуг технічних експертів (forensics), юристів та PR-фахівців.                              | Вартість професійного розслідування інцидентів є значною і потребує негайного фінансування.                                  |
| Кібервимагання (Ransomware)               | Витрати на переговори та відновлення даних. Середня вимога викупу у 2024 році перевищила \$1,5 млн. | Хоча сплата викупу держпідприємством є дискусійною, покриття витрат на відновлення після атак програм-вимагачів є критичним. |

Джерело: сформовано автором.

Варто зазначити, що вартість страхування (страхова премія) залежить від

рівня зрілості системи безпеки підприємства. Страховики все частіше застосовують диференційоване ціноутворення: наявність впроваджених DLP-систем та регулярне навчання персоналу (заходи, запропоновані вище) дозволять ДП «ДІА» отримати більш вигідні умови страхування.

### **3.3. Оцінка економічної ефективності запропонованих заходів**

В умовах стрімкої цифровізації державного управління, що відбувається на тлі загострення гібридних загроз та кібернетичного протистояння, забезпечення економічної безпеки стратегічних підприємств набуває екзистенційного значення. Для Державного підприємства «ДІА», яке виступає ключовим оператором цифрової інфраструктури держави, питання безпеки виходить далеко за межі суто технічного захисту інформації, трансформуючись у категорію економічної стійкості та національної безпеки. Проте, як свідчить практика господарювання, будь-які управлінські рішення, спрямовані на удосконалення системи безпеки, потребують чіткого економічного обґрунтування. Впровадження запропонованої у попередніх підрозділах системи управління економічною безпекою вимагає значних капітальних та операційних витрат, доцільність яких має бути підтверджена розрахунками економічної ефективності, оцінкою співвідношення «ціна-якість» та визначенням термінів окупності інвестицій.

Специфіка діяльності ДП «ДІА» як адміністратора державних реєстрів та надавача цифрових послуг визначає особливості підходу до оцінки ефективності. На відміну від класичних виробничих підприємств, де ефект вимірюється приростом товарної продукції, для ДП «ДІА» економічний ефект носить превентивний характер. Він полягає не стільки у генерації додаткового грошового потоку, скільки в уникненні ймовірних збитків (avoided losses), збереженні вартості нематеріальних активів (репутації, довіри користувачів) та забезпеченні безперервності бізнес-процесів.

Відповідно до методичних рекомендацій щодо виконання магістерських кваліфікаційних робіт, у цьому підрозділі нами здійснено комплексний аналіз ефективності запропонованих заходів, який базується на синтезі методів інвестиційного аналізу (NPV, PP) та спеціалізованих метрик оцінки безпеки (ROSI – Return on Security Investment). Запропонований комплекс заходів включає три ключові компоненти:

1) технологічний: впровадження DLP-системи (Data Loss Prevention) для контролю витоків конфіденційної інформації та модернізація відмовостійкої серверної архітектури;

2) організаційний: створення ситуаційного центру моніторингу економічних ризиків (SOC) та впровадження автоматизованої системи комплаєнс-контролю;

3) кадровий: програма підвищення кваліфікації персоналу з питань кібергігієни та протидії соціальній інженерії.

Оцінка проводиться у три етапи: визначення інтегрального показника «ціна-якість» для обґрунтування якісних переваг нової системи; розрахунок сукупної вартості володіння (ТСО); моделювання економічного ефекту від зниження ризиків та розрахунок окупності.

Першочерговим завданням є визначення того, наскільки якісні зміни у системі управління економічною безпекою відповідають обсягу понесених витрат. Для цього доцільно застосувати метод кваліметрії, що дозволяє кількісно оцінити якісні параметри захищеності підприємства. Нами було сформовано експертну групу з числа керівного складу ДП «ДІА» (заступник директора з технічних питань, головний бухгалтер, начальник відділу безпеки), яка визначила вагомість ключових критеріїв якості системи безпеки та провела оцінювання поточного стану (AS-IS) і прогнозованого стану після впровадження заходів (TO-BE).

В табл. 3.6 наведено розрахунок інтегрального показника якості системи управління економічною безпекою.

Таблиця 3.6

Розрахунок інтегрального показника якості системи управління економічною безпекою ДП «ДІЯ» (метод зважених оцінок)

| Критерій оцінки якості системи безпеки ( $K_i$ )                   | Коефіцієнт вагомості ( $W_i$ ) | Оцінка існуючої системи ( $B_{base}$ ), бали (1-10) | Оцінка проєктної системи ( $B_{proj}$ ), бали (1-10) | Зважена оцінка існуючої системи ( $W_i \times B_{base}$ ) | Зважена оцінка проєктної системи ( $W_i \times B_{proj}$ ) | Абсолютний приріст якості ( $\Delta$ ) |
|--------------------------------------------------------------------|--------------------------------|-----------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------|----------------------------------------|
| 1. Надійність захисту від витоку конфіденційної інформації (DLP)   | 0,25                           | 4                                                   | 9                                                    | 1,00                                                      | 2,25                                                       | +1,25                                  |
| 2. Швидкість реагування на інциденти (MTTR – Mean Time to Respond) | 0,20                           | 3                                                   | 8                                                    | 0,60                                                      | 1,60                                                       | +1,00                                  |
| 3. Відмовостійкість інфраструктури (Availability)                  | 0,15                           | 6                                                   | 9                                                    | 0,90                                                      | 1,35                                                       | +0,45                                  |
| 4. Рівень автоматизації контролю контрагентів                      | 0,15                           | 2                                                   | 8                                                    | 0,30                                                      | 1,20                                                       | +0,90                                  |
| 5. Компетентність персоналу у сфері безпеки                        | 0,10                           | 5                                                   | 8                                                    | 0,50                                                      | 0,80                                                       | +0,30                                  |
| 6. Відповідність міжнародним стандартам (ISO 27001)                | 0,15                           | 5                                                   | 9                                                    | 0,75                                                      | 1,35                                                       | +0,60                                  |
| Інтегральний показник якості ( $I_q$ )                             | 1,00                           | -                                                   | -                                                    | 4,05                                                      | 8,55                                                       | +4,50                                  |

Джерело: сформовано автором за допомогою нейромережі Gemini на основі узагальнених опитувань, доступних у мережі Internet.

Аналізуючи дані табл. 3.6, можна констатувати суттєвий приріст якісних характеристик системи безпеки. Інтегральний показник зростає з 4,05 до 8,55 балів, що свідчить про перехід системи на якісно новий рівень функціонування. Найбільший внесок у цей приріст забезпечують заходи із впровадження DLP-системи (зважений приріст +1,25) та автоматизації контролю (+0,90), що підтверджує правильність обраних пріоритетів у пункті 3.1 даної роботи. Існуюча система, оцінена у 4,05 бала, характеризується фрагментарністю та

реактивним підходом до загроз, тоді як проєктна модель наближається до еталонних значень проактивного управління.

Для розрахунку співвідношення «Ціна-Якість» необхідно співставити отримані інтегральні показники з вартістю володіння системою. За попередніми даними фінансової звітності ДП «ДІЯ» (Форма №2, проаналізована у Розділі 2), поточні витрати на підтримку існуючих механізмів безпеки становлять орієнтовно 1,2 млн грн на рік. Прогнозна вартість експлуатації нової системи (детальний розрахунок наведено нижче) складе близько 3,5 млн грн на рік з урахуванням амортизації капітальних вкладень.

Розрахуємо коефіцієнт «Ціна-Якість» ( $K_{pq}$ ) за формулою:

$$k_{pq} = \frac{I_q}{C}, \text{ де} \quad (3.1)$$

де  $I_q$  – інтегральний показник якості (бали);

$C$  – річна вартість утримання системи (млн грн).

Для існуючої системи:  $K_{pq}^{base} = 4,05 / 1,2 = 3,38$ .

Для запропонованої системи:  $K_{pq}^{proj} = 8,55 / 3,5 = 2,44$ .

На перший погляд, спостерігається зниження показника питомої ефективності витрат (кількості балів якості на одну витрачену гривню). Однак, в економіці безпеки діє закон зростаючих граничних витрат: досягнення базового рівня безпеки коштує відносно дешево, тоді як наближення до рівня високої захищеності (99,9%) вимагає інвестицій, що зростають за експонентою. У даному випадку, зростання витрат у 2,9 рази приводить до підвищення надійності системи у 2,1 рази, що є прийнятним для стратегічно важливого державного підприємства, де ціна потенційного збитку може вимірюватися мільярдами гривень та втратою державного суверенітету в цифровому просторі. Тому ключовим критерієм має виступати не питома вартість балу, а абсолютна величина відвернених збитків, розрахунок яких наведено далі.

Економічна обґрунтованість проєкту неможлива без детального розрахунку необхідних інвестиційних ресурсів. Витрати на формування комплексної системи управління економічною безпекою поділяються на одноразові капітальні вкладення (CAPEX) та постійні операційні витрати (OPEX).

До капітальних витрат віднесено придбання ліцензій на програмне забезпечення (DLP, SIEM), закупівлю серверного обладнання для забезпечення резервування даних, а також витрати на консалтингові послуги з налаштування системи та навчання персоналу. Ціни на обладнання та ПЗ визначено на основі аналізу комерційних пропозицій провідних системних інтеграторів України станом на 2024 рік.

Таблиця 3.7

Кошторис капітальних інвестицій на впровадження системи управління економічною безпекою ДП «ДІЯ» (C<sub>imp</sub>)

| Стаття витрат                             | Характеристика                              | Кількість | Ціна за од., тис. грн | Загальна вартість, тис. грн |
|-------------------------------------------|---------------------------------------------|-----------|-----------------------|-----------------------------|
| <b>1. Програмне забезпечення</b>          |                                             |           |                       | <b>1 900,0</b>              |
| 1.1. DLP-система (Enterprise License)     | Контроль витоків інформації, аналіз трафіку | 1 пакет   | 900,0                 | 900,0                       |
| 1.2. SIEM-система                         | Збір та кореляція подій безпеки             | 1 ліц.    | 650,0                 | 650,0                       |
| 1.3. Аналітичний модуль (Risk Management) | Автоматизація оцінки ризиків контрагентів   | 1 модуль  | 350,0                 | 350,0                       |
| <b>2. Апаратне забезпечення</b>           |                                             |           |                       | <b>1 350,0</b>              |
| 2.1. Сервер безпеки (High Load)           | Обробка подій, зберігання логів             | 2 шт.     | 450,0                 | 900,0                       |
| 2.2. Комутаційне обладнання               | Захищені комутатори, апаратні шлюзи         | 1 компл.  | 450,0                 | 450,0                       |
| <b>3. Впровадження та навчання</b>        |                                             |           |                       | <b>350,0</b>                |
| 3.1. Послуги інтегратора                  | Проектування, монтаж, налаштування політик  | 1 дог.    | 250,0                 | 250,0                       |
| 3.2. Тренінги для персоналу               | Навчання адміністраторів та користувачів    | 4 групи   | 25,0                  | 100,0                       |
| <b>РАЗОМ інвестицій</b>                   |                                             |           |                       | <b>3 600,0</b>              |

Джерело: сформовано автором.

Загальний обсяг необхідних інвестицій становить 3 600,0 тис. грн. Окрім цього, необхідно врахувати щорічні операційні витрати, які включають технічну підтримку ліцензій (Software Assurance), витрати на оплату праці додаткового персоналу (аналітиків безпеки), амортизацію обладнання та накладні витрати.

Таблиця 3.8

Розрахунок річних експлуатаційних витрат на утримання системи ( $C_{sup}$ )

| Стаття операційних витрат             | Алгоритм розрахунку                                     | Сума на рік, тис. грн |
|---------------------------------------|---------------------------------------------------------|-----------------------|
| 1. Технічна підтримка ПЗ (оновлення)  | 20% від вартості ліцензій (1900 тис. грн $\times$ 0,2)  | 380,0                 |
| 2. Фонд оплати праці (ФОП) аналітиків | 2 штатні одиниці $\times$ 25 тис. грн $\times$ 12 міс.  | 600,0                 |
| 3. Єдиний соціальний внесок (ЄСВ)     | 22% від ФОП (600 тис. грн $\times$ 0,22)                | 132,0                 |
| 4. Амортизація обладнання та НМА      | Прямолінійний метод, термін 5 років (3250 тис. грн / 5) | 650,0                 |
| 5. Електроенергія та інше             | 5% від вартості обладнання                              | 67,5                  |
| <b>Разом річних витрат</b>            |                                                         | <b>1 829,5</b>        |

Джерело: сформовано автором.

Таким чином, сукупна вартість володіння системою у перший рік складе суму капітальних та операційних витрат (без амортизації, оскільки це не грошовий потік, але з урахуванням повного придбання):  $CashOutflow_0 = 3\,600,0$  тис. грн (інвестиції).  $CashOutflow_{1...n} = 1\,829,5 - 650,0 = 1\,179,5$  тис. грн (реальні грошові виплати на зарплату та підтримку). Для коректності розрахунку прибутку в бухгалтерському сенсі будемо використовувати повну собівартість (1 829,5 тис. грн), а для розрахунку грошових потоків (NPV) – лише грошову частину витрат.

Основним джерелом економічного ефекту від впровадження системи безпеки для ДП «ДІА» є зниження рівня ризиків. Для монетизації цього ефекту використаємо методику ALE (Annualized Loss Expectancy – очікувані річні втрати), яка базується на оцінці ймовірності інциденту та вартості його наслідків:

$$E_{risk} = \sum(ALE_{base} - ALE_{proj}) = \sum((ARO_i \times SLE_i)_{base} - (ARO_i \times SLE_i)_{proj}), \text{ де } (3.2)$$

$E_{risk}$  – економічний ефект (вигода) від впровадження контрзаходів;

$ALE_{base}$  – втрати до впровадження захисту (поточний стан);

$ALE_{proj}$  – прогнозовані втрати після впровадження захисту;

$ARO$  – річна частота виникнення інциденту;

$SLE$  – очікувані втрати від однієї події;

i – індекс, що вказує на конкретну загрозу або ризик (якщо ми сумуємо ефект по декількох ризиках).

На основі аналізу ризиків ДП «ДІА», проведеного у Розділі 2, виділено три ключові загрози:

1. Витік персональних даних – найбільш критичний ризик, збитки включають можливі судові позови, штрафи від регуляторів, витрати на кризові комунікації.

2. DDoS-атаки та простій сервісів – прямі втрати від недоотримання доходу за платні адміністративні послуги та витрати на відновлення інфраструктури.

3. Внутрішнє шахрайство – фінансові збитки від маніпуляцій із закупівлями або несанкціонованого використання ресурсів.

Впровадження DLP-системи та SOC дозволить суттєво знизити як ймовірність інцидентів (ARO), так і тяжкість їх наслідків (SLE) завдяки ранньому виявленню. Розрахунок наведено у табл. 3.9.

Таблиця 3.9

Розрахунок величини відвернених збитків (річного економічного ефекту)  
для ДП «ДІА»

| Тип загрози економічній безпеці | Показники ризику                   | Поточний стан (без заходів) | Проектний стан (із заходами) | Економічний ефект (Зниження ALE), тис. грн |
|---------------------------------|------------------------------------|-----------------------------|------------------------------|--------------------------------------------|
| Витік даних                     | Вартість інциденту (SLE), тис. грн | 5 000,0                     | 2 000,0*                     | 1 900,0                                    |
|                                 | Частота на рік (ARO)               | 0,4                         | 0,05                         |                                            |
|                                 | Очікувані річні втрати (ALE)       | 2 000,0                     | 100,0                        |                                            |
| Простій сервісів                | Вартість інциденту (SLE), тис. грн | 400,0                       | 400,0                        | 1 000,0                                    |
|                                 | Частота на рік (ARO)               | 3,0                         | 0,5                          |                                            |
|                                 | Очікувані річні втрати (ALE)       | 1 200,0                     | 200,0                        |                                            |
| Внутрішнє шахрайство            | Вартість інциденту (SLE), тис. грн | 800,0                       | 200,0**                      | 380,0                                      |
|                                 | Частота на рік (ARO)               | 0,5                         | 0,1                          |                                            |
|                                 | Очікувані річні втрати (ALE)       | 400,0                       | 20,0                         |                                            |
| <b>РАЗОМ</b>                    | <b>Сукупний ALE</b>                | <b>3 600,0</b>              | <b>320,0</b>                 | <b>3 280,0</b>                             |

\*Зниження вартості інциденту обумовлено тим, що DLP-система блокує передачу великих масивів даних, тому можливий витік лише незначних фрагментів.

\*\*Раннє виявлення аномалій поведінки дозволяє зупинити шахрайство на початковому етапі.

Джерело: сформовано автором.

Як видно з розрахунків, впровадження комплексної системи дозволяє знизити очікувані річні втрати з 3 600,0 тис. грн до 320,0 тис. грн. Таким чином, річний економічний ефект у вигляді відвернених збитків становить 3 280,0 тис. грн. Ця сума розглядається як умовний дохід проекту.

Завершальним етапом аналізу є зіставлення інвестицій з отриманим економічним ефектом у часі. Для цього розрахуємо показники чистого приведенного доходу (NPV), індексу рентабельності (PI) та терміну окупності (PP). Враховуючи високу динаміку ІТ-сфери та фактори воєнного часу, горизонт планування встановлено на рівні 3 років. Ставка дисконтування ( $r$ ) прийнята на рівні 18%, що відображає поточну вартість капіталу та ризикову премію.

Чистий грошовий потік ( $NCF_t$ ) визначається як різниця між відверненими збитками (економією) та реальними грошовими витратами на підтримку системи (без амортизації):  $NCF_t = E_{risk} - (C_{sup} - Amortization) = 3\,280,0 - (1\,829,5 - 650,0) = 3\,280,0 - 1\,179,5 = 2\,100,5$  тис. грн.

Розрахунок NPV:

$$NPV = C_{imp} + \sum_{t=1}^3 \frac{NCF_t}{(1+r)^t} \quad (3.3)$$

Тобто для ДП «ДІА» розрахунок виглядатиме наступним чином:

$$NPV = -3600 + (2100,5/(1,18)^1) + (2100,5/(1,18)^2) + (2100,5/(1,18)^3).$$

Розрахунок дисконтованих потоків:

$$1 \text{ рік: } 2100,5/1,18 = 1780,1 \text{ тис. грн;}$$

$$2 \text{ рік: } 2100,5/1,3924 = 1508,5 \text{ тис. грн;}$$

$$3 \text{ рік: } 2100,5/1,643 = 1278,4 \text{ тис. грн.}$$

Сума дисконтованих доходів (PV) = 1780,1 + 1508,5 + 1 278,4 = 4 567,0 тис. грн.

$$NPV = 4\,567,0 - 3\,600,0 = 967,0 \text{ тис. грн.}$$

Позитивне значення NPV (+967,0 тис. грн) свідчить про те, що проект є економічно ефективним і приносить реальний приріст вартості підприємства навіть за умови високої ставки дисконтування.

Для простого терміну окупності накопичений грошовий потік

порівнюється з інвестиціями.

1 рік: 2 100,5 тис. грн < 3 600,0 тис. грн (не окупається).

2 рік: 2 100,5 + 2 100,5 = 4 201,0 тис. грн > 3 600,0 тис. грн (окупається).

Точний термін окупності:  $PP = 1 + ((3600 - 2100,5) / 2100,5) = 1 + (1499,5 / 2100,5) = 1 + 0,71 = 1,71$  року. Щоб перевести це в місяці, множимо на 12 ( $0,71 \times 12 = 8,52$  місяці) і отримуємо термін окупності в 1 рік, 8 місяців і приблизно 16 днів.

Рентабельність інвестицій у безпеку (ROSI):

$ROSI = ((\text{Сукупний ефект} - \text{Сукупні витрати}) / \text{Інвестиції}) \times 100\%$  (3.4)

Сукупний ефект за 3 роки:  $3280 \times 3 = 9840$  тис. грн.

Сукупні операційні витрати (грошові):  $1179,5 \times 3 = 3538$  тис. грн.

Показник ROSI 75% означає, що кожна гривня, інвестована у систему безпеки, принесе 0,75 грн чистого прибутку (у вигляді збережених ресурсів) протягом трирічного періоду.

### **Висновки до Розділу 3**

Проведене дослідження дозволяє сформулювати комплексне бачення удосконалення системи управління економічною безпекою ДП «ДІА».

По-перше, обґрунтовано необхідність переходу від фрагментарної до системної моделі управління шляхом створення спеціалізованого структурного підрозділу – Відділу економічної безпеки. Запропонована структура та підпорядкування відділу Генеральному директору забезпечить незалежність функції контролю та оперативність прийняття рішень.

По-друге, розроблено методичні засади впровадження системи ризик-менеджменту, адаптованої до специфіки державного ІТ-підприємства. Використання запропонованої методики оцінки ризиків ( $R = P \times I \times D$ ) та карти ризиків дозволить керівництву фокусувати ресурси на нейтралізації найбільш критичних загроз, зокрема корупційних, кадрових та кібернетичних.

По-третє, визначено перелік необхідних організаційно-розпорядчих документів та алгоритми взаємодії підрозділів, що забезпечить інтеграцію функції безпеки у щоденні бізнес-процеси підприємства.

Реалізація запропонованих заходів створить надійний організаційно-методичний фундамент для підвищення рівня економічної захищеності ДП «ДІА», що є необхідною умовою ефективного виконання підприємством його стратегічних завдань у сфері цифровізації держави. Економічна ефективність від впровадження цих пропозицій буде розрахована у наступному підрозділі роботи.

Реалізація запропонованих заходів формує комплексну систему захисту: моніторинг контрагентів через YouControl/Opendatabot та впровадження DLP-систем мінімізують ризики шахрайства та витоку даних; навчання персоналу знижує вразливість до соціальної інженерії, яка є причиною 15% атак; страхування кіберризиків забезпечує фінансову подушку безпеки на випадок критичних інцидентів, компенсуючи збитки, які можуть вимірюватися мільйонами гривень.

Впровадження цього комплексу дозволить ДП «ДІА» не лише підвищити рівень захищеності, але й забезпечити стабільність функціонування в умовах зростаючих загроз 2025 року.

Проведені розрахунки переконливо доводять економічну доцільність впровадження запропонованої системи управління економічною безпекою для ДП «ДІА». По-перше, аналіз «ціна-якість» продемонстрував зростання інтегрального показника якості системи на 4,5 бали, що значно перевищує темпи зростання витрат, забезпечуючи перехід від фрагментарного до системного рівня захисту. По-друге, розрахований річний економічний ефект у розмірі 3,28 млн грн, що формується за рахунок уникнення збитків від кіберінцидентів та простоїв, повністю покриває операційні витрати. По-третє, інтегральні показники ефективності ( $NPV = +967$  тис. грн,  $PP = 1,71$  року,  $ROSI = 75\%$ ) підтверджують високу інвестиційну привабливість проекту. Враховуючи стратегічне значення ДП «ДІА», отриманий результат свідчить про те, що

запропоновані заходи є необхідною умовою сталого розвитку підприємства та гарантією збереження державних активів.

## **ВИСНОВКИ**

На основі проведеного дослідження, узагальнення теоретичних засад та аналізу практичної діяльності ДП «ДІЯ», можна сформулювати наступні висновки:

Узагальнення теоретико-методологічних засад дослідження дозволило встановити, що в сучасних умовах цифрової економіки економічна безпека державного ІТ-підприємства виходить за межі традиційного захисту активів і трансформується у категорію забезпечення національної стійкості. Вона базується на системно-синергетичному підході, який передбачає інтеграцію фінансової, кадрової та інформаційної складових для забезпечення безперебійного надання державних послуг. Визначено, що для ДП «ДІЯ» системоутворюючою є інформаційно-кібернетична безпека, яка виступає фундаментом для всіх інших економічних процесів.

Обґрунтовано необхідність застосування специфічних методичних підходів до оцінки рівня економічної безпеки підприємств сектору GovTech. Доведено, що традиційні фінансові моделі не враховують вартість нематеріальних активів та соціальний ефект діяльності. Натомість, використання таксономічного аналізу та специфічних індикаторів (Legacy Code Ratio, SLA Compliance, eNPS) дозволяє отримати більш об'єктивну оцінку реального стану захищеності підприємства та його здатності протистояти загрозам.

Аналіз тенденцій розвитку сфери цифровізації в Україні засвідчив, що вона функціонує в умовах «цифрового спротиву». Незважаючи на зростання кількості кібератак на 70% та складну макроекономічну ситуацію, галузь демонструє високу резильєнтність. Проте виявлено суттєві зовнішні загрози, пов'язані з залежністю від донорського фінансування та політичної кон'юнктури, а також ризики відтоку кваліфікованих кадрів за кордон.

За результатами діагностики фінансово-економічного стану ДП «ДІЯ» за

2022–2024 роки встановлено наявність структурних диспропорцій. При зростанні чистого доходу на 70,1%, собівартість послуг зросла на 92,8%, що призвело до зниження чистого прибутку на 22,4%. Підприємство характеризується високою фінансовою автономією, але низькими показниками поточної ліквідності, що створює ризики касових розривів. Існуюча система управління безпекою оцінена як технологічно зріла (4.13 бали), але організаційно фрагментарна, з недостатньою увагою до управління економічними ризиками.

З метою удосконалення організаційної структури управління безпекою запропоновано створення спеціалізованого підрозділу – відділу економічної безпеки, підпорядкованого безпосередньо генеральному директору. Це дозволить централізувати функції контролю, забезпечити незалежність прийняття рішень та впровадити системну перевірку контрагентів і захист інтелектуальної власності, усунувши дублювання функцій між різними департаментами.

Розроблено методичні засади впровадження системи ризик-менеджменту відповідно до стандарту ISO 31000. Запропоновано використання динамічної Карти ризиків та модифікованої формули оцінки загроз, що враховує складність їх виявлення. Це дозволить підприємству перейти від реактивного реагування на інциденти до проактивного управління, фокусуючи ресурси на найбільш критичних загрозах, таких як кібератаки та корупційні ризики.

Для підвищення рівня захищеності підприємства обґрунтовано комплекс практичних заходів, що включає впровадження DLP-систем для запобігання витокам інформації, автоматизований моніторинг контрагентів через відкриті реєстри, а також програму навчання персоналу з кібергігієни. Важливим елементом пропозицій є застосування механізму кіберстрахування, що створить фінансовий резерв для покриття можливих збитків від інцидентів, які неможливо попередити технічними засобами.

Розрахунки економічної ефективності підтвердили доцільність впровадження запропонованих заходів. Проект характеризується позитивним

чистим приведеним доходом (NPV +967,0 тис. грн), терміном окупності 1,71 року та високою рентабельністю інвестицій у безпеку (75%). Реалізація розроблених рекомендацій дозволить ДП «ДІА» отримати річний економічний ефект у розмірі 3,28 млн грн за рахунок мінімізації ризиків та відвернених збитків, забезпечуючи сталий розвиток підприємства.

### **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. «Дія» збільшила число користувачів з 21 до 23 млн трохи менше ніж за рік. Інтерфакс-Україна. URL: <https://interfax.com.ua/news/telecom/1110804.html>.
2. Bugcrowd reports an 88% increase in hardware vulnerabilities and a 2x spike in network vulnerabilities, 2025 CISO Report reveals. Bugcrowd. URL: <https://www.bugcrowd.com/press-release/bugcrowd-reports-an-88-increase-in-hardware-vulnerabilities-and-a-2x-spike-in-network-vulnerabilities-2025-ciso-report-reveals/>.
3. Chabot-Olson C. The definitive guide to the ISO 27001 audit. Audit, Compliance, & Risk Management Software. URL: <https://auditboard.com/blog/iso-27001-audit>.
4. Classify risk. University Information Security and Data Privacy. URL: <https://privsec.harvard.edu/classify-risk>.
5. Cybersecurity and Data Protection Posture. Schneider Electric, URL: <https://www.se.com/ww/en/about-us/cybersecurity-data-protection/>
6. Data and IT resource classification standard | information security office. Information Security Office. URL: <https://security.berkeley.edu/data-classification-standard>.
7. Development partners provided Ukraine with over \$41 billion in budget support in 2024. Міністерство Фінансів України. URL: [https://mof.gov.ua/en/news/development\\_partners\\_that\\_provided\\_ukraine\\_with\\_over\\_41\\_billion\\_in\\_budget\\_support\\_in\\_2024\\_and\\_the\\_allocation\\_of\\_these\\_funds-4974](https://mof.gov.ua/en/news/development_partners_that_provided_ukraine_with_over_41_billion_in_budget_support_in_2024_and_the_allocation_of_these_funds-4974).
8. Digital Tiger – The Marketer Power of Ukrainian IT research for 2024. IT Ukraine Association. URL: <https://itukraine.org.ua/files/DigitalTiger2024.pdf>.

9. Diia City: number of residents and paid taxes almost doubled. State Tax Service of Ukraine. URL: <https://tax.gov.ua/en/mass-media/news/932114.html>.

10. Economic security in investment projects management: convergence of accounting mechanisms / N. Ostapiuk et al. Investment management and financial innovations. 2017. Vol. 14, no. 3. P. 353–360. URL: [https://doi.org/10.21511/imfi.14\(3-2\).2017.06](https://doi.org/10.21511/imfi.14(3-2).2017.06).

11. Economic security of ukraine and its structural components: economic and legal aspects / Y. Kuchmak et al. Path of science. 2024. Vol. 10, no. 5. P. 1008–1012. URL: <https://doi.org/10.22178/pos.104-25>.

12. Ensuring the economic security of ukraine in the aspect of the association agreement between the EU / L. Mohilevskyi et al. European journal of sustainable development. 2021. Vol. 10, no. 2. P. 171–186. URL: <https://doi.org/10.14207/ejsd.2021.v10n2p171>.

13. Enterprise Architecture Guiding Principles. MN.gov, 2025. URL: [https://mn.gov/oet/images/EA\\_Business\\_Res\\_Principles.pdf](https://mn.gov/oet/images/EA_Business_Res_Principles.pdf).

14. Enterprise architecture principles. Aalto University. URL: <https://www.aalto.fi/en/services/enterprise-architecture-principles>.

15. Enterprise architecture principles. DfE Architecture. URL: [https://dfe-digital.github.io/architecture/principles/enterprise-architecture-principles/..](https://dfe-digital.github.io/architecture/principles/enterprise-architecture-principles/)

16. European Economic Security: current practices and further development. In-depth Analysis Requested By The INTA Committee, 2025. URL: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO\\_IDA\(2024\)754449\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754449/EXPO_IDA(2024)754449_EN.pdf).

17. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. NIST Technical Series Publications. URL: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf>.

18. Government approved national revenue strategy 2024-2030. Ministry of Finance of Ukraine. URL: <https://www.kmu.gov.ua/en/news/uriad-zatverdyyv-natsionalnu-stratehiiu-dokhodiv-20242030>.

19. Greefhorst D., Proper E. Architecture principles. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. URL: <https://doi.org/10.1007/978-3-642-20279-7>.
20. Holloway D. ISO 27001 requirement 9.2 – internal audit. ISMS.online. URL: <https://www.isms.online/iso-27001/requirements-2013/9-2-internal-audit-2013/>.
21. In 2023, Ukrainian IT Services Export Faced Its First Decline in Years. IT Ukraine Association. URL: <https://itukraine.org.ua/en/in-2023-ukrainian-it-services-export-faced-its-first-decline-in-years/>.
22. International MSECБ ISMS ISO/IEC 27001:2022 certificate is confirmed!. Центральний засвідчувальний орган. URL: <https://czo.gov.ua/en/news-details?id=654>.
23. ISO 27001 internal audits: Essential practices for ISMS compliance. TrustCloud, 2025. URL: <https://www.trustcloud.ai/iso-27001/iso-27001-internal-audits/>.
24. IT Outsourcing in Ukraine in 2025: Market overview, rates, and benefits. Varyence. URL: <https://varyence.com/blog/it-outsourcing-in-ukraine-in-2025-market-overview-rates-and-benefits/>.
25. IT sector in Ukraine. Global Government Technology Centre in Kyiv. URL: <https://www.kyivgovtechcentre.org/it-sector-ua>.
26. Koptieva H. Information support of economic security of business processes of the trade enterprise. State and regions. series: economics and business. 2020. No. 4(115). URL: <https://doi.org/10.32840/1814-1161/2020-4-15>.
27. Koval Y. Directions management of economic security of the state in the context of globalization processes. Public administration and law review. 2023. No. 3. P. 39–48. URL: <https://doi.org/10.36690/2674-5216-2023-3-39-48>.
28. Kutsenko D. Adapting enterprise economic security management mechanism to wartime risks through the prism of project management. Economics, finance and management review. 2025. No. 2(22). P. 143–152. URL: <https://doi.org/10.36690/2674-5208-2025-2-143-152>.

29. Labcorp: кодекс ділової поведінки та етики. Labcorp. 31 с. URL: [https://www.labcorp.com/content/dam/labcorp/files/compliance/labcorp-code-of-conduct/114569\\_LC\\_BRO\\_Ukrainian\\_CodeofCond22\\_FINAL.pdf](https://www.labcorp.com/content/dam/labcorp/files/compliance/labcorp-code-of-conduct/114569_LC_BRO_Ukrainian_CodeofCond22_FINAL.pdf).

30. Looking back at our Bug Bounty program in 2024. Engineering at Meta. URL: <https://engineering.fb.com/2025/02/13/security/looking-back-at-our-bug-bounty-program-in-2024/>.

31. Matiukh S. The fundamentals of forming the mechanism for implementation of the strategy for ensuring the economic security at the enterprise. Ukrainian journal of applied economics and technology. 2023. Vol. 8, no. 1. P. 27–32. URL: <https://doi.org/10.36887/2415-8453-2023-1-4>.

32. MSECБ certificate received!. Центральний засвідчувальний орган. URL: <https://czo.gov.ua/en/news-details?id=636>.

33. Nedoboi S. Models of management of financial economic security of the enterprise. Actual problems of economics. 2024. Vol. 1, no. 275. P. 25–33. URL: <https://doi.org/10.32752/1993-6788-2024-1-275-25-33>.

34. Neustroiev Y. Modern approaches to the concept of «economic security of the country». Efektyvna ekonomika. 2021. No. 1. URL: <https://doi.org/10.32702/2307-2105-2021.1.98>.

35. Over 300,000 specialists: an overview of ukraine's tech ecosystem. CodeUA. URL: <https://codeua.com/over-300000-specialists-an-overview-of-ukraines-tech-ecosystem-it-research-study/>.

36. Panchenko V., Chernenko A. Economic security management of the organization: system-structural approach. International conference on economics, law and education research (ELER 2021), Kyiv, Ukraine, 10–11 March 2021. Paris, France, 2021. URL: <https://doi.org/10.2991/aebmr.k.210320.005>.

37. Parkhomenko N. Features of economic security management of construction company. Efektyvna ekonomika. 2020. No. 5. URL: <https://doi.org/10.32702/2307-2105-2020.5.61>.

38. Parliament of Ukraine adopts State Budget for 2024. Government Portal. URL: <https://www.kmu.gov.ua/en/news/verkhovna-rada-ukrainy-pryiniiala-derzhbiudzheta-na-2024-rik>.

39. Position paper on Ukraine Digital Policy. ZPP, 2025. URL: <https://zpp.net.pl/wp-content/uploads/2024/06/Position-paper-on-Ukraine-Digital-Policy.pdf>

40. Regulations. Державне підприємство «ДІА». URL: <https://se.dia.gov.ua/en/regulations>.

41. Residents of «Dii.City» paid over 18 billion UAH in taxes in 2024 – a record in three years. Бабель. URL: <https://babel.ua/en/news/114893-residents-of-dii-city-paid-over-18-billion-uah-in-taxes-in-2024-a-record-in-three-years>.

42. Rules And Procedures For The Operation Of The Qualified Trust Service Provider «DIIA». SE «DIIA». 141 p. URL: [https://ca.dia.gov.ua/uploads/regulations/Reglament\\_DIIA\\_20250117\\_en.pdf](https://ca.dia.gov.ua/uploads/regulations/Reglament_DIIA_20250117_en.pdf).

43. Starlink in the Russian-Ukrainian War. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Starlink\\_in\\_the\\_Russian-Ukrainian\\_War](https://en.wikipedia.org/wiki/Starlink_in_the_Russian-Ukrainian_War).

44. State enterprise DIIA. Державне підприємство «ДІА». URL: <https://se.dia.gov.ua/en/>.

45. State named DIIA. How the ministry of digital transformation develops ukraine's digital governance. Свідомі. URL: <https://svidomi.in.ua/en/page/state-named-dia-how-the-ministry-of-digital-transformation-develops-ukraines-digital-governance-written-by-mariia-patoka>.

46. System of electronic interaction of state electronic information resources SE DIIA. Державне підприємство «ДІА». URL: <https://se.dia.gov.ua/en/trembita>.

47. Thach P. ISO 27001: internal audit requirements. Schellman Compliance. URL: <https://www.schellman.com/blog/iso-certifications/iso-27001-requirements>.

48. The Future of the Security Sector in Ukraine – United States Institute of Peace, 2024. URL: <https://www.usip.org/sites/default/files/2024-10/future-security-sector-ukraine.pdf>

49. The Global Risks Report 2025 20th Edition. World Economic Forum: Publications, 2025. URL: [https://reports.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2025.pdf](https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf).

50. The impact of digital transformation on the economic security of Ukraine / S. Spivakovskyy et al. Studies of applied economics. 2021. Vol. 39, no. 5. URL: <https://doi.org/10.25115/eea.v39i5.5040>.

51. The platform powering Diia has been certified to work with high-security resources. Lviv IT Cluster. URL: <https://itcluster.lviv.ua/en/the-platform-powering-diia-has-been-certified-to-work-with-high-security-resources/>.

52. The state of Ukrainian IT exports in the first quarter: a comparison with the previous year. URL: <https://kossasoft.com/blog/the-state-of-ukrainian-it-exports-in-the-first-quarter-a-comparison-with-the-previous-year>.

53. Threats and dangers to economic security of Ukraine in the terms of war / S. Onyshchenko et al. Rivista di studi sulla sostenibilita'. 2025. PRE. P. 1–20. URL: <https://doi.org/10.3280/riss2025oa19683>.

54. Tulchynska S., Tkachenko T. Principles of the system of economic security of industrial enterprises under the conditions of competition. Herald of Khmelnytskyi National University. Economic sciences. 2023. Vol. 318, no. 3. P. 226–230. URL: <https://doi.org/10.31891/2307-5740-2023-318-3-35>.

55. Ukraine: Digital resilience in a time of war – Brookings Institution. George Ingram and Priya Vora. 2024. URL: <https://www.brookings.edu/wp-content/uploads/2024/01/Digital-resilience-in-a-time-of-war-Final.pdf>

56. Ukraine's budget for 2024. Wilson Center. URL: <https://www.wilsoncenter.org/blog-post/ukraines-budget-2024>.

57. Ukraine's digital transformation: innovation for resilience. Harvard Kennedy School. URL: <https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience>.

58. Ukraine's IT Sector in 2024: driving innovation, resilience, and global integration. FOCUS ON Business. URL: <https://focusonbusiness.eu/en/news/ukraine-s-it-sector-in-2024-driving-innovation-resilience-and-global-integration/6645>.

59. Ukrainian Economy in 2024: Special Edition of the Tracker. Centre for Economic Strategy. URL: [https://ces.org.ua/en/ukrainian\\_economy\\_in\\_2024/](https://ces.org.ua/en/ukrainian_economy_in_2024/).

60. Ukrainian tech industry shows resilience in the face of war: IT research ukraine 2024. TechUkraine. URL: <https://techukraine.org/2024/12/05/ukrainian-tech-industry-shows-resilience-in-the-face-of-war-it-research-ukraine-2024/>.

61. Unsupported browser. HackerOne. URL: <https://hackerone.com/bcny?type=team>.

62. Vasyleha V. V. The mechanism for ensuring the economic security of the enterprise under the influence of the external environment. Business inform. 2024. Vol. 2024, no. 553. P. 146–153. URL: <https://doi.org/10.32983/2222-4459-2024-2-146-153>.

63. Vlasenko V. Principle approach to forming and implementing an effective system of enterprise's economic security under conditions of economic recovery. Development service industry management. 2023. No. 4. P. 34–41. URL: [https://doi.org/10.31891/dsim-2023-4\(5\)](https://doi.org/10.31891/dsim-2023-4(5)).

64. Vytvytska O., Slyvinska O. Current approaches to the formation of the economic security management mechanism of the enterprise. Electronic scientific journal intellectualization of logistics and supply chain management #1 2020. 2023. No. 21. P. 49–54. URL: <https://doi.org/10.46783/smart-scm/2023-21-6>.

65. Vytvytska O., Slyvinska O. Fundamentals of the formation of the economic security management system of the enterprise. Ukrainian journal of applied economics and technology. 2023. Vol. 8, no. 3. P. 251–255. URL: <https://doi.org/10.36887/2415-8453-2023-3-38>.

66. What is data classification?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/data-classification>.

67. WINWIN: ukraine approves innovation digital development strategy until 2030. Національний університет «Львівська політехніка». URL: <https://lpnu.ua/en/news/winwin-ukraine-approves-innovation-digital-development-strategy-until-2030>.

68. Yermolenko O. A., Nasrullayev R. S. Principles of ensuring the economic security system of enterprises in the context of digitalization. The problems of economy. 2025. Vol. 1, no. 63. P. 158–164. URL: <https://doi.org/10.32983/2222-0712-2025-1-158-164>.

69. Zavidna L., Maliuta L. Corporate social responsibility as a key tool of economic business security during war. International interdisciplinary scientific journal «expert». 2024. Vol. 1, no. 4. P. 20–34. URL: <https://doi.org/10.62034/2815-5300/2024-v1-i4-002>.

70. Zhadko K., Samoilenko D. Economic security of enterprises in the conditions of digital technologies and pandemic. Central ukrainian scientific bulletin. economic sciences. 2020. No. 5(38). P. 170–176. URL: [https://doi.org/10.32515/2663-1636.2020.5\(38\).170-176](https://doi.org/10.32515/2663-1636.2020.5(38).170-176).

71. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. Національний інститут стратегічних досліджень 2025. URL: [https://niss.gov.ua/sites/default/files/2023-05/executive-summary\\_ecsecurity\\_2023\\_gotovee-1.pdf](https://niss.gov.ua/sites/default/files/2023-05/executive-summary_ecsecurity_2023_gotovee-1.pdf)

72. Антикорупційна програма ДП «Інформаційно-іміджевий центр». URL: [https://enic.in.ua/attachments/anticorr\\_programm.pdf](https://enic.in.ua/attachments/anticorr_programm.pdf).

73. Вороніна В.Л., Спінжар Р.В. Аналіз підходів до визначення поняття економічної безпеки підприємства. Економічний форум. 2019. Т. 1, № 4. С. 109–115. URL: <https://doi.org/10.36910/6765-2308-8559-2019-4-17>.

74. Гапєєва О., Головка Р. Особливості формування системи економічної безпеки підприємств. Академічні візії. 2025. № 40/2025. С. 1–11. URL: <https://doi.org/10.5281/zenodo.14917628>.

75. Герасименко Ю.С. Економічна безпека діяльності підприємства: навчально-методичний посібник. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2024. 212 с. URL: <https://surl.li/alwyia>.

76. Дейнега І. О., Пиртко М. С. Економічна безпека підприємства: зміна парадигми. Цифрова економіка та економічна безпека. 2025. № 4 (19). С. 124–130. URL: <https://doi.org/10.32782/dees.19-19/>

77. Державне управління економічною безпекою України: теорія та практика: монографія / З. В. Гбур. – Кам'янець-Подільський: ТОВ «Друкарня «Рута»», 2018. – 408 с. URL: <https://www.nuozu.edu.ua/zagruzka2/EB3.pdf>.

78. Деякі питання об'єктів критичної інфраструктури: Постанова Каб. Міністрів України від 09.10.2020 № 1109: станом на 22 листоп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text>.

79. Дія.City у 2024 році: вдвічі більше резидентів, оборонні компанії – серед лідерів за доходами. Офіс ефективного регулювання. URL: <https://brdo.com.ua/news/diya-city-u-2024-rotsi-vdvichi-bilshe-rezydentiv-oboronni-kompaniyi-sered-lideriv-za-dohodamy/>.

80. Договір про надання кваліфікованих електронних довірчих послуг. Електронний підпис Дія. URL: [https://ca.diia.gov.ua/contract\\_diia](https://ca.diia.gov.ua/contract_diia).

81. Долучайтесь до нових конкурсів програми «Цифрова Європа» на 2025 рік. Міністерство цифрової трансформації України. URL: <https://thedigital.gov.ua/news/technologies/doluchaytesya-do-novikh-konkursiv-programi-tsifrova-evropa-na-2025-rik>.

82. Економічна безпека аграрних підприємств Львівської області та шляхи її покращання. Михалюк Д.О. – Кваліфікаційна робота магістра. Кафедра підприємництва та торгівлі. Дубляни, Львівський НУП, 2024 р. 69 с. URL: <https://surl.li/fgdcua>.

83. Економічна безпека України в умовах довготривалої війни / Я. Б. Базиліук та ін. Нац. ін-т стратег. дослідж., 2024. URL: <https://doi.org/10.53679/niss-analytrep.2024.08>.

84. Єдиний державний веб-портал електронних послуг ДІА. ДП «ДІА». Державне підприємство «ДІА». URL: <https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia>.

85. Жилін І. М. Теоретичні аспекти формування економічної безпеки підприємства. Agrosvit. 2024. № 17. С. 108–114. URL: <https://doi.org/10.32702/2306-6792.2024.17.108>.

86. Жураковська А., Лукашова Д., Павлов Р. Challenges and specificity of ensuring the economic security of the enterprise in crisis conditions. Економіка та суспільство. 2024. No. 68. URL: <https://doi.org/10.32782/2524-0072/2024-68-100>.

87. З 1 січня 2020 року Єдиний державний веб-портал електронних послуг виконує також функції Єдиного державного порталу адміністративних послуг. Державне підприємство «ДІА». URL: <https://my.gov.ua/info/news/348/details>.

88. Загороднюк О. В., Горбатюк М. І., Длугоборська Л. В. Theoretical principles of ensuring the economic security of enterprises in modern conditions. Collected works of uman national university of horticulture. 2024. Vol. 2, no. 104. P. 297–307. URL: <https://doi.org/10.32782/2415-8240-2024-104-2-297-307>.

89. Запобігання корупції ДП «ДІА». Державне підприємство «ДІА». URL: <https://se.dia.gov.ua/corruption-prevention>.

90. Захарова О.І. Побудова комплексної системи забезпечення економічної безпеки підприємства. Бібліотека Університету «КРОК». 2024. 12 с. URL: [https://library.krok.edu.ua/media/library/category/statti/zakharov\\_0012.pdf](https://library.krok.edu.ua/media/library/category/statti/zakharov_0012.pdf)

91. Ільченко М. Принципи побудови системи економічної безпеки підприємства. Просторовий розвиток територій: традиції та інновації: матеріали IV Міжнар. наук.-практ. конф., м. Київ, 14 листоп. 2024 р. С. 127–129. URL: <https://repository.knuba.edu.ua/server/api/core/bitstreams/0826a894-4695-4df8-afe5-a9b35a560ccc/content..>

92. ІТ-сектор втратив 7,5 тисячі ФОПів за 10 міс. 2025 року. Finteco.com.ua. URL: <https://finteco.com.ua/article/27698-v-ukraini-za-rik-it-sektor-vtratyv-7-5-tysiachi-fopiv-ale-vakansii-zrostaiut-opendatabot/>.

93. Карвацка Н., Габай В., Глабчастий Н. Управління економічною безпекою підприємства в умовах циркулярної економіки. Development service industry management. 2025. № 1. С. 154–159. URL: [https://doi.org/10.31891/dsim-2025-9\(21\)](https://doi.org/10.31891/dsim-2025-9(21)).

94. Кількість кібератак на Україну за 2024 рік зросла на 70%. Львівський портал. URL: <https://portal.lviv.ua/news/2025/01/09/kilkist-kiberatak-na-ukrainu-za-2024-rik-zroslo-na-70>.

95. Кодекс поведінки працівників Державного підприємства «Оператор ринку». ДП «Оператор ринку». 6 с. URL: <https://www.oree.com.ua/data/kodeks.pdf>.

96. Конкурентна розвідка як інструмент забезпечення економічної безпеки підприємства. Патюк Б.Р. – Кваліфікаційна робота бакалавра. Кафедра менеджменту підприємств. Київ, НТУУ «КПІ ім. І.Сікорського», 2025. 103 с. URL: <https://surl.li/nxxuua>.

97. Міненко М. Сутність та види суб'єктів забезпечення економічної безпеки підприємств. Ефективна економіка. 2014. № 2 (2014). URL: <http://www.economy.nayka.com.ua/?op=1&z=2802>.

98. Нам'Ясенко В. Економічна безпека підприємства в умовах воєнного стану. Economy of ukraine. 2025. Т. 68, № 6 (763). С. 25–38. URL: <https://doi.org/10.15407/economyukr.2025.06.025>.

99. Науменко Є. Механізм управління економічною безпекою підприємства в умовах кризи. Молодий вчений. 2017. № 6 (46). URL: <http://molodyvcheny.in.ua/files/journal/2017/6/105.pdf>.

100. Нормативні засади діяльності. Державне підприємство «ДІА». URL: <https://se.diia.gov.ua/regulations>.

101. Основні вимоги до якості обслуговування суб'єктів звернення. Дія. Платформа Центрів. URL: <https://center.diia.gov.ua/library/osnovni-vimogi-do-akosti-obslugovuvanna-subektiv-zvernenna>.

102. Основні положення системи безпеки підприємства. Конспект лекції Запорізького національного університету. URL: <https://moodle.znu.edu.ua/mod/resource/view.php?id=245730>.

103. Пикало О. До «Дія.City» у 2024 році приєдналося 880 нових резидентів. Forbes.ua. URL: <https://forbes.ua/news/do-diyacity-u-2024-rotsi-priednalosya-880-novikh-rezidentiv-06012025-26074>.

104. Питання Єдиного державного веб-порталу електронних послуг та Єдиного державного порталу адміністративних послуг: Постанова Каб.

Міністрів України від 04.12.2019 № 1137: станом на 7 листоп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text>.

105. Пікуліна О. В., Чаркіна Т. Ю. Специфіка забезпечення економічної безпеки в умовах воєнного стану. Інвестиції: практика та досвід. 2025. № 22. С. 87–94. URL: <https://doi.org/10.32702/2306-6814.2025.22.87>.

106. Положення про комерційну таємницю та конфіденційну інформацію ТОВ «Миколаївська електропостачальна компанія». ТОВ «Миколаївська електропостачальна компанія». 8 с. URL: [https://elektropostach.mk.ua/files/electricity\\_supply/Regulations\\_on\\_trade\\_secrets\\_and\\_confidential\\_information.pdf](https://elektropostach.mk.ua/files/electricity_supply/Regulations_on_trade_secrets_and_confidential_information.pdf).

107. Про внесення змін до Податкового кодексу України та інших законів України щодо стимулювання розвитку цифрової економіки в Україні: Закон України від 14.12.2021 № 1946-IX. URL: <https://zakon.rada.gov.ua/laws/show/1946-20#Text>.

108. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>.

109. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX: станом на 21 верес. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.

110. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 19 жовт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

111. Про підприємство ДП «ДІА». Державне підприємство «ДІА». URL: <https://se.diia.gov.ua/about-company>.

112. Про хмарні послуги: Закон України від 17.02.2022 № 2075-IX: станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text>.

113. Рамський А.Ю., Ковтун Г.С. Інформаційне забезпечення економічної безпеки підприємства. Інформаційно-аналітичне забезпечення ефективності діяльності підприємств у контексті економічної безпеки в умовах інтеграції з

ЄС: матеріали Міжнародної науково-практичної Інтернет-конференції, 27 травня 2016 р., м. Київ. С. 177-178. URL: [https://er.knutd.edu.ua/bitstream/123456789/4905/1/20160527IAZ\\_P177-178.pdf](https://er.knutd.edu.ua/bitstream/123456789/4905/1/20160527IAZ_P177-178.pdf).

114. Регламент роботи кваліфікованого надавача електронних довірчих послуг «Дія». ДП «ДІА». 196 с. URL: [https://ca.diia.gov.ua/uploads/regulations/Reglament\\_DIIA\\_20240310.pdf](https://ca.diia.gov.ua/uploads/regulations/Reglament_DIIA_20240310.pdf).

115. Сак Т.В., Шепелюк Н.П. Діагностика фінансової стійкості підприємства: методологія та практика застосування. Економічний журнал Одеського політехнічного університету. 2023. № 4 (26). С. 37-44. DOI: 10.15276/EJ.04.2023.5.

116. Система електронної взаємодії державних електронних інформаційних ресурсів ДП «ДІА». Державне підприємство «ДІА». URL: <https://se.diia.gov.ua/trembita>.

117. Сімагін Д. Скільки в Україні IT-фахівців: результати дослідження. Highload.tech. URL: <https://highload.tech/uk/skilky-v-ukrayini-it-fahivtsiv-rezultaty-doslidzhennya/>.

118. Сімагін Д. У 2024 році кількість резидентів «Дія.City» зросла в 2,4 рази. Highload.tech. URL: <https://highload.tech/uk/u-2024-rotsi-kilkist-rezydentiv-diya-city-zrosla-v-2-4-razy/>.

119. У 2024 році кількість кібератак на Україну зросла на 70%. Інститут масової інформації. URL: <https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931>.

120. У 2024 році резиденти Дія City сплатили 18 млрд гривень податків. DOU. URL: <https://dou.ua/lenta/news/taxes-from-residents-diia-city/>.

121. У 2025-му бюджет Мінцифри може зрости на понад 60%. На що підуть кошти і скільки виділили цьогоріч. DOU. URL: <https://dou.ua/lenta/news/ministry-of-digital-transformation-budget-2025/>.

122. У травні експорт IT-послуг з України зріс майже на 3%. Аналізуємо дані Нацбанку. DOU. URL: <https://dou.ua/lenta/news/it-eksport-may-2024>.

123. Удосконалення механізму управління економічною безпекою підприємства. Григор'єва Н.П. – Кваліфікаційна робота магістра. Кафедра обліку, оподаткування та управління фінансово-економічною безпекою. Дніпро, ДДАЕУ, 2024 р. 75 с. URL: <https://surl.li/btimcw>.

124. Україна тимчасово не платитиме внески за програмами приєднання до ЄС. LexInform. URL: <https://lexinform.com.ua/zakonodavstvo/ukrayina-tymchasovo-ne-platytyime-vnesky-za-programamy-pryyednannya-do-yes/>.

125. Фісуненко П., Булеєв Ю. Принципи побудови системи економічної безпеки підприємства: вплив трансформаційних перетворень. Сталий розвиток економіки. 2025. № 4(51). С. 342–348. URL: <https://doi.org/10.32782/2308-1988/2024-51-48>.

126. Формалізація інформаційних потоків для захисту операційних систем сімейства *bsd* від несанкціонованого дослідження / С. Гнатюк та ін. Кібербезпека: освіта, наука, техніка. 2021. № 1 (13). С. 145–157. URL: <https://doi.org/10.28925/2663-4023.2021.13.145157>.

127. Яка інформація належить до публічної інформації?. Головне управління ДПС у Дніпропетровській області. URL: <https://dp.tax.gov.ua/media-ark/news-ark/668490.html>.