

ВІДГУК

офіційного опонента, доцента кафедри менеджменту, бізнесу і адміністрування
Державного біотехнологічного університету, доктора філософії з менеджменту,
доц. Міненко С.І.

на дисертацію Черкаського Григорія Ігоровича «Організаційно-управлінські
механізми забезпечення інформаційної безпеки підприємницької діяльності в
умовах глобальної економічної турбулентності», здобувача наукового ступеня
доктор філософії зі спеціальності 073 «Менеджмент»

АКТУАЛЬНІСТЬ ТЕМИ ДОСЛІДЖЕННЯ ТА ЇЇ ЗВ'ЯЗОК ІЗ НАУКОВИМИ ПРОГРАМАМИ

В умовах стрімкої цифровізації економічних процесів та масштабування цифрових технологій інформаційні ресурси стають ключовим стратегічним активом і джерелом конкурентних переваг сучасного бізнесу. Водночас вихід підприємницької діяльності у цифровий простір супроводжується значним зростанням кіберризиків, несанкціонованих витоків конфіденційних даних та уразливості корпоративних ІТ-інфраструктур. Ескалація геополітичної напруженості, гібридні загрози та глобальна економічна турбулентність додатково посилюють виклики для цифрової стійкості вітчизняних суб'єктів господарювання. Традиційні підходи до забезпечення безпеки, орієнтовані виключно на програмно-апаратний захист, виявляються недостатньо гнучкими та не враховують комплексний вплив людського й соціально-психологічного чинників. У зв'язку з цим виникає гостра потреба у формуванні адаптивних організаційно-управлінських механізмів, здатних оперативно реагувати на дестабілізуючі фактори та мінімізувати потенційні збитки. Окремого наукового й практичного опрацювання потребують методи оцінювання доцільності та ефекту від цифрових інвестицій у заходи кіберзахисту, зокрема із застосуванням інструментарію розрахунку спеціалізованого показника ROI_{dig} . Окрім того, відсутність цілісних стратегічних орієнтирів та адаптивних структурно-функціональних моделей суттєво ускладнює процес прийняття обґрунтованих управлінських рішень щодо захисту цифрових активів у секторі МСБ. Отже, висока практична затребуваність прикладного інструментарію захисту інформаційно-комунікаційного середовища підприємств та потреба в поглибленні теоретико-методичних засад його формування зумовлюють беззаперечну актуальність обраної теми дослідження.

Дисертаційна робота виконана в межах наукових досліджень кафедри менеджменту Національного університету кораблебудування імені адмірала Макарова та відповідає напрямам науково-дослідних тем, спрямованих на розроблення теоретико-методичних засад і практичного інструментарію

забезпечення конкурентоспроможності, цифровізації та інформаційної безпеки підприємницької діяльності. Результати дослідження логічно продовжують і розвивають зазначені наукові напрями.

ОБГРУНТОВАНІСТЬ І ДОСТОВІРНІСТЬ РЕЗУЛЬТАТІВ

Обґрунтованість і достовірність результатів дисертаційної роботи Черкаського Г. І. «Організаційно-управлінські механізми забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності» забезпечуються цілісністю методологічного підходу, коректним добором методів, логічною узгодженістю теоретичних положень з емпіричними результатами, а також апробацією напрацювань у науковому середовищі та практичним використанням окремих рекомендацій.

Теоретична надійність висновків ґрунтується на положеннях теорії економіки підприємства, менеджменту, системного аналізу, концепцій цифрової трансформації та інформаційної безпеки. Критичне опрацювання фундаментальних праць вітчизняних і зарубіжних науковців дало змогу уточнити сутність і специфіку інформаційної безпеки підприємства у цифровому середовищі, обґрунтувати структуру організаційно-управлінського механізму з урахуванням соціально-психологічних чинників та сформулювати методологічну логіку цифрового кіберзахисту бізнесу.

Методична достовірність підтверджується застосуванням комплексу взаємодоповнювальних методів. Теоретичні узагальнення отримано із використанням аналізу й синтезу, індукції та дедукції, формалізації, класифікації, системного й порівняльного аналізу. Емпіричну частину виконано на основі аналізу нормативно-правової бази, статистичних даних щодо цифровізації бізнес-процесів, капітальних інвестицій, а також динаміки розвитку малого та середнього підприємництва, що дозволило ідентифікувати й кількісно оцінити ключові загрози інформаційній безпеці суб'єктів господарювання. Репрезентативність та надійність масиву аналітичних даних посилена застосуванням індексного підходу, методів порівняльного та структурно-динамічного аналізу.

Обґрунтованість результатів моделювання забезпечено розробленням інструментарію оцінювання, сценарного прогнозування та розробки адаптивної структурно-функціональної моделі розвитку підприємництва. Оцінювання ефективності цифрових інвестицій та заходів безпеки здійснювалося із застосуванням розрахунку показника ROI_{dig} ; прогнозування розвитку та реакції системи на загрози — на основі багатофакторного сценарного підходу. Адаптивну модель побудовано із застосуванням структурно-функціонального

та процесного підходів, що дало змогу формалізувати алгоритми реагування підприємства на кіберризики та оптимізувати витрати на ІТ-захист.

Додатковим підтвердженням достовірності є апробація результатів на наукових конференціях, обговорення на засіданнях випускової кафедри, а також публікація основних положень у наукових фахових виданнях України та матеріалах конференцій.

Таким чином, поєднання обґрунтованої теоретичної бази, адекватного методичного інструментарію, репрезентативної емпіричної основи та коректності моделювання забезпечує високий рівень достовірності положень, висновків і рекомендацій дисертаційної роботи.

СТРУКТУРА ТА ЗМІСТ ДИСЕРТАЦІЇ

Дисертаційна робота є логічно вибудованим, завершеним науковим дослідженням, спрямованим на розроблення та вдосконалення теоретико-методичних засад забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації.

Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальна структура забезпечує послідовний перехід від теоретичного обґрунтування проблематики до аналітичного дослідження та розроблення прикладного інструментарію.

У вступі обґрунтовано актуальність теми, визначено мету, завдання, об'єкт і предмет дослідження, розкрито методологічну основу, наукову новизну та практичне значення отриманих результатів, наведено інформацію про апробацію та публікації.

У першому розділі – «Теоретико-методичні засади організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності» – систематизовано наукові підходи до трактування сутності інформаційної безпеки підприємництва в умовах цифрової трансформації. Розкрито зміст та елементи організаційно-управлінського механізму забезпечення інформаційної безпеки з урахуванням соціально-психологічних чинників. Систематизовано та уточнено методичні підходи до оцінювання цифрових інвестицій та ефективності заходів захисту даних на основі розрахунку показника ROI_{dig} .

У другому розділі – «Аналіз організаційно-управлінських передумов забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності» – здійснено комплексне аналітичне дослідження середовища функціонування суб'єктів господарювання та факторів впливу на їхню цифрову стійкість. Досліджено динаміку розвитку підприємницької діяльності, оцінено стан капітальних інвестицій та рівень

цифровізації бізнес-процесів. Ідентифіковано ключові загрози та тенденції в системі забезпечення інформаційної безпеки вітчизняних підприємств в умовах глобальної економічної турбулентності.

У третьому розділі – «Стратегічні вектори організаційно-управлінських засад інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності» – розроблено концептуальні засади формування системи інформаційної безпеки та побудовано адаптивну структурно-функціональну модель розвитку підприємництва в умовах цифрової трансформації. Запропоновано стратегічні пріоритети та практичні засади реагування на кіберризики із застосуванням сценарного підходу та інструментів цифрового моделювання. Сформовано практичні рекомендації щодо підвищення ефективності управління інформаційними ресурсами та забезпечення довгострокової безпеки бізнесу.

У висновках узагальнено основні результати дослідження, сформульовано теоретичні положення та практичні рекомендації, що розвивають методологію та інструментарій забезпечення інформаційної безпеки підприємницької діяльності.

Загалом структура дисертації є внутрішньо узгодженою, забезпечує системність викладу матеріалу та відображає логіку досягнення поставленої мети – від теоретичного обґрунтування до прикладної реалізації запропонованих моделей і методів.

НАУКОВА НОВИЗНА

У дисертаційній роботі викладено теоретико-методичні засади і практичні рекомендації щодо удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки підприємницької діяльності в умовах глобальної економічної турбулентності. Наукові результати дослідження орієнтовані на розроблення комплексу сучасних економічних механізмів та моделей інформаційної безпеки підприємницької діяльності. Найбільш важливими науковими результатами, що характеризуються новизною, є наступні положення:

удосконалено:

- систему стратегічних векторів підприємницької діяльності в умовах глобальної економічної турбулентності (розділ 3, п.3.3.), що на відміну від існуючих, диференційовано за трьома взаємопов'язаними векторами, що дозволить уникнути уніфікації управлінських рішень та врахувати галузеву специфіку капіталомісткості й поточний рівень діджиталізації бізнесу. Особливістю вектора А є те, що закупівля нового технологічного обладнання, верстатів чи побудова логістичних комплексів має супроводжуватися одночасним розгортанням цифрових систем управління та спрямованим на

переробну промисловість, будівництво, сільське господарство. Вектор Б є базовим для сектору малого та середнього підприємництва (із чисельністю зайнятих 10–249 осіб), а також для підприємств сфери торгівлі та послуг, що передбачає відмову від капіталомістких ІТ-проектів «з нуля» на користь готових хмарних рішень. Вектор В орієнтований на високотехнологічні сегменти української економіки (ІТ-сектор, фінансову діяльність та інноваційні наукомісткі стартапи) особливістю є сертифікація українських цифрових продуктів за стандартами GDPR, інтеграцію в європейські цифрові ланцюги створення вартості та масштабування рішень у сферах FinTech, AgTech, GovTech та MilitaryTech; створення консорціумів між національними ІТ-компаніями та вітчизняними індустріальними підприємствами;

- методику оцінки інтегральної фінансово-економічної захищеності підприємств (розділ 3, п.3.3.), яка, на відміну від існуючих підходів фінансового аналізу, пов'язує коефіцієнти ліквідності та капітальних інвестицій із вартісною оцінкою безпекових ризиків. Це дозволяє диференціювати управлінські стратегії системи інформаційної безпеки між капіталомісткою (CAPEX) та сервісною (OPEX) моделями захисту на основі масштабу та реального фінансового буфера підприємства;

набули подальшого розвитку:

- порівняльний аналіз моделей управління інформаційною безпекою підприємств в ЄС та Україні (розділ 3, п.3.1.), який показав наявність суттєвих концептуальних та інституціональних розбіжностей між двома системами, що дозволило сформулювати стратегічні шляхи імплементації європейського досвіду. Це свідчать про необхідність модернізації системи захисту інформаційних ресурсів вітчизняних підприємств в умовах турбулентності та базування не на пасивному копіюванні регуляторних вимог, а на принципах цифрової операційної резильєнтності та економічної доцільності;

- результати структурно-динамічного аналізу макроекономічних детермінант розвитку бізнес-систем (розділ 2, п.2.2), що дозволяють виокремити децентралізований контур контрагентів та партнерів, враховують критично високу щільність мікросуб'єктів та фізичних осіб-підприємців у структурі національної економіки. Впровадження цього контуру науково обґрунтовує необхідність відмови від застарілих концепцій локального захисту корпоративного периметра на користь гнучкої архітектури нульової довіри. Практична реалізація сформованого підходу дозволяє великим та середнім підприємствам здійснювати безперервний експрес-скоринг рівня кібергігієни зовнішніх суб'єктів, що підключаються до їхніх інформаційних ресурсів. Представлена модель мінімізує вразливість бізнес-систем до масових і скоординованих атак через ланцюги постачання в умовах воєнного стану.

ПРАКТИЧНЕ ЗНАЧЕННЯ РЕЗУЛЬТАТІВ

Практичне значення результатів дисертаційної роботи полягає у розробленні та апробації комплексного методичного інструментарію забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації, який може бути безпосередньо впроваджений у діяльність суб'єктів господарювання різних галузей.

Запропоновані в роботі: метод оцінювання цифрових інвестицій та ефективності заходів захисту даних із використанням показника ROI_{dig} ; адаптивний метод прогнозування й реагування на кіберзагрози на основі сценарного аналізу та структурно-функціонального моделювання; організаційно-управлінський механізм забезпечення інформаційної безпеки із урахуванням соціально-психологічних чинників — забезпечують підвищення обґрунтованості управлінських рішень, своєчасну ідентифікацію критичних інформаційних ризиків, формування проактивних стратегій кіберзахисту та зниження рівня фінансових і репутаційних втрат у коротко- і довгостроковій перспективі.

Практична цінність одержаних результатів полягає також у можливості: інтеграції техніко-технологічних, організаційних і людських чинників у єдину систему корпоративного менеджменту інформаційної безпеки; підвищення адаптивності та цифрової стійкості підприємств до змін регуляторного середовища та кіберзагроз; оптимізації витрат на IT-інфраструктуру та захист даних; формування стратегічних конкурентних переваг на основі безпеки цифрових активів та високого рівня довіри клієнтів і партнерів.

Розроблені підходи можуть бути використані при формуванні внутрішніх регламентів та положень з інформаційної безпеки, розробленні корпоративних стратегій цифрової трансформації, побудові систем внутрішнього контролю та антикризового управління кіберінцидентами. Результати дослідження впроваджені у діяльність підприємств (що підтверджено відповідними довідками) та використовуються у навчальному процесі закладу вищої освіти під час викладання дисциплін з підприємництва, інформаційної безпеки та цифрової економіки. Це підтверджує їх прикладну спрямованість, практичну релевантність та можливість масштабування в умовах цифровізації економіки.

ВІДОБРАЖЕННЯ РЕЗУЛЬТАТІВ У ПУБЛІКАЦІЯХ

Основні наукові положення, висновки та рекомендації дисертаційної роботи повною мірою відображені в опублікованих працях здобувача та відповідають змісту й логіці проведеного дослідження.

За темою дисертації опубліковано 11 наукових праць загальним обсягом 2,73 авт. арк., з яких особисто автору належить 1,55 авт. арк. Із них: 5 статей у наукових фахових виданнях, 1 – стаття у наукометричній базі Web of Science, 5 – у матеріалах науково-практичних конференцій.

У фахових статтях висвітлено теоретико-методичні засади забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації, удосконалені методи оцінювання, моніторингу та управління кіберризиками, а також результати розробки та впровадження адаптивної структурно-функціональної моделі з використанням інструментарію оцінки цифрових інвестицій (ROI_{dig}), сценарного та індексного підходів. Публікації містять обґрунтування концептуальних положень, систематизацію чинників впливу та ключових загроз у цифровому середовищі, а також результати аналізу сучасного стану та тенденцій розвитку інформаційної безпеки суб'єктів господарювання.

Матеріали конференцій відображають апробацію ключових положень дисертації, обговорення отриманих результатів у науковому середовищі та уточнення окремих методичних аспектів дослідження.

Опубліковані праці забезпечують повноту розкриття наукової новизни, практичного значення та основних результатів дисертаційної роботи. Кількість і зміст публікацій відповідають встановленим вимогам до дисертацій на здобуття наукового ступеня доктора філософії та підтверджують самостійність і системність проведеного дослідження.

ДИСКУСІЙНІ АСПЕКТИ

Попри високий рівень теоретичної обґрунтованості та методичної завершеності дослідження, окремі положення дисертації можуть бути предметом наукової дискусії та подальшого уточнення.

1. Обґрунтовуючи сутність поняття організаційно-управлінського механізму, автор акцентує увагу на соціально-психологічних чинниках та моніторингу дій персоналу (розділ 1). У зв'язку з цим виникає дискусійне питання: де саме проходить межа між необхідним контролем дій працівників для забезпечення інформаційної безпеки та порушенням їхнього права на приватність і нормами законодавства про захист персональних даних? Практичне впровадження таких заходів без належного регуляторного балансу може спричинити зростання внутрішньої напруги в колективі.

2. Аналіз стану та тенденцій розвитку інформаційної безпеки здебільшого обмежується графічним висвітленням та описом динаміки окремих показників (структура інвестицій, рівень цифровізації, динаміка ВДВ). Водночас у розділі 2 бракує економетричного інструментарію (наприклад,

кореляційно-регресійного аналізу чи факторного моделювання), який би математично довів ступінь і щільність впливу конкретних показників інформаційної безпеки на підсумкові результати фінансово-господарської діяльності підприємств.

3. Розроблена адаптивна структурно-функціональна модель орієнтована на реагування в умовах «градаційного» цифрового розвитку (розділ 3). Водночас лишається відкритим питання її функціонування під час форс-мажорних екстремальних впливів (наприклад, повної втрати фізичної ІТ-інфраструктури, блек-аутів чи тривалих кібервійн).

4. Запропонована методологічна оцінка ефективності цифрових інвестицій (ROI_{dig}) передбачає наявність чіткого управлінського обліку витрат на захист даних (розділ 3). Проте для суб'єктів малого та мікробізнесу характерна відсутність відокремленого обліку ІТ-витрат та складнощі у виокремленні прямого економічного ефекту від відсутності витоків інформації. Потребує додаткового обґрунтування застосовність цієї методики саме для МСБ, а не лише для великих корпорацій.

5. При формуванні загальних концептуальних засад формування системи інформаційної безпеки підприємств, однак, запропоновані принципи та етапи мають переважно якісний, описовий характер (розділ 3). У тексті бракує чіткої формалізованої карти (або матриці) ідентифікації та ранжування інформаційних ризиків за ступенем їхнього впливу і ймовірністю виникнення. Це робить запропоновану концептуальну основу занадто загальною і ускладнює її безпосереднє застосування на практиці.

Водночас дискусійним залишається питання збалансування рівнів безпеки та операційної ефективності підприємства у короткостроковому й довгостроковому періодах. Зокрема, для окремих підприємств (особливо сектору МСБ) впровадження комплексних систем інформаційної безпеки та цифрового захисту може супроводжуватися значними капітальними витратами, додатковим бюрократичним навантаженням на бізнес-процеси та уповільненням операційної діяльності через жорсткий регламент контролю. Це потребує подальшого розвитку методичних підходів до оцінювання економічної доцільності, співвідношення «витрати–ризик» та реальної ефективності інтеграції інструментів кіберзахисту в загальну систему управління підприємством.

ЗАГАЛЬНИЙ ВИСНОВОК

Дисертаційна робота Черкаського Григорія Ігоровича є завершеним, цілісним і концептуально узгодженим науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання щодо розвитку теоретико-

методичних засад і розробки практичного інструментарію забезпечення інформаційної безпеки підприємницької діяльності в умовах цифрової трансформації та глобальної економічної турбулентності.

У роботі здійснено системне переосмислення сутності інформаційної безпеки підприємства як комплексної системи захисту інформаційних ресурсів, бізнес-процесів і цифрових активів, обґрунтовано концептуально-понятійні засади її формування, уточнено систематизацію чинників впливу та ключових загроз у цифровому середовищі, а також розроблено й удосконалено методи їх оцінювання, моніторингу та протидії. Запропоновані підходи базуються на поєднанні адаптивного та структурно-функціонального моделювання, інструментарію оцінки цифрових інвестицій (ROI_{dig}), сценарного й індексного аналізу, що забезпечує підвищення ефективності управлінських рішень і цифрової стійкості суб'єктів господарювання до кіберризиків. Наукові результати відзначаються новизною, логічною узгодженістю та методологічною цілісністю. Вони розширюють теоретико-прикладні засади менеджменту інформаційної безпеки шляхом інтеграції техніко-технологічних, організаційних і соціально-психологічних чинників у єдину адаптивну систему управління, орієнтовану на забезпечення довгострокової безпеки та конкурентоспроможності бізнесу.

Дисертаційна робота заслуговує на позитивну оцінку, відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12.01.2017 року «Про затвердження вимог до оформлення дисертації», постанови Кабінету Міністрів України №44 від 12.01.2022 року «Порядок присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» зі змінами і доповненнями.

Усе вищевикладене дає змогу дійти висновку про те, що автор дисертаційної роботи, Черкаський Григорій Ігорович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент» (галузь знань 07 – Управління та адміністрування).

ОФІЦІЙНИЙ ОПОНЕНТ

Доцент кафедри менеджменту, бізнесу і адміністрування
Державного біотехнологічного університету,
доктор філософії з менеджменту, доцент



Софія МІНЕНКО

Підпис Міненко С.
ЗАСВІДЧУЮ
Керівник відділу діловодства ДЕТУ
В. Корисів