До разової спеціалізованої вченої ради Національного університету «Одеська юридична академія»

РЕЦЕНЗІЯ

рецензента, кандидата економічних наук, доцента,
доцента кафедри економіки та менеджменту
Національного університету «Одеська юридична академія»,
Котлубая Вячеслава Олексійовича
на дисертацію Саврацького Олександра Олександровича на тему:
«Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз»,
подану на здобуття ступеня доктора філософії за спеціальністю
073 «Менеджмент»

Актуальність теми дисертаційної роботи. Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією усіх сфер життєдіяльності держави та бізнесу, що формує нові можливості для підвищення ефективності управління та одночасно суттєво розширює площину потенційних кіберзагроз. Особливої гостроти ця проблематика набуває в умовах війни, коли об'єкти критичної інфраструктури, зокрема енергетичні, телекомунікаційні, транспортні, фінансові системи, перетворюються на першочергові цілі кібератак. Кількість зареєстрованих кіберінцидентів щодо об'єктів критичної інфраструктури України неухильно зростає, а їхні наслідки дедалі частіше виходять за межі суто технічних порушень і набувають характеру загроз національній безпеці та сталому функціонуванню держави. У таких умовах традиційні технічні підходи до захисту об'єктів критичної інфраструктури виявляються недостатніми без відповідної управлінської підтримки, яка передбачає формування організаційних структур кібербезпеки, навчання персоналу, упорядкування процесів реагування на інциденти, оптимізації інвестицій у захисні заходи.

Незважаючи на значну увагу, яку приділяють питанням кібербезпеки фахівці в галузі інформаційних технологій та правового регулювання, управлінський вимір цієї проблеми залишається значною мірою поза увагою академічної спільноти. Відсутні комплексні наукові праці, які б відображали результати досліджень кіберзахисту критичної інфраструктури через призму управлінських інновацій як інструментів підвищення організаційної стійкості та ефективності реагування на загрози. Отже, дослідження, присвячене формуванню концептуальних засад оптимізації системи захисту критичної інфраструктури України від кіберзагроз шляхом впровадження управлінських інновацій, є своєчасним, актуальним і відповідає нагальним потребам наукової теорії та управлінської практики.

Наукова обґрунтованість представлених теоретичних та/або експериментальних результатів проведених здобувачем. Дисертаційна робота Саврацького О.О. характеризується системним та комплексним підходом до вивчення предмету - управлінських засад захисту критичної інфраструктури України від кіберзагроз в умовах активного впровадження управлінських інновацій.

Метою дисертації є обґрунтування наукових засад та розробка практичного інструментарію впровадження управлінських інновацій у сфері кіберзахисту критичної інфраструктури.

Для досягнення зазначеної мети у дисертації вирішено такі завдання: дослідити науковий базис управління безпековими процесами на основі впровадження інновацій; охарактеризувати критичну інфраструктуру як об’єкт управління та систематизувати загрози її функціонуванню з позиції управлінського реагування; проаналізувати методичні підходи та міжнародні стандарти управління захистом критичної інфраструктури від кіберзагроз; визначити особливості процесу управління кіберзахистом критичної інфраструктури з урахуванням нормативно-правового базису та технологічних можливостей; оцінити доступність та управлінську доцільність використання наявних ринкових рішень для кіберзахисту об’єктів критичної інфраструктури; проаналізувати механізми управлінського впливу на забезпечення кіберзахисту

критичної інфраструктури із застосуванням управлінських інновацій; розробити організаційні та інституційні підходи до реалізації інноваційних перетворень в управлінні кіберзахистом критичної інфраструктури; обґрунтувати інноваційний управлінський підхід до захисту критичної інфраструктури від кіберзагроз з використанням інструментів штучного інтелекту для підтримки управлінських рішень; розробити модель впливу управлінських інновацій на ефективність захисту об’єктів критичної інфраструктури.

Методологічним підґрунтям дисертаційного дослідження є комплекс загальнонаукових та спеціальних методів наукового пізнання. Діалектичний метод застосовано при дослідженні еволюції понять «критична інфраструктура» та «управлінські інновації» (розділ 1). Системно-структурний аналіз дозволив здійснити структурування об'єктів критичної інфраструктури за рівнем критичності та ступенем впливу інформаційної складової на операційну діяльність. Економіко-математичне моделювання застосовано при побудові моделі взаємозв'язку між технічною, організаційно-управлінською та кадровою складовими системи кібербезпеки (розділ 3). Статистичні методи використані для прогнозування розвитку ринку кібербезпеки в Україні (розділ 2). Модель Гордона-Льоба застосована для оцінки доцільності двоканального інвестування в кібербезпеку (розділ 2). Графо-аналітичний метод «Квадрат потенціалу» застосовано для визначення рівня готовності підприємств енергетичного сектору до використання інструментів штучного інтелекту (розділ 3).

Обґрунтованість результатів роботи підтверджується опрацюванням здобувачем значної кількості наукових праць вітчизняних і зарубіжних авторів, широкої бази нормативно-правових джерел, зокрема Стратегії кібербезпеки України, Законів України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», відповідних постанов Кабінету Міністрів України, міжнародних стандартів. Список використаних джерел налічує 215 найменувань. Емпіричну базу дослідження забезпечили дані щодо функціонування ринку кібербезпеки в Україні, практика підприємств і організацій, де були впроваджені результати роботи.

Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності. Дисертація складається з анотації, переліку умовних позначень, вступу, трьох розділів, що включають дев'ять підрозділів, висновків, списку використаних джерел (215 найменувань) та додатків. Загальний обсяг дисертації становить 229 сторінок загального тексту, з них основного тексту – 177 сторінок та 28 сторінок додатків. Структура дисертації Саврацького О.О. є логічно обґрунтованою та відповідає меті й завданням дослідження.

У вступі обґрунтовано актуальність обраної теми, сформульовано мету та завдання дослідження, визначено об'єкт, предмет і методи дослідження, розкрито наукову новизну, теоретичну та практичну значимість отриманих результатів, наведено відомості про апробацію результатів та публікації.

У першому розділі «Теоретико-методичні основи управління захистом критичної інфраструктури в умовах кіберзагроз» здобувачем досліджено понятійно-категоріальний апарат управління кібербезпекою критичної інфраструктури, обґрунтовано управлінські інновації як інструмент забезпечення безпеки в кіберпросторі, а також визначено методологічні підходи до захисту об'єктів критичної інфраструктури. Зокрема, здобувач здійснив структурування об'єктів критичної інфраструктури за рівнем критичності та ступенем залучення інформаційних технологій до операційної діяльності; обґрунтована доцільність застосування управлінського циклу PDCA для захисту критичної інфраструктури від кіберзагроз. Розділ відрізняється ґрунтовним опрацюванням зарубіжних і вітчизняних наукових джерел та нормативно-правової бази.

У другому розділі «Аналіз управлінських аспектів захисту критичної інфраструктури України від кіберзагроз» проведено комплексний аналіз нормативно-правового забезпечення прийняття управлінських рішень у сфері кібербезпеки критичної інфраструктури, визначено обсяг і структуру українського ринку продуктів і послуг у сфері кібербезпеки, побудовано кон'юнктурний прогноз подальшого розвитку ринку. Здобувач застосував модель Гордона-Льоба для оцінки доцільності двоканального інвестування в

кібербезпеку, концепцію «точки плато» як порогу, за яким подальші інвестиції в один із каналів стають економічно неефективними без відповідного зростання вкладень у інший. Прогнозний аналіз ринку кібербезпеки з верифікацією методом експоненційного згладжування свідчить про значний рівень методологічної підготовки здобувача та опанування ним сучасного інструментарію економічного аналізу.

У третьому розділі «Оптимізація кіберзахисту критичної інфраструктури України на основі управлінських інновацій» сформульовано напрями оптимізації управління персоналом на об'єктах критичної інфраструктури; розроблено командну модель управління кібербезпекою; обґрунтовано доцільність створення кластеру кібербезпеки в Україні у межах трикутника «влада – бізнес – наука»; запропоновано рішення для підтримки управлінських рішень із захисту енергетичної складової критичної інфраструктури із застосуванням технологій штучного інтелекту; розроблено економіко-математичну модель взаємозв'язку між технічною, організаційно-управлінською та кадровою складовими системи кібербезпеки – модифіковану функцію кіберстійкості.

Усі поставлені у дисертації завдання виконано в повному обсязі, зроблено відповідні висновки та сформульовано конкретні рекомендації й пропозиції, що мають теоретичне та практичне значення.

Повнота викладених наукових положень в опублікованих працях. Основні наукові положення дисертації, висновки та рекомендації Саврацького О.О. достатньо повно відображені у 12 наукових публікаціях, у тому числі в 1 статті, опублікованій у виданні, яке індексується в наукометричній базі Scopus, у 6 статтях, опублікованих у наукових фахових виданнях України категорії «Б», у 1 тезах у виданнях іноземних держав та у 4 тезах доповідей на науково-практичних конференціях. Загальний обсяг публікацій складає 4,45 авторських аркуші, з яких особисто автору належить 3,05 авторських аркуші. Публікаційна активність здобувача відповідає вимогам щодо апробації результатів дисертаційного дослідження.

Теоретична та практична значимість результатів дисертаційного дослідження. Розроблені здобувачем і викладені у дисертації наукові

положення, висновки та рекомендації можуть бути використані в науково-дослідній роботі для подальших наукових досліджень управлінських аспектів кібербезпеки критичної інфраструктури, розвитку теорії управлінських інновацій у сфері безпеки; правотворчій та регуляторній діяльності для вдосконалення нормативно-правового забезпечення управління кібербезпекою критичної інфраструктури, зокрема у частині стимулювання кластерного підходу та впровадження штучного інтелекту в захист стратегічних об'єктів; практичній управлінській діяльності керівниками організацій, що належать до об'єктів критичної інфраструктури, для оптимізації систем управління кібербезпекою, раціоналізації інвестицій у захисні заходи та підготовки кадрів; навчальному процесі при викладанні дисциплін «Менеджмент та маркетинг інновацій», «Проєктний менеджмент», «Інноваційний менеджмент», «Управління та організаційне забезпечення кібербезпеки», «Цифрові технології в бізнесі» тощо.

Практична цінність дослідження підтверджена актами та довідками про впровадження результатів у діяльність ПрАТ «Одескабель», КП «Теплопостачання міста Одеси», ТОВ «Кіпсолід Україна», Державної служби спеціального зв'язку та захисту інформації України, ГО «Odesa IT Family».

Наукова новизна одержаних результатів. Вивчення змісту дисертації дає підстави стверджувати, що всі сформульовані здобувачем елементи наукової новизни є доведеними та несуть у собі низку концептуальних висновків і рекомендацій, що мають теоретичне та практичне значення. Серед найбільш вагомих наукових результатів, що формують новизну роботи, слід виокремити такі:

Вперше розроблено інтегровану модель кіберстійкості, яка на відміну від суто технічних підходів формалізує взаємозв'язок між організаційно-управлінською, кадровою та технічною складовими захисту критичної інфраструктури з урахуванням галузевої специфіки (енергетика, телекомунікації, державне управління). Це дозволяє перевести кіберзахист із площини IT-менеджменту в площину стратегічного управління організацією.

Удосконалено методичний інструментарій оцінки та оптимізації інвестицій у кібербезпеку шляхом адаптації моделі Гордона-Льоба та впровадження концепції «точки плато», що надає менеджменту об'єктів критичної інфраструктури практичний інструмент для обґрунтування рівня витрат на захист. Суттєво також удосконалено механізм оцінки управлінських альтернатив через застосування методів найменших квадратів та ETS-алгоритму для аналізу ринку кібербезпеки.

Набули подальшого розвитку кластерний підхід до організації кіберзахисту (із наголосом на інституціоналізації комерціалізації безпекових інновацій), методичний підхід до впровадження ШІ в управлінські процеси критичної інфраструктури, а також понятійно-категоріальний апарат у частині визначення «менеджменту кібербезпеки» як управлінської категорії.

Дотримання принципів академічної доброчесності. У дисертаційній роботі та наукових публікаціях здобувача не виявлено текстових запозичень без посилання на першоджерело, фабрикації, фальсифікації та інших порушень принципів академічної доброчесності. Усі наведені дані підкріплено відповідними посиланнями; список використаних джерел є повним і коректно оформленим.

Щодо конфлікту інтересів. Рецензент не має реального чи потенційного конфлікту інтересів щодо здобувача Саврацького Олександра Олександровича, його наукового керівника та не є їхньою близькою особою.

Зауваження та питання для публічного захисту. Позитивно оцінюючи проведене дисертаційну роботу, у порядку наукової дискусії вважаємо за необхідне звернути увагу на окремі питання, що потребують уточнення або додаткового обґрунтування під час публічного захисту дисертації:

1. Запропонована в роботі концепція кластеру кібербезпеки є, безперечно, актуальною та перспективною. Разом із тим, залишається дискусійним питання щодо правового механізму функціонування такого кластеру в умовах чинного законодавства України, зокрема щодо розподілу прав та обов'язків між учасниками трикутника «влада – бізнес – наука» стосовно захисту інформації, що становить державну таємницю або конфіденційну інформацію окремих

підприємств. Тому для підвищення наукової обґрунтованості роботи доцільним було б розширити теоретичну базу дослідження щодо організаційно-правових умов створення та функціонування запропонованого кластеру.

2. У третьому розділі дисертаційного дослідження здобувач пропонує командну модель управління кібербезпекою, яка передбачає запровадження ролей, відповідальності та механізмів взаємодії в межах організаційних структур об'єктів критичної інфраструктури. Проте залишається відкритим питання щодо механізму адаптації запропонованої моделі до специфіки малих і середніх підприємств, що також можуть належати до об'єктів критичної інфраструктури, але не мають достатніх кадрових ресурсів для повноцінного розгортання окремого підрозділу кібербезпеки.

3. У розділі 3 запропоновано застосування технологій штучного інтелекту для підтримки управлінських рішень у сфері захисту енергетичної складової критичної інфраструктури. Водночас упровадження ШІ-рішень у критично важливі системи пов'язане з ризиками цілеспрямованого впливу на моделі машинного навчання. Разом із тим, у роботі не розкрито, чи передбачає запропонована модель механізми захисту самих ШІ-систем від подібних атак, що знижує повноту обґрунтування її практичної надійності.

Висловлені зауваження та запитання жодним чином не применшують наукову цінність дисертаційної роботи, відображають дискусійний і рекомендаційний характер наукового діалогу та суттєво не впливають на загальну позитивну оцінку роботи Саврацького Олександра Олександровича.

ЗАГАЛЬНИЙ ВИСНОВОК

Узагальнюючи викладене, дисертація Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз» є самостійною кваліфікаційною науковою працею, яка виконана здобувачем особисто, містить нові науково обґрунтовані теоретичні та прикладні результати, що мають важливе значення для розвитку науки управління та практики кібербезпеки. Рецензована робота

відповідає спеціальності 073 «Менеджмент» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами, внесеними постановою Кабінету Міністрів України від 08 квітня 2025 року № 426), Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами, внесеними постановою Кабінету Міністрів України від 03 травня 2024 року № 507), а також Вимогам до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12 січня 2017 року № 40 (зі змінами), а її автор Саврацький Олександр Олександрович заслуговує на присудження ступеня доктора філософії з галузі знань 07 «Управління та адміністрування» за спеціальністю 073 «Менеджмент».

Рецензент:
кандидат економічних наук, доцент,
доцент кафедри економіки та менеджменту
Національного університету
«Одеська юридична академія» Вячеслав КОТЛУБАЙ