НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

САВРАЦЬКИЙ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК 351.746.1:004.056.5:658.589

ДИСЕРТАЦІЯ

ВПРОВАДЖЕННЯ УПРАВЛІНСЬКИХ ІННОВАЦІЙ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ

073 – Менеджмент
07 – Управління та адміністрування

Подається на здобуття ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ О.О. Саврацький

Науковий керівник – **Горбаченко Станіслав Анатолійович**,
доктор економічних наук, професор

Одеса – 2026

АНОТАЦІЯ

Савpацький О. О. Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз. – Кваліфікаційна робота на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент» (галузь знань 07 – Управління та адміністрування). – Національний університет «Одеська юридична академія», Одеса, 2026.

У дисертації розроблено концептуальні засади оптимізації системи захисту критичної інфраструктури України від кіберзагроз на основі впровадження управлінських інновацій з урахуванням іноземного досвіду та вітчизняних реалій.

В першому розділі «Теоретико-методичні основи управління захистом критичної інфраструктури в умовах кіберзагроз» сформовано науковий фундамент для управлінського втручання у забезпечення безпеки (насамперед, у кіберпросторі), який ґрунтується на закономірностях функціонування складних соціально-економічних і технічних систем, методах управління ризиками, принципах стійкості та адаптивності, що дає змогу забезпечувати збалансоване поєднання превентивних, реактивних і відновлювальних заходів. Доведено доцільність використання управлінських інновацій при вирішенні безпекових питань, адже вони дозволяють підвищити ефективність використання людського капіталу, створюють сприятливі умови для розробки та поширення технологічних інновацій, скорочують час реагування на загрози та забезпечують гнучкість та адаптивність при протидії ним. Охарактеризовано критичну інфраструктуру як сферу активної інтеграції інформаційних технологій з одночасним збільшенням вразливості до кіберзагроз. Проведено структуризацію об’єктів критичної інфраструктури з огляду на рівень критичності та впливовість інформаційної складової на здійснення діяльності. Доведено доцільність застосування циклу управління PDCA для захисту критичної інфраструктури від кіберзагроз.

В другому розділі «Аналіз управлінських аспектів захисту критичної інфраструктури України від кіберзагроз» проаналізовано нормативно-правовий фундамент прийняття управлінських рішень в сфері кіберзахисту критичної інфраструктури до якого, зокрема, належать «Стратегія кібербезпеки України», Закони України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», спеціалізовані постанови Кабінету Міністрів України, а також міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework тощо. Досліджено ринкові можливості для придбання та подальшої інтеграції сучасних безпекових рішень в межах об'єктів критичної інфраструктури. Визначено обсяг та структуру українського ринку продуктів і послуг кібербезпеки, окреслено чинники, що впливають на попит та пропозицію на вказаному ринку. Розроблено кон'юнктурний прогноз подальшого розвитку ринку методом найменших квадратів з подальшою верифікацією за допомогою методу експоненційного згладжування. Оцінено доцільність двоканального інвестування у кіберзахист за технічним та організаційно-управлінським напрямами на основі моделі Гордона-Льоба. Запроваджено поняття «точки плато», як межі, коли додаткові інвестиції в один канал стають економічно неефективними без відповідного зростання вкладень в інший.

В третьому розділі «Оптимізація кіберзахисту критичної інфраструктури України на основі управлінських інновацій» як процес планування, розробки, впровадження та управління комплексом організаційних, технічних і правових заходів, спрямованих на забезпечення сталого та безпечного функціонування життєво важливих об'єктів, а також їхній захист від актуальних і потенційних кіберзагроз. Сформульовано напрями оптимізації управління персоналом об'єктів критичної інфраструктури з метою збільшення ефективності протидії кіберзагрозам. Запропоновано розробку індивідуальних навчальних програм для управлінського персоналу, технічних фахівців та інших співробітників, які мають доступ до інформаційних ресурсів. Задля забезпечення ефекту синергії сформовано модель управління кіберзахистом на основі командного підходу. Доведено доцільність створення в Україні кластера кібербезпеки з метою

збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів в сфері кібербезпеки в межах трикутника «влада-бізнес-наука». Сформовано пропозицію підтримки управлінських рішень в сфері захисту енергетичної складової критичної інфраструктури від кіберзагроз технологіями штучного інтелекту. За допомогою алгоритму графоаналітичного методу «Квадрат потенціалу» визначено рівень готовності підприємств енергетичної сфери до застосування ШІ-інструментів в межах процесу децентралізації енергетики, який передбачає перехід від централізованих систем до локальних енергетичних осередків, керованих на рівні територіальних громад. Розроблено економіко-математичну модель взаємозв'язку технічної, організаційної та кадрової складової кіберзахисту, у межах якої модифікована функція кіберстійкості відображає інтегральний вплив управлінських інновацій на здатність організації протидіяти кіберзагрозам. Доведено, що управлінські інновації забезпечують мультиплікативний ефект, адже зростання компетентності персоналу зменшує потребу в додаткових технічних інвестиціях і одночасно підвищує ефективність уже впроваджених рішень.

Головна наукова цінність дисертації полягає у зміні вектору дослідження питань протидії кіберзагрозам із суто технічної площини в сферу управлінського втручання, зокрема за допомогою управлінських інновацій. На цій основі: розроблено модель, яка відображає взаємозв'язок між організаційною (управлінською), кадровою та технічною складовими системи кіберзахисту, розраховано інтегральний індекс інноваційної пріоритетності і визначено найбільш перспективні складові критичної інфраструктури для подальшого впровадження управлінських інновацій, визначена межа виправданого інвестування в кіберзахист, сформовано пропозицію щодо застосування кластерного підходу для збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів в сфері кібербезпеки в межах трикутника «влада-бізнес-наука», оцінено потенціал окремих бізнес-структур до цифрової трансформації системи управління кібербезпекою.

Практичну цінність дослідження підтверджують довідки та акти впровадження в діяльність ПАТ «ОДЕСКАБЕЛЬ», КП «Теплопостачання міста Одеси», ТОВ «КІПСОЛІД УКРАЇНА», Державної служби спеціального зв'язку та захисту інформації України, ГС «Odesa IT Family».

Результати дослідження інтегровано в освітній процес Національного університету «Одеська юридична академія» при викладанні дисциплін «Менеджмент та маркетинг інновацій», «Проєктний менеджмент», «Інноваційний менеджмент», «Управління та організаційне забезпечення кібербезпеки», «Цифрові технології в бізнесі».

Ключові слова: управлінські інновації, критична інфраструктура, загрози, безпека, управління ризиками, цифровізація, розвиток, ефективність менеджменту, підтримка прийняття рішень, штучний інтелект в управлінні, стійкість, інноваційний проєкт.

ABSTRACT

Savratskyi O. O. Implementation of Managerial Innovations in the Protection of Critical Infrastructure from Cyber Threats. – Qualification paper in the form of a manuscript.

Thesis for the degree of Doctor of Philosophy in the specialty 073 Management (field of knowledge 07 – Management and Administration). – National University «Odesa Law Academy», Odesa, 2026.

The dissertation develops conceptual foundations for optimizing the system of protecting Ukraine's critical infrastructure from cyber threats through the implementation of managerial innovations, taking into account foreign experience and national realities.

In the first chapter «Theoretical And Methodological Foundations Of Critical Infrastructure Protection Management In The Context Of Cyber Threats», a scientific foundation is established for managerial intervention in security assurance (primarily in cyberspace). This foundation is based on the patterns of functioning of complex socio-economic and technical systems, risk management methods, and the principles of resilience and adaptability. These elements enable a balanced combination of preventive, reactive, and restorative measures. The expediency of using managerial innovations to address security issues is substantiated, as they enhance the efficiency of human capital utilization, create favorable conditions for the development and dissemination of technological innovations, reduce response time to threats, and ensure flexibility and adaptability in countering them. Critical infrastructure is characterized as a sphere of active integration of information technologies accompanied by an increase in vulnerability to cyber threats. A structuring of critical infrastructure objects is carried out according to the level of criticality and the influence of the information component on operational activities. The expediency of applying the PDCA management cycle for protecting critical infrastructure from cyber threats is proven.

In the second chapter «Analysis Of The Management Aspects Of Protecting Ukraine's Critical Infrastructure From Cyberthreats», the normative-legal framework

for decision-making in the field of cybersecurity of critical infrastructure is analyzed. This framework includes, in particular, the «Cybersecurity Strategy of Ukraine», the Laws of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» and «On Critical Infrastructure» specialized resolutions of the Cabinet of Ministers of Ukraine, as well as international standards ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework, etc. Market opportunities for the procurement and subsequent integration of modern security solutions into critical infrastructure facilities are examined. The volume and structure of the Ukrainian market for cybersecurity products and services are determined, and the factors influencing demand and supply in this market are outlined. A conjunctural forecast of further market development is developed using the least-squares method, followed by verification via exponential smoothing. The expediency of two-channel investment in cybersecurity along technical and organizational-managerial lines is assessed on the basis of the Gordon-Loeb model. The concept of a “plateau point” is introduced as the threshold beyond which additional investments in one channel become economically inefficient without corresponding growth in investments in the other channel.

In the third chapter «Optimization of Cyber Security For Ukraine's Critical Infrastructure Through Management Innovations» the category «cybersecurity management» is defined as the process of planning, developing, implementing, and managing a complex of organizational, technical, and legal measures aimed at ensuring the sustainable and secure functioning of vital facilities and their protection from current and potential cyber threats. Directions for optimizing personnel management at critical infrastructure facilities are formulated with the aim of increasing the effectiveness of countering cyber threats. The development of individualized training programs for managerial personnel, technical specialists, and other employees with access to information resources is proposed. To achieve a synergy effect, a team-based cybersecurity management model is developed. The expediency of establishing a cybersecurity cluster in Ukraine is substantiated in order to increase the effectiveness of countering cyber threats through the implementation of innovative projects in the field of cybersecurity within the «government–business–science» triangle. A proposal

is formulated for supporting managerial decisions in the protection of the energy component of critical infrastructure from cyber threats using artificial intelligence technologies. Using the graph-analytical «Square of Potential» algorithm, the readiness level of energy-sector enterprises for the application of AI tools within the process of energy decentralization is determined. This process involves the transition from centralized systems to local energy hubs managed at the level of territorial communities. An economic-mathematical model of the interrelationship among the technical, organizational, and personnel components of cybersecurity is developed. Within this model, a modified cyber-resilience function reflects the integral impact of managerial innovations on the organization's ability to counter cyber threats. It is proven that managerial innovations produce a multiplicative effect: an increase in personnel competence reduces the need for additional technical investments while simultaneously enhancing the efficiency of already implemented solutions.

The main scientific value of the dissertation lies in shifting the vector of research on countering cyber threats from a purely technical plane to the sphere of managerial intervention, in particular through managerial innovations. On this basis, a model reflecting the interrelationship between the organizational (managerial), personnel, and technical components of the cybersecurity system has been developed, an integral index of innovation priority has been calculated and the most promising components of critical infrastructure for further implementation of managerial innovations have been identified, the boundary of justified investment in cybersecurity has been determined, a proposal for applying a cluster approach to increase the effectiveness of countering cyber threats through the implementation of innovative projects in cybersecurity within the «government–business–science» triangle has been formulated, and the potential of individual business structures for the digital transformation of cybersecurity management systems has been assessed.

The practical value of the research is confirmed by certificates and acts of implementation into the activities of PJSC «Odeskabel», Municipal Enterprise «Teplopostachannya mista Odesy», LLC «Kipsolid Ukraine», the State Service of

Special Communications and Information Protection of Ukraine, and the GS «Odesa IT Family».

The research results have been integrated into the educational process of the National University «Odesa Law Academy» in the teaching of the disciplines «Management and Marketing of Innovations», «Project Management», «Innovation Management», «Cybersecurity Management and Organisational Support», «Market Conjuncture Forecasting» and «Digital Technologies in Business».

Keywords: management innovations, critical infrastructure, security, threats, risk management, digitalization, management efficiency, decision support, artificial intelligence in management, resilience, innovative project.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Соколов А. В., Кілко В. В., Трофименко О. Г., Саврацький О. О. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об'єктах критичної інфраструктури. *Вісті вищих учбових закладів. Радіоелектроніка.* 2026. URL: https://radio.kpi.ua/article/view/S0021347025040028. DOI: https://doi.org/10.20535/S0021347025040028.

2. Саврацький О. О. Адаптація системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів. *Трансформаційна економіка*. 2024. №1(06). С. 53–57. DOI: https://doi.org/10.32782/2786-8141/2024-6-10.

3. Саврацький О. О. Аналіз кон'юнктури ринку продуктів та послуг кібербезпеки. *Науково-виробничий журнал «Бізнес-навігатор».* 2025. №1. С. 443-449. DOI: https://doi.org/10.32782/business-navigator.78-74.

4. Саврацький О. О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. *Актуальні питання економічних наук*. 2025. № 13. DOI: https://doi.org/10.5281/zenodo.16885042.

5. Горбаченко С. А., Саврацький О. О. Transformation of the innovative component of management processes in the context of digitalization. *Приазовський економічний вісник.* 2025. № 3 (43). С. 62-67. DOI: https://doi.org/10.32782/2522-4263/2025-3-11.

6. Саврацький О. О., Слатвінська В. М. Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень. *Наука і техніка сьогодні.* 2025. № 8 (49). С. 1704-1716. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716.

7. Саврацький О. О., Чепурна О. Є. Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних системах з урахуванням спадної віддачі інвестицій. *Успіхи і досягнення у науці*.

2026. № 1(23). С. 1305-1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317.

наукові праці, які засвідчують апробацію матеріалів дисертації:

8. Саврацький О. О. Критична інфраструктура як об'єкт кіберзахисту. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика :* матеріали Міжнар. наук.-практ. конф., м. Одеса, 24 листопад. 2023 р. Одеса, 2023. С. 76-78.

9. Саврацький О. О. Особливості підготовки фахівців з кібербезпеки в умовах війни. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар. наук.-практ. конф., м. Одеса, 26 квітн. 2024 р. НУ "ОЮА" ; за заг. ред. С. В. Ківалова ; відп. за вип. М. Р. Аракелян. Одеса : Фенікс, 2024. С. 905-907.

10. Саврацький О.О. Нормативно-правовий фундамент управління кібербезпекою підприємства. *Конкурентоспроможна модель інноваційного розвитку економіки України :* матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 7-8 листопад. 2024 р. Кропивницький, 2024. С. 116-118.

11. Саврацький О. О. Системний підхід при управління кіберризиками в умовах війни. *Кібербезпека в сучасному світі: актуальні виклики*: матеріали Міжнар. наук.-практ. конф., м. Одеса, 22 листопад. 2024 р. Одеса. 2024. С. 274-277.

12. Саврацький О. О. Current trends in security management. *Achievements of Science and Applied Research :* матеріали III Міжнар. наук.-практ. конф., м. Дублін 21-23 липн. 2025. С. 70-75. DOI: http://dx.doi.org/10.70286/EOSS-21.07.2025 .

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Стрімке впровадження цифрових технологій у ключові сфери життєдіяльності суспільства, зокрема енергетику, транспорт, зв'язок, фінанси, охорону здоров'я та оборону, не лише створює нові можливості для підвищення ефективності функціонування відповідних систем, а й супроводжується зростанням ризиків та появою нових загроз, які генерує кіберпростір. Критична інфраструктура дедалі більше залежить від цифрових систем управління, інформаційно-комунікаційних технологій та автоматизованих процесів, що підвищує її вразливість до кіберінцидентів і комплексних кібератак.

Для України в умовах повномасштабного вторгнення значення кіберзагроз суттєво зростає, а традиційні технічні й нормативно-правові заходи кіберзахисту виявляються недостатніми для забезпечення належного рівня стійкості об'єктів критичної інфраструктури. Відтак, протидія кіберзагрозам поступово виходить за межі суто технічної проблематики та набуває комплексного управлінського характеру, що вимагає перегляду підходів до планування, координації і прийняття рішень у сфері кібербезпеки.

Кіберзагрози постійно трансформуються, а отже, навіть вдалі управлінські рішення швидко втрачають власну актуальність. За таких умов особливої важливості набуває впровадження управлінських інновацій, спрямованих на підвищення кіберстійкості критичної інфраструктури, інтеграцію питань кіберзахисту в систему стратегічного управління та формування ефективних механізмів взаємодії між державними органами й операторами критично важливих об'єктів. У зв'язку з цим дослідження проблеми впровадження управлінських інновацій для захисту критичної інфраструктури є своєчасним, має науково-прикладне значення та сприяє формуванню ефективної національної системи кіберстійкості, а також розвитку управлінських компетенцій у сфері цифрової безпеки.

Теоретичні, методологічні, методичні та прикладні положення управління захистом критичної інфраструктури від кіберзагроз висвітлювалися в багатьох наукових працях, у тому числі міждисциплінарних. Зокрема, фундаментальні наукові основи управління захистом критичної інфраструктури в контексті національної та економічної безпеки заклали Д. Бірюков, Т. Васильців, О. Єрменчук, С. Кондратов, О. Суходоля, С. Теленик, В. Франчук, А. Штангрет. Зокрема, вони досліджували підходи до ідентифікації та захисту об'єктів критичної інфраструктури, з урахуванням іноземного досвіду та національних особливостей. Інша група авторів, а саме С. Гончар, В. Гречанінов, Ю. Кожедуб, Ю. Лісовська, З. Свердлик, зосереджувалася на організаційних аспектах інформаційної та кібербезпеки, зокрема на моделях інтелектуального захисту систем критичної інфраструктури та цифровій гігієні в умовах гібридних загроз. Окрему увагу заслуговують міждисциплінарні напрацювання І. Веселової, О. Власенка, О. Довганя, С. Дорогих, М. Драпатого, І. Дячкова, В. Козачок, М. Комарова, І. Коржа, О. Короля, Т. Лаптєвої, Л. Литвинової, І. Субача, В. Тихого, які сформували організаційно-правові засади управлінських трансформацій, спрямованих на протидію кіберзагрозам.

Управлінське підґрунтя вирішення безпекових питань знайшло відображення у працях А. Васильціва, А. Гайдученка, Г. Гончаренко, Р. Дацківа, О. Кібік, Б. Коломієць, М. Копитко, Я. Котляревського, В. Панченка, С. Пономарьова, які наголошували і на важливості інноваційних перетворень. Окремої уваги заслуговують дослідження наукової школи Львівського державного університету безпеки життєдіяльності (О. Зачко, Д. Кобилкін, І. Павук та ін.), зокрема, у питаннях управління інфраструктурними проєктами. Спроба систематизувати окремі управлінські елементи протидії кіберзагрозам в концепцію менеджменту кібербезпеки проводилася в наукових працях С. Горбаченка.

Теоретичний фундамент інноваційної складової управлінської діяльності сформувався на основі наукових праць Д. К. Норта, П. Розенштейна-Родана, П. Самуельсона, Й. Шумпетера. Сучасні тренди в сфері управлінських інновацій

розглядаються в наукових працях Р. Августин, О. Божанової, В. Зянька, В. Котлубая, Т. Куклінової, Ю. Ольвінської, С. Прохорчук, Н. Чухрай. Водночас практичне застосування інноваційних підходів у вирішенні питань кібербезпеки відбувається під впливом досліджень К. Дж. Альберта, Р. Андерсона, Т. Мура, Дж. Фрега, Р. Філіппіні.

Разом із тим проблема інтеграції управлінських інновацій у систему кіберзахисту критичної інфраструктури ще недостатньо висвітлена в наукових дослідженнях. Адже в переважній більшості наукових праць або оглядово розглядається весь комплекс управлінських питань безпеки критичної інфраструктури, або висвітлюються підходи до забезпечення кібербезпеки в технічному або нормативно-правовому аспектах або досліджуються тренди інноваційного управління але без фокусування на завданнях запобігання кіберзагрозам. Вказана ситуація дозволяє стверджувати про наукові перспективи формування окремої гілки досліджень за напрямом «менеджмент кібербезпеки», в межах якої окрема увага має приділятися впровадженню управлінських інновацій в безпекові процеси.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до планів науково-дослідної роботи Національного університету «Одеська юридична академія» за темою: «Правове і соціальне життя сучасної України у людиноцентристському вимірі в цифрову еру» (державний реєстраційний номер 0122U000266) та кафедри кібербезпеки – за темою «Безпека інформації та її складових в інформаційно-комунікаційних системах». В межах кафедральної теми автор проводив дослідження управлінських аспектів забезпечення безпеки інформації та її складових, на прикладі об'єктів критичної інфраструктури.

Мета і завдання дослідження. Метою дисертаційної роботи є обґрунтування наукових засад та розробка практичного інструментарію впровадження управлінських інновацій у сфері кіберзахисту критичної інфраструктури.

Задля досягнення визначеної мети поставлені 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.

Об’єктом дослідження є процес управління захистом критичної інфраструктури від кіберзагроз.

Предметом дослідження є комплекс теоретичних, організаційних, методичних і практичних основ управління кіберзахистом критичної інфраструктури з використанням управлінських інновацій.

Методи дослідження. В дисертаційній роботі використано такі методи: аналізу та синтезу – для узагальнення наукових джерел, систематизації понять

безпеки, інновацій та кібербезпеки з огляду на їхнє використання в управлінських дослідженнях (підрозділи 1.1, 1.2); абстрагування – з метою виділення ключових складових елементів безпеки, таких як фізична, економічна, екологічна та кібербезпека (підрозділ 1.3); порівняльного аналізу – для дослідження кон'юнктури ринку продуктів та послуг кібербезпеки та його окремих сегментів (підрозділ 2.2), а також аналізу нормативно-правової бази та міжнародних стандартів (підрозділи 2.1, 2.2); графоаналітичного («Квадрат потенціалу») – для оцінки управлінської готовності підприємств енергетичної сфери до інтеграції штучного інтелекту, що передбачає ранжування об'єктів дослідження за технологічними, управлінськими, комунікаційними та фінансовими блоками з розрахунком сум місць та довжин векторів (підрозділ 3.2); графічного – для наочного і всебічного відображення результатів проведеного дослідження (розділи 2, 3); абстрактно-логічного – під час проведення теоретичних узагальнень і формування висновків дослідження (висновки до розділів). Застосовано економіко-математичне моделювання раціонального розподілу інвестицій у кіберзахист об'єктів критичної інфраструктури. Для інтерпретації комплементарності заходів запроваджено управлінський індикатор кіберстійкості (підрозділ 3.3).

Інформаційною базою дослідження є чинні нормативні документи (Верховної Ради України, Кабінету Міністрів України тощо), актуальна вітчизняна та зарубіжна наукова література, офіційні статистичні дані, аналітичні звіти, фінансова звітність і первинна документація суб'єктів підприємництва, що належать до критичної інфраструктури, результати опитування профільних фахівців, інформаційні ресурси мережі Інтернет.

Наукова новизна одержаних результатів

Вперше:

Розроблено інтегровану модель, яка формалізує взаємозв'язок між організаційною (управлінською), кадровою та технічною складовими системи кіберзахисту та враховує диференційований вплив управлінських інновацій на окремі категорії персоналу (управлінський, технічний, користувачі

інформаційних систем) і галузеву специфіку секторів критичної інфраструктури (енергетика, телекомунікації, державне управління). На основі результатів оцінювання запропоновано управлінські рішення для підвищення кіберстійкості об’єктів критичної інфраструктури.

Вдосконалено:

- Структуризацію об’єктів критичної інфраструктури, в якій, на відміну від існуючих варіантів, до нормативного показника критичності та рівня інформатизації окремих об’єктів додано управлінський показник організаційної схильності до інновацій, визначений на основі бального методу. В результаті розраховано інтегральний індекс інноваційної пріоритетності і визначено найбільш перспективні складові критичної інфраструктури для подальшого впровадження управлінських інновацій, спрямованих на протидію кіберзагрозам.

- Модель оптимізації інвестицій у кібербезпеку на основі адаптації моделі Гордона–Льоба, яка, на відміну від базової версії, інтегрує функцію кіберстійкості об’єктів критичної інфраструктури, що дозволяє інтерпретувати кіберзахист як економічно обумовлений управлінський процес із властивими йому закономірностями зростання граничної ефективності інвестицій до визначеного порогового значення та її подальшого зниження. В результаті менеджмент об’єктів критичної інфраструктури може визначити економічно обґрунтований рівень інвестування у заходи кібербезпеки.

- Механізм оцінки управлінських альтернатив при формуванні системи кіберзахисту, який, на відміну від існуючих, при виборі конкретних інструментів передбачає дослідження кон’юнктури ринку продуктів та послуг кібербезпеки із застосуванням методів найменших квадратів та експоненційного згладжування за алгоритмом ETS. Застосування зазначеного механізму дозволяє науково обґрунтовувати рівень доступності та управлінську доцільність придбання готових рішень для забезпечення кібербезпеки критичної інфраструктури.

Набуло подальшого розвитку:

- Застосування кластерного підходу для збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів в сфері кібербезпеки. Запропоновано створення кластеру кібербезпеки, який, на відміну від існуючих, орієнтується не стільки на координацію учасників та інформаційно-комунікаційну підтримку, скільки на інституціоналізацію процесів апробації, впровадження та комерціалізації інноваційних безпекових рішень. В результаті об’єкти критичної інфраструктури в межах новоствореного кластеру можуть виступати замовниками продуктів та послуг кібербезпеки, стейкхолдерами для закладів вищої освіти, інвесторами стартапів безпекового напряму, тестувальниками інноваційних рішень.

- Методичний підхід до впровадження інструментів штучного інтелекту в управлінські процеси енергетичної критичної інфраструктури із застосуванням графоаналітичних розрахунків, який, на відміну від існуючих підходів, дозволяє кількісно оцінити рівень готовності управлінської структури до цифрової трансформації системи управління кібербезпекою.

- Визначення категорії «менеджмент кібербезпеки» як цілеспрямованого процесу планування, розробки, впровадження та управління комплексом організаційних, технічних і правових заходів, спрямованих на забезпечення сталого та безпечного функціонування життєво важливих об’єктів, а також їхній захист від актуальних і потенційних кіберзагроз, яке, на відміну від існуючих, конкретизує управлінський пріоритет на захисті «життєво важливих об’єктів», тобто, критичної інфраструктури.

- Управлінську модель застосування командного підходу для вирішення завдань протидії кіберзагрозам, яка, на відміну від існуючих, передбачає наявність окремої посади менеджера з кібербезпеки, який приймає участь у стратегічному плануванні, відповідає за інтеграцію управлінських і технічних рішень, а також здійснює координацію діяльності команди з аналітика, фахівця з комунікацій та дослідження ринку, фахівців технічного блоку. В результаті сформована команда може швидше адаптуватися до нових безпекових викликів, генерувати інноваційні рішення та ефективно розподіляти ресурси.

- Теоретичний підхід до застосування циклу PDCA для управління кіберзахистом критичної інфраструктури, який, на відміну від традиційних підходів, інтегрує принципи проактивності, комплексності та адаптивності. В результаті поєднання безперервного процесного управління із сучасними аналітичними моделями попередження загроз створюються умови для ефективного впровадження інноваційних управлінських рішень.

Практичне значення отриманих результатів полягає в тому, що на основі наукових та практичних матеріалів дослідження запропоновані рекомендації з впровадження інновацій в управлінську діяльність об’єктів критичної інфраструктури, спрямовану на протидію кіберзагрозам. Результати дослідження та пропозиції отримали позитивні відгуки та впроваджені в управлінську практику Державної служби спеціального зв'язку та захисту інформації України, ПАТ «ОДЕСКАБЕЛЬ», КП «Теплопостачання міста Одеси», ТОВ «КІПСОЛІД Україна», а також бізнес-структур, що є членами ГС «Odesa IT Family».

Результати дисертаційної роботи впроваджено в освітній процес Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «Менеджмент та маркетинг інновацій», «Проєктний менеджмент», «Інноваційний менеджмент», «Управління та організаційне забезпечення кібербезпеки», «Цифрові технології в бізнесі» (акт впровадження від 22.12.2025 р.).

Особистий внесок здобувача. Дисертаційна робота є самостійним і завершеним науковим дослідженням. Усі наукові положення, розроблені рекомендації, пропозиції та висновки, викладені в дисертації, є результатом особистої роботи автора. У тих наукових публікаціях, що виконані у співавторстві та використані в роботі, автором використовуються виключно положення та ідеї, які є наслідком його власних досліджень і розробок.

У статті «Transformation of the innovative component of management processes in the context of digitalization» (пер. «Трансформація інноваційної складової управлінських процесів в умовах цифровізації». Приазовський

економічний вісник. 2025. № 3 (43). С. 62-67. DOI: https://doi.org/10.32782/2522-4263/2025-3-11 автор дослідив вплив цифрових технологій (зокрема, штучного інтелекту Big Data, Інтернету речей, блокчейн, хмарних обчислень) на управлінські процеси.

У статті «Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень». Наука і техніка сьогодні. 2025. № 8 (49). С. 1704-1716. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716 автор сформував основні напрями застосування інноваційних управлінських рішень, спрямованих на вирішення завдань кіберзахисту.

У статті «Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних системах з урахуванням спадної віддачі інвестицій». Успіхи і досягнення у науці. 2026. № 1(23). С. 1305–1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317 автор обґрунтував припущення, що ефективність не зростає необмежено зі збільшенням вкладень, а має характер поступового насичення, що аналітично проявляється у зменшенні граничного приросту результативності за кожної додаткової одиниці інвестицій.

У статті «Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об’єктах критичної інфраструктури». Вісті вищих учбових закладів. Радіоелектроніка. 2026. DOI: https://doi.org/10.20535/S0021347025040028 автор сформулював особливості критичної інфраструктури як середовища для впровадження технологічних інновацій.

Апробація результатів дисертації. Положення та висновки дисертаційного дослідження обговорювались під час засідання кафедри кібербезпеки Національного університету «Одеська юридична академія». Основні результати наукового дослідження були висвітлені у доповідях на наукових, науково-практичних конференціях, зокрема на: Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.); Міжнародна

науково-практична конференція «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.); VII Міжнародна науково-практична конференція «Конкурентоспроможна модель інноваційного розвитку економіки України» (м. Кропивницький, 7-8 листопада 2024 р.); Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.); III Міжнародна науково-практична конференція «Achievements of Science and Applied Research» (м. Дублін, 21-23 липня 2025); Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.).

Публікації. Результати дисертаційної роботи та основні положення викладені в 12 наукових працях, із них:

- 1 стаття у виданні, що включене до наукометричної бази Scopus;
- 6 статей у наукових фахових виданнях категорії «Б»;
- 1 тези у виданнях іноземних держав;
- 4 тези у матеріалах науково-практичних конференцій.

Загальний обсяг наукових праць становить 4,45 друк. арк. (особисто автору належить 3,05 друк. арк.)

Структура та обсяг дисертації. Дисертація складається з вступу, трьох розділів, що включають 9 підрозділів, висновків, списку використаних джерел (215 найменувань) та 18 додатків. Загальний обсяг дисертації складає 229 сторінок, з них основний текст – 177 сторінок. Додатки розміщені на 28 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ УПРАВЛІННЯ ЗАХИСТОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ КІБЕРЗАГРОЗ

1.1. Науковий базис застосування управлінських інновацій для вирішення безпекових питань

В останні роки основною рушійною силою суспільного розвитку є промислові та інформаційні технології насамперед у військовому сегменті. Завдяки потужному військово-технологічному драйверу формується конкурентне портфоліо окремих країн, створюються нові ринки, а деякі військові технології успішно адаптуються й під цивільні потреби. Однак зазначені технології не тільки генерують різноманітні можливості, а й створюють загрози як для окремих країн, так і для людства в цілому. І, в цьому сенсі, безпека вже по-новому реалізує себе в індивідуальній і суспільній свідомості, а вирішення безпекових питань потребує не лише політичної волі чи технічних засобів, але й ґрунтовного наукового підходу.

Протягом усієї історії людства питання безпеки знаходилися в центрі уваги дослідників з різних галузей знань: істориків, правників, філософів, політиків, військових, економістів. Означений факт обумовлює й наявність низки визначень категорії «безпека».

Так, на думку А. Федорової, «безпека – відсутність загроз в усіх сферах життя, що сприяє сталому людському розвитку і залежить від рівня правової культури, свідомості та відповідальності кожного члена громади, досягнення якої можливо шляхом взаємодії органів публічної влади з громадянським суспільством та збільшення кількості превентивних заходів» [97, с. 148]. Вказане визначення виглядає занадто ідеалістичним, адже загрози об’єктивно супроводжують будь-яку діяльність.

Більш точним виглядає визначення В. Циганова стосовно того, що безпека – це діяльність людей, суспільства, держави, світового співтовариства народів з

виявлення, запобігання, послаблення, відвернення загрози, здатної загубити їх, позбавити матеріальних і духовних цінностей, завдати невідшкодованих збитків, заблокувати шляхи для прогресивного розвитку [101, с. 32]. Тут варто погодитися, що безпеку, а точніше – її забезпечення, потрібно розглядати як певний процес.

В філософському аспекті безпекою можна вважати певний стан захищеності, в якому перебувають соціальні суб'єкти та системи, а також сукупність засобів та методів, що дозволяють блокувати джерела небезпеки [39]. Але вказане визначення є розмитим і не дозволяє сформувати комплекс заходів для підтримки зазначеного «стану захищеності»

В соціальному розумінні безпека передбачає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних та потенційних загроз або уникнути їх, що, своєю чергою, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їх розвиток [47].

З огляду на вищесказане, можна погодитися з Г. Гончаренко, що категорія безпеки має поліфункціональний характер. Тобто безпека як соціальна цінність суспільства – діяльність певної групи різних суб'єктів, а як соціальна потреба – це цілеспрямований результат такої діяльності [15].

При використанні терміну «безпека» в економічних та управлінських дослідженнях доцільно насамперед звернути увагу на Державний стандарт України 2293:2014 «Охорона праці. Терміни та визначення основних понять» [27] де вказаний термін означає стан захищеності особи та суспільства від ризику зазнати шкоди. В цьому сенсі безпека охоплює різні аспекти життєдіяльності та має на меті забезпечення стабільності, добробуту і розвитку.

На рівні окремих суб'єктів підприємництва під безпекою розуміють здебільшого такий стан суб'єкта господарювання, що характеризується

організованою сукупністю концептуальних і прагматичних чинників, які забезпечують цій системі: захист від небажаних впливів; динамічний розвиток; ефективність життєво важливих процесів; незалежність; можливість досягнення цілей [9, с. 72]. А отже, загрози безпеці розглядають як певні чинники, що формують небезпеку, тобто наявну та об'єктивну ймовірність негативного впливу на систему.

Враховуючи усі різноманіття наявних загроз, можна стверджувати, що зміст безпеки і засоби її досягнення залежать від багатьох обставин, зокрема від характеру предметів, безпека яких забезпечується, характеру джерел загроз, її ступеня тощо. Означені обставини здійснюють вплив на структуризацію безпеки та виділення її окремих складових. Так, Р. Дацків зауважив, що безпека охоплює військові, економічні, технологічні, екологічні, соціальні та гуманітарні аспекти. До її сфери також входить питання збереження національної ідентичності й захист базових прав і свобод громадян [24, с. 8]. Однак слід зауважити, що, враховуючі сучасні цифрові трансформації, потрібно звертати увагу не на «технологічний аспект», а на кіберсередовище, яке саме по собі вже включає військові, економічні та інші аспекти.

С. Пономарьов систематизував типи безпеки таким чином: 1) за суб'єктами (особиста, суспільна, національна, колективна, державна); 2) за масштабами (міжнародна, регіональна, локальна); 3) за суспільними сферами (політична, військова, економічна, екологічна, радіаційна); 4) залежно від характеру та спрямування певних видів суспільної діяльності (безпека праці, безпека життєдіяльності, безпека дорожнього руху, безпека авіаційна, безпека мореплавства, інформаційна безпека) тощо [70, с. 70]. Знов-таки вказану систематизацію доцільно було б доповнити таким чином: «…за сферою безпеки (безпека у фізичному середовищі, безпека у кіберсередовищі)…».

Можна спиратися на думку М. Копитко, що при дослідженні складових безпеки потрібно опиратися на поняття «безпечна діяльність». Остання має включати фізичну безпеку, під якою розуміється забезпечення захисту від загрози життю людей; економічну безпеку; інформаційну безпеку; матеріальну

безпеку, тобто збереження матеріальних цінностей від різних загроз –від їхніх крадіжок і до загроз пожежі та інших стихійних лих [46].

Враховуючи усе вищезазначене, в проведеному дослідженні пропонується розглядати категорію «безпека» як сукупність таких складових елементів (рис. 1.1).

Рис. 1.1. Основні складові елементи безпеки *(складено автором)*

Фізична безпека передбачає захист від фізичних загроз (злочини, тероризм, природні катастрофи тощо); економічна безпека охоплює захист економічних ресурсів, стабільність фінансової системи та економічне зростання; екологічна безпека спрямована на збереження навколишнього середовища та запобігання екологічним катастрофам; кібербезпека включає заходи та технології, захисту інформаційних систем, мереж і даних від кіберзагроз.

При цьому в епоху цифрових перетворень можна стверджувати про повноцінне інтегрування окремих елементів фізичної та кібербезпеки у єдину систему, яка знаходиться і під постійною увагою управлінської науки та практики. Адже безпека охоплює різні аспекти захисту та стабільності і одночасно вимагає координації зусиль на всіх рівнях для ефективного запобігання і реагування на загрози. Крім того, наявність належного рівня безпеки сприятливо впливає на імідж, викликає довіру у контрагентів, клієнтів

та органів державної та місцевої влади, зменшує вірогідність фінансових втрат, мотивує персонал тощо [17].

Відповідно вирішення питань безпеки передбачає використання специфічного підходу до управлінської діяльності. Мова йде про такий напрям, як менеджмент безпеки, під яким розуміють систематизовані й скоординовані види діяльності, методи та засоби, за допомогою яких організація оптимально управляє своїми ризиками і пов'язаними з ними потенційними загрозами і впливами [103].

З метою впорядкування окремих інструментів менеджменту безпеки Б. Коломієць застосовує категорію «безпекове управління на підприємстві» і виділяє такі його рівні, як стратегічний, тактичний, операційний, рівень моніторингу та контролю [42]. На стратегічному рівні керівництво визначає загальні політики та стратегії безпеки (інтегровані в загальну бізнес-стратегію), а також встановлює основні принципи та цілі безпеки. Далі на тактичному рівні менеджмент середньої ланки розробляє конкретні плани та процедури для реалізації стратегій безпеки. На операційному рівні виконуються щоденні заходи з безпеки, до яких можна віднести дотримання інструкцій та процедур, проведення тренінгів та навчання, а також регулярне тестування систем безпеки. І, нарешті, рівень моніторингу та контролю забезпечує постійне спостереження за виконанням заходів безпеки та своєчасне реагування на інциденти. На цьому рівні особливої актуальності набуває концепція проактивного менеджменту безпеки, що передбачає не лише реагування на інциденти, а й прогнозування потенційних ризиків та їхню випереджувальну нейтралізацію.

Загрози безпеці постійно еволюціонують, стають все більш непередбачуваними, носять комплексний характер (кіберфізичні атаки, інформаційні впливи, гібридні війни), а також швидко поширюються, здебільшого в цифровому середовищі. Отже, навіть ефективні управлінські рішення з часом втрачають свою актуальність, що викликає потребу у розробці та впровадженні управлінських інновацій.

В менеджменті інновація виступає одним із загальних та фундаментальних понять і відображає наслідок впровадження або матеріалізації новаторської ідеї з новими споживчими властивостями у вигляді товару, технології, послуги, засобу праці, які допомагають досягти економічного, екологічного, соціального чи інших видів ефектів [37].

Ще Й. Шумпетер визначив місце управлінських інновацій серед інших типів інновацій, таких як:

1. Виробництво невідомої споживачам нової продукції, товару, послуги або продукту з якісно новими властивостями.

2. Впровадження нового способу виробництва, в основу якого покладено нове наукове відкриття або новий підхід до комерційного використання продукції.

3. Освоєння нового ринку збуту.

4. Залучення нових матеріалів, видів сировини та її джерел.

5.Впровадження нових або удосконалення старих форм організаційного та управлінського процесів [104].

З огляду на наведену класифікацію можна стверджувати, що стійка конкурентна позиція кожної бізнес-структури потребує постійного оновлення та вдосконалення не тільки товарів та послуг, виробничих та збутових технологій, але й управлінського процесу. Управлінською інновацією може бути нова система організації і управління, управлінська технологія, бізнес-процес чи навіть спеціалізований програмний продукт або мобільний застосунок. Тобто усе те, що є креативним та водночас дієвим способом забезпечення неповторності всієї системи управління з одночасним збереженням її ефективності та результативності.

В умовах цифрових трансформацій управлінські інновації нерозривно пов’язані з інноваціями у сфері інформаційних технологій. Майже кожна управлінська інновація останніх років має під собою технологічне підґрунтя у вигляді інструментів штучного інтелекту, блокчейну, Інтернету речей, хмарних

технологій, Big Data тощо. Але, в той же час і за кожною технологічною інновацією стоїть відповідний запит та управлінське рішення.

Незважаючи на наявність низки визначень категорії «управлінська інновація», більшість з них підкреслює елементи новизни, змін та творчого підходу. Зокрема, можна спиратися на визначення управлінських інновацій Д. Біркіншау як впровадження нових практик, процесів і структур, котрі характеризуються значним відривом від поточних норм [119, с. 310]. Однак в епоху цифрових перетворень деякі аспекти управлінської діяльності змінюються настільки швидко, що складно взагалі казати про якісь норми.

З іншого боку, О. Божанова та О. Грицина запропонували розуміти під управлінською інновацією будь-яке прийняте і впроваджене в діяльність підприємства рішення, що стосується зміни системи або методів управління, які суттєво відрізняються від тих, що застосовували раніше, вперше використані на промисловому підприємстві для підвищення його ефективного економічного розвитку [7]. Однак це визначення є занадто вузьким, адже спрямоване виключно на промисловий сектор.

Обов’язковість творчої складової управлінських інновацій підкреслюють А. Осокіна та Н. Сергієнко, які вважають управлінською інновацією особливу форму зміни наявних принципів, структури, процедур, методів, технік та/або будь-яких елементів системи управління організацією на кардинально нові, що є результатом творчої діяльності [66].

Зі свого боку, Р. Августин та І. Деміків слушно підмітили, що управлінська інновація може бути результатом конкурентної боротьби і є інноваційним продуктом, отриманим від вкладання інтелектуального капіталу в нові форми, способи та методи планування, організування, мотивування і оцінювання результатів діяльності та конкурентоспроможності соціально-економічних систем на всіх рівнях управління та реалізується у матеріалізованій або іншій формі (наприклад, соціальний ефект) [2].

З огляду на специфіку дослідження найбільш прийнятним виглядає визначення С. Горбаченка, що управлінські інновації передбачають генерацію та

інтеграцію сучасних методів та технологій управління на основі творчого та креативного підходу, спрямованих на збільшення ефективності та результативності управлінських рішень на тлі зростання загальної професіоналізації управлінської діяльності [21]. Єдине доповнення стосується необхідності конкретизації впливу цифрових трансформацій на інноваційні процеси в управлінні. Відтак у вказаному визначенні доцільно було б додати «… на основі креативного підходу та сучасних ІТ-рішень…».

Для розробки та подальшого впровадження управлінських інновацій необхідні такі умови: проблема, що не має наявного вирішення та потребує нових ідей; нові принципи та погляди, що мають забезпечити нові підходи; перегляд традицій та догм, які обмежують творче мислення; приклади та аналоги, які допоможуть по-новому переосмислити можливості [147]. До цього переліку можна додати вищезгадане технологічне підґрунтя та наявність відповідної управлінської (зокрема й безпекової) культури.

Остання передбачає схильність керівників до ризику та експериментування, а також здійснення ними постійного моніторингу зовнішнього середовища. Крім того, задля успішної реалізації управлінські інновації мають забезпечуватися відповідними ресурсами (матеріальними, інтелектуальними, кадровими, інформаційними, правовими тощо) [20].

Що стосується наявності проблем як основного джерела управлінських інновацій, то найпростіше ідентифікувати вказані проблеми за допомогою діагностики управлінських процесів, що передбачає відповідь на такі запитання: хто керує процесом, хто має повноваження змінити його, яка мета процесу, чим вимірюється його успіх або невдача, хто є споживачем означеного процесу, хто бере в ньому участь, яке потрібне інформаційне супроводження чи аналітичні інструменти, які питання створює процес та яких потребує рішень, яким чином він пов’язаний із іншими системами управління тощо [147].

Вирішення вищевказаних проблем може передбачати повний цикл розробки, тестування та впровадження інновації або інтеграцію вдалих інструментів, рішень чи досвіду інших підприємств та організацій. Адже, на

відміну від технологічних інновацій, управлінські інновації набагато складніше захистити в правовому полі (авторським свідоцтвом, патентом тощо). З іншого боку, управлінські інновації дають ефект лише у певному середовищі, тому їх не завжди вдається вдало скопіювати.

На рівні окремих бізнес-структур управлінські інновації є в ролі складових стратегічного управління інноваційним розвитком підприємства, яке поєднує такі процеси: визначення вектору інноваційних перетворень, формування моделі стратегічного інноваційного розвитку, розробка систем управління проєктами інноваційного розвитку, розробка інструментів моніторингу та аналізу результатів інноваційної стратегії [161].

Впровадження управлінських інновацій безпекового спрямування відбувається в тих самих умовах, що й будь-яких інших управлінських інновацій: потреба у підтримці вищого керівництва, кадрова залежність, високий рівень ризику, потреба в попередніх дослідженнях, креативний характер, високий рівень цифровізації, наявність зовнішніх бар'єрів та внутрішнього опору.

Серед конкретних напрямів впровадження управлінських інновацій в процесі вирішення безпекових питань слід виокремити роботу з персоналом, організаційні трансформації та використання інформаційних технологій. Більшість управлінських інновацій ґрунтуються на людиноцентричному підході, а отже, передбачають роботу з персоналом. Дійсно, саме людський фактор є найуразливішим елементом будь-якої системи безпеки. Це веде до зростання інвестицій у навчання персоналу, створення культури безпеки, психологічної підготовки та розробки політик поведінки.

Впровадження управлінських інновацій у безпековій сфері все частіше пов'язують з концепціями стійкості (resilience) та антикрихкості (antifragility) [93]. Перша передбачає здатність системи витримувати зовнішні стреси без втрати функціональності, друга − можливість використовувати кризові ситуації як каталізатор для вдосконалення. У практиці безпекового управління це означає, що організації повинні не лише розробляти плани реагування, але й створювати умови для інноваційного зростання після подолання криз.

Крім того, управлінські інновації дедалі частіше впроваджуються в межах концепції «business continuity management» (BCM) [194] та «enterprise risk management» (ERM) [150], які, зі свого боку, інтегрують безпекові процедури у стратегічне планування. Це дозволяє не лише знижувати ймовірність кризових подій, а й забезпечувати стійкість бізнесу навіть в умовах масштабних зовнішніх трансформацій.

Як вже зазначалося вище, в основу управлінських інновацій зазвичай покладено сучасні інформаційні технології (табл. 1.1). Деякі з них вже повноцінно інтегровані в управлінські процеси і довели власну ефективність. Наприклад, використання цифрових «панелей управління» (dashboards) у режимі реального часу дає змогу топменеджменту отримувати консолідовану картину ризиків і миттєво координувати дії всіх підрозділів. У той час як інші інструменти все ще розглядаються виключно з позиції перспектив інтеграції в менеджмент у майбутньому.

Таблиця 1.1

Оцінка інформаційних технологій як підґрунтя управлінських інновацій

Технологія	Характеристика	Поточний рівень використання	Перспективи застосування в менеджменті безпеки
Штучний інтелект	Аналіз великих обсягів даних, виявлення аномалій, прогнозування загроз, автоматизація прийняття рішень на основі машинного навчання та нейронних мереж	Високий: активно застосовується в кібербезпеці, системах моніторингу, аналізі поведінки користувачів	Виявлення атак у реальному часі, прогнозування нових типів загроз, автоматизація реагування на інциденти, персоналізація заходів безпеки
Блокчейн	Децентралізоване зберігання даних, забезпечення прозорості транзакцій, захист від несанкціонованих змін, криптографічна безпека	Середній: використовується в фінансових системах, логістиці, смарт-контрактах	Захист цілісності даних, ускладнення компрометації систем, створення надійних ланцюгів поставок, забезпечення безпеки транзакцій
Квантові обчислення	Надвисока швидкість обробки даних, здатність до складних криптографічних обчислень, захист фінансових транзакцій і комунікаційних мереж	Низький: перебуває на етапі досліджень і пілотних проєктів	Створення стійких до злому систем шифрування, захист критичної інфраструктури, розробка нових стандартів кібербезпеки

Продовження таблиці 1.1

Технологія	Характеристика	Поточний рівень використання	Перспективи застосування в менеджменті безпеки
Інтернет речей (IoT)	Моніторинг і управління енергетичними, транспортними, промисловими системами, збір даних із підключених пристроїв у реальному часі	Високий: застосовується в розумних містах, промислових системах, побутових пристроях	Розширення мережі пристроїв, що потребують захисту, створення інтелектуальних систем моніторингу, захист від атак на IoT-пристрої
Прогнозна аналітика	Аналіз історичних даних для прогнозування майбутніх подій, протидія складним атакам (APT), виявлення аномалій у реальному часі	Середній: використовується в кібербезпеці, фінансових системах, управлінні ризиками	Виявлення та запобігання складним атакам на ранніх етапах, прогнозування ризиків, оптимізація стратегій реагування на загрози

Джерело*: складено за [52, 211, 175, 215, 127, 106]*

Так, штучний інтелект (ШІ) трансформує підходи до безпеки завдяки здатності аналізувати великі обсяги даних у реальному часі, виявляти аномалії та прогнозувати потенційні загрози. Технології блокчейну пропонують децентралізований підхід до забезпечення безпеки даних, що значно ускладнює їх компрометацію. Крім цього, блокчейн створює надійне середовище для обміну конфіденційною управлінською інформацією між організаціями. Квантові обчислення відкривають нові горизонти там, де потрібна обробка величезних обсягів даних, складна оптимізація та моделювання складних сценаріїв атак. Інтернет речей (IoT) набуває особливої актуальності у зв’язку зі зростанням кількості підключених пристроїв – від «розумних» лічильників електроенергії та промислових сенсорів до медичного обладнання та автономних транспортних засобів. Управлінські інновації у цій сфері включають розробку автоматизованих систем моніторингу та реагування, здатних у реальному часі виявляти підозрілу активність, блокувати потенційно небезпечні вузли та забезпечувати централізований контроль над тисячами пристроїв одночасно. Прогнозна аналітика на основі ШІ стає ключовим інструментом у боротьбі з найбільш витонченими кібератаками, зокрема з Advanced Persistent Threats [210] – тривалими, цілеспрямованими вторгненнями, які можуть залишатися

непоміченими протягом місяців або навіть років. Використовуючи алгоритми машинного навчання, прогнозна аналітика здатна не лише фіксувати поточні аномалії, але й передбачати розвиток потенційних сценаріїв атак на основі історичних даних, поведінкових моделей користувачів і загальних тенденцій у кіберпросторі.

З метою інституційної підтримки в межах проведеного дослідження сформовано гіпотезу стосовно доцільності застосування для вирішення безпекових питань кластерного підходу. Його можна розглядати як інноваційну управлінську технологію, що дає змогу підвищити конкурентоспроможність окремих регіонів, галузей та держави в цілому за рахунок ефективного вирішення безпекових питань [79, с. 13]. Основним важелем при цьому виступає неформальне об’єднання різних організацій (дослідних центрів, промислових підприємств, індивідуальних підприємців, органів державного управління, громадських організацій, закладів вищої освіти тощо) задля вирішення спільної мети − підвищення рівня безпеки.

Таким чином, можна стверджувати, що основні тренди в сфері управлінських інновацій формуються під впливом кіберсередовища, яке водночас створює нові технології та породжує загрози. Найбільшу небезпеку становлять кібератаки, спрямовані на фінанси, логістику, корпоративний імідж, клієнтів та їх персональні дані. В цьому сенсі особлива увага повинна приділятися захисту критичної інфраструктури, оскільки саме вона є пріоритетною ціллю більшості масштабних кібератак і від її стійкості залежить стабільність економіки, безпека громадян та національна обороноздатність.

1.2. Критична інфраструктура як об’єкт управління: сутність, структура та загрози стійкому функціонуванню

Функціонування національної економіки, а також зміцнення її конкурентоспроможності є неможливими без належного інфраструктурного забезпечення, тобто без військової, соціальної, транспортної, виробничої,

освітньої, ринкової, інноваційно-інвестиційної, інформаційної та інших видів інфраструктури.

В науковому середовищі ще й досі не існує єдиного підходу до визначення сутності та складових інфраструктури. Власне, сам термін інфраструктура (infrastructure) походить від латинського infra – «знизу», «під» та structura – «структура», «місце розташування». В економіці вперше термін «інфраструктура» був використаний П. Розенштейном-Роданом, який визначав інфраструктуру як «умови навколишнього суспільного середовища, необхідні для того, щоб приватна промисловість була в змозі зробити перший ривок» [184].

Протягом тривалого періоду часу відбувалася наукова дискусія стосовно матеріальної чи нематеріальної природи інфраструктури. Адже окремі науковці (наприклад, П. Самуельсон) розглядали її переважно як сукупність матеріальних об'єктів, що забезпечують функціонування виробничої сфери та підтримують соціально-економічну взаємодію [185]. В той же час як представники інституційного підходу (зокрема, Д. Норт та О. Вільямсон) акцентували увагу на значенні інституційної та інформаційної складових інфраструктури та її ролі у формуванні ефективних інституційних механізмів та оптимізації інформаційних потоків у господарських системах [174, 212, 213].

В сучасних дослідженнях інфраструктури більшість науковців схиляються до територіального або галузевого підходів. Згідно з першим під інфраструктурою розуміється комплекс основних об'єктів і систем, які обслуговують країну, місто чи район, включно з послугами та засобами, необхідними для функціонування економіки [195]. Тобто увага концентрується саме на території, яку має обслуговувати інфраструктура. З галузевого погляду інфраструктура виступає як комплекс галузей, що обслуговують промисловість і сільське господарство, будівництво, енергетичне господарство, залізничний транспорт, зв'язок, водопостачання та каналізацію, загальну та професійну освіту, науку, медицину тощо [34].

Якщо розвинути вищевказані підходи, категорію «інфраструктура» можна деталізувати таким чином. Насамперед, інфраструктура може функціонувати в

межах іншої економічної системи (наприклад, транспортна інфраструктура»), однак із власними принципами розвитку, властивостями та завданнями. Також інфраструктура (наприклад, соціальна чи інноваційна) може розглядатися в межах дослідження економічних процесів, які є загальними для усіх галузей національної економіки. В деяких випадках інфраструктура розглядається виключно в якості елементу іншої галузі господарства і прив'язана до неї (наприклад, інноваційна інфраструктура банківської сфери) або у межах просторових економічних систем (наприклад, інфраструктура регіонів чи більш деталізовано – транспортна інфраструктура Одеської області) [50].

З точки зору впливу на суспільні процеси розвинена інфраструктура є необхідною передумовою для соціально-економічного розвитку будь-якої країни, крім того, інфраструктурна складова є ключовою для фінансово-економічних центрів, технопарків, інноваційних кластерів тощо. З іншого боку, саме порушення стабільного функціонування інфраструктури є головним завданням в процесі військових конфліктів, терористичних актів, а в останні роки, насамперед, кібератак.

При цьому слід зауважити, що жодна країна не в змозі забезпечити повний та абсолютний захист власної інфраструктури від впливу зовнішніх чинників. Відтак виникає нагальна потреба у зосередження ресурсів на захисті критично важливих інфраструктурних об'єктів. «Критичність» вказує на можливість небезпеки та скрутних обставин, які в майбутньому можуть призвести до кризи або інших негативних наслідків. В цьому сенсі, наприклад, використовується визначення «критичні обставини» як скрутне, небезпечне становище. З цього погляду критична інфраструктура є особливим підвидом інфраструктури, що відіграє ключову роль у забезпеченні життєдіяльності суспільства, економіки та держави загалом.

У контексті управлінського впливу критична інфраструктура може розглядатися як сукупність об'єктів, які є стратегічно важливими для економіки та національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [13].

З функціонального погляду критична інфраструктура – це сукупність об’єктів незалежно від форми власності, що реалізують функції, виробляють товари (послуги), які є життєво необхідними для людей і діяльності країни та порушення яких призведе до дестабілізації суспільних відносин [99].

З точки зору прив’язки до економічної діяльності критичну інфраструктуру також можна розглядати як сукупність об’єктів, систем, мереж, послуг, які є стратегічно важливими для економіки та безпеки країни, суспільства, населення, пошкодження, знищення або порушення діяльності яких може завдати шкоди життєво важливим інтересам України [59].

За ресурсним підходом критичною інфраструктурою України є системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призводять до найсерйозніших негативних наслідків для життя суспільства та соціально-економічного розвитку країн та національної безпеки [36].

Враховуючи процеси цифрової трансформації, що відбуваються у сучасному суспільстві, в деяких визначеннях фігурує й інформаційна (нематеріальна) складова. Зокрема, критична інфраструктура – система надзвичайно важливих матеріальних та нематеріальних об’єктів національної інфраструктури (а також їх власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків із найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки [33].

Зважаючи на галузевий підхід, критична інфраструктура – системний комплекс стратегічних матеріальних та інформаційних об’єктів виробничої, невиробничої, соціальної сфери, а також окремих складових частин цього комплексу, у т. ч. ключових ресурсних, покликаних забезпечувати повноцінний життєвий цикл, безпеку, охорону здоров’я, добробут людини, сталий розвиток суспільства й економіки держави, підтримання її суверенітету з огляду на те, що зловмисне втручання у функціонування, а також пошкодження, руйнація або виведення з ладу системи або її елементів внаслідок диверсій, техногенних чи

природних катастроф спроможне призвести до тяжких наслідків: жертв чи поневірянь, шкоди національним інтересам, знецінення надбань людини і держави (у широкому сенсі) [94].

Зі вказаним визначенням перекликається й ідентифікація критичної інфраструктури як підприємств й установ (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв.

У випадку дослідження дефініції категорії «критична інфраструктура», можна стверджувати, що терміни «система» і «сукупність» використовуються в різних контекстах і можуть мати різне значення. Насамперед, система передбачає ефективну внутрішню взаємодію між окремими частинами або компонентами, задля досягнення спільної мети. Сукупність об'єктів які навіть територіально знаходяться поруч, не призводить автоматично до їхньої взаємодії, не кажучи вже про її ефективність. Далі система обов'язково має власну організаційну структуру, яка сприяє досягненню поставленої мети, в той час як сукупність є простим набором об'єктів чи елементів. Крім того, система зазвичай взаємодіє з довкіллям, може реагувати на зміни в ньому і навіть здійснювати зворотний вплив. В той же час для сукупності об'єктів вплив зовнішнього середовища на один з елементів не означає автоматичного впливу й на інші. Відтак, враховуючи внутрішню неоднорідність критичної інфраструктури України, зокрема з точки зору сфер діяльності та форм власності, можна стверджувати, що в стабільному стані вона є сукупністю об'єктів. Однак при вирішенні завдань протидії кіберзагрозам, особливо в умовах війни, критичну інфраструктуру потрібно розглядати виключно як систему. Складовими вказаної системи теж виступають певні об'єкти, що створює

теоретичне підґрунтя і для конкретизації категорії «об'єкт критичної інфраструктури».

В Україні під об'єктами критичної інфраструктури розуміють об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [75]. Віднесення до об'єктів критичної інфраструктури відбувається під впливом низки характеристик (табл. 1.2).

Таблиця 1.2

Основні характеристики об'єктів критичної інфраструктури

№	Характеристика	Опис	Приклад
1	Забезпечення важливих функцій	Об'єкти критичної інфраструктури надають послуги, без яких суспільство не може ефективно функціонувати.	Найбільш важливі послуги для населення (комунальні послуги, охорона здоров'я, освіта) надають саме об'єкти критичної інфраструктури.
2	Джерело ризиків для національної безпеки	Пошкодження або зрив функціонування об'єктів критичної інфраструктури може мати серйозні наслідки на макрорівні.	До об'єктів критичної інфраструктури відносяться, зокрема, підприємства оборонної промисловості.
3	Уразливість в кібер-середовищі	Об'єкти критичної інфраструктури потребують високого рівня захисту не тільки від фізичних, а й від кібератак.	Такі сфери критичної інфраструктури, як телекомунікації, енергетика, фінанси, державні інформаційні ресурси мають вагому інформаційну складову і часто стають об'єктами для кібератак.
4	Державне втручання	Держава часто встановлює спеціальні правила та норми для регулювання функціонування об'єктів критичної інфраструктури, забезпечуючи їхню надійність та безперебійність.	Для сфери кіберзахисту - діяльність Держспецзв'язку та Департаменту кіберполіції.
5	Залежність від міжнародної співпраці	Забезпечення ефективного захисту об'єктів критичної інфраструктури вимагає міжнародної координації та співпраці, особливо в сферах, де вказана інфраструктура перетинає національні кордони.	Синхронізація енергосистеми України з ENTSO-E, співпраця з FATF, підтримка у відновленні енергетичної інфраструктури, "зерновий коридор".

Джерело: *складено автором за [75, 105]*

В Україні критична інфраструктура є достатньо неоднорідною. Так, до критичної інфраструктури належать як фізичні об'єкти (наприклад, електростанції чи водопостачальні системи), так і інформаційно-комунікаційні (наприклад, телекомунікаційні мережі). Зі свого боку більшість фізичних об'єктів критичної інфраструктури також має власну інформаційну складову. Далі об'єкти критичної інфраструктури можуть відноситись до державної (енергетичні об'єкти, порти), муніципальної (заклади охорони здоров'я) та приватної (мобільні оператори) власності. Крім того, діяльність об'єктів критичної інфраструктури може бути неприбутковою (системи очищення води), умовно-прибутковою (лікарні) та комерційною (банки, підприємства агропромислового комплексу).

Якщо мова йде про іноземний досвід, ідентифікація критичної інфраструктури та її окремих об'єктів відбувається на основі низки програм та законодавчих актів (Додаток А). Наприклад, у США зазначений термін почав використовуватися після терористичних атак 11 вересня 2001 року, коли стало очевидним, що певні об'єкти та системи є критично важливими для безпеки держави [201].

В рамках європейських програм, критична інфраструктура не лише забезпечує функціонування окремого суспільства чи держави, але й має міжсуб'єктний характер, впливаючи на стабільність на регіональному та міжнародному рівнях. Це означає, що порушення роботи таких об'єктів може мати серйозні наслідки не лише для однієї держави, але й для кількох країн, що підкреслює важливість міжнародного співробітництва у сфері її захисту. Наприклад, у 2015 році було наголошено, що забезпечення безпеки та стійкості фізичної та кіберкритичної інфраструктури сприяє мінімізації наслідків від надзвичайних ситуацій, включаючи терористичні акти та кібератаки [72].

Характерною рисою критичної інфраструктури є її залежність від складних взаємопов'язаних систем, які включають як фізичні об'єкти (наприклад, електростанції, транспортні вузли), так і кібернетичні компоненти (інформаційні системи, бази даних). Це поєднання створює унікальні умови для забезпечення

безпеки, оскільки загрози можуть мати як фізичний, так і цифровий характер. У законодавстві США та Німеччини підкреслюється, що критична інфраструктура охоплює не лише матеріальні активи, але й нематеріальні, такі як інформаційні потоки та програмне забезпечення, що забезпечують її функціонування [141].

Одним із ключових аспектів, що ускладнює уніфікацію поняття критичної інфраструктури, є відсутність єдиного підходу до класифікації об'єктів, які вважаються критично важливими. Конкретний перелік об'єктів, що належать до критичної інфраструктури формується індивідуально в кожній окремій країні (Додаток Б).

У національних законодавствах спостерігається значна варіативність у визначенні секторів критичної інфраструктури. Наприклад, у Туреччині законодавство виділяє шість ключових секторів, що включають електронні комунікації, управління водними ресурсами, енергетику, функціонування критично важливих державних служб, транспорт, а також банки та фінанси [179]. У той же час у Бельгії та Сальвадорі кількість таких секторів обмежена чотирма. У Бельгії до критичної інфраструктури відносять енергетику, транспорт, фінанси та електронні комунікації, тоді як у Сальвадорі замість фінансового сектору акцент робиться на водні ресурси [62]. Зазначені відмінності відображають різні пріоритети держав, зумовлені їхніми соціально-економічними та географічними особливостями.

Інші країни, такі як Індія та Індонезія, включають до переліку критичної інфраструктури сектори, пов'язані з дослідженням і використанням космосу та електронним урядом, що підкреслює важливість технологічного прогресу для їхнього розвитку. Норвегія, зі свого боку, акцентує увагу на супутниковій інфраструктурі, що є унікальним для її національного контексту [129]. Найширший підхід демонструють США, де визначено 16 секторів критичної інфраструктури, включаючи не лише традиційні сектори, такі як енергетика чи транспорт, а й унікальні, як-от сектор комерційних об'єктів (об'єкти, що приваблюють натовпи людей для покупок, бізнесу, розваг чи проживання), сектор гребель (дамби, навігаційні замки, ураганні бар'єри тощо) та промислова

база оборони. Американське законодавство підкреслює, що до критичної інфраструктури належать як фізичні, так і віртуальні системи та ресурси, недієздатність яких може серйозно вплинути на національну безпеку, економіку чи громадське здоров'я [204]. Такий широкий підхід контрастує з більш вузькими визначеннями, де перелік обмежується чотирма секторами.

Варіативність у підходах до визначення критичної інфраструктури створює певний консенсус стосовно ключових секторів, які найчастіше згадуються в національних законодавствах. До них належать банки та фінанси, центральний уряд, інформаційно-комунікаційні технології, енергетика, медичні послуги, транспорт, водопостачання, продовольство та екологічний захист. Проте різні держави надають перевагу різним акцентам: одні включають максимальну кількість секторів, вважаючи їх критично важливими для функціонування суспільства, тоді як інші обмежуються кількома ключовими сферами. Такий розрив у підходах породжує низку проблем, зокрема у випадках, коли кібератака спрямована на об'єкти, які в одній державі вважаються критичними, а в іншій – ні. Це, зі свого боку, викликає питання стосовно того, як національні визначення впливають на міжнародно-правову оцінку таких порушень [62].

Ще однією проблемою є тенденція держав створювати закриті переліки об'єктів критичної інфраструктури, що обмежує гнучкість у реагуванні на нові виклики, зумовлені технологічним прогресом. Наприклад, бельгійське законодавство ігнорує важливість систем водопостачання, що виглядає нелогічним з огляду на їхню життєву необхідність. У цьому сенсі підхід Франції видається найбільш прогресивним, оскільки визначення критичної інфраструктури базується не на жорсткому переліку секторів, а на функціях, які виконують певні об'єкти [152].

На основі дослідження наявного наукового фундаменту, а також вивчення іноземного досвіду та вітчизняних реалій можна сформулювати авторське визначення критичної інфраструктури, як сукупності фізичних, кібернетичних і гібридних систем, об'єктів, мереж та ресурсів, які є життєво важливими для

забезпечення основних функцій суспільства, держави та її безпеки, включаючи економічну стабільність, громадське здоров'я, обороноздатність, управління, а також соціальну та екологічну стійкість. Вказані системи характеризуються високим ступенем взаємопов'язаності та незамінності, а їхня недієздатність чи порушення функціонування може спричинити значні негативні наслідки на національному, регіональному чи міжнародному рівнях, включно із загрозами життю населення, економіці, безпеці чи демократичним інститутам. Таке визначення є універсальним, але водночас адаптивним, розвиває наявні підходи до дослідження критичної інфраструктури і сприяє їхній гармонізації з огляду на необхідність захисту критичної інфраструктури від глобальних загроз.

Наступним етапом дослідження є ідентифікація загроз критичній інфраструктурі. З точки зору їхньої природи загрози для критичної інфраструктури поділяються на природні, техногенні та антропогенні. Природні загрози, такі як землетруси, повені чи урагани, можуть мати катастрофічні наслідки для фізичних компонентів інфраструктури, таких як електромережі чи транспортні вузли. Техногенні загрози, зокрема аварії на промислових об'єктах, збій у роботі програмного забезпечення або вихід з ладу обладнання через зношеність, становлять значний ризик через складність і взаємозалежність сучасних систем. Антропогенні загрози, включно з кібератаками, терористичними актами або саботажем, набувають особливої актуальності в умовах цифровізації та глобалізації (наприклад, кібератаки, спрямовані на системи керування енергетичними мережами чи фінансовими платформами, можуть спричинити каскадний збій, що вплине на значну кількість інших секторів).

На тлі ідентифікації загроз необхідне й розуміння вразливостей критичної інфраструктури. Вони можуть бути пов'язані з фізичними характеристиками об'єктів, наприклад, розташуванням у сейсмічно активних зонах, або з організаційними недоліками, такими як недостатній рівень підготовки персоналу чи застарілі протоколи безпеки. Зокрема, у цифровій сфері вразливості часто виникають через слабкі системи кіберзахисту, незахищені канали зв'язку або

використання застарілих програмних платформ. Ідентифікація вказаних вразливостей потребує регулярного аудиту, тестування на проникнення та аналіз ризиків, що базується на актуальних даних про загрози.

Визначення загроз та вразливостей передбачає категоризацію об’єктів критичної інфраструктури з метою встановлення кількісних і якісних вимог до системи захисту. Ці вимоги формуються залежно від рівня потенційних втрат, які можуть виникнути внаслідок порушення функціонування об’єкта, та відповідної категорії, присвоєної об’єкту на основі оцінки його потенційної небезпеки. При цьому оцінка має враховувати ймовірність і масштаби таких видів втрат, як економічні, соціальні, екологічні чи безпекові [31].

Віднесення окремих об’єктів до критичної інфраструктури здійснюється в чітко визначеному порядку, встановленому Кабінетом Міністрів України, а їхня ієрархія ґрунтується, насамперед, на показнику критичності. Вказаний показник визначає ступінь (відносний рівень) важливості об’єкта і його вплив на виконання життєво важливих функцій та/або надання життєво важливих послуг [31]. Згідно з показником критичності до першої категорії відносяться об’єкти, що мають високу важливість для держави в цілому і здатні суттєво впливати на інші об’єкти критичної інфраструктури. Якщо їхня робота буде порушена, виникне кризова ситуація державного значення. Друга категорія включає об’єкти, що є життєво важливими, а припинення чи порушення їх роботи спричинить кризову ситуацію регіонального значення. Третя категорія - це важливі об’єкти, порушення чи припинення роботи яких спричинить кризову ситуацію місцевого значення. І, нарешті, четверта категорія складається з об’єктів, порушення чи припинення роботи яких спричинить кризову ситуацію локального значення [28].

Процес категоризації передбачає комплексний аналіз об’єктів критичної інфраструктури, що включає не лише їх фізичні характеристики, але й їхню роль у забезпеченні ключових суспільних функцій. Для цього створюється спеціальна комісія, яка на першому етапі складає перелік усіх процесів організації, що стосуються використання об’єктів інфраструктури.

До цього переліку включаються: управлінські процеси, які охоплюють організацію та координацію діяльності; технологічні процеси, пов’язані з функціонуванням технічних систем; виробничі процеси, що забезпечують випуск продукції чи надання послуг; фінансово-економічні процеси, які стосуються управління ресурсами та фінансами; інші процеси, що мають значення для функціонування об’єкта.

Формально правила категоризації вимагають включення до переліку всіх процесів, однак на практиці процеси, які базуються виключно на ручній або механізованій праці, зазвичай виключаються з подальшого розгляду, оскільки вони не мають прямого впливу на критичність об’єкта [71].

Система державного управління у сфері охорони критичної інфраструктури формується через нормативно-правовий механізм, який включає сукупність правових засобів, методів і способів регулювання суспільних відносин у цій галузі. Цей механізм спрямований на забезпечення безпеки об’єктів, запобігання загрозам і мінімізацію ризиків, пов’язаних із їх функціонуванням.

Нормативно-правовий механізм охоплює законодавчі акти, підзаконні нормативні документи, а також організаційні та адміністративні заходи, які регулюють діяльність суб’єктів, відповідальних за охорону критичних об’єктів.

Серед категорій критичних об’єктів, що підлягають державному управлінню, виділяються такі:

− об’єкти, що реалізують важливі функції державного управління, такі як здійснення загального державного управління, управління конкретними територіями, координація діяльності окремих груп державних органів;

− об’єкти безпеки життєдіяльності населення, включаючи об’єкти транспортного призначення, які забезпечують мобільність і логістику;

− потенційно небезпечні об’єкти, які можуть становити загрозу для населення чи довкілля у разі аварій чи атак;

− об’єкти оборонного призначення, які мають стратегічне значення для національної безпеки;

− об’єкти з постійним або періодичним масовим зібранням людей, такі як стадіони, торговельні центри чи громадські заклади;

− об’єкти історії та культури, які мають високу суспільну та історичну цінність.

Функціональне призначення об’єктів, що реалізують важливі функції державного управління, полягає в забезпеченні стабільності та ефективності державного апарату (рис. 1.2.).

Рис. 1.2. Функції державного управління об’єктами критичної інфраструктури *(складено автором за [31])*

Для ефективного управління цими об’єктами необхідна чітка координація між різними відомствами, а також застосування сучасних технологій і методів аналізу ризиків. Категоризація дозволяє не лише визначити пріоритетність захисту об’єктів, але й оптимізувати розподіл ресурсів для їхньої охорони. У подальшому розвитку системи охорони критичної інфраструктури доцільно акцентувати увагу на вдосконаленні нормативно-правової бази, впровадженні інноваційних технологій захисту та підвищенні кваліфікації персоналу, залученого до цього процесу.

Основною метою забезпечення безпеки об’єктів критичної інфраструктури є оперативне отримання даних про потенційні загрози та їхнє використання для впровадження ефективних заходів захисту. Ключову роль у цьому процесі відіграють сучасні технології та обладнання, зокрема:

– автоматизовані системи забезпечення безпеки життєдіяльності міст;

– створення та функціонування ситуаційних і кризових центрів;

– організація систем відеоспостереження для моніторингу територій;

– оснащення найважливіших елементів інфраструктури засобами екстреного виклику оперативних підрозділів [31].

Ці заходи спрямовані на підвищення рівня захищеності об’єктів, забезпечення швидкого реагування на загрози та мінімізацію можливих наслідків.

Сукупність загроз, що стосуються об’єктів критичної інфраструктури, можна умовно поділити на дві основні категорії: загрози, спрямовані на сам об’єкт, і загрози, що походять від об’єкта та становлять небезпеку для навколишнього середовища чи населення.

Перша категорія охоплює внутрішні загрози, які виникають у межах самого об’єкта. До них належать локальні пошкодження систем життєзабезпечення, злочинна діяльність, крадіжки, побутові правопорушення, а також нещасні випадки. Запобігання таким загрозам є частиною повсякденної роботи правоохоронних органів і служб безпеки об’єктів, які забезпечують стабільне функціонування та захист від внутрішніх ризиків.

Друга категорія включає загрози, які створюють небезпеку для життєдіяльності населення, зокрема для прилеглих населених пунктів, що знаходяться в зоні впливу критично важливих об’єктів. Такі об’єкти можуть стати джерелом надзвичайних ситуацій через природні чи техногенні фактори, а також внаслідок несанкціонованих дій порушників.

Подібні інциденти здатні спричинити серйозні порушення в життєдіяльності населення, включаючи економічні, соціальні чи екологічні наслідки. Між цими двома групами загроз існує взаємозв’язок, оскільки

внутрішні проблеми об’єкта можуть посилювати зовнішні ризики. Однак особливу увагу в подальшому аналізі приділено загрозам, що впливають на безпеку життєдіяльності населення, оскільки вони є найбільш складними та недостатньо дослідженими. Основний акцент зроблено на загрозах, спричинених несанкціонованими діями порушників, які можуть мати значний деструктивний вплив.

Також загрози для об’єктів критичної інфраструктури можна класифікувати залежно від наявності чи відсутності систем безпеки. Перша група включає об’єкти, оснащені сучасними системами захисту, такими як відеоспостереження, системи контролю доступу чи екстреного реагування. Для таких об’єктів характерні певні особливості реалізації загроз. Так, акції можуть відбуватися як у робочий, так і в неробочий час, що розширює вікно можливостей для порушників. Також існує ризик змови з персоналом об’єкта, що значно полегшує підготовку та здійснення протиправних дій. Ба більше, такі акції можуть бути реалізовані невеликою групою виконавців без залучення терористів, що знижує складність їх організації

Крім того, порушники можуть обирати об’єкти з найбільшою вразливістю, що дозволяє проводити дії приховано та максимально ефективно. Підготовка таких акцій зазвичай не обмежена в часі, а їхні наслідки можуть бути надзвичайно серйозними для життєдіяльності населення, включно з економічними збитками, порушенням інфраструктури чи загрозою здоров’ю.

Друга група загроз стосується об’єктів і територій, які не оснащені системами безпеки або мають обмежений захист. Для таких об’єктів характерна доцільність здійснення акцій у моменти масового скупчення людей, що підвищує їхній потенційний вплив. Такі загрози зазвичай спрямовані на завдання фізичної шкоди, наприклад, через організацію пожеж, вибухів чи використання небезпечних речовин, або на психологічний вплив, зокрема через захоплення заручників.

Реалізація подібних акцій викликає значний політичний і психологічний резонанс на міському, регіональному чи навіть загальнодержавному рівнях, що

робить їх привабливими для порушників. Однак такі дії часто потребують залучення терористів і мають обмежений час для підготовки та виконання, що підвищує складність їхньої організації.

Крім того, необхідно враховувати як внутрішні, так і зовнішні фактори, що можуть впливати на безпеку об’єкта. Внутрішні загрози, такі як локальні пошкодження систем життєзабезпечення, крадіжки чи побутові правопорушення, вимагають постійного контролю з боку внутрішніх служб безпеки. Зовнішні загрози, зокрема терористичні акти, кібератаки чи природні явища, потребують інтеграції з регіональними та національними системами моніторингу.

Система ідентифікації загроз передбачає використання автоматизованих технологій, таких як системи відеоспостереження, сенсори для виявлення хімічних чи радіаційних загроз, а також програмне забезпечення для аналізу великих обсягів даних. Наприклад, інтелектуальні системи на основі штучного інтелекту дозволяють обробляти інформацію в реальному часі, виявляючи аномалії в поведінці персоналу чи відвідувачів, а також прогнозуючи потенційні ризики на основі історичних даних.

Доречною є інтеграція системи ідентифікації загроз із ситуаційними та кризовими центрами, які координують дії оперативних підрозділів у разі виникнення надзвичайних ситуацій.

Регулярні тренінги персоналу та симуляції надзвичайних ситуацій допомагають підвищити готовність до реагування на потенційні загрози. Наприклад, моделювання сценаріїв кібератак чи фізичних проникнень дозволяє виявити слабкі місця в системі безпеки та розробити ефективні контрзаходи.

Серед основних проблем при впровадженні системи ідентифікації загроз слід відзначити високу вартість сучасного обладнання, складність інтеграції різних технологій і необхідність постійного оновлення програмного забезпечення для протидії новим видам загроз, зокрема кібератакам. Крім того, існує проблема нестачі кваліфікованих фахівців, здатних ефективно управляти складними системами безпеки.

Перспективи розвитку системи ідентифікації загроз пов’язані з впровадженням технологій штучного інтелекту та машинного навчання, які дозволяють автоматизувати процеси моніторингу та прогнозування. Наприклад, алгоритми аналізу великих даних можуть виявляти патерни, що вказують на підготовку до протиправних дій, ще до їхньої реалізації.

Відтак можна стверджувати, що в Україні критична інфраструктура є базою для забезпечення основних функцій суспільства та держави. Її важливість з точки зору національної безпеки набула найвищого рівня з початком повномасштабного вторгнення. Майже усі об’єкти критичної інфраструктури підлягають постійним загрозам (природним, техногенним, антропогенним), а отже, й потребують надійного захисту. В цьому сенсі важливим є впровадження системи ідентифікації загроз для об’єктів критичної інфраструктури.

Адже, за умови ефективності вказаної системи, вона дозволяє не лише своєчасно виявляти потенційні ризики, але й забезпечувати швидке реагування для їхньої нейтралізації. Це, зі свого боку, сприяє підвищенню стійкості критичної інфраструктури до різноманітних загроз, забезпечуючи безпеку населення та стабільність суспільних процесів.

1.3. Методичні підходи до управління захистом критичної інфраструктури від кіберзагроз

Кожна країна формує свої унікальні управлінські підходи та стратегії для забезпечення безпеки об’єктів критичної інфраструктури, враховуючи специфічні загрози та вразливості. Під захистом критичної інфраструктури України слід розуміти комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [28, 36].

З початком повномасштабного вторгнення розробка та впровадження ефективних стратегій захисту об’єктів критичної інфраструктури постає одним із найважливіших аспектів національної безпеки України. Насамперед, мова йде

про створення комплексних систем безпеки, включаючи фізичний захист, кібербезпеку, а також розробку планів реагування на надзвичайні ситуації [43].

Зі свого боку, відсутність координованого управлінського підходу до кіберзахисту критичної інфраструктури створює ризики для стабільності та безпеки країни.

Адже наявні управлінські системи є недостатньо адаптованимиз до кіберзагроз. Під останніми, згідно з Законом України «Про основні засади забезпечення кібербезпеки України», розуміють наявні та потенційні явища і фактори, що становлять небезпеку життєво важливим національним інтересам України у кіберпросторі та негативно впливають на стан кібербезпеки держави [77].

Кіберзагрози як категорія управлінських досліджень включають кілька ключових складових. Насамперед, це об’єкт загрози, тобто інформація та її носії, які потребують захисту, а також суб’єкти загрози, до яких належать іноземні держави, вітчизняні чи іноземні підприємства та організації, окремі особи або групи осіб, самоорганізовані технічні системи тощо. Останніми роками основними суб’єктами кіберзагроз стали міжнародні злочинні групи кіберзлочинців, а також терористичні та екстремістські угруповання. Крім того, сучасна геополітична ситуація збільшила роль державних структур як суб’єктів кіберзагроз.

Методи реалізації кіберзагроз включають послідовність узгоджених дій, які можуть завдати шкоди об’єкту. При цьому можливими наслідками є негативні зміни (наприклад, збій у роботі системи, втрата грошей на рахунках, отримання зловмисниками доступу до конфіденційних даних) або відсутність позитивних змін у стані об’єкта загрози, які відповідають поставленим завданням суб’єкта загрози.

Існує залежність між видами кіберзагроз, їхніми джерелами, можливими негативними наслідками, а також управлінськими інструментами здатними мінімізувати вказані загрози (табл. 1.3). Розвиток інформаційних технологій надає зловмисникам усе більше можливостей для впровадження шкідливих дій.

Наприклад, постійне зростання кількості підключених до мережі пристроїв також створює нові вектори для атак, оскільки багато з них мають вразливості у системах безпеки [30].

Таблиця 1.3.

Характеристика кіберзагроз об'єктам критичної інфраструктури та управлінських інструментів їхньої мінімізації

Вид	Джерело загроз	Негативні наслідки	Інструменти
DDoS атаки	Державні структури, хактивісти, кіберзлочинці	Перебої в роботі, зупинка систем	Управлінські рішення про впровадження ШІ для виявлення загроз; оптимізація інвестування в технічні засоби та організаційні заходи; управлінська підтримка в межах кластеру кібербезпеки; підвищення кваліфікації технічного персоналу щодо реагування на інциденти.
Програми-вимагачі	Кіберзлочинці	Прямі фінансові втрати, шифрування даних з подальшим вимаганням грошей.	Управлінське моделювання потенційних втрат; оптимізація інвестування в технічні засоби та організаційні заходи; впровадження ШІ для виявлення загроз; планування резервного копіювання; вдосконалення внутрішніх організаційних політик; міжнародна співпраця.
Шкідливе ПЗ (наприклад, Industroyer).	Кіберзлочинці, хактивісти	Виведення обладнання з ладу, призупинення діяльності	Управлінське моделювання потенційних втрат; оптимізація інвестування в технічні засоби та організаційні заходи; управління на основі моделі Zero Trust; впровадження ШІ для виявлення загроз; вдосконалення внутрішніх організаційних політик.
Фішинг та соціальна інженерія	Інсайдери, кіберзлочинці	Витік даних, несанкціонований доступ, компрометація систем, прямі фінансові втрати	Управління на основі моделі Zero Trust; оцінка кіберризиків; проведення тренінгів з кібергігієни; формування корпоративної безпекової культури; моніторинг поведінки користувачів; управлінська підтримка в межах кластеру кібербезпеки.
Кібер шпигунство	Державні структури, терористичні групи	Витік конфіденційної інформації	Управління на основі моделі Zero Trust, проведення тренінгів з кібергігієни; формування корпоративної безпекової культури; міжнародна співпраця.

Джерело: *складено автором*

Тобто з погляду окремих об’єктів критичної інфраструктури можна стверджувати про наявність прямої залежності кіберзагроз від вагомості інформаційної складової в діяльності зазначених об’єктів. Відтак в дослідженні пропонується авторська класифікація об’єктів критичної інфраструктури України за вагомістю інформаційної складової в їхньому функціонуванні (табл. 1.4).

Таблиця 1.4

Класифікація об’єктів критичної інфраструктури України за вагомістю інформаційної складової

Категорія	Характеристика	Приклади
Інформаційно-залежна критична інфраструктура	Функціонування повністю або переважно базується на інформаційних технологіях, збій у яких може спричинити масштабні наслідки.	Об’єкти телекомунікацій (національні оператори, інтернет-мережі), банківський сектор (платіжні системи), енергосистеми (Smart Grid), центри обробки даних, державні цифрові сервіси.
Інформаційно-керована критична інфраструктура	Основні фізичні процеси керуються IT-рішеннями. Порушення інформаційної складової може зумовити збій, але не повну зупинку.	Енергетика, транспорт, охорона здоров’я.
Інформаційно-допоміжна критична інфраструктура	Основна діяльність менш залежна від цифрових технологій, які використовуються здебільшого для підтримки операцій. Порушення в IT-складовій не зупиняє функціонування об’єкту, але ускладнює його діяльність.	Харчова промисловість, комунальні служби, освітні установи.
Мінімально залежна від інформаційних систем критична інфраструктура	Цифрові технології мають обмежене застосування, а критичність інформаційної складової досить низька.	Гідротехнічні та інженерні споруди, об’єкти цивільного захисту та укриття, меліоративні системи механічного типу.

Джерело: *розроблено автором*

Другою умовою є людський фактор, який включає помилки користувачів, недостатній рівень кіберграмотності та невідповідне управління паролями. Важливу роль відіграє і соціальна інженерія, що спрямована на маніпулювання людьми з метою отримання доступу до конфіденційної інформації [58].

Третьою умовою є недостатній рівень захисту інформаційних систем. Це може бути викликано як застарілими технологіями, так і відсутністю сучасних засобів захисту, таких як міжмережеві екрани, системи виявлення та запобігання вторгненням, а також антивірусні програми. Відсутність регулярних оновлень програмного забезпечення також створює додаткові ризики [87, 4, 12].

Четвертою умовою є складність та взаємозалежність сучасних інформаційних систем, що ускладнює процеси захисту і робить системи більш вразливими до комплексних атак. Взаємозалежність означає, що уразливість в одній частині системи може призвести до компрометації інших частин [54].

П’ятою умовою є економічні та політичні мотиви зловмисників. Кіберзлочинці можуть бути мотивовані фінансовою вигодою, викраденням інтелектуальної власності або дестабілізацією роботи критичних об'єктів інфраструктури з політичних міркувань. Держави-агресори також можуть використовувати кібератаки для проведення шпигунських операцій або кібервійни [54, 38].

Таким чином, кіберзагрози виникають через комбінацію технологічних, людських, управлінських та мотиваційних факторів і вимагають не лише технічних змін, але й оновлення управлінських практик. Це, зі свого боку, передбачає застосування комплексних, проактивних і адаптивних принципів кіберзахисту [54, 38].

Так, комплексність захисту є фундаментальним принципом забезпечення кібербезпеки об’єктів критичної інфраструктури, що вимагає інтегративного підходу до поєднання технічних, організаційних і правових заходів. Технічні засоби, такі як системи виявлення вторгнень і міжмережеві екрани, доповнюються організаційними політиками, включно з регулярними аудитами безпеки, та відповідністю нормативно-правовим стандартам. Такий синтез забезпечує всебічний захист від багатогранних кіберзагроз, мінімізуючи системні вразливості.

Переходячи до принципу проактивності, варто зазначити, що він акцентує увагу на передбаченні загроз через постійний моніторинг і аналіз кіберпростору.

Впровадження превентивних заходів, таких як оновлення програмного забезпечення та використання систем прогнозування на основі штучного інтелекту, дозволяє виявляти потенційні атаки до їхньої реалізації, значно знижуючи ризик успішного проникнення.

Принцип конфіденційності зосереджується на захисті чутливих даних від несанкціонованого доступу. Використання шифрування та механізмів контролю доступу є критично важливим для об’єктів критичної інфраструктури, де витік інформації може спричинити значні економічні чи безпекові наслідки. Подібним чином, цілісність даних забезпечує їхню достовірність і незмінність, що є основою для надійного функціонування систем. Застосування цифрових підписів і хеш-функцій запобігає маніпуляціям, що особливо важливо для систем управління енергопостачанням чи транспортом, де порушення цілісності може призвести до катастрофічних збоїв.

Не менш важливим є принцип аутентифікації та авторизації, який забезпечує надійну ідентифікацію користувачів і контроль їхніх прав доступу. Багатофакторна аутентифікація та ролеве управління доступом знижують ризик несанкціонованих дій, що є критично важливим для захисту систем від внутрішніх і зовнішніх загроз. Цей підхід доповнюється моніторингом і реагуванням, які забезпечують постійне відстеження стану систем і оперативне реагування на інциденти. Використання спеціалізованих інструментів для виявлення аномалій дозволяє мінімізувати шкоду від атак, забезпечуючи швидке відновлення нормального функціонування.

Відтак управління кіберзахистом вимагає методичних підходів, що мають поєднувати системність, безперервність, адаптивність, пріоритетність та співпрацю. І при цьому бути відкритими для інтеграції інновацій як технологічних так і управлінських.

В технологічному аспекті в межах окремих об’єктів критичної інфраструктури вже використовується низка моделей кіберзахисту, зокрема: «Піраміда болю», «Діамант», «MITRE ATT&CK», концепція «глибинного захисту». Однак слід зауважити, що вони не є «вбудованими» в окремі

технології, а радше застосовуються як методологічні та практичні підходи у системах кіберзахисту. Наприклад, CERT-UA активно застосовують MITRE ATT&CK у практиці моніторингу кіберзагроз, а в межах Smart Grid «глибинний захист» використовують у SCADA-системах (багаторівневий поділ між корпоративною мережею, зоною керування виробництвом і польовим рівнем, таким як датчики чи контролери).

Зупинимось на зазначених моделях більш детально. «Піраміда болю» − це концепція, яка ілюструє, наскільки складно і «болісно» для зловмисників змінювати свої методи атаки, коли захисники виявляють і блокують певні індикатори компрометації.

Модель допомагає менеджменту зосереджуватися на ефективних стратегіях захисту, підвищуючи витрати для атакуючих і зменшуючи ефективність їхніх дій (рис. 1.3). Візуально «Піраміда болю» може бути представлена у вигляді ієрархічної структури, де нижні рівні включають індикатори, які легко змінити, наприклад, хеш-значення шкідливих файлів, що зловмисник може швидко модифікувати, додавши незначні зміни до коду.

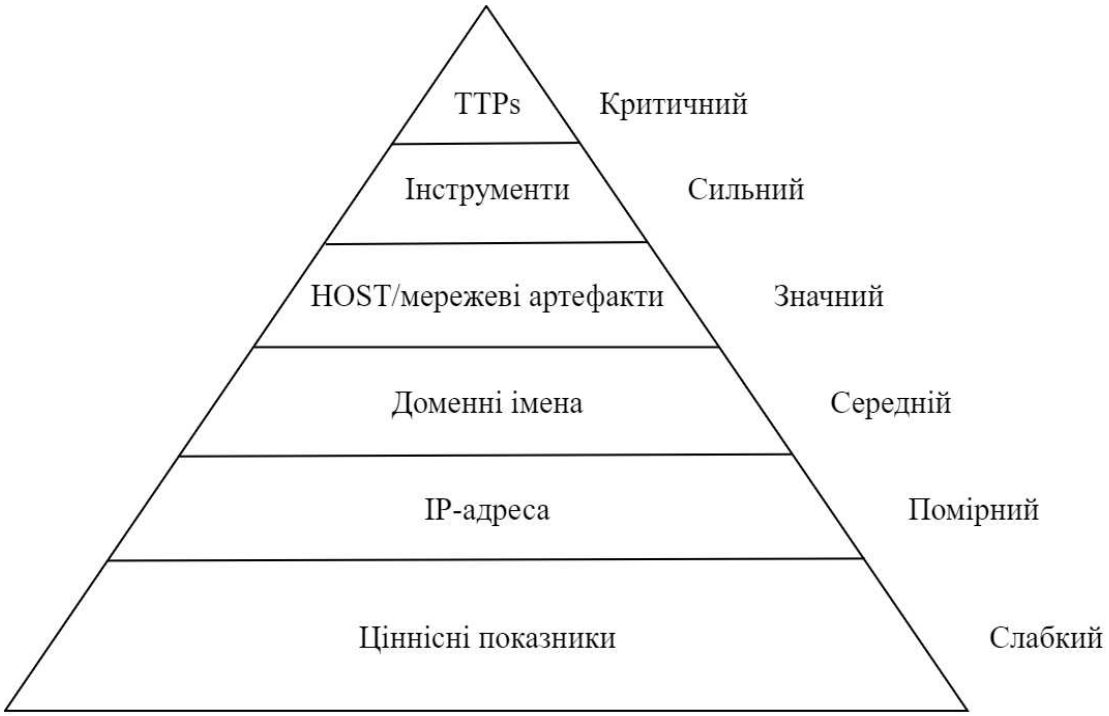

Рис. 1.3. Модель формування політики інформаційної безпеки за допомогою «Піраміди болю» *(складено за [32, 125])*

Вище розташовані IP-адреси, які також відносно просто замінити, використовуючи, наприклад, VPN або хмарні сервіси. Доменні імена, що стоять на наступному рівні, вимагають більше зусиль для заміни через необхідність нової реєстрації. Ще складніше змінити артефакти мережі чи хосту, такі як патерни трафіку або сигнатури, оскільки це потребує переробки інструментів атаки.

На вищих рівнях знаходяться інструменти, наприклад, специфічне програмне забезпечення для атак, зміна якого вимагає навчання або розробки нових засобів. На вершині піраміди розташовані тактики, техніки та процедури (TTPs), такі як методи соціальної інженерії чи експлуатації вразливостей, зміна яких є надзвичайно витратною і може вимагати повної перебудови стратегії атаки. Мета моделі – спрямувати зусилля захисників на верхні рівні, де блокування завдає зловмисникам максимальних труднощів [32, 125].

Формування політики інформаційної безпеки на основі «Піраміди болю» передбачає перехід від реактивного захисту, наприклад, блокування окремих IP-адрес, до проактивного підходу, орієнтованого на виявлення поведінки та TTPs. Такий підхід вимагає інвестування в інструменти для поведінкового аналізу, машинного навчання для моніторингу аномалій та інтеграції з фреймворками. Політика, яку впроваджує бізнес-структура, має включати регулярне оновлення знань про загрози через дані кіберрозвідки, що дозволяє створювати правила виявлення, орієнтовані на інструменти та артефакти, а не лише на нижні рівні піраміди.

Модель «Діамант» характеризується високим рівнем абстракції та застосовується до дослідницьких процесів, пов’язаних із подіями та інцидентами інформаційної безпеки, зокрема кібератаками. Для менеджменту ключовий аспект даної моделі полягає в тому, що кожну подію ініціює сам порушник, який може діяти самостійно або у складі групи, і кожна подія спрямована на досягнення певної мети. Порушник використовує тактики, техніки та процедури, застосовуючи можливості інфраструктури проти жертви для реалізації своїх цілей (рис. 1.4) [32, 40].

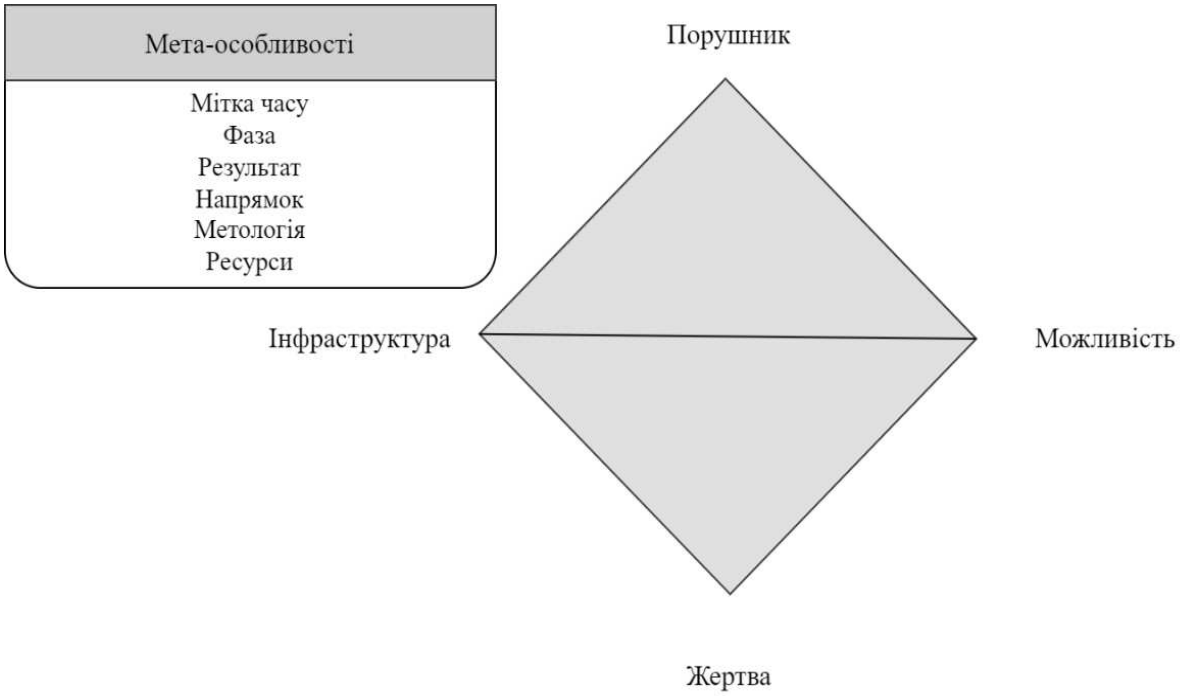

Рис. 1.4. Модель «Діамант» *(складено за [32, 40])*

Між порушником і жертвою завжди існує взаємозв'язок, навіть якщо він опосередкований. Жертва, яка може бути як матеріальним активом, так і людиною, обирається як найбільш «сприятлива». Зловмисна активність може бути спрямована на одну або кілька жертв, а також на подолання захисних заходів [40].

Модель «MITRE ATT&CK» (Adversarial Tactics, Techniques, and Common Knowledge; Тактики, Техніки та Загальновідомі Факти про порушників) характеризується середнім рівнем абстракції та застосовується менеджментом для забезпечення інформаційної безпеки комп'ютерних мереж (рис. 1.5) [32, 40].

Її функціонування залежить від розгортання сенсорів на кінцевих пристроях, які забезпечують безперервний моніторинг стану інформаційної безпеки, дозволяючи своєчасно виявляти потенційні загрози та реагувати на них. Основні принципи моделі базуються на перспективі атакуючого, використовуючи дані з реальних інцидентів, задокументованих у відкритих звітах [32, 40]. Це дозволяє створювати реалістичні сценарії кібератак і розробляти відповідні стратегії захисту.

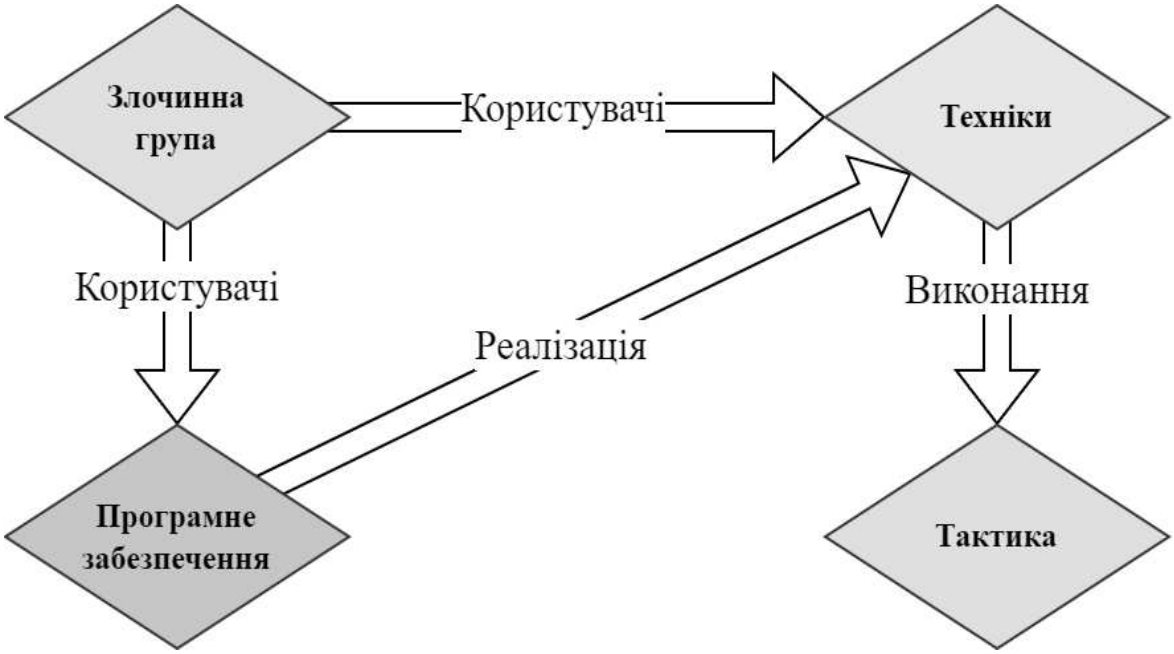

Рис. 1.5. Модель «MITRE ATT&CK» *(складено за [40, 48])*

Модель застосовує принцип Парето, що передбачає фокус на найбільш поширених тактиках і техніках кібератак, які становлять основну частину загроз. Такий підхід сприяє переходу від реактивних до проактивних захисних заходів і дозволяє передбачати та нейтралізувати короткострокові цілі зловмисників. Завдяки цьому створюються умови для глибшого захисту, що включають вибір і застосування оптимального набору тактик і технік для протидії кіберзагрозам. [40, 48].

Модель «MITRE ATT&CK» є цінним інструментом для аналізу поведінки зловмисників, прогнозування їхніх дій і розробки ефективних стратегій захисту комп’ютерних мереж.

Концепція «глибинного захисту» (Defense in Depth) базується на ідеї створення багатошарової системи захисту для забезпечення стійкості інформаційних систем. Цей підхід передбачає розподіл механізмів управління безпекою на кілька рівнів, що дозволяє мінімізувати ризик компрометації системи навіть у разі збою одного з них. Така концепція не лише підвищує загальну безпеку, але й ускладнює завдання зловмисникам, змушуючи їх долати численні бар’єри (рис. 1.6).

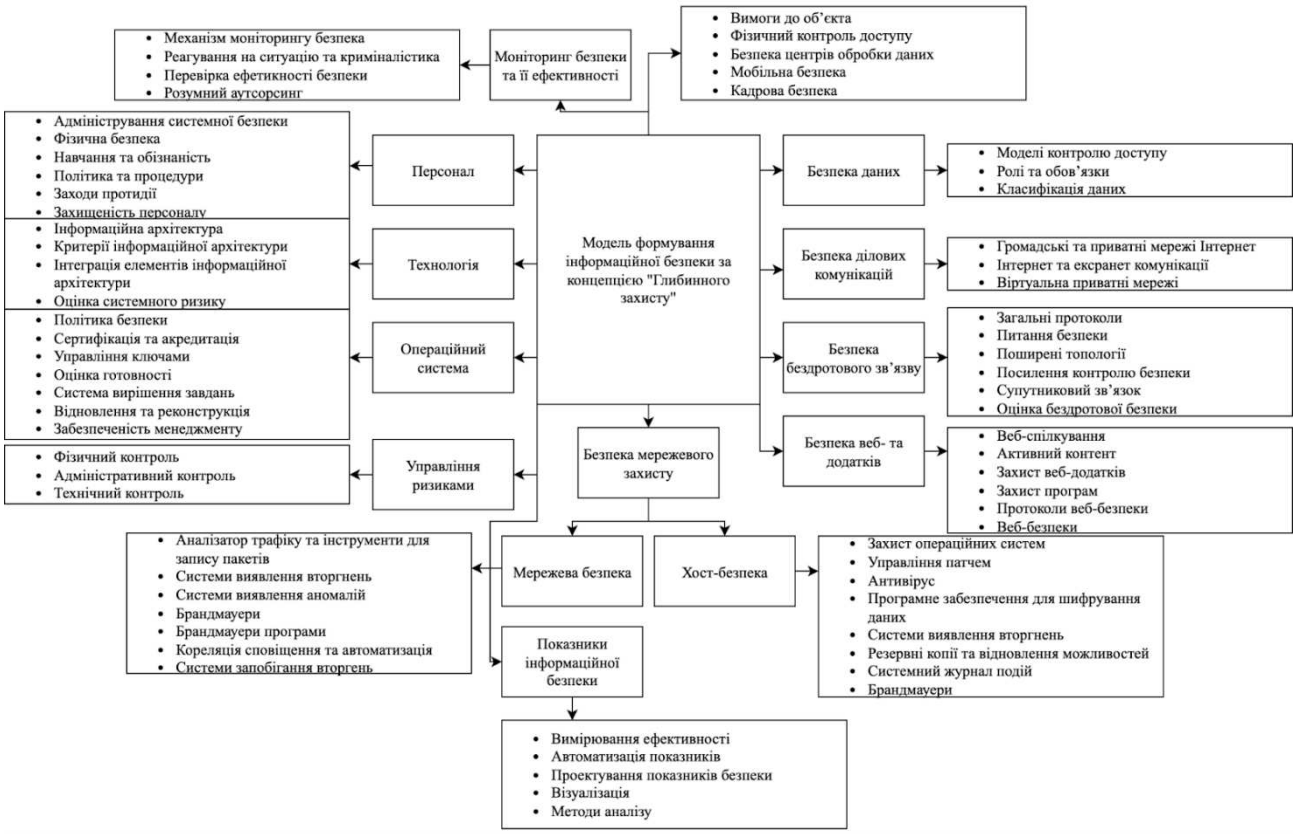

Рис. 1.6. Модель за концепцією «глибинного захисту» *(розроблено автором за [125, 140])*

Вона включає широкий спектр компонентів: менеджмент, персонал, технології, операційні та бізнес-процеси, моніторинг і показники безпеки, які разом формують комплексну систему захисту. На основі концепції створюється «карта розуму», яка систематизує організаційні та технічні аспекти, враховуючи ключові елементи: людей, політику, моніторинг і метрики безпеки

Основою «глибинного захисту» є три ключові рівні організації інформаційної безпеки. Фізичний рівень охоплює заходи для обмеження несанкціонованого доступу до IT-інфраструктури. Це включає використання фізичних засобів безпеки, таких як охорона приміщень, системи контролю доступу, відеоспостереження, сигналізації та захищені телекомунікаційні шафи. Вони покликані створити перший бар'єр, запобігаючи фізичному доступу до критичних активів.

Технічний рівень охоплює апаратні та програмні засоби захисту, які контролюють доступ до інформаційних систем. Сюди входять міжмережеві

екрани (фаєрволи), антивірусне програмне забезпечення, проксі-сервери, системи аутентифікації та авторизації, а також інструменти для шифрування даних і захисту мережевого трафіку. Цей рівень забезпечує технічну основу для протидії кібератакам.

Адміністративний рівень тобто рівень менеджменту включає політики, процедури та регламенти, які регулюють управління захистом інформації, обробку критичних даних, використання технічних засобів і взаємодію співробітників з інформаційною системою та зовнішніми суб'єктами. Ці документи формують організаційну основу, забезпечуючи чіткі правила та відповідальність [125, 140].

Формування політики інформаційної безпеки на основі «глибинного захисту» передбачає інтеграцію всіх трьох рівнів у єдину систему, де кожен компонент доповнює інші. Наприклад, фізична безпека гарантує, що сервери не будуть скомпрометовані через несанкціонований доступ, технічні засоби захищають від мережевих атак, а адміністративні політики забезпечують правильне використання систем і навчання персоналу. Важливою особливістю є те, що модель не вимагає реалізації всіх компонентів одночасно за принципом «все або нічого». Натомість доцільно застосовувати покроковий підхід, що дозволяє досягати швидких результатів із мінімальними витратами. Наприклад, організація може спочатку впровадити базові технічні засоби, як антивірусний захист і фаєрволи, а згодом додати складніші елементи, такі як системи виявлення вторгнень (IDS/IPS) або розширені програми навчання персоналу.

Перевагою концепції «глибинного захисту» є її гнучкість і адаптивність. Вона дозволяє організаціям адаптувати політику до їхніх потреб, масштабів і доступних ресурсів. Водночас модель враховує людський фактор, наголошуючи на важливості навчання співробітників, оскільки вони часто є найслабшою ланкою в системі безпеки.

Можна стверджувати, що кожна з досліджених моделей має власні переваги, але ефективне управління кіберзахистом критичної інфраструктури вимагає комплексного підходу з інтеграцією усіх найкращих практик

вищевказаних моделей. Зрештою подібна інтеграція і має отримати форму управлінської інновації.

Якщо мова йде про конкретну конфігурацію, доцільно запропонувати застосування моделі «Діамант» в управлінських процесах для зосередження зусиль на стратегічному аналізі вразливостей інформаційних систем і формуванні відповідних управлінських рішень, які максимально враховують тактику та інструменти зловмисників. За допомогою вказаної моделі менеджмент визначає пріоритетні активи, що потребують найбільшого захисту, і координує діяльність окремих підрозділів. Зі свого боку, модель «MITRE ATT&CK» має застосовуватися при формуванні управлінських рішень при переході від реактивного до проактивного захисту. В такій ситуації менеджменту доцільно застосовувати принцип Парето, щоб зосередитися на найпоширеніших тактиках атак, і розробляти плани для нейтралізації загроз ще до їхнього фактичного виникнення. Таким чином, з'являється можливість не лише адаптувати досліджені моделі до потреб критичної інфраструктури, а й отримати додатковий ефект від їхньої гнучкості та стійкості перед трансформаціями кіберзагроз.

Важливим управлінським інструментом протидії кіберзагрозам є формування складу основних і додаткових засобів захисту. Основні засоби захисту інформації являють собою мінімальний набір інструментів і заходів, які забезпечують необхідний рівень безпеки, визначений політикою інформаційної безпеки організації [40]. Ці засоби є базовими та спрямовані на гарантування захисту ключових інформаційних активів від найпоширеніших загроз, забезпечуючи стабільне функціонування систем і мереж.

Додаткові засоби захисту інформації включають елементи з комплекту засобів захисту, які не входять до основного набору, але можуть бути застосовані для посилення безпеки в специфічних сценаріях або для протидії менш поширеним загрозам. Вони слугують як доповнення до базового комплекту, забезпечуючи гнучкість і адаптивність системи захисту.

Визначення основного комплекту засобів захисту здійснюється через послідовне вирішення задачі оптимального вибору з широкого діапазону доступних інструментів. Цей процес передбачає покрокове скорочення кількості засобів захисту, де кожен крок відповідає виключенню однієї одиниці засобу конкретного типу. Такий підхід дозволяє систематично оцінювати ефективність засобів і формувати оптимальну конфігурацію, яка відповідає вимогам політики безпеки та ресурсам організації [40]. Завдяки цьому забезпечується баланс між рівнем захисту та економічною доцільністю, що є критично важливим для ефективного управління інформаційною безпекою.

Крім вищевказаних моделей в межах проведеного дослідження пропозиції з впровадження інноваційних управлінських рішень передбачають інтеграцію циклу управління PDCA (Plan-Do-Check-Act) або, як його інакше називають, цикл Демінга. Він складається з таких етапів, як «Планування», «Виконання», «Контроль» і «Корекція» і спрямований на постійне поліпшення безпеки організації з використанням об’єктивно вимірюваних індикаторів [63].

Його суть полягає в тому, що будь-яке управлінське рішення чи процес в межах об’єктів критичної інфраструктури має проходити послідовні етапи планування, реалізації, перевірки результатів та коригування дій. Це дозволяє не лише впроваджувати зміни, а й робити їх обґрунтованими, контрольованими, ефективними в довгостроковій перспективі, а також підтримувати високий рівень інновацій.

Починається все з етапу планування − формування цілей, завдань і шляхів їх досягнення. Тут аналізується ситуація, виявляються проблеми або можливості, оцінюються ризики та ресурси, і на основі отриманої інформації розробляється план дій. Особливо важливо на цьому етапі чітко окреслити очікувані результати та критерії, за якими керівництво в подальшому буде оцінювати успішність впроваджених змін.

Другий етап − це реалізація запланованих заходів. На цьому рівні йде практичне виконання завдань відповідно до розробленого плану. Важливо не просто впровадити зміни, а забезпечити їх документування, супровід і, за

можливості, впроваджувати їх у контрольованому середовищі або в обмеженому масштабі − для зниження ризику негативних наслідків.

Надалі після етапу виконання переходять до перевірки. На цьому етапі аналізуються результати діяльності: чи справдилися прогнози, чи досягнуто поставлених цілей, які відхилення були зафіксовані та що саме стало причиною успіху або невдачі. Перевірка повинна ґрунтуватися на об’єктивних даних, тому важливо ще на етапі планування закладати інструменти збору та оцінки інформації.

Завершує цикл етап коригувальних дій. Якщо зміни принесли позитивний результат, підприємство може масштабувати нові практики, інтегрувати їх у стандарти або процедури, закріпити досягнення. Якщо ж результат виявився неефективним, проводиться аналіз причин, вносяться корективи у план, і цикл повторюється. І саме зазначена повторюваність забезпечує постійне вдосконалення. Зокрема, як практичний приклад аналізу причин та застосування корегувальних дій, в проведеному дослідженні розглядатиметься доцільність використання управлінсько-наглядової системи контролінгу для мінімізації ризиків інструментів штучного інтелекту в процесі забезпечення кіберзахисту об’єктів критичної інфраструктури в енергетичному секторі.

Забезпечення ефективності та безперервності функціонування об’єктів критичної інфраструктури вимагає впровадження структурованого управлінського процесу (на основі загальної методології оцінки ризиків), який складається з чотирьох ключових етапів: ідентифікації ризиків, їх оцінки, пріоритезації та постійного моніторингу. Такий підхід дозволяє мінімізувати негативний вплив на економічні та соціальні компоненти діяльності, забезпечуючи довгострокову стійкість проєктів [160].

Оцінка ризиків об’єктам критичної інфраструктури передбачає ідентифікацію та класифікацію загроз, ідентифікацію вразливостей та оцінку наслідків. Ключовою особливістю оцінки ризиків для критичної інфраструктури є врахування численних взаємозв’язків між її об’єктами (зокрема за допомогою інформаційних систем та комп’ютерних мереж) [183].

Методологія оцінки ефективності управлінських інновацій, спрямованих на зниження кіберзагроз, також базується на застосуванні таких підходів, як OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) та CRAMM (CCTA Risk Analysis and Management Method), впроваджений Central Computer and Telecommunications Agency (CCTA). Зазначені підходи дозволяють систематично ідентифікувати активи критичної інфраструктури, оцінювати вразливості та визначати ймовірність реалізації загроз (рис. 1.7) [109, 159, 198].

Для кількісної оцінки ефективності управлінських інновацій застосовуються статистичні методи, такі як регресійний аналіз для оцінки кореляції між впровадженням інноваційних рішень і зниженням частоти кіберінцидентів, а також методи аналізу чутливості для визначення ключових факторів впливу. Наприклад, використання метрик, як-от Mean Time to Detect (MTTD) і Mean Time to Respond (MTTR), дозволяє оцінити швидкість реагування на інциденти, тоді як показник Return on Security Investment (ROSI) допомагає визначити економічну доцільність впровадження інновацій [176, 107, 116].

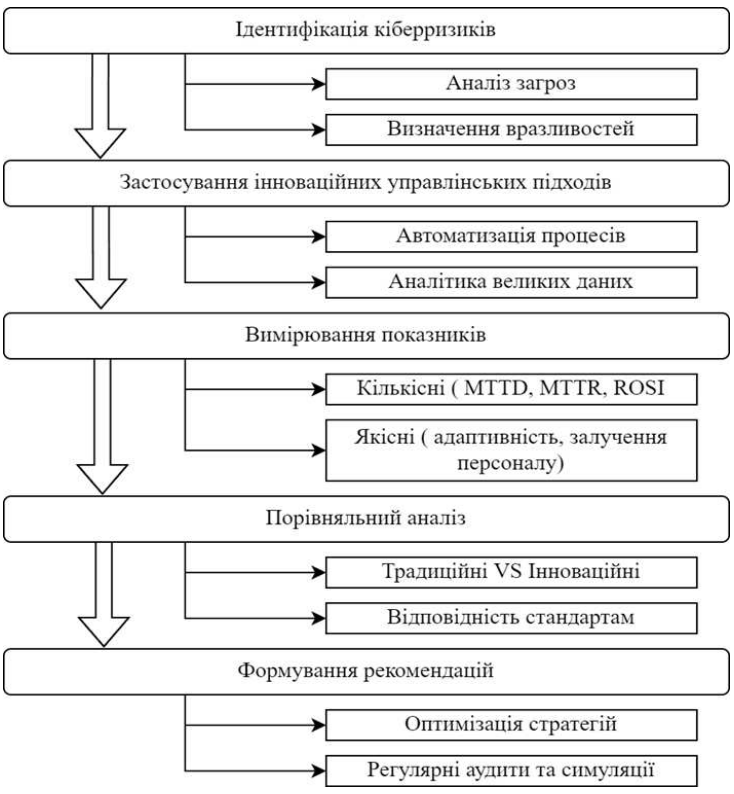

Рис. 1.7. Методика оцінки ефективності управлінських інновацій спрямованих на зниження кіберризиків *(складено за [109, 159, 198, 176, 107, 116])*

У процесі формування методичних підходів до управління захистом об’єктів критичної інфраструктури від кіберзагроз доцільним є використання математичного апарату для формалізації управлінських рішень щодо розподілу ресурсів.

Залежно від конкретних управлінських ситуацій використання ресурсів на організацію кіберзахисту бізнес-структур може розглядатися як витрати чи як інвестиції. Про кіберзахист, як витрати (operational expenditures, OPEX), доцільно вести мову, коли він має підтримувальний характер, не створює самостійної майбутньої економічної вигоди, спрямований на забезпечення поточної працездатності систем. Типовими прикладами подібних витрат є оплата підписки на антивірусне прогрмне забезпечення, заробітна плата фахівців з кібербезпеки, витрати на аудит інформаційної безпеки, реагування на інциденти тощо. Отже, це неминучі управлінські витрати, аналогічні витратам на фізичну охорону.

Зі свого боку, кіберзахист, як інвестиції (capital expenditures, CAPEX), передбачає орієнтацію на довгострокову цінність, зменшення стратегічних ризиків, підвищення не тільки кіберстійкості, але й загальної конкурентоспроможності бізнес-структури. Як приклад можна використати створення або модернізацію власного центру кіберзахисту, впровадження комплексних систем управління кіберризиками, розробку власних захисних IT-рішень, створення окремої посади менеджера з кібербезпеки, організацію тренінгів з кібербезпеки для персоналу. Зазначені вкладення запобігають значно більшим втратам у майбутньому та забезпечують безперервність діяльності. Відтак для подальшого моделювання використовуватимуться, насамперед, інвестиції у кіберзахист.

У класичних моделях управління інвестиціями в заходи захисту відповідне завдання формулюється як визначення такого рівня інвестування, за якого сукупні очікувані витрати, пов’язані з імовірністю реалізації негативних подій та витратами на захисні заходи, набувають мінімального значення, що описується таким співвідношенням.

$$\min_{I}\{p(I)\cdot D + I\}, \qquad (1.1)$$

де I– обсяг інвестицій у заходи захисту, $p(I)$– імовірність реалізації негативної події, що зменшується зі збільшенням інвестицій, D – величина потенційних втрат.

У вказаній постановці оптимум досягається тоді, коли граничні витрати на захист дорівнюють очікуваному скороченню ризику. Проте така модель є надто агрегованою, тобто враховує лише один канал витрат і не відображає комплементарність між технічними та управлінськими заходами.

Альтернативою для вказаної моделі є ігрові моделі «захисник–зловмисник», у яких розглядається стратегічна взаємодія сторін, у яких інвестиції розглядаються як стратегічна взаємодія двох сторін [149]. Формально це може бути записано як задача двох гравців з функціями виграшу $U_G(I)$ для захисника та $U_{\mathrm{A}}(\mathrm{A})$ для того, хто атакує, де I – вектор інвестицій в захист, а A – зусилля атакуючого. Хоча такі моделі краще описують динамічний характер протидії, вони є складними для практичної реалізації, оскільки вимагають знання стратегій і ресурсів противника.

Відтак при вирішенні управлінських завдань стосовно захисту критичної інфраструктури від кіберзагроз математичний апарат базується на теорії очікуваної корисності, яка використовується в економіці для моделювання прийняття рішень в умовах невизначеності [156].

$$\max_{z\geq 0} E[U(W)] = \big(1-p(z)\big)\,U\big(Y - C(z)\big) + p(z)\,U(Y - C(z) - L), \qquad (1.2)$$

де Y– початковий інвестиційний ресурс, що перебуває в розпорядженні суб'єкта управління; $C(z)$– вартість захисних заходів, безпосередньо пов'язана з обраним рівнем інвестування z; L – величина потенційних втрат у разі виникнення інциденту; $p(z)$– імовірність настання інциденту, яка зменшується зі зростанням рівня інвестування; $U(\cdot)$ – функція корисності, що відображає ставлення суб'єкта управління до ризику.

Важливо врахувати, що існують різні підходи до трактування функції корисності, яка відображає ставлення суб'єкта до ризику. Якщо рішення ухвалюються, виходячи виключно з очікуваної величини втрат, то корисність описується лінійною залежністю $U(W) = W$, що відповідає нейтральному ставленню до ризику.

Значно поширенішим у практиці є випадок ризик-несхильності, коли організація схильна уникати значних втрат і надає перевагу більш прогнозованим результатам. У цьому разі функція набуває вигляду, наприклад $U(W) = \ln(W)$ або $U(W) = W^{\gamma}$ де$0 < \gamma < 1$.

Така залежність адекватно описує управлінські стратегії, орієнтовані на зниження ризику в умовах невизначеності. Натомість ситуації, коли організація демонструє готовність приймати надмірні ризики, відповідають опуклій формі функції [144].

Отже використання функцій корисності створює основу для подальшої побудови формалізованих моделей прийняття управлінських рішень, де оцінюється не лише очікувана величина збитків, але й чутливість до ризику. В контексті проведеного дослідження це підводить до застосування більш складних моделей, що враховують ефективність інвестицій, спрямованих на зменшення ймовірності кіберінцидентів (рис. 1.8).

Серед ключових моделей, що визначили сучасні управлінські підходи до інформаційної безпеки, особливе місце посідає модель Гордона-Льоба.

Вказана модель була розроблена для формалізації проблеми вибору оптимального рівня інвестицій у захист інформаційних активів і базується на припущенні, що кожен актив має початкову уразливість $v \in (0; 1)$ а у випадку успішної атаки можливі збитки становлять $L > 0$ та витрати на захист – $z \geq 0$, то ймовірність реалізації загрози можна подати у вигляді функції $g(v, z)$, де $g(v, 0) = v$, $\frac{\partial g}{\partial z} < 0$, тобто інвестиції зменшують уразливість із власним зростанням, але, з іншого боку $\frac{\partial^2 g}{\partial z^2} > 0 -$ спадна гранична віддача.

Тоді очікувані втрати, пов’язані з реалізацією негативних подій, можуть бути подані у вигляді добутку функції ризику та величини потенційних збитків L, а сукупні очікувані витрати, зумовлені прийнятими управлінськими рішеннями щодо рівня інвестування в захист, набувають такого вигляду:

$$TC(z) = z + g(v, z) \cdot L, \tag{1.3}$$

де z характеризує обсяг інвестицій у заходи захисту, а функція $g(v, z)$відображає імовірність реалізації негативної події з урахуванням впливу управлінських та організаційних чинників v.

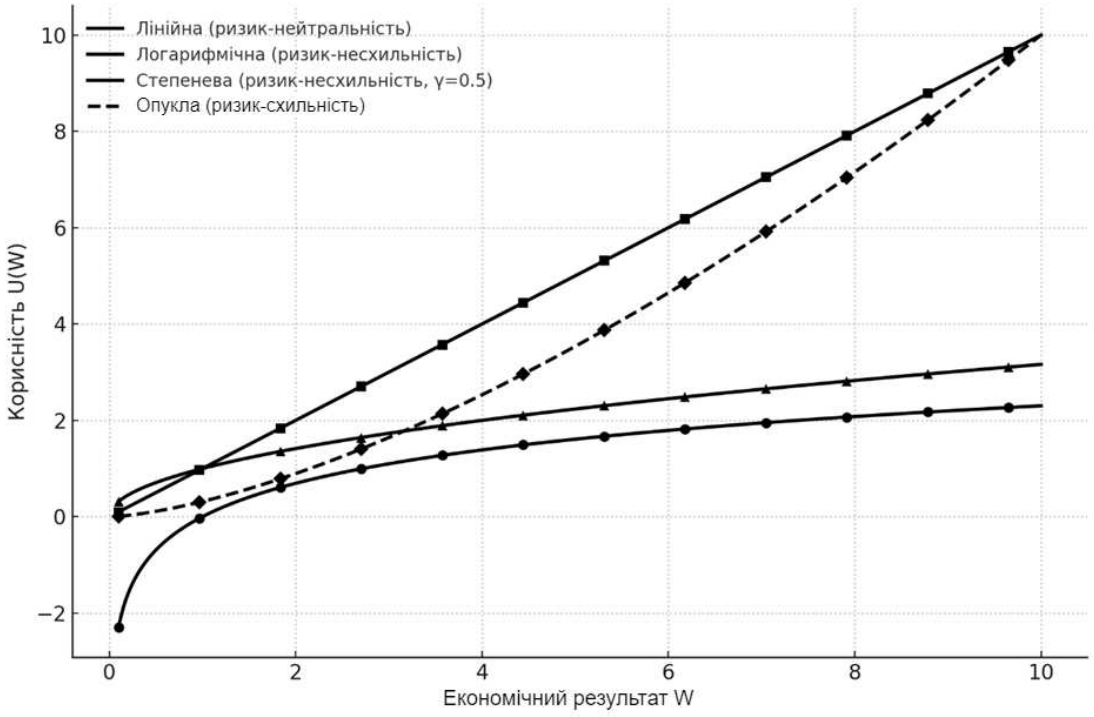

Рис. 1.8. Графіки функцій корисності у моделюванні прийняття рішень для захисту критичної інфраструктури *(розроблено автором на основі [149, 144])*

У межах базової аналітичної постановки задача вибору рівня інвестування може бути зведена до пошуку такого значення z, за якого сукупні очікувані витрати досягають мінімального значення:

$$\min_{z \geq 0} TC(z) = z + g(v, z) \cdot L\,, \tag{1.4}$$

необхідна умова оптимальності, для якої визначається з рівняння першої похідної:

$$TC'(z) = 1 + L \cdot \frac{\partial g(v,z)}{\partial z} = 0, \text{звідки} \frac{\partial g(v,z^*)}{\partial z} = -\frac{1}{L} \quad (1.5)$$

Тобто в точці оптимуму граничне зменшення уразливості дорівнює $1/L$. Це означає, що додаткове зниження ризику більше не окупає додаткову одиницю витрат. Ключовим результатом є існування верхньої межі для оптимальних витрат:

$$z^* \leq \frac{1}{e} \cdot vL \quad (1.6)$$

Це відоме у наукових колах «правило однієї третини» або правило $1/e$, яке накладає універсальне обмеження на доцільність інвестицій. Інакше кажучи, витрати на безпеку не можуть перевищувати певної частки можливих збитків, оскільки після цієї межі спостерігається різке зниження ефективності додаткових витрат (рис. 1.9) [149, 148].

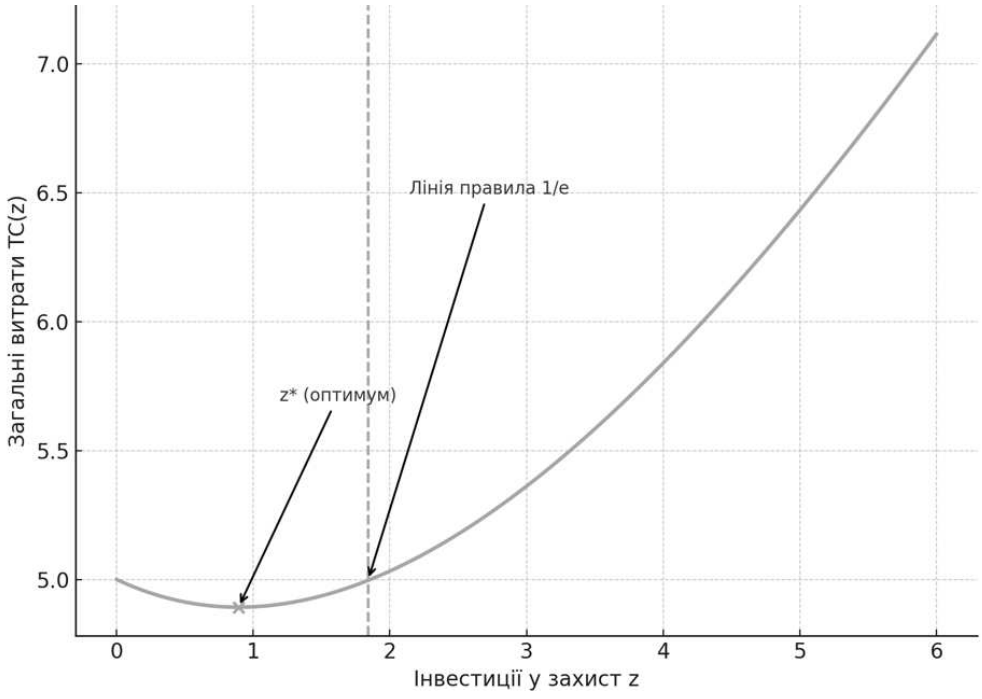

Рис. 1.9. Загальні витрати $TC(z)$ та межа $1/e$ у моделі Гордона-Льоба

(розроблено автором на основі [149, 144, 148])

З практичного погляду використання вищевказаної моделі дає змогу менеджменту об’єктів критичної інфраструктури встановлювати стратегічно виправдані рівні фінансування заходів кібербезпеки. Вона також підкреслює фундаментальний принцип спадної віддачі: кожна додаткова одиниця інвестицій приносить усе менший ефект зниження ризику [114]. Це створює підґрунтя для подальших модифікацій моделі, які враховують кілька напрямів інвестування одночасно.

Узагальнюючи результати аналізу, можна зробити висновок, що традиційна постановка моделі Гордона-Льоба, орієнтована на один напрям інвестування, вже не відображає повною мірою потреб сучасного управління захистом критичної інфраструктури.

На практиці менеджмент не може обмежуватися виключно технічними інструментами (мережеві засоби захисту, міжмережеві екрани, системи моніторингу), тому що значну роль відіграють також організаційні інвестиції, що включають навчання персоналу, формування політик доступу, розвиток культури інформаційної безпеки та відпрацювання процедур реагування на інциденти. При цьому важливо не просто впроваджувати системи захисту, а й діяти на випередження шляхом оцінки загроз і завчасного планування дій у разі інцидентів.

Висновки до 1-го розділу

1. Як елемент управлінської діяльності вирішення проблем безпеки ґрунтується на закономірностях функціонування складних соціально-економічних і технічних систем, методах управління ризиками, принципах стійкості та адаптивності, що дає змогу забезпечувати збалансоване поєднання превентивних, реактивних і відновлювальних заходів для гарантування безпеки на всіх рівнях, зокрема в кіберпросторі. Адже з огляду на тотальну цифровізацію можна стверджувати про інтегрування окремих елементів фізичної та кібербезпеки у єдину систему, яка, зі свого боку, є об’єктом управлінської діяльності. Управлінські інновації є вагомим важелем при вирішенні безпекових питань, адже вони дозволяють підвищити ефективність використання людського капіталу, створюють сприятливі умови для розробки та поширення технологічних інновацій, скорочують час реагування на загрози та забезпечують гнучкість та адаптивність при протидії ним. Проте впровадження управлінських інновацій є достатньо складним процесом, що потребує фінансових ресурсів та організаційної готовності до змін.

2. Управління критичною інфраструктурою передбачає втручання у діяльність складних взаємопов’язаних систем, які включають як фізичні об’єкти (наприклад, електростанції, транспортні вузли), так і кібернетичні компоненти (інформаційні системи, бази даних). Вказана ситуація знаходить відображення у авторському визначенні критичної інфраструктури як сукупності фізичних, кібернетичних і гібридних систем, об’єктів, мереж та ресурсів, які є життєво важливими для забезпечення основних функцій суспільства, держави та її безпеки, включаючи економічну стабільність, громадське здоров’я, обороноздатність, управління, а також соціальну та екологічну стійкість. Високий рівень інформатизації критичної інфраструктури значно підвищує її ефективність, але робить вкрай вразливою до кіберзагроз. Останні здатні впливати не тільки на інформаційну складову, а й на реальні фізичні процеси.

3. Посилення кіберзагроз критичній інфраструктурі України, а також їхня постійна трансформація потребують відповідного управлінського реагування на основі методичних підходів, що мають поєднувати системність, безперервність, адаптивність, пріоритетність та співпрацю і при цьому бути відкритими для інтеграції інновацій як технологічних, так і управлінських. В процесі генерації управлінських рішень можна застосовувати класичні моделі кіберзахисту, такі як «Піраміда болю», «Діамант», «MITRE ATT&CK», концепція «глибинного захисту». Реалізація вказаних рішень має відбуватися в межах циклу управління PDCA (Plan-Do-Check-Act), що складається з таких етапів, як «Планування», «Виконання», «Контроль» і «Корекція» і спрямований на постійне поліпшення безпеки організації з використанням об’єктивно вимірюваних індикаторів. Крім того, формування методичних підходів до управління захистом об’єктів критичної інфраструктури від кіберзагроз передбачає використання відповідного математичного апарату, зокрема, для формалізації управлінських рішень щодо розподілу ресурсів.

РОЗДІЛ 2. АНАЛІЗ УПРАВЛІНСЬКИХ АСПЕКТІВ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ВІД КІБЕРЗАГРОЗ

2.1. Управлінські альтернативи організації кіберзахисту критичної інфраструктури в умовах наявних нормативних та технологічних обмежень

Побудова ефективної системи управління кіберзахистом критичної інфраструктури України охоплює широкий спектр нормативно-правових, організаційних, технологічних і процедурних аспектів. На державному рівні з метою превенції та успішної протидії кіберзагрозам здійснюється нормотворча діяльність, а також вносяться зміни в чинне законодавство, наприклад, для виокремлення об’єктів інфраструктури, які є критично важливими.

Ключовим показником усвідомлення на державному рівні важливості захисту критичної інфраструктури, зокрема й від кіберзагроз, стало внесення змін до Закону України «Про національну безпеку України». Зокрема, 21.06. 2018 р., частина 4 статті 3 вищезгаданого Закону була викладена в такій редакції: «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [76], порівняно із попередньою наведена норма була доповнена додатковим об’єктом державної політики у сфері національної безпеки - безпека критичної інфраструктури.

Не менш важливим чинником стало висвітлення проблем забезпечення кібербезпеки критичної інфраструктури у прийнятій в 2016 році «Стратегії кібербезпеки України». Зокрема, серед умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, одним із засобів визначено: забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога до захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме

негативний вплив на стан національної безпеки і оборони України (які безпосередньо складають критичну інформаційну інфраструктуру) [90].

Зі свого боку, серед можливих кіберзагроз виокремлено ті, що впливають на критичну інфраструктуру, а саме: «сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури» [90].

Важливим також було виділення чинників, пов'язаних з критичною інфраструктурою, які спричиняють кіберзагрози:

– недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога до захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів [90].

Чинна «Стратегія кібербезпеки України» була затверджена 26 серпня 2021 року (рис. 2.1), і в ній, зокрема, зазначається, що кіберпростір разом з іншими фізичними просторами потрібно розглядати в якості можливих театрів воєнних дій.

В межах вказаної Стратегії розбудова національної системи кібербезпеки ґрунтується на принципах стримування, кіберстійкості та взаємодії з акцентом на посилення спроможності до протидії агресії, швидкого відновлення інфраструктури та координації між державними органами, приватним сектором і міжнародними партнерами. Пріоритети включають захист суверенітету, прав громадян та євроатлантичну інтеграцію, з визначенням стратегічних цілей, таких як створення кібервійськ у складі Міністерства оборони, посилення протидії

кібертероризму через контррозвідувальні заходи та розвиток асиметричних інструментів стримування, включно з санкціями та дипломатією.

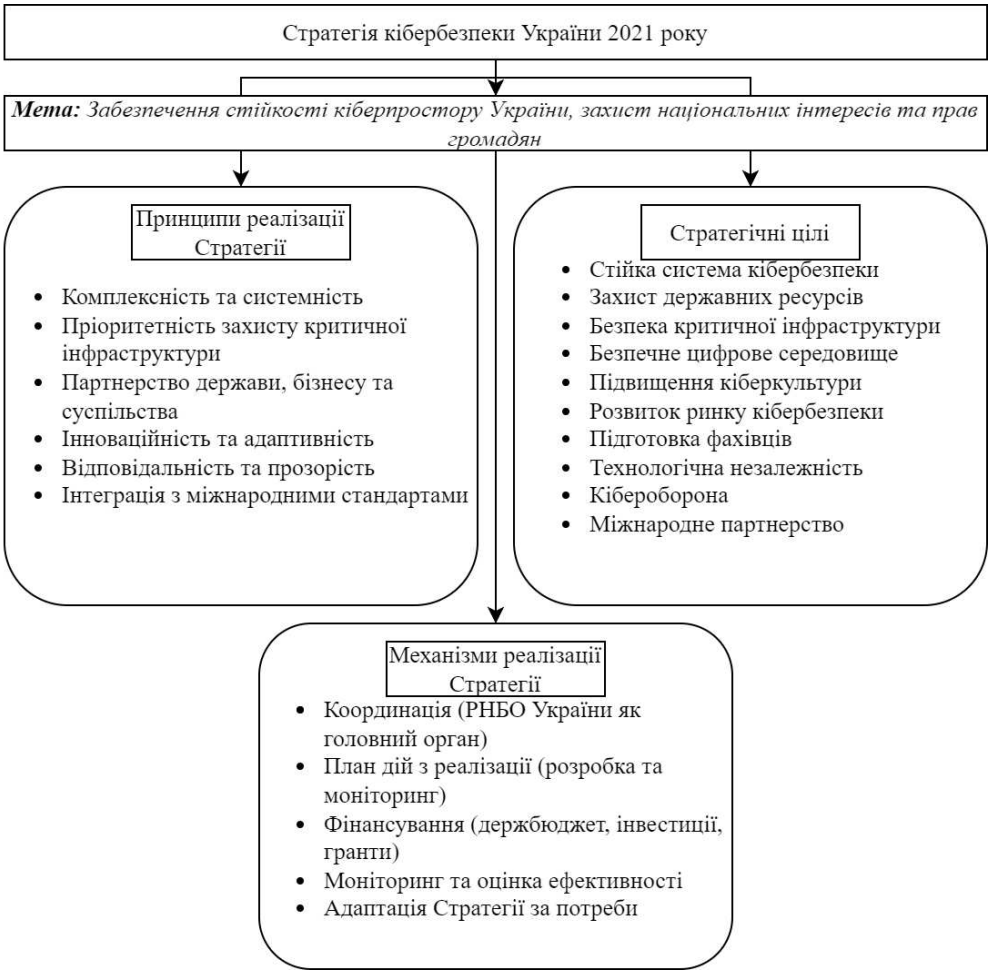

Рис. 2.1. Основні складові чинної «Стратегії кібербезпеки України» *(складено за [76, 90])*

Так, захист об’єктів критичної інфраструктури є складовою частиною цілей, що формують потенціал як стримування, так і кіберстійкості.

У межах розбудови потенціалу стримування особливої ваги набуває стратегічна ціль С.2, що передбачає мінімізацію загроз розвідувально-підривної діяльності та кібертероризму. Реалізація цієї цілі в Україні здійснюватиметься через комплекс заходів, а саме:

– впровадження загальнодержавної системи моніторингу та протидії кібершпигунству щодо критичної інформаційної інфраструктури;

– розширення практики «стрес-тестування» (негласних перевірок) захищеності стратегічних об'єктів від кіберінцидентів;

– автоматизацію процесів ідентифікації та блокування кібератак у реальному часі безпосередньо в державних ІТ-системах [91].

Реалізація стратегічного вектору набуття кіберстійкості (К) безпосередньо залежить від успішного виконання цілі К.1, що полягає у забезпеченні належної національної кіберготовності та розбудові надійного кіберзахисту. Досягнення цього завдання Україна вбачає у межах інклюзивної взаємодії державних структур із приватним сектором, науковими колами та громадськістю. Ключовим інструментом такої політики є розробка та впровадження Національного плану реагування на надзвичайні ситуації в кіберпросторі, який має чітко регламентувати алгоритми відбиття атак на критичну інфраструктуру та процедури подальшої регенерації систем. Паралельно з цим передбачається перехід до ризик-орієнтованої моделі захисту державних ресурсів, що супроводжуватиметься формуванням та оновленням реєстру об’єктів критичної інформаційної інфраструктури та постійною актуалізацією вимог безпеки відповідно до міжнародних стандартів. Важливим аспектом посилення стійкості є запровадження безперервного моніторингу вразливостей, розгортання систем аудиту інформаційної безпеки, а також пріоритетний розвиток вітчизняних технологій технічного і криптографічного захисту, що має забезпечити технологічну незалежність і надійність цифрового контуру держав [91].

В процесі реалізації Стратегії формується підґрунтя для генерації управлінських рішень не тільки на державному рівні, а й у межах окремих об’єктів критичної інфраструктури. Зокрема, менеджери можуть застосовувати цикл PDCA для інтеграції стратегічних цілей таким чином.

1. Plan – проведенні оцінки ризиків (згідно з цілями С.2 і К.1);
2. Do – розподілення ресурсів на навчання персоналу та впровадження IDS/IPS;
3. Check – моніторинг KPI;
4. Act – коригування плану на основі аудиту.

Орієнтація на такий цикл дозволяє перейти від реактивного управління до проактивного, зменшуючи витрати на відновлення після атак. Управлінською альтернативою може бути гібридна модель, де державні стратегії поєднуються з приватними ініціативами [53]. При цьому ефективність реалізації Стратегії визначається у проведених у встановленому порядку оглядах стану, зокрема, кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури [91].

Законодавчий базис управління захистом критичної інфраструктури від кіберзагроз включає низку документів, наведених в Додатку В. Так, Закон України «Про критичну інфраструктуру» визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури і є складовою частиною законодавства у сфері національної безпеки. Він регулює загальний порядок віднесення об'єктів до критичної інфраструктури, зокрема, визначає сектори критичної інфраструктури, категоризацію, реєстр та паспортизацію об'єктів критичної інфраструктури, а також містить значний перелік термінів, що стосуються критичної інфраструктури, закріплює основні засади державної політики у сфері захисту критичної інфраструктури. У Законі визначено суб'єктів національної системи захисту критичної інфраструктури, встановлено режими функціонування національної системи захисту критичної інфраструктури, визначено повноваження уповноваженого органу у сфері захисту критичної інфраструктури, закріплено завдання, права та обов'язки операторів критичної інфраструктури [75].

Прийняття вказаного Закону створює перспективи для децентралізації управління, адже оператори критичних об'єктів зможуть самостійно розробляти паспорти безпеки, але координувати цей процес із секторальними органами за матрицею RACI (Responsible-Accountable-Consulted-Informed) (табл. 2.1).

Роль Responsible (R) передбачає працівника або команду, які безпосередньо відповідають за виконання конкретної частини роботи. Роль Accountable (A) належить керівнику або установі, які несуть повну

відповідальність за досягнення поставлених цілей у визначені терміни, в рамках виділеного бюджету та з високим рівнем якості [5].

Таблиця 2.1

Структура моделі управління за матрицею RACI

Завдання	Оператор критичної інфраструктури	Секторальний орган	Національний координаційний центр кібербезпеки	CERT-UA / СБУ	Керівництво об'єкта (менеджмент)
Ідентифікація та категоризація об’єктів критичної інфраструктури	R	A	C	I	R
Розробка паспортів безпеки об’єктів	R	A	C	I	A
Моніторинг рівня безпеки об’єктів	R	C	A	R	R
Реагування на кіберінциденти	R	I	C	A	R
Аудит та оцінка ризиків	R	C	A	I	A
Впровадження міжнародних стандартів (ISO, NIST)	R	C	I	C	A

Джерело*: розроблено автором за [5]*

Consulted (C) відповідає консультанту, який разом із відповідальними особами бере участь у керуванні, але, насамперед, фокусується на стратегічних питаннях, і цю роль зазвичай виконують менеджери вищого рівня. Informed (I) позначає інформованого спостерігача, який діє як адміністратор, займаючись організацією документів [5]. Зазначена матриця відповідальності є ефективним методом при визначенні ключових напрямів діяльності та критеріїв прийняття рішень у ситуаціях непорозумінь, дозволяючи виносити розбіжності на колективне обговорення для спільного вирішення. Крім того, вона допомагає уникнути дублювання функцій, а в разі суперечок керівник може спиратися на

призначену відповідальну особу, яка контролює послідовність процесу, де виникли проблеми.

Таким чином, організація управління за матрицею RACI дозволяє зменшити бюрократію, але вимагає налагодження системи контролю та відповідної мотивації з боку персоналу. Управлінською альтернативою при цьому виступає централізований підхід, коли Національний координаційний центр кібербезпеки встановлює уніфіковані KPI, що полегшує контроль, але підвищує витрати на встановлення відповідності.

Далі слід згадати Постанову КМУ «Деякі питання об’єктів критичної інфраструктури», яка містить порядок віднесення об’єктів до критичної інфраструктури, визначає механізм віднесення об’єктів до критичної інфраструктури та їхньої категоризації, а також додатки до переліку секторів критичної інфраструктури [28]. У зазначеній Постанові наведена і, власне, методика категоризації об’єктів критичної інфраструктури, яка використовувалася у проведеному дослідженні.

Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури» визначає механізм проведення моніторингу рівня безпеки об’єктів критичної інфраструктури, зокрема його періодичність. Мета проведення моніторингу полягає у встановленні відповідності стану захищеності об’єкта критичної інфраструктури вимогам законодавства, достовірності інформації, наданої визначеним суб’єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об’єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури [73].

І, нарешті, у Постанові КМУ «Деякі питання паспортизації об’єктів критичної інфраструктури» сформовано вимоги до розроблення оператором критичної інфраструктури паспорта безпеки на об’єкт критичної інфраструктури та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури [28].

Крім законодавчого базису, важливим аспектом при побудові системи управління кіберзахистом об’єктів критичної інфраструктури є впровадження міжнародних стандартів, таких як ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework [153, 154, 202]. Зазначені стандарти дозволяють, насамперед, структурувати процеси ідентифікації, оцінки та мінімізації ризиків, сприяючи формуванню стійких систем менеджменту, адаптованих до динамічного середовища кіберзагроз.

Так, ISO/IEC 27001 регламентує вимоги до створення й підтримки СУІБ, забезпечуючи чітку структуру для розробки політик, ідентифікації ризиків, контролю доступу, шифрування інформації та забезпечення безпеки мереж [153]. Зі свого боку, ISO/IEC 27002 доповнює цей стандарт практичними рекомендаціями до реалізації конкретних заходів захисту [154]. В управлінському контексті стандарти ISO/IEC 27001 та NIST Cybersecurity Framework передбачають наявність альтернатив для моделювання процесів. Так, менеджмент може обрати ітеративний підхід (Agile-менеджмент) для впровадження, де цикли PDCA адаптуються до змін загроз (наприклад, щоквартальний аудит ризиків). Зазначений підхід контрастує з водоспадною моделлю, де впровадження стандартів відбувається лінійно, але з вищим ризиком старіння.

На практиці наведені стандарти регламентують увесь циклічний процес планування, впровадження, моніторингу та вдосконалення, який інтегрується менеджментом в загальну стратегію об’єктів критичної інфраструктури. Ба більше, вони є основою для застосування ризикоорієнтованого підходу, адже на етапі планування проводиться аналіз ризиків, що дозволяє керівництву визначити пріоритети інвестицій у захист, на етапі впровадження формуються політики та процедури, які забезпечують координацію між підрозділами (при цьому відбувається фокусування на заходах, що мають найбільший вплив на зниження вразливостей), а моніторинг передбачає регулярні аудити, що сприяють оперативному реагуванню на загрози.

Стандарт ISO 31000 надає універсальний фреймворк для інтеграції ризик-менеджменту на усіх управлінських рівнях. Він акцентує увагу на таких принципах, як інтеграція, структурованість та інклюзивність і дозволяє адаптувати управлінські процеси до викликів кібербезпеки. Ризики оцінюються в контексті організаційних цілей, що сприяє прийняттю рішень на основі сценарного аналізу. Сам стандарт успішно інтегрується з іншими, наприклад, з ISO/IEC 27001, для створення єдиної системи, де управлінські рішення враховують не лише технічні, але й економічні та соціальні аспекти ризиків, що посилює стратегічну орієнтацію, дозволяючи керівництву прогнозувати та мінімізувати потенційні втрати.

NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США, передбачає циклічну модель управління кібербезпекою. Цей фреймворк базується на п’яти функціях: ідентифікація, захист, виявлення, реагування та відновлення – і дозволяє бізнес-структурам не лише будувати надійний кіберзахист, але й адаптувати його до конкретних загроз, особливостей інфраструктури та організаційного контексту [202]. З погляду управлінських рішень NIS2 є своєрідним регуляторним каркасом, адже вимагає від керівництва об’єктів критичної інфраструктури впровадження політик ризик-менеджменту, включаючи оцінку постачальників та регулярні аудити, що інтегруються в стратегічне планування.

Інтеграція вищевказаних стандартів у систему управління дозволяє трансформувати їх з переважно інформаційних джерел у повноцінну структурну базу для кіберризик-менеджменту. Вони забезпечують узгодженість рішень на всіх рівнях – від стратегічного планування до операційного виконання, сприяючи формуванню культури безпеки та оптимізації ресурсів.

Що ж до технологічної складової, насамперед, прийняття управлінських рішень щодо застосування тих чи інших управлінських інструментів відбувається в межах підходів Zero Trust Architecture, Defense-in-Depth та Cyber Threat Intelligence [193, 173, 108].

Zero Trust – це концепція безпеки, що ґрунтується на принципі «нікому не довіряй, все перевіряй». На відміну від традиційних моделей, які надають довіру користувачам і пристроям, що знаходяться всередині мережі, Zero Trust передбачає, що кожен користувач, пристрій та застосунок, незалежно від того, де він знаходиться – всередині чи ззовні периметра мережі – має бути верифікований перед тим, як йому буде надано доступ [193]. При впровадженні Zero Trust також виникає управлінська альтернатива: застосування гібридного підходу (поетапне впровадження для ключових секторів) або повна трансформація (для високоризикових об'єктів).

Defense-in-Depth – це стратегія безпеки, що використовує багатошаровий підхід для захисту даних та систем (мережевий, системний, прикладний, фізичний). Ідея полягає в тому, щоб, навіть якщо зловмисник подолає один рівень захисту, інші шари зможуть його стримати, що спрощує організацію системи управління [173].

Cyber Threat Intelligence (CTI) – це процес збору, аналізу та надання даних про поточні та потенційні кіберзагрози. Мета CTI – надати повну, своєчасну та достовірну інформацію, яка дозволяє приймати обґрунтовані управлінські рішення для проактивного захисту [108].

Технологічним підґрунтям системи моніторингу та виявлення атак є системи виявлення та запобігання вторгнень (IDS/IPS). IDS (Intrusion Detection System) діє як цифровий страж, який постійно спостерігає за мережевим трафіком. Коли він виявляє щось потенційно шкідливе, він реєструє подію та надсилає сповіщення адміністратору безпеки. Проте він не вживає жодних дій, щоб зупинити загрозу. Його роль суто пасивна: виявити та повідомити. IPS (Intrusion Prevention System) не лише виявляє шкідливу активність, але й вживає негайних, автоматизованих заходів для її блокування або запобігання в реальному часі [113].

Для централізованого збору логів та аналізу використовують SIEM (Security Information and Event Management) – систему, яка поєднує в собі функції SIM (Security Information Management) та SEM (Security Event Management) для

забезпечення централізованого управління безпекою. Вона збирає, аналізує та корелює дані з різних джерел у режимі реального часу, допомагаючи ефективно виявляти та реагувати на загрози [143].

Важливу роль при забезпеченні безпеки критичної інформаційної інфраструктури становлять криптографічні методи. Вони визначають рівень захищеності каналів комунікації, стійкість до атак з боку високотехнологічних противників та здатність систем протистояти глобальним загрозам кіберпростору. У поєднанні зі стеганографічними механізмами криптографія утворює фундаментальний каркас сучасних засобів кіберзахисту, здатних забезпечити стратегічну стійкість державних і корпоративних інформаційних ресурсів.

Сучасні дослідження дозволяють ефективно об’єднати криптографію та стеганографію в єдиний захисний механізм. Для цього зі сторони стеганографії розроблена концепція кодового управління [165], яка стала основою нових високоефективних методів прихованого вбудовування інформації. Сутність кодового управління полягає в тому, що процес прихованого вбудовування не відбувається «хаотично», як у класичних методах, а строго регламентується за допомогою спеціальних кодових слів. Ці кодові слова визначають, у які позиції, з якою інтенсивністю та за якими законами вбудовується додаткова інформація. Таким чином, вбудовування набуває керованого, прогнозованого і відтворюваного характеру.

Математичною основою кодового управління стали функції Уолша – ортогональні функції, які задають унікальні шаблони для розподілу інформації по контейнеру.

Кожне кодове слово на основі функцій Уолша дозволяє розосереджувати енергію прихованого сигналу так, щоб він був майже невидимим, але водночас легко відновлюваним у процесі декодування. Завдяки ортогональності зазначених функцій можливо організувати множинний доступ – коли кілька користувачів чи кілька потоків інформації одночасно приховано передаються в одному контейнері без взаємних завад [165, 192].

Серед технологічних досягнень останніх років слід звернути увагу на зростання функціональних можливостей інструментів штучного інтелекту (ШІ), які дедалі активніше інтегруються в процеси забезпечення кібербезпеки, сприяючи підвищенню ефективності ідентифікації загроз, підвищенню якості аналізу даних та автоматизації засобів захисту (табл. 2.2).

Таблиця 2.2

Етапи розвитку ШІ в кібербезпеці

Етап	Характеристика	Технології / Особливості	Роль в управлінні кіберзахистом
Початковий етап (до 2000-х рр.)	Основна увага на ручному налаштуванні правил, обмежена реакція на нові загрози.	Експертні системи, сигнатурний аналіз, евристичні методи	Виявлення шаблонних атак (наприклад, DoS), контроль доступу до SCADA-систем. Висока залежність від людського чинника.
Машинне навчання (2000–2010 рр.)	Системи починають аналізувати великі масиви даних та самостійно вчитися.	Decision Trees, SVM, прості нейронні мережі	Оптимізація аналізу логів, автоматичне виявлення аномалій у роботі мережевих елементів. Початок впровадження IDS/IPS з машинним навчанням.
Глибоке навчання (2010–2020 рр.)	Зростання потужності аналізу, детектування складних патернів і атак у реальному часі.	CNN, RNN, LSTM, автоенкодери	Виявлення zero-day атак у промислових мережах (ICS), аналіз трафіку між підсистемами, визначення поведінкових відхилень.
Генеративний ШІ (з 2020-х рр.)	ШІ не лише аналізує, а й передбачає загрози, генерує сценарії атак і захисту.	LLM (GPT, Claude), мультиагентні системи, предиктивна аналітика	Створення динамічних стратегій реагування на атаки, імітація вторгнень (red teaming), автономний моніторинг і захист в умовах гібридної війни.

Джерело: *складено автором за [113, 143, 165, 192, 102, 111, 142]*

Однією з найбільш вагомих переваг використання ШІ є його здатність до високоточної ідентифікації потенційних атак на початкових етапах їхньої реалізації. На відміну від традиційних підходів, які передбачають переважно фільтрацію мережевого трафіку або блокування вже відомого зловмисного програмного забезпечення, алгоритми машинного навчання дозволяють здійснювати глибокий аналіз поведінкових аномалій у мережі. Це, зі свого боку,

дає змогу виявляти нові та складні типи атак, які раніше не зустрічалися в системі. ШІ-орієнтовані системи можуть суттєво оптимізувати процес реагування на інциденти. Зокрема, алгоритми машинного навчання здатні реалізовувати заходи з протидії загрозам в автономному режимі. Мова йде, зокрема, про відключення доступу до мережі, ізоляцію уражених сегментів інфраструктури чи блокування підозрілого трафіку [1]. Такий рівень автоматизації значно підвищує загальну ефективність системи кіберзахисту, що є критично важливим в умовах, коли кібератаки розгортаються з високою динамікою – у межах кількох хвилин або навіть секунд. Крім того, сучасний фокус управління безпекою зміщується від суто захисних заходів до концепції кіберстійкості (cyber resilience), яка передбачає здатність не лише запобігати атакам, але й швидко відновлюватися після них із мінімальними втратами для бізнес-процесів. Вона вимагає тісної інтеграції планів безперервності бізнесу (BCP) та планів відновлення після катастроф (DRP) [155].

Таким чином, управління кіберзахистом критичної інфраструктури ґрунтується на комплексності (поєднання профілактики, моніторингу та реагування) та гнучкості (адаптації до нових загроз) і передбачає використання низки інструментів (рис. 2.2).

Рис. 2.2. Основні напрями та інструменти управління кіберзахистом *(складено за [11, 6, 92, 41])*

Водночас ефективність кіберзахисту залежить не тільки від технологічного підґрунтя, а й від людського фактору та культурних практик безпеки, що обумовлюють здатність швидко відновлювати працездатність після атак і мінімізувати їхній негативний вплив. І ці питання знаходяться вже виключно в компетенції менеджменту. Крім того, у перспективі розвиток кіберстійкості критичної інфраструктури буде визначатися не тільки якістю технологічних інновацій, а й їхньою привабливістю для кінцевих споживачів в ринкових умовах.

2.2. Аналіз впливу кон'юнктури ринку продуктів та послуг кібербезпеки на управління захистом критичної інфраструктури від кіберзагроз

В останні роки стрімке зростання кіберзагроз, поява нових технологій захисту, а також посилення регуляторних вимог створили умови для виникнення потреб у сучасних та ефективних рішеннях на усіх рівнях: від окремих фізичних осіб до держави в цілому. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» кібербезпека ідентифікується як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [77]. Однак, окрім домінуючої захисної ролі, кібербезпека у вигляді відповідних продуктів та послуг є і об'єктом купівлі-продажу, елементом ринкових відносин та відповідних кон'юнктурних досліджень. Тож і питання ефективного управління кіберзахистом, опираються на наявність та доступність на ринку відповідних безпекових рішень.

Під кон'юнктурою ринку в проведеному дослідженні розуміється або стан ринку, або економічна ситуація на ньому, яка характеризується співвідношенням

попиту і пропозиції, ринковою активністю суб’єктів, динамікою цін, обсягами продажів, рухом процентних ставок, валютного курсу, заробітної плати тощо [78]

Звісно, в кон’юнктурних дослідженнях розглядаються лише ті продукти та послуги кібербезпеки, які можуть бути об’єктом купівлі-продажу, тому до аналізу не потрапили, наприклад, «закриті» військові розробки. З огляду на ринкову специфіку продукти кібербезпеки включають програмне забезпечення, наприклад антивіруси чи системи виявлення вторгнень, а також апаратні рішення, такі як захищені сервери чи шифрувальні пристрої. В той же час як послуги охоплюють інтеграцію та адаптацію готових продуктів під потреби замовника, консультації з оцінки ризиків, аудит безпеки, тестування на проникнення, реагування на кіберінциденти тощо. Інколи,в управлінських дослідженнях застосовується ще й термін «кіберрішення» – продукти або послуги, адаптовані до унікальних вимог організацій з урахуванням їхнього ландшафту ризиків і стратегій безпеки [64]. Саме кон’юнктура визначає їхню комерційну цінність, а також впливає на специфіку цільової аудиторії, економічну доцільність комерціалізації та подальшого масштабування, вибір моменту та способу виходу на ринок тощо.

Глобальний ринок продуктів та послуг кібербезпеки демонструє стійке зростання, зумовлене збільшенням кількості та складності кібератак (рис. 2.3). Ще у 2020 році він оцінювався у 122 млрд дол., що вже тоді підкреслювало значущість цифрової безпеки в умовах посилення кіберзагроз і готовність бізнес-структур витрачати на неї гроші. У 2021 році ринок збільшився до 140 млрд дол., а темпи зростання склали майже 15 %, що відображає активізацію інвестицій саме у кіберзахист на тлі хвилі масових атак з одночасною масштабною цифровізацією бізнесу та переходом на роботу у віддаленому форматі [134, 132, 131].

У 2022 році ринок продовжив нарощувати обсяги, досягнувши 150 млрд дол., однак темп приросту знизився до 7,1 %, що можна пояснити певною стабілізацією після стрімкого зростання попереднього року та частковим

насиченням окремих сегментів. Ситуація кардинально змінилася у 2023 році, коли глобальний ринок кібербезпеки зріс до 219 млрд дол. США, продемонструвавши рекордний стрибок у 46 % [134, 132, 131].

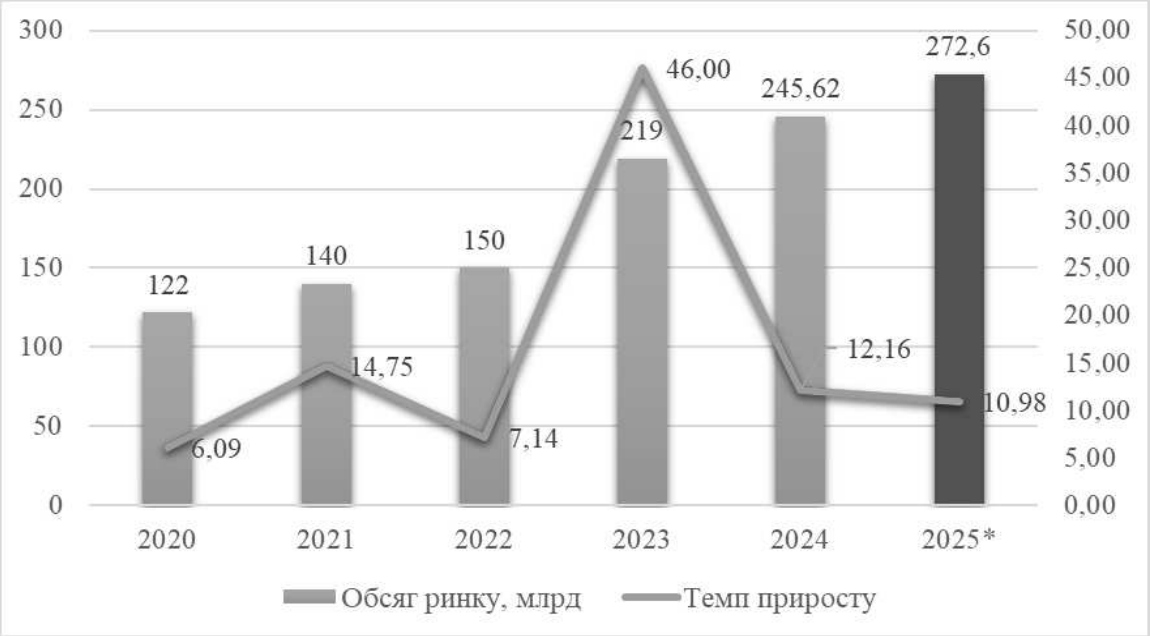

Рис. 2.3. Динаміку обсягу ринку продуктів та послуг кібербезпеки у світі, 2020-2025 рр., млрд. дол. *(складено за [134, 132, 131])*

Така динаміка пояснюється поєднанням кількох чинників: стрімким поширенням хмарних технологій, масштабним впровадженням IoT-рішень, підвищеною увагою держав та корпорацій до захисту критичної інфраструктури на фоні геополітичної нестабільності, зростанням загального рівня кіберзлочинності [134, 132, 131].

У 2024 році ринок досягнув 245,6 млрд дол., зберігаючи високу динаміку зростання на рівні понад 12 %. Можна стверджувати, що інвестиції в захист інформації стають невід’ємною частиною стратегій розвитку як на рівні бізнес-структур, так і для держави в цілому. Прогноз на 2025 рік із показником 272,6 млрд дол. та очікуваним приростом близько 11 % підтверджує, що ринок переходить у фазу стабільного зростання, уникаючи різких коливань, але водночас продовжуючи розширюватися під впливом технологічних інновацій,

розвитку штучного інтелекту у сфері захисту даних та зростання вимог регуляторів [134, 132, 131].

Міжнародна структура ринку продуктів і послуг кібербезпеки у 2024 році демонструє чіткий регіональний розподіл (рис. 2.4), що відображає рівень цифрової зрілості економік, масштаби використання інформаційних технологій та характер загроз у різних частинах світу.

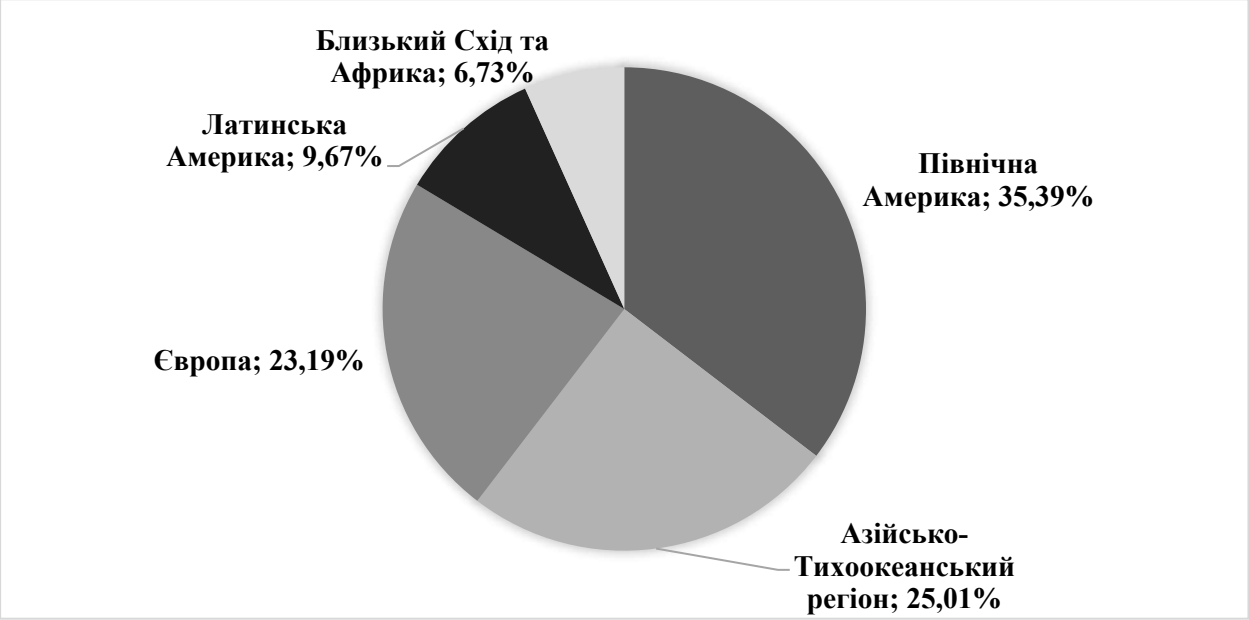

Рис. 2.4. Структура ринку продуктів і послуг кібербезпеки у 2024 р. *(складено за [134, 132, 131])*

Найбільшу частку ринку займає Північна Америка з виручкою 86,94 млрд дол. США, що становить понад 35% світового обсягу. Лідерство регіону зумовлене високим рівнем цифровізації економіки США та Канади, а також зростаючою кількістю кібератак на критичну інфраструктуру, бізнес та урядові установи. У США розвиток кібербезпеки додатково стимулюється нормативними ініціативами на федеральному рівні, такими як Cybersecurity Maturity Model Certification (CMMC), що зобов’язують організації впроваджувати надійні механізми захисту. Це не тільки формує стабільний попит на продукти і послуги кіберзахисту, а й закріплює домінантні позиції регіону на глобальному ринку [134, 132, 131].

Європа займає понад 23% світового ринку з виручкою 56,96 млрд дол. США, що свідчить про її стратегічне значення. Зростання тут пов’язане з активним розвитком IT-інфраструктури, швидким поширенням цифрових технологій та високим рівнем підключених пристроїв, які створюють численні точки доступу для кіберзлочинців [134, 132, 131].

Азійсько-Тихоокеанський регіон із виручкою 61,43 млрд дол. США та часткою понад 25% демонструє найвищі темпи зростання і розглядається як найбільш динамічний сегмент світового ринку. Основними драйверами є масове розгортання дата-центрів, активне впровадження хмарних технологій, поширення IoT-пристроїв і швидке зростання числа спеціалістів у сфері кіберзахисту. У країнах Азії, зокрема в Китаї, Індії та Південній Кореї, активно розробляються власні рішення з вбудованими механізмами виявлення вразливостей, що створює сприятливе середовище для подальшого розвитку ринку [134, 132, 131].

Ринки Латинської Америки та країн Близького Сходу й Африки наразі займають відносно невелику частку – 9,67% та 6,73% відповідно. Проте їхня роль поступово зростає завдяки підвищенню рівня цифровізації державних і комерційних структур та необхідності захисту від дедалі складніших кібератак. Особливу увагу приділяють кіберзахисту фінансового сектору та енергетичної інфраструктури, що створює умови для стабільного зростання в середньостроковій перспективі.

Стосовно подальшого розвитку глобального ринку продуктів та послуг кібербезпеки, очікується, що за результатами 2025 року він досягне 272,6 млрд дол. з річним темпом зростання (CAGR) 12,9%, що збережеться до 2030 року, тоді як український ринок, оцінений у 138 млн дол. у 2024 році, зросте до 209 млн дол. до 2029 року з CAGR 8,5% [64]. Однак, щодо України такий прогноз можна вважати занадто песимістичним (стосовно того, що темп зростання вітчизняного ринку менший, ніж глобального), адже в ньому не враховуються успіхи країни на кіберфронті і той факт, що після закінчення війни деякі з

розробок можуть успішно експортуватися як для військових, так і для цивільних потреб.

Ринок продуктів та послуг кібербезпеки в Україні має перспективи розвитку завдяки низці чинників. По-перше, в Україні існує значний потенціал для розвитку кібербезпеки на локальному рівні, де багато підприємств чи навіть ринкових сегментів ще й досі не забезпечені належним кіберзахистом. Зазначений факт відкриває перспективи для впровадження сучасних технологій захисту даних та кіберінфраструктури. Уряд, комерційні організації, освітні установи та навіть медичні заклади все частіше стають об’єктами кібератак, що створює попит на комплексні рішення у сфері кіберзахисту [65].

По-друге, в України є досвід протистояння кіберзагрозам, отриманий в умовах повномасштабного вторгнення Росії. Починаючи з 2022 року, Україна займає друге місце у світі за кількістю кібератак, поступаючись лише США. Кількість атак на критично важливу інфраструктуру та організації країни зросла майже втричі, що свідчить про безпрецедентний рівень загроз. У таких умовах українські фахівці розробили і впровадили інноваційні підходи до боротьби з хакерськими атаками, включаючи відбиття масових DDoS-атак, захист від шкідливого програмного забезпечення та побудову ефективних систем моніторингу кіберзагроз [3].

Досягненням України у сфері кібербезпеки стало створення та удосконалення національної системи захисту. Синергія зусиль державних органів, приватного сектору та міжнародних партнерів забезпечила розробку передових технологій та підвищила стійкість до зовнішніх загроз. Активно впроваджується і перетворюється на стандарт безпеки принцип нульової довіри, який передбачає сувору перевірку всіх пристроїв і користувачів. Це особливо потрібно державному сектору, адже, наприклад, в 2023 р. 22% кібератак спрямовувалися на урядові органи.

По-третє, середній вік вітчизняних фахівців з кібербезпеки становить приблизно 30 років, що майже на 10 років менше порівняно з аналогічними фахівцями у США. Таке демографічне співвідношення свідчить про домінування

в українському професійному середовищі молодих та адаптивних кадрів, а отже, і про довгостроковий потенціал розвитку галузі.

По-четверте, наявність екосистеми кібербезпеки, яка включає стартапи, професійні спілки, міжнародних донорів, державні ініціативи тощо. Яскравим прикладом є CyberAccelerator – перший в Україні акселератор у сфері кібербезпеки, започаткований у квітні 2021 року в рамках програми USAID Cybersecurity for Critical Infrastructure in Ukraine. Він об'єднує менторів, які надають підтримку стартапам при виході на світовий ринок, а також проєктам, спрямованим на захист критичної інфраструктури [133]. Дуже важливим інструментом у цьому напрямку стало створення Security Operations Center (SOC) Kitsoft. Вказаний Центр кіберзахисту, який фінансується в межах програми EU «Seeds of Bravery» (загальний бюджет складає понад 2,2 млн євро, по 50 тис. на прототип), забезпечує цілодобовий моніторинг, аналіз загроз та швидке реагування на інциденти для державного сектора [164].

Однак варто відзначити, що однією з головних проблем екосистем є конфіденційність та безпека даних. З огляду на величезний обсяг даних, які відстежуються, передаються та обробляються в екосистемі, існує значний ризик витоку даних, неправомірного використання та, звичайно, кібератак з метою отримання цих даних. Крім того, залежність від одного або декількох постачальників платформ може призвести до монопольного контролю над даними, що в довгостроковій перспективі обмежує конкуренцію та інновації, і наявні тенденції також намагаються запобігти цьому за допомогою регуляторних та правових засобів [180].

З погляду історіографії, ринок продуктів та послуг кібербезпеки розвивався в декілька етапів під впливом геополітичних викликів, технологічних проривів та міжнародної співпраці (Додаток Г). До 2014 року ринок розвивався повільно, попит зосереджувався на базових іноземних рішеннях, таких як антивіруси та фаєрволи. Хоча в той час Україна вже була відомою в світі як хаб для ІТ-фахівців, але кібербезпека не мала пріоритетного статусу в державній політиці. Перші значні інциденти, як-от атаки на фінансові системи в 2010–2013

рр., підкреслили вразливість системи, але все одно не призвели до кардинальних змін. Кількісно у цей період ринок оцінювався в 10-20 млн дол. [130].

Переломним моментом для ринку продуктів та послуг кібербезпеки можна вважати 2014 рік, коли анексія Криму та конфлікт на Донбасі відкрили еру гібридної війни, де кіберпростір став полем бою. Це змусило Україну прискорити створення спеціалізованих структур: у 2016 році було ухвалено Національну стратегію кібербезпеки, а CERT-UA (Команда реагування на комп'ютерні надзвичайні події України) посилила свою роль у моніторингу загроз [190]. Ринок почав зростати, в тому числі й з появою локальних стартапів, орієнтованих на захист мереж і даних.

Наступною віхою розвитку ринку став 2017 рік, коли атака NotPetya в Україні паралізувала банківську систему, транспортну логістику та діяльність державних установ. У відповідь уряд посилив законодавство, ввівши обов'язкові аудити безпеки для критичної інфраструктури, а ринок зріс на 11 млн дол. (+28,2%) завдяки інвестиціям від USAID та ЄС [64]. Цей період також стимулював розвиток технологій на основі ШІ для виявлення загроз, оскільки традиційні методи виявилися недостатніми проти складних APT-атак.

З 2018 року еволюція ринку набула динамічного характеру з фокусом на стійкість та інновації. Масові кіберінциденти в 2021 році призвели до створення Національного центру кібербезпеки та посилення співпраці з НАТО. Повномасштабне вторгнення 2022 року стало каталізатором: атаки WhisperGate та AcidRain на початку року змусили Україну активізувати міграцію даних до хмарних платформ і впроваджувати принципи нульової довіри [178, 120]. У 2023–2024 роках кількість фахівців з кібербезпеки продовжувала зростати, а інновації зосередилися на автоматизованих SOC і квантовій криптографії. В 2025-2027 рр. Україна має остаточно перетворитися на потужного експортера продуктів в сфері кібербезпеки [206].

Стосовно кількісних показників обсягів ринку продуктів та послуг кібербезпеки в Україні можна стверджувати про наявну позитивну динаміку як за базисним темпом зростання, так і за ланцюговим (табл. 2.3).

Таблиця 2.3

Динаміка ринку продуктів та послуг кібербезпеки в Україні 2014-2024 рр.

Роки	Обсяг ринку, млн дол.	Темп зростання, коефіцієнти	
		ланцюговий	базисний
2014	13	-	1,000
2015	21	1,62	1,62
2016	32	1,52	2,29
2017	39	1,22	3,0
2018	50	1,28	3,85
2019	64	1,28	4,92
2020	70	1,09	5,38
2021	92	1,31	7,08
2022	105	1,14	8,07
2023	122	1,16	9,38
2024	138	1,13	10,62

Джерело*: складено автором за [64]*

За допомогою методу найменших квадратів можна проаналізувати динаміку обсягу ринку продуктів та послуг кібербезпеки в Україні в 2014-2024 рр. (рис. 2.5). Сутність методу найменших квадратів (МНК) у контексті аналізу часових або просторових рядів полягає в ідентифікації параметрів моделі тренду, яка найбільш адекватно апроксимує тенденцію розвитку досліджуваного явища. Тренд у даному випадку виступає аналітичним вираженням закономірності динаміки процесу. Основним завданням методу є пошук оптимальної моделі, що забезпечує найвищий ступінь відповідності теоретичних даних фактичним спостереженням. Модель вважається оптимальною за умови мінімізації суми квадратів відхилень між емпіричними значеннями та відповідними розрахунковими величинами, отриманими на основі побудованого рівняння тренду.

Як показав аналіз, лінія з найбільшою апроксимацією (наближене вираження будь-яких величин або геометричних/математичних об’єктів через інші, відоміші або простіші величини) – пряма з наступними параметрами: $y = 12{,}491x - 7{,}1273$, та значення $R^2 = 0{,}9821$.

Високий рівень апроксимації є підтвердженням достовірності подальшого прогнозу.

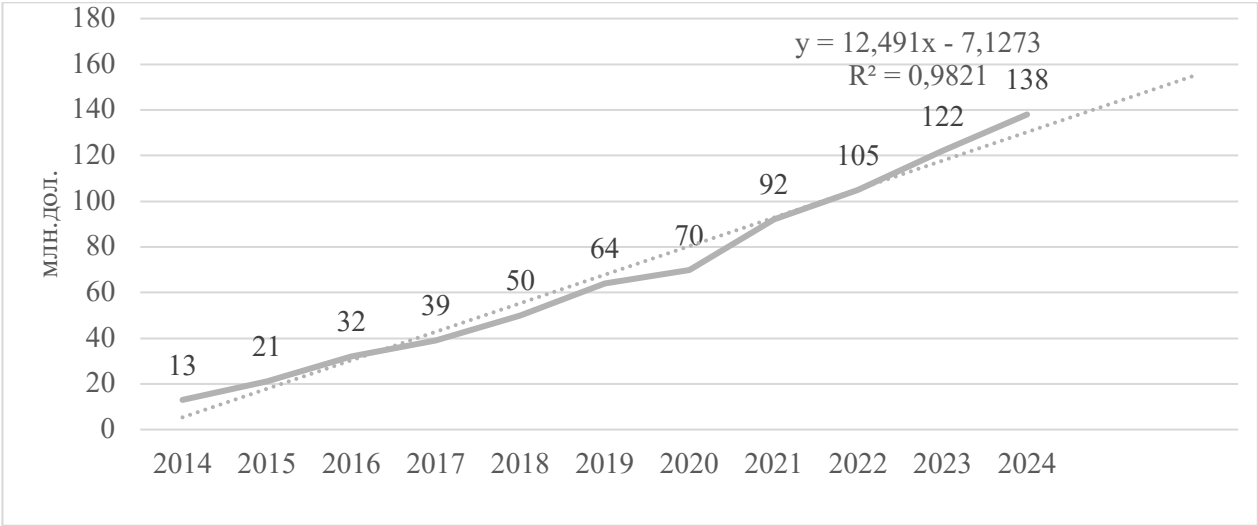

Рис. 2.5. Аналіз динаміки ринку продуктів та послуг кібербезпеки в Україні за 2014-2024 рр. та прогноз на 2025-2027 рр., млн дол. *(складено за [64])*

Кількість історичних рівнів аналізу обсягу ринку продуктів та послуг кібербезпеки дорівнює 11, що дозволяє, виходячи зі значення критерію Кендела (він є мірою рангової кореляції, тобто подібності упорядкування даних, коли вони упорядкуванні за своєю величиною), оцінити прогноз із достатньо високою ймовірністю на наступні 3 роки (табл. 2.4), звісно за умови відсутності тектонічних змін зовнішнього середовища.

Таблиця 2.4

Прогноз ринку продуктів та послуг кібербезпеки в Україні на 2025-2027 рр.

№	Рік	Значення, млн. дол.
1.	2025	142,7647
2.	2026	155,2557
3.	2027	167,7467

Джерело*: розроблено автором*

Тим не менш, вказані близько 2% динаміки становлять деяку циклічність тренду.

Тому для впевненості прогнозу слід використати інший метод оцінки динаміки числового ряду. Методика «Аркуш прогнозу» в «Microsoft Excel» - це функція для створення прогнозів на основі історичних даних за допомогою експоненційного згладжування (алгоритм ETS) (рис. 2.6).

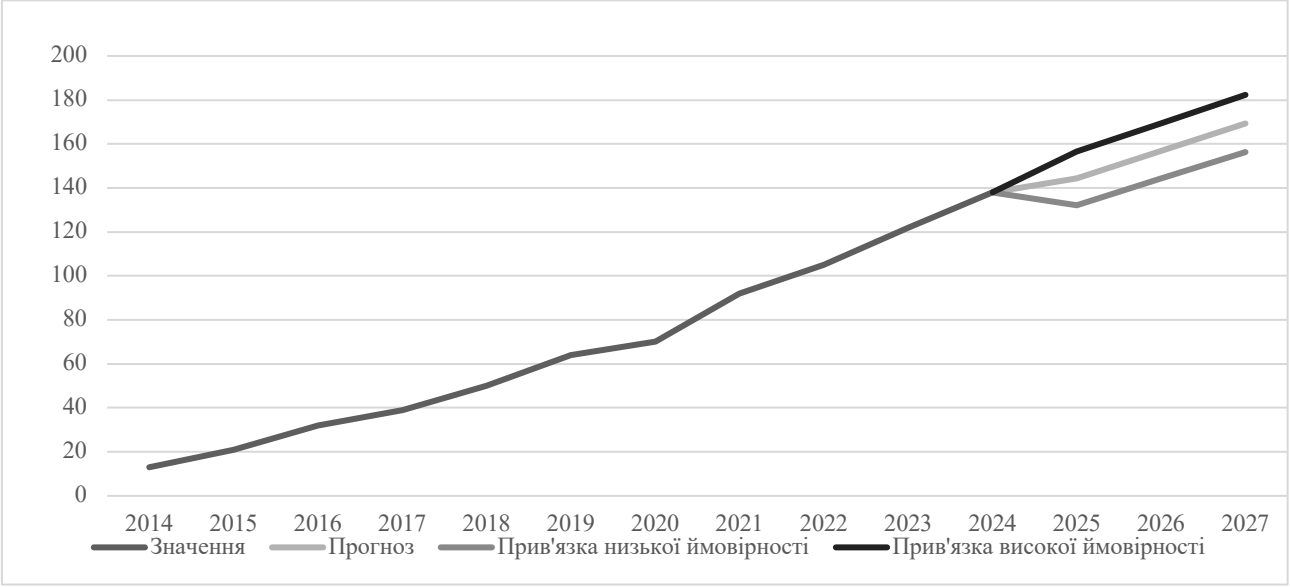

Рис. 2.6. Аналіз динаміки ринку продуктів та послуг кібербезпеки в Україні за 11 років з 2014 по 2024рр.та прогноз на 2025-2027рр. на основі методу згладжування (алгоритм ETS) *(розраховано автором)*

Останнє розглядається як метод математичного перетворення, який застосовується при прогнозуванні часових рядів. При кожній наступній ітерації враховуються всі попередні значення ряду, але ступінь врахування зменшується за експоненційним законом.

Результати розрахунку прогнозу ринку продуктів та послуг кібербезпеки в Україні на 2025-2027рр. на основі методу згладжування складено в таблиці 2.5.

Таблиця 2.5

Розрахунок прогнозу ринку продуктів та послуг кібербезпеки в Україні на 2025-2027рр. на основі методу згладжування (алгоритм ETS)

Тимчасова шкала	Значення	Прогноз	Прив'язка низької ймовірності	Прив'язка високої ймовірності	Статистика	Значення
2014	13				Alpha	0,25
2015	21				Beta	0,00
2016	32				Gamma	0,00
2017	39				MASE	0,48
2018	50				SMAPE	0,04
2019	64				MAE	4,60
2020	70				RMSE	5,29
2021	92					
2022	105					

Продовження таблиці 2.5

Тимчасова шкала	Значення	Прогноз	Прив'язка низької ймовірності	Прив'язка високої ймовірності	Статистика	Значення
2023	122					
2024	138	138	138,00	138,00		
2025		**144,37136**	**132,12**	**156,63**		
2026		**156,83921**	**144,20**	**169,47**		
2027		**169,30705**	**156,30**	**182,31**		

Джерело: *розраховано автором*

Порівняльний аналіз обох методів показує їхній практичний збіг, але згладжування вказує на прискоренні в останні роки тренду. Таким чином, з урахуванням прискорення динаміки в останні воєнні роки, кращим є прогноз подальшого розвитку ринку продуктів та послуг кібербезпеки на основі згладжування.

З погляду функціональної структури, ринок кібербезпеки охоплює продукти та послуги, спрямовані на захист інформаційних систем, мереж, даних і додатків від кібератак, включаючи мережеву безпеку, хмарну безпеку, захист кінцевих точок, безпеку даних і додатків, а також професійні й керовані послуги. За даними на кінець 2024 р., співвідношення між продуктами та послугами кібербезпеки складає 57% проти 43%. Серед окремих сегментів лідерами є мережева безпека (майже 33%) та професійні послуги (більш ніж 31%) (рис. 2.7).

Подібна структура зумовлена низкою факторів. Насамперед, війна спричинила значне зростання частоти та складності кібератак, що спонукало підприємства та організації до швидкого впровадження автоматизованих рішень, таких як шифрування даних і системи автоматизованого виявлення загроз.

Крім того, потреба в негайних рішеннях для протидії кіберзагрозам призвела до зменшення попиту на послуги з розробки індивідуальних систем захисту на користь покупки готових продуктів. Також негативний тиск чинять прямі втрати активів від бойових пошкоджень об’єктів інфраструктури та виробництв, складнощі в отриманні зовнішнього фінансування розвитку бізнесу, відтік кадрів та інвестицій з країни [68]. Загалом дефіцит кваліфікованих

спеціалістів надав поштовх до використання автоматизованих систем, які мінімізують потребу в людському втручанні.

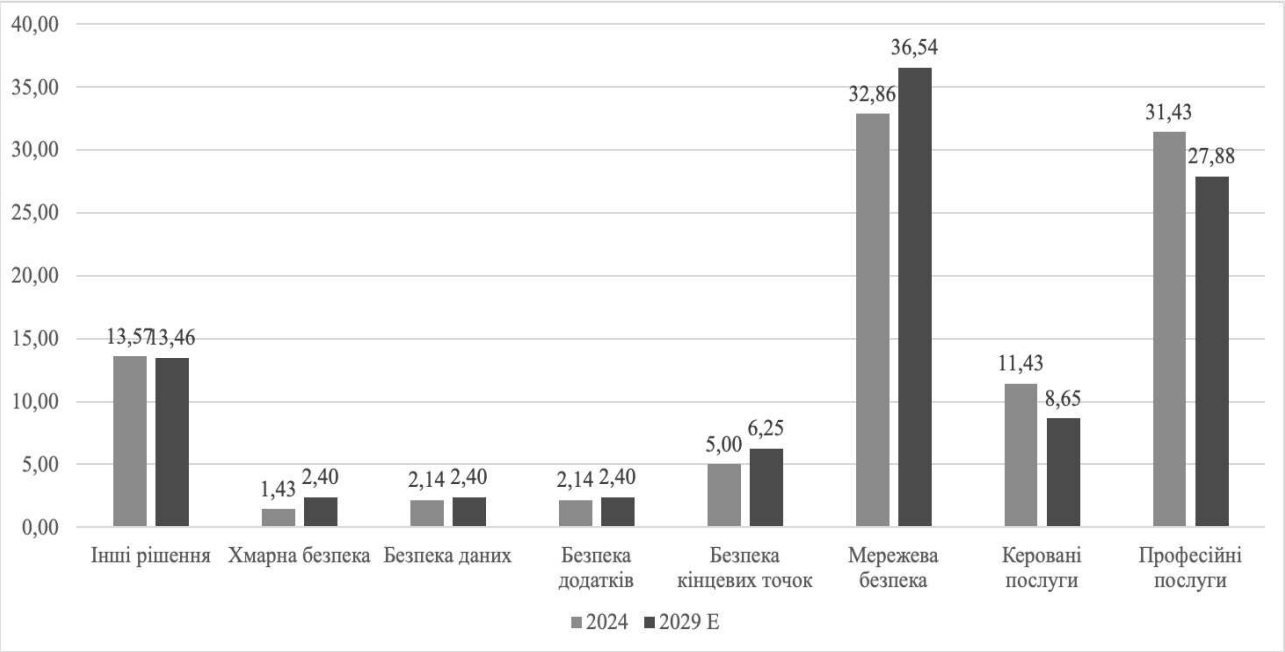

Рис. 2.7. Структура ринку кібербезпеки в Україні за сегментами, %

(складено за [78])

Згідно зі структурним прогнозом до 2029 р. мережева безпека має зберегти лідерство, частка послуг зменшуватиметься, а найбільші темпи зростання очікуються в сегменті хмарної безпеки. Крім того, розвиток ринку продуктів та послуг кібербезпеки значною мірою залежить від адаптації до нових технологічних трендів, які формують глобальні стандарти захисту інформації. Так, у 2025 році ключовими напрямами є автоматизація кіберзахисту, впровадження технологій 5G та використання OSINT для прогнозування загроз. Ці тренди створюють нові можливості для українських розробників, але водночас потребують значних інвестицій [64].

Диференціація споживачів продуктів та послуг кібербезпеки (а в ролі замовників найчастіше є саме управлінський персонал) за масштабами їхньої діяльності дозволяє окреслити ключові сегменти ринку. Основними суб’єктами попиту є представники великого та середнього бізнесу, для яких стан захищеності інформаційно-комунікаційних мереж є критичним чинником

забезпечення операційної стійкості. У цьому сегменті впровадження інноваційних технологій захисту розглядається як інструмент мінімізації стратегічних ризиків, зокрема репутаційних втрат або дестабілізації бізнес-процесів. Натомість сегмент малого підприємництва характеризується низьким рівнем обізнаності щодо кіберзагроз та обмеженими ресурсними можливостями, що створює бар'єри для реалізації повноцінних проєктів із кіберзахисту.

Галузевий аналіз інвестиційної активності у сфері кібербезпеки свідчить про пріоритетність захисту стратегічно важливих секторів економіки. Насамперед, це стосується військово-промислового комплексу, який в умовах воєнного стану вимушений форсовано впроваджувати прогресивні методи протидії атакам. Не менш значущим є фінансово-банківський сектор, де висока концентрація конфіденційної інформації та фінансових активів зумовлює стабільно високі ризики кіберінцидентів. Для установ цієї галузі інвестиції у кібербезпеку є не лише технічною необхідністю, а й фундаментальною умовою збереження довіри клієнтів та дотримання жорстких регуляторних вимог [57]. Окремим стратегічним вектором попиту на рішення у сфері кібербезпеки виступає енергетика. Враховуючи потенційно катастрофічні наслідки дестабілізації енергетичної інфраструктури для національної безпеки, енергетичні компанії спрямовують інвестиції у розбудову інтелектуальних систем моніторингу та превентивного виявлення загроз у реальному часі. Аналогічна залежність від кібертехнологій спостерігається у функціонуванні транспортної інфраструктури, де інтеграція цифрових систем управління вимагає надійних механізмів захисту від втручання, здатних паралізувати логістичні ланцюги. Висока інтенсивність витрат на кіберзахист характерна також для IT-індустрії, зокрема для розробників програмного забезпечення, де безпека кінцевого продукту є фундаментом ринкової репутації та конкурентоспроможності.

Узагальнюючи управлінську мотивацію щодо фінансування заходів із кібербезпеки, доцільно виділити групу критичних ризиків, мінімізація яких є пріоритетом для сучасного менеджменту:

1. Репутаційні та правові ризики, пов’язані з компрометацією конфіденційних даних та порушенням нормативних вимог;

2. Фінансові втрати внаслідок прямого викрадення активів або блокування платіжних систем;

3. Комунікаційні бар'єри, що виникають через недоступність публічних інформаційних ресурсів та сервісів взаємодії з контрагентами;

4. Загрози економічній безпеці, зокрема промислове шпигунство та використання методів недобросовісної конкуренції в цифровому середовищі;

5. Операційні ризики, що полягають у частковому або повному призупиненні ключових бізнес-процесів, що може призвести до втрати ринкових позицій.

Все вищевказане дозволяє сформувати певний «портрет клієнта», в сегменті продуктів та послуг кібербезпеки та заходи управлінського впливу на нього (табл. 2.6).

Таблиця 2.6

Характеристика покупців продуктів та послуг кібербезпеки з точки зору можливості управлінського впливу

Параметр	Опис	Інструменти впливу на рішення про покупку
Індивідуальність запитів	Майже кожний замовник бажає придбати персоніфіковане рішення, наприклад, з урахуванням особливостей власних бізнес-процесів.	Консультації та аудит бізнес-процесів; презентація кейсів аналогічних рішень; модульні рішення з інтеграцією.
Варіативність	На ринку присутня значна кількість готових рішень, а також розробників та інтеграторів, які пропонують власні послуги у сфері кіберзахисту. Отже, клієнт обирає з декількох варіантів, які можуть відрізнятися, навіть концептуально.	Порівняльні таблиці переваг; безкоштовні пілотні проєкти; партнерства з брендами (Cisco, Fortinet тощо).
Технічна обізнаність	Кожне замовлення обов’язково погоджується із технічним відділом або іншими профільними фахівцями.	Вебінари для IT-фахівців; сертифікати (GDPR, ISO 27001); пряма комунікація з IT-командами.

Продовження таблиці 2.6

Параметр	Опис	Інструменти впливу на рішення про покупку
Значні бюджети замовлень та велика середня сума чеку	Основними замовниками є представники великого та середнього бізнесу, діяльність яких залежить від рівня захищеності комп'ютерних та інформаційних мереж.	Демонстрація ROI від захисту; гнучкі моделі оплати (наприклад, SaaS); пріоритетна підтримка.
Прагнення до комплексного захисту	Джерела кіберзагроз можуть бути дуже різними, але замовник зазвичай вимагає рішення, яке захистить від усіх, що призводить до формування системи кіберзахисту суб'єкта підприємництва.	Пакетні рішення (SIEM, EDR, DLP); інтеграція з інфраструктурою; модель Zero Trust.
Бажання швидкого виконання	Здебільшого потенційний замовник розуміє потребу у кібербезпеці після інциденту та оцінки понесених збитків. І негайно бажає отримання надійного кіберзахисту, щоб унеможливити подібні збитки у майбутньому.	Хмарні SaaS-платформи, маркетинг кіберінцидентів; попередньо налаштовані продукти.

Джерело*: складено автором на основі [18]*

Сучасна архітектура пропозиції на ринку продуктів та послуг кібербезпеки передбачає наявність первинної ланки глобальних вендорів апаратного та програмного забезпечення, причому український ринок характеризується високим рівнем інтеграції світових лідерів, таких як Cisco, Fortinet, Mikrotik, McAfee, PaloAlto та FireEye. Водночас спостерігається певний структурний дисбаланс: на фоні домінування рішень із відкритим вихідним кодом (open source) відзначається дефіцит великих вітчизняних розробників із повним циклом операційного управління в Україні. Специфічний сегмент ринку охоплюють розробники рішень для оборонного сектору, чия продукція має закритий характер і не представлена у вільному обігу.

Логістичне та операційне забезпечення трансферу технологій від вендорів до кінцевого споживача здійснюють спеціалізовані компанії-дистриб'ютори, серед яких провідні позиції займають ERC, МУК, Бакотек та Softprom. Подальша кастомізація та адаптація цих технологічних рішень під індивідуальні запити клієнтів реалізується системними інтеграторами. Така категорія є найбільш

масовою за кількістю учасників, проте відзначається значною неоднорідністю за масштабами діяльності та обсягами капіталізації.

Доповнюють ринкову екосистему консалтингові структури, які спеціалізуються на наданні інтелектуальних послуг, зокрема проведенні аудитів ІТ-інфраструктури, тестуванні на проникнення, аналізі програмного коду, забезпеченні комплаєнсу з нормативними вимогами та здійсненні кіберрозвідки. Серед лідерів в цьому сегменті Berezha Security, 10Guards, Advantio, UnderDefense, Імпрувмент Сервіс. Усі перелічені компанії спеціалізуються здебільшого на високорівневих технічних аспектах кібербезпеки, відтак їхня кількість є незначною відносно загальної кількості учасників українського ринку [49].

Окремим специфічним напрямом в сфері послуг кібербезпеки є етичний або «білий» хакінг, тобто знаходження прогалин в системі безпеки замовника для вчасного виправлення помилок.

Задля цього здебільшого використовуються bug-bounty платформи, тобто своєрідні фриланс біржі для «білих» хакерів. Вказані платформи (наприклад, HackerOne та Bugcrowd у США або HackenProof в Україні) допомагають регламентувати процеси, визначити розмір винагород і залучити етичних хакерів з власної бази.

На рисунку 2.8 представлено аналіз ключових виробників та продавців на ринку продуктів та послуг кібербезпеки в Україні за обсягом доходу та кількістю працівників у 2024 році. Дані включають основні групи учасників ринку, серед них розробники, дистриб’ютори та інтегратори, що формують пропозицію на локальному ринку. Вибір саме цих суб’єктів для аналізу зумовлений їхньою провідною роллю у забезпеченні кіберзахисту та розташуванням головного офісу в Україні.

Згідно зі структурою збуту переважна більшість виробників (60-70%) орієнтується на внутрішній ринок, ще приблизно 15-20% поєднують роботу на внутрішньому та зовнішньому ринках з пріоритетом на останній і, нарешті, виключно на зовнішніх споживачів працює не більше 5-10% виробників.

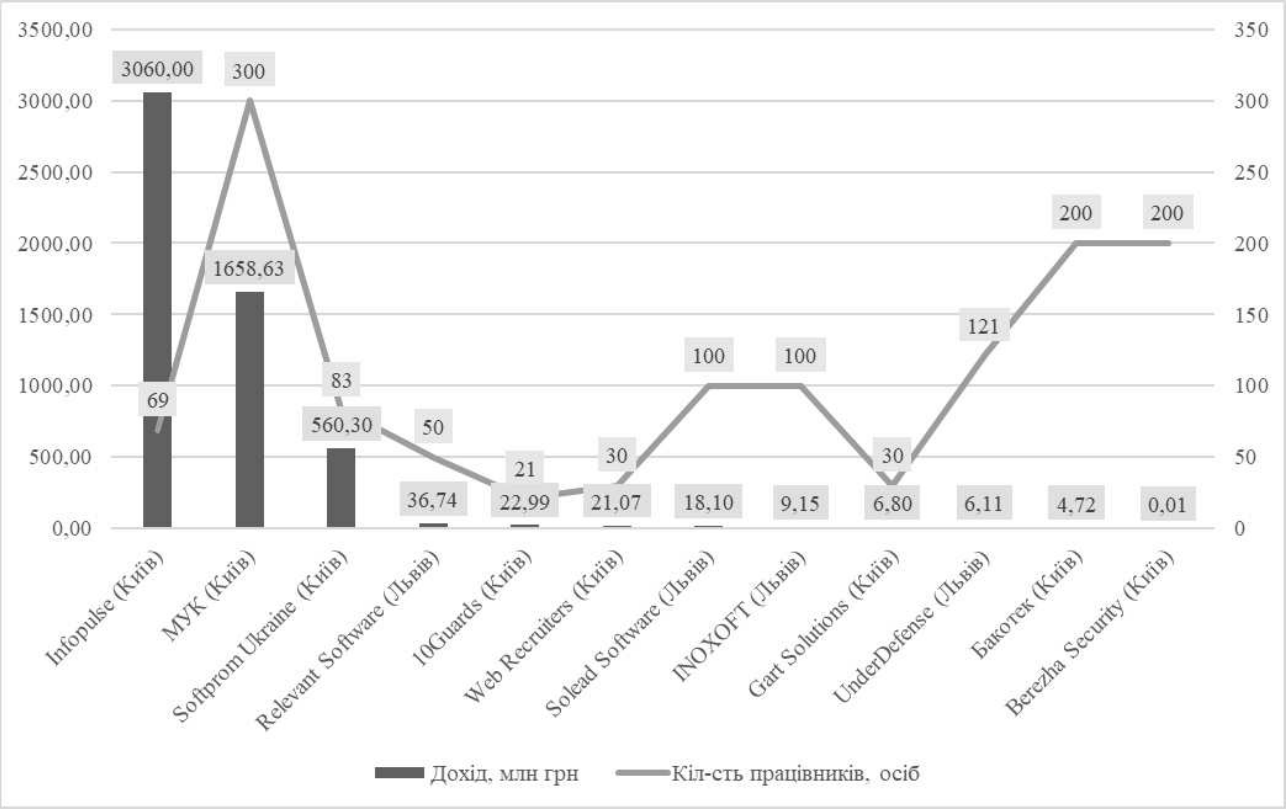

Рис. 2.8. Аналіз виробників та продавців за обсягом доходу та кількості працівників в Україні на 2024 р. *(складено за даними [199, 177])*

З метою узагальнення сильних та слабких сторін суб'єктів підприємництва, що формують пропозицію на ринку продуктів та послуг кібербезпеки, а також можливостей стосовно його подальшого розвитку та потенційних загроз доцільно застосувати метод SWOT-аналізу (табл. 2.7).

Таблиця 2.7

SWOT-аналіз сектору виробництва продуктів та послуг кібербезпеки в Україні

Strengths (Сильні сторони)	Weaknesses (Слабкі сторони)
Досвід протидії кібервійні, що підвищує експертизу в автоматизованих рішеннях. Зростання кількості фахівців з ШІ. Міжнародна фінансова підтримка розробників. Цифровізація державних послуг (63% у 2022 році), що генерує попит. Гнучка цінова політика	Втрата кадрового резерву. Недостатнє фінансування через воєнні ризики. Недостатня увага до маркетингу вітчизняних розробок.

Продовження таблиці 2.7

Opportunities (Можливості)	Threats (Загрози)
Диверсифікація ринку через наративну безпеку та OSINT. Зростання попиту на хмарну безпеку. Інтеграція ШІ для автоматизації реагування. Міжнародні гранти для R&D.	Спад фінансування донорів після 2024 року. Економічна нестабільність, що знижує інвестиції. Посилення кібератак від міжнародних хакерських груп.

Джерело*: складено автором*

З даних таблиці можна дійти висновків, що зростання кількості фахівців у сфері штучного інтелекту та машинного навчання забезпечує потенціал для створення інноваційних продуктів, здатних конкурувати на світовому ринку. Гнучка цінова політика українських компаній також дозволяє ефективно конкурувати з міжнародними гравцями, пропонуючи доступні та якісні продукти.

Проте втрата кадрового резерву через міграцію фахівців за кордон або їх залучення до інших галузей послаблює інноваційний потенціал. Недостатнє фінансування, зумовлене воєнними ризиками, обмежує можливості для масштабування бізнесу та впровадження нових технологій. Крім того, недостатня увага до маркетингової складової безпекових рішень, знижує видимість українських продуктів на міжнародних ринках, що ускладнює залучення клієнтів і партнерів.

Зростаючий попит на хмарну безпеку та автоматизацію реагування на кіберзагрози за допомогою інструментів ШІ створює перспективи для розробки передових рішень. Міжнародні гранти для досліджень і розробок (R&D) надають додаткові ресурси для інновацій, дозволяючи українським суб’єктам підприємництва створювати конкурентоспроможні продукти. Однак сектор стикається із серйозними загрозами. Економічна нестабільність в Україні, спричинена війною, знижує інвестиційну привабливість галузі. Спад фінансування від міжнародних донорів після 2024 року може обмежити ресурси для розвитку. А посилення кібератак з боку міжнародних хакерських груп

вимагає адаптації та створення комплексних рішень, що відповідають світовим стандартам.

Обсяги продажу продуктів та послуг кібербезпеки значною мірою залежать від обраної цінової моделі, яка може варіюватися залежно від потреб клієнта та специфіки бізнесу. Існує кілька основних підходів до ціноутворення, кожен із яких має свої особливості та приклади компаній, що їх використовують.

Модель разової оплати передбачає одноразову інвестицію в розробку та впровадження рішень кібербезпеки. Бюджет залежить від масштабів діяльності замовника, складності організаційної структури, обсягу даних, рівня ризику, бажаного рівня захисту та типу інфраструктури. Наприклад, Symantec (Broadcom) пропонує персональні ліцензії на антивірусне програмне забезпечення та інструменти захисту платежів, де клієнти платять за встановлення, з наявною опцією доплати за подальше оновлення. Geobridge спеціалізується на криптографічному захисті, надаючи одноразові рішення, такі як EMV-чіпи та токенізація, без регулярних платежів. Entrust застосовує цю модель для видачі цифрових сертифікатів, дозволяючи клієнтам самостійно керувати системами після разового впровадження.

Модель підписки базується на регулярних платежах за використання програмного забезпечення чи послуг, таких як Security as a Service (SECaaS). Цей підхід забезпечує постійні оновлення, моніторинг та підтримку. Наприклад, CrowdStrike пропонує хмарний SaaS для захисту endpoint'ів із щомісячною підпискою, що включає автоматичне виявлення загроз. Palo Alto Networks використовує підписку для Prisma Cloud, надаючи захист хмарних середовищ із SIEM-моніторингом. Proofpoint фокусується на захисті email та хмарних застосунків, пропонуючи підписку для боротьби з фішингом та витоками даних.

Гібридна модель поєднує початкові інвестиції з регулярними виплатами за підтримку та оновлення. Вона підходить для розробників, що потребують кастомізації на старті та гнучкості фінансових потоків у майбутньому. Наприклад, Salesforce комбінує разову плату за інтеграцію CRM із підпискою для захисту даних клієнтів. Twilio пропонує гібрид для комунікаційних

платформ із кібербезпекою, де разова оплата за API поєднується з подальшими регулярними виплатами.

Попит на модель «під ключ» підтримується завдяки комплексному підходу, що охоплює оцінку ризиків, розробку, впровадження та підтримку без залучення сторонніх підрядників. За такою схемою Cybersecurity and Privacy Solutions (TCPS) пропонує NIST-сумісні програми для малого та середнього бізнесу, а CyberSecOp надає повний цикл MSSP-послуг, зосереджуючись на персоналізованих планах.

Підсумовуючи проведений аналіз, можна стверджувати про те, що, незважаючи на кількісне зростання обсягів ринку і сприятливі кон'юнктурні тенденції в процесі управління кіберзахистом, керівництво об'єктів критичної інфраструктури все ще не може орієнтуватися виключно на придбання готових безпекових рішень. Адже на ринку наявний дисбаланс, а попит значно перевищує пропозицію, насамперед, через ескалацію кіберзагроз і геополітичні виклики.

Попит стимулюється зростанням кількості кібератак (3 мільйони кіберінцидентів лише в 2024 році) та цифровізацією (наприклад 63% громадян в Україні користуються цифровими державними послуги). Найвищі темпи зростання пропозиції спостерігаються в секторі оборони, що пояснюється прискореним впровадженням технологій в умовах повномасштабного вторгнення.

Водночас пропозиція обмежена, в першу чергу, кадровими ресурсами (лише близько 6500 спеціалістів у 2024 році, за даними LinkedIn). Звісно, вказана ситуація обумовлена здебільшого внутрішніми викликами: багато фахівців виїхало з країни з початком повномасштабного вторгнення, деякі інші доєдналися до ЗСУ. Однак і на глобальному рівні в останні роки попит на фахівців у сфері кібербезпеки перевищує пропозицію. Це створює можливості для зростання ринку, але за умови інвестування в наукову та освітню сфери. Іншим проблемним аспектом є занадто велика залежність від зовнішнього фінансування в умовах його потенційного скорочення.

2.3. Оцінка можливостей мінімізації кіберзагроз критичній інфраструктурі за допомогою управлінських інновацій

В теоретичній частині проведеного дослідження знайшла підтвердження гіпотеза, що сучасні цифрові трансформації потребують відповідної модернізації системи управління, причому, навіть не з погляду її технічного переоснащення, а у контексті впровадження управлінських інновацій, формування нових організаційних структур, трансформації механізмів управління персоналом, збільшення уваги до безпекових питань. При протидії кіберзагрозам особливості управлінського втручання зумовлені, насамперед, тим, що тривалий час кіберзлочинність функціонувала на принципах, дуже схожих з принципами законного бізнесу, який намагається отримати найвищий рівень прибутку.

Відтак ефективно знижувати рівень кіберзагроз, як ключових загроз безпеці, означало систематично знищувати бізнес-модель, за якою в умовах невисокого ризику нескладні для застосування інструменти використовуються для отримання значних прибутків [69].

У вказаній ситуації метою ефективного кіберзахисту було зробити кібератаку невигідною (першочергово у фінансовому аспекті). Задля цього суб’єкти господарювання намагалися не тільки безпосередньо забезпечувати технологічну підтримку системи кібербезпеки, а й проводити систематичну оцінку активів з огляду на їхню вразливість у кіберсередовищі та розмір потенційних збитків. Насамперед, оцінювалися можливі репутаційні втрати, збитки від крадіжки фінансової інформації, персональних даних працівників та клієнтів, блокування роботи серверів, проблем з функціонуванням сайту.

Проте в останні роки використання інформаційних технологій в процесі гібридної війни зумовило виникнення принципово нових кіберзагроз вищого рівня, які спрямовано на національну та міжнародну безпеку. Зокрема, зростає кількість та потужність кібератак, вмотивованих геополітичними інтересами окремих держав, груп та осіб. І при їхньому здійсненні вже не враховуються такі поняття як фінансова ефективність чи рентабельність атаки.

Відповідно підприємства та організації (насамперед, ті, що відносяться до критичної інфраструктури), які зазнавали невпинних атак, зрозуміли, що можуть захистити свої дані, лише інвестуючи в комплексну стратегію управління кібербезпекою.

Можна стверджувати, що існує відмінність між термінами «управління кібербезпекою» та «кібербезпека». Адже управління кібербезпекою зосереджується на способах організації активів, людей та процесів безпеки, в той час як кібербезпека виступає як загальна назва для захисту цифрової інфраструктури організації [17].

Для побудови ефективних і безпечних систем, забезпечуючи їхній життєвий цикл від проєктування до експлуатації, використовують технічні моделі управління – підходи та фреймворки, що визначають, як організувати, контролювати та оптимізувати процеси управління в IT-сфері. Зазначені моделі здебільшого використовуються у великих та складних системах та зосереджуються на конкретних аспектах, таких як безпека, послуги або IT-інфраструктура.

При виборі конкретних управлінських інструментів, спрямованих на забезпечення кібербезпеки менеджмент об’єктів критичної інфраструктури спирається, насамперед, на Куб МакКамбера (McCumber Cube) – модель, яка використовується для аналізу, побудови та оцінювання систем безпеки [137]. Вона допомагає структурувати знання та визначати всі ключові аспекти, які слід враховувати при прийнятті управлінських рішень з метою забезпечення захисту інформації (рис. 2.9).

Вказаний Куб виглядає як тривимірна геометрична фігура, де однією з трьох видимих поверхонь є цілі кібербезпеки, а саме: конфіденційність (Confidentiality) – захист інформації від несанкціонованого доступу; цілісність (Integrity) – забезпечення точності та повноти даних, запобігаючи їх несанкціонованій зміні; доступність (Availability) – гарантія того, що системи та дані доступні для авторизованих користувачів, коли це необхідно.

Рис. 2.9. Куб кібербезпеки (куб МакКамбера) *(складено автором)*

Іншою спостережною поверхнею є стадії обробки інформації (життєвий цикл): зберігання (Storage), передача (Transmission), обробка (Processing). Третя видима поверхня цього кубу відноситься до складових, пов’язаних із забезпеченням безпеки: технологіями (Technology), процесами та процедурами (Policy) та людським фактором (People) [137]. Тобто будь-яке управлінське рішення орієнтується на забезпечення безпеки в будь-якій із 27 можливих комбінацій Кубу, які, зі свого боку, відображають повний спектр завдань у сфері кіберзахисту.

Формування відповідних рішень в процесі управління кіберзахистом передбачає формування певної системи, в межах якої міжнародні стандарти формують стратегічний фундамент, сучасні технології забезпечують технічну реалізацію, управлінські процеси створюють організаційну основу, а людський фактор виступає каталізатором ефективності всієї системи. Кінцевим результатом їхньої синергії є формування вже згадуваної кіберстійкості, тобто здатності інфраструктури протидіяти атакам, мінімізувати наслідки та швидко відновлювати працездатність (рис. 2.10).

Ефективне функціонування системи управління кіберзахистом критичної інфраструктури передбачає одночасне здійснення інвестицій/витрат за технічним та організаційним напрямами.

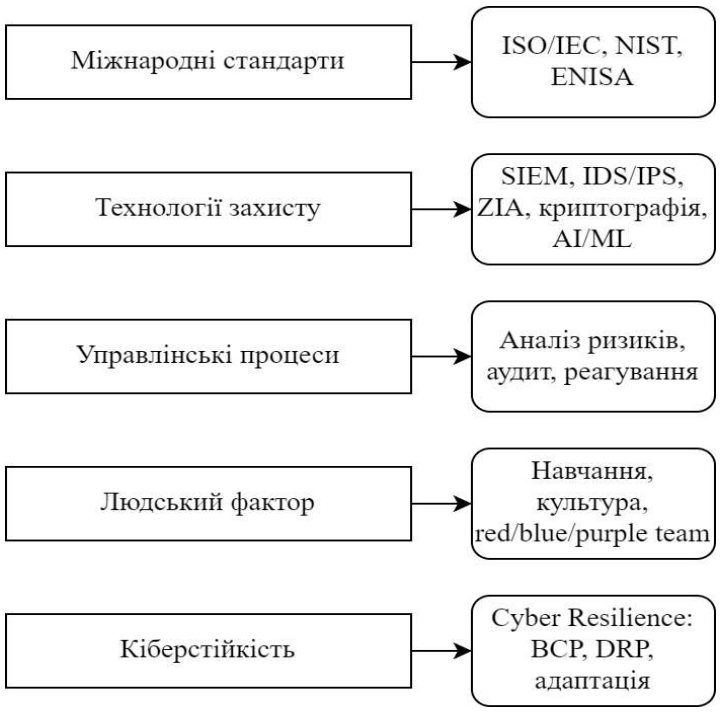

Рис. 2.10. Система управління кіберзахистом критичної інфраструктури *(складено за даними [23])*

У кількісному значенні для малих підприємств, які зазвичай концентруються виключно на технічних аспектах і потребують базових рішень для захисту даних, таких як антивірусне програмне забезпечення, системи фільтрації електронної пошти чи базова політика управління доступом, витрати на кіберзахист можуть бути відносно невеликими – від 0,5-1,5 тис. дол. залежно від кількості користувачів та особливостей конфігурації. Для середнього та, особливо, великого бізнесу вказані витрати значно зростають через необхідність впровадження комплексних рішень, таких як розробка та впровадження спеціалізованих систем виявлення загроз (IDS/IPS), шифрування даних або розгортання багаторівневих систем моніторингу та реагування на інциденти. Крім того, представники середнього та великого бізнесу мають враховувати

додаткові витрати на підтримку та регулярне оновлення програмного забезпечення, проведення аудитів безпеки, навчання персоналу тощо [17].

Вказана ситуація на тлі обмеженості в ресурсах спонукає менеджмент об'єктів критичної інфраструктури шукати шляхи для оптимізації витрат на протидію кіберзагрозам за рахунок інвестицій у технічні рішення та управлінські заходи. Традиційні економіко-математичні моделі, зокрема вже згадувана модель Гордона-Льоба, здебільшого орієнтуються на однофакторне уявлення витрат і не відображають всього різноманіття напрямів, на які можуть спрямовуватися інвестиційні ресурси. Тому в проведеному дослідженні пропонується додати два типи змінних: z_T – технічні інвестиції та z_H – організаційні. Тоді загальні інвестиції можна подати у вигляді:

$$TC(z_T, z_H) = c_T z_T + c_H z_H + p(z_T, z_H) \cdot L, \qquad (2.1)$$

де c_T та c_H характеризують питомі інвестиції у реалізацію відповідно технічних та організаційно-управлінських заходів захисту, z_T і z_H – обсяги інвестування за відповідними напрямами, функція $p(z_T, z_H)$ відображає імовірність реалізації загрози з урахуванням спільного впливу двох каналів інвестування на рівень ризику, L – величина потенційних втрат у разі реалізації негативної події.

На відміну від початкової постановки, в зазначеному варіанті з'являється властивість комплементарності. Тобто висувається гіпотеза, що підвищення ефективності технічних інвестицій можливе лише за наявності достатнього рівня організаційної (управлінської) підтримки, і навпаки. Наприклад, упровадження новітніх систем виявлення вторгнень буде малоефективним, якщо управлінський персонал не має відповідної кваліфікації для інтерпретації сигналів небезпеки, які надходять від технічних фахівців. Аналогічно організаційні заходи, навчальні курси, тренінги, втрачають сенс без наявності адекватної технічної інфраструктури.

Введення управлінського фактору як рівноправної змінної моделі дозволяє перейти від традиційної інтерпретації ефективності як похідної від обсягу інвестицій до розуміння її як результату взаємодії ресурсних та управлінських

компонентів. У межах такого підходу управлінські рішення перестають виконувати допоміжну або коригувальну функцію та набувають статусу самостійного джерела зростання ефективності, здатного змінювати траєкторію розвитку системи навіть за умов інвестиційного насичення. Аналітичне включення управлінського фактору у виробничу функцію забезпечує можливість порівняльної оцінки впливу інвестиційних і управлінських змінних, що раніше залишалося поза межами формалізованого аналізу [85].

Формальний аналіз двоканальної моделі дає змогу показати, що оптимальні інвестиції (z_T^*, z_H^*) визначаються з умов першого порядку:

$$\frac{\partial TC}{\partial z_T}=0, \quad \frac{\partial TC}{\partial z_H}=0 \tag{2.2}$$

Вони означають рівність граничних витрат кожного виду інвестицій відповідній граничній вигоді у вигляді скорочення очікуваних втрат від кіберінцидентів. Внаслідок цього в межах окремих об’єктів критичної інфраструктури не доцільно розглядати технічні та організаційні заходи ізольовано, адже раціональна стратегія передбачає їхнє збалансоване поєднання.

Наприклад, серед підприємств енергетичного сектору та фінансової сфери найкращих результатів досягають ті, які інвестують одночасно у технології та в розвиток людського капіталу, тоді як однобічні стратегії виявляються суттєво менш ефективними (рис. 2.11).

Ізокванти загальних витрат $TC(z_T, z_H)$ демонструють комбінації технічних та організаційних інвестицій, які забезпечують однаковий рівень витрат із урахуванням очікуваних збитків. Криві ізоквант ілюструють принцип комплементарності: зростання технічних витрат має обмежений ефект за низьких організаційних інвестицій і навпаки. Це означає, що ефективність системи захисту визначається не лише абсолютною величиною окремих витрат, а й збалансованістю їхнього розподілу.

Оптимізація досягається в точках, де гранична вигода від обох видів інвестицій відповідає їхнім граничним витратам.

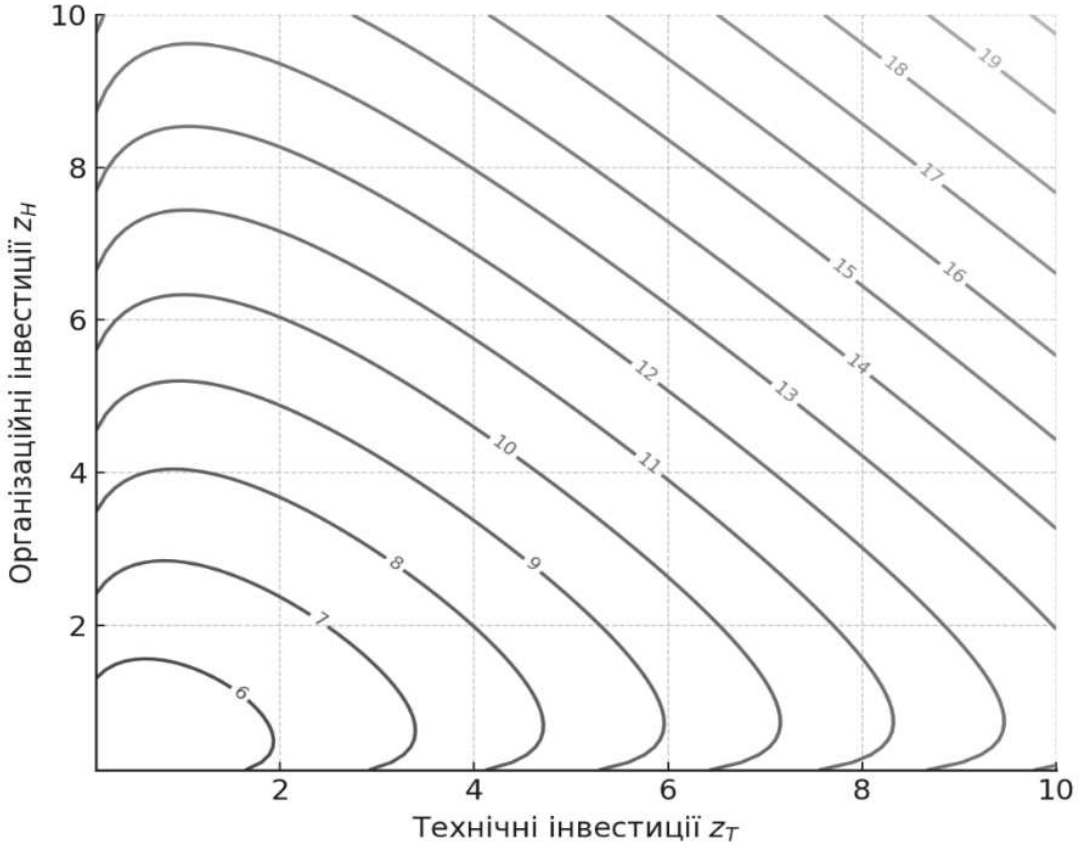

Рис. 2.11. Ізокванти загальних витрат $TC(z_T, z_H)$ *(сформовано автором на основі [151, 181, 208, 214]*

Подальша формалізація взаємозв'язку між технічними та організаційно-управлінськими інвестиціями потребує використання функціональної залежності, здатної відобразити їх комплементарний та нелінійний вплив на результуючий рівень кіберстійкості. З огляду на те, що ефективність системи кіберзахисту формується внаслідок спільної дії кількох взаємопов'язаних напрямів інвестування, доцільним є застосування мультиплікативної функціональної форми типу Кобба-Дугласа, яка широко використовується в економіко-математичному моделюванні для опису результатів взаємодії комплементарних ресурсів і дозволяє врахувати нелінійний характер залежності між обсягом інвестицій та досягнутим рівнем захищеності, а також ефект спадної граничної віддачі інвестицій. У межах цього дослідження функцію кіберстійкості або інтегральної ефективності управління захистом подано у вигляді:

$$S(z_T, z_H) = \theta \cdot z_T^{\alpha} \cdot z_H^{\beta} \quad (2.3)$$

де z_T – обсяг інвестицій у технічні заходи захисту, включно з програмно-апаратними засобами, системами моніторингу, виявлення та реагування на кіберінциденти; z_H– обсяг інвестицій у організаційно-управлінські та кадрові складові системи безпеки, зокрема підготовку персоналу, впровадження політик безпеки, організацію процесів управління кіберризиками; параметри α та β характеризують еластичність функції кіберстійкості за відповідними напрямами інвестування та відображають відносний внесок технічних і організаційних складових у формування загального рівня захищеності; коефіцієнт $\theta > 0$ визначає масштабний параметр ефективності, який інтегрує вплив зовнішніх та внутрішніх організаційно-економічних умов функціонування об’єкта, включаючи рівень управлінської зрілості, технологічну базу та специфіку галузі критичної інфраструктури.

Економічний зміст цієї залежності полягає в тому, що підвищення рівня кіберстійкості є результатом синергетичної взаємодії технічних і організаційних інвестицій, причому граничний ефект кожного напряму має спадний характер, що відповідає фундаментальним положенням економічної теорії інвестицій та ризику. Така функціональна форма узгоджується з управлінськими підходами до кібербезпеки, зокрема на основі моделі Гордона-Льоба, яка передбачає існування оптимального рівня інвестицій у безпеку та наявність спадної граничної ефективності захисних заходів, що дозволяє використовувати функцію (2.3) як інструмент формалізації задачі оптимального розподілу ресурсів між технічними та організаційними складовими системи кіберзахисту.

Завдяки цьому з’являється можливість розглядати кіберзахист як цілісний управлінський процес із характерними для нього закономірностями зростання та спадної граничної віддачі. Зі свого боку, поєднання виробничого та корисністного підходів забезпечує багатогранність аналізу та дозволяє формувати оптимальні інвестиційні стратегії з урахуванням як технічних, так і людських чинників.

Для подальшого аналізу доцільно розглянути властивості функції кіберстійкості, побудованої на основі функціональної форми типу Кобба–Дугласа. З цією метою функцію (2.3) доцільно подати у стандартному вигляді:

$$S(K, L) = \Theta \cdot K^{\alpha} \cdot L^{\beta}, \alpha, \beta \in (0,1),\ \Theta > 0, \qquad (2.4)$$

Параметри α та β мають чіткий економічний зміст і характеризують еластичність функції кіберстійкості за відповідними напрямами інвестування. Зокрема, параметр α відображає відносну ефективність технічних інвестицій та показує, на скільки відсотків змінюється рівень кіберстійкості при збільшенні обсягу технічних заходів захисту на 1% за незмінного рівня організаційно-управлінських інвестицій. Аналогічно параметр β характеризує еластичність кіберстійкості за організаційно-управлінською складовою та відображає внесок людського, управлінського та організаційного факторів у забезпечення загального рівня захищеності системи.

Обмеження $\alpha, \beta \in (0,1)$ відповідає економічно обґрунтованій властивості спадної граничної ефективності інвестицій, згідно з якою кожна додаткова одиниця вкладених ресурсів забезпечує менший приріст рівня кіберстійкості, як поівняти з попередньою. Така властивість відображає об’єктивну економічну закономірність функціонування систем кіберзахисту, оскільки початкові інвестиції дозволяють усунути найбільш критичні вразливості, тоді як подальше підвищення рівня захищеності потребує непропорційно більших витрат.

Коефіцієнт $\theta > 0$ виконує роль масштабного параметра ефективності та інтегрує вплив загальних організаційно-економічних умов функціонування системи, включаючи рівень технологічної зрілості, якість управління, галузеву специфіку та початковий рівень захищеності об’єкта критичної інфраструктури.

Таким чином, функція $S(K, L)$ дозволяє формалізувати інтегральний результат взаємодії технічних і організаційно-управлінських інвестицій та узгоджується з положеннями економіки кібербезпеки, зокрема моделлю Гордона-Льоба, відповідно до якої ефективність інвестицій у безпеку має нелінійний

характер і характеризується наявністю оптимального рівня вкладень, після досягнення якого гранична ефективність інвестицій зменшується.

В цьому сенсі функція $S(K, L)$ демонструє рівень зниження ризику та підвищення стійкості функціонування системи в результаті комбінованого впливу різних напрямів інвестування. Таке трактування узгоджується з сучасними підходами до аналізу стійкості складних організаційно-економічних систем, у яких акцент робиться на забезпеченні їх безперервного функціонування [214, 172].

Слід зазначити, що функція типу Кобба-Дугласа історично була запропонована для моделювання виробничих процесів у промисловості, однак її математична форма не є обмеженою виключно виробничими системами. З позицій економіко-математичного моделювання вона є універсальною мультиплікативною функцією ефективності, яка описує залежність результуючого показника від взаємодії декількох комплементарних факторів.

У сучасних дослідженнях така функціональна форма широко застосовується для аналізу інвестиційних процесів, інноваційної діяльності, управлінської ефективності, людського капіталу, інформаційних технологій та систем безпеки, де результат визначається спільним впливом різних типів ресурсів.

У контексті цього дослідження функція типу Кобба-Дугласа використовується не як виробнича функція у класичному розумінні, а як аналітичний інструмент формалізації інтегрального ефекту взаємодії технічних і організаційно-управлінських інвестицій. Такий підхід дозволяє врахувати комплементарність відповідних напрямів інвестування, їх нелінійний вплив на рівень кіберстійкості та наявність спадної граничної ефективності інвестицій, що відповідає сучасним підходам економіки кібербезпеки, зокрема положенням моделі Гордона-Льоба щодо існування оптимального рівня інвестицій у безпеку.

Для оцінювання віддачі від масштабу слід розглянути зміну значення функції $S(K, L)$ при пропорційному зростанні обсягів інвестування. Для довільного $t > 0$має місце співвідношення:

$$S(tK, tL) = \Theta \cdot (tK)^{\alpha} \cdot (tL)^{\beta} = t^{\alpha+\beta} \cdot S(K, L). \quad (2.5)$$

Звідси висновок, що при $\alpha + \beta = 1$функція характеризується постійною віддачею від масштабу, тоді як за умови $\alpha + \beta < 1$має місце спадна віддача від масштабу.

Останній випадок є більш адекватним для опису процесів управління кіберзахистом, оскільки зростання обсягів інвестування супроводжується організаційною та технологічною інерцією, додатковими витратами на координацію та обмеженнями спостережуваності, що зумовлює сублінійний приріст інтегрального показника кіберстійкості.

Після цього потрібно оцінити граничну віддачу та маржинальну продуктивність функції кіберстійкості. Якщо проаналізувати перші похідні:

$$\frac{\partial S}{\partial K} = \Theta \cdot \alpha K^{\alpha-1} L^{\beta} \quad \text{та} \quad \frac{\partial S}{\partial L} = \Theta \cdot \beta K^{\alpha} L^{\beta-1} \quad (2.6)$$

За $\alpha, \beta \in (0; 1), \Theta > 0$ кожна похідна є додатною (монотонне зростання S у кожному аргументі), але зменшується з ростом відповідної змінної:

$$\frac{\partial^2 S}{\partial K^2} = \Theta \cdot \alpha(\alpha - 1) K^{\alpha-2} L^{\beta} \quad \frac{\partial^2 S}{\partial L^2} = \Theta \cdot \beta(\beta - 1) K^{\alpha} L^{\beta-2} \quad (2.7)$$

Отже, можна стверджувати про наявність спадної граничної віддачі інвестицій. Далі потрібно оцінити граничну норму технологічної заміни (комплементарність):

$$MRTS_{K,L} = \frac{\partial S / \partial K}{\partial S / \partial L} = \frac{\alpha}{\beta} \cdot \frac{L}{K} \quad (2.8)$$

Зростання L/K підвищує готовність системи «замінювати» технічні інвестиції K організаційними L, що відображається опуклими ізоквантами та комплементарністю каналів. В подальшому використовуватиметься абсолютне значення граничної норми технологічного заміщення. В цьому сенсі доцільно побудувати поверхню та ізокванти вказаної функції, яка дозволяє наочно проілюструвати, як змінюється рівень захисту залежно від комбінацій технічних

і організаційних витрат, а також дає змогу визначати оптимальні поєднання інвестицій, за яких загальні витрати мінімізуються при заданому рівні ризику (рис. 2.12 та рис. 2.13).

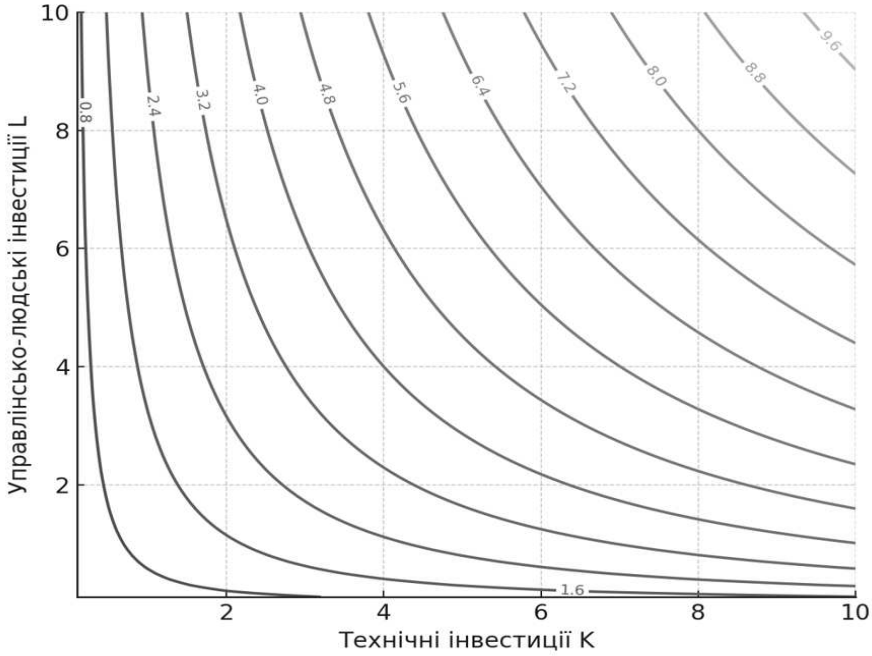

Рис. 2.12. Ізокванти адаптованої функції Кобба-Дугласа *(побудовано автором на основі власних розрахунків)*

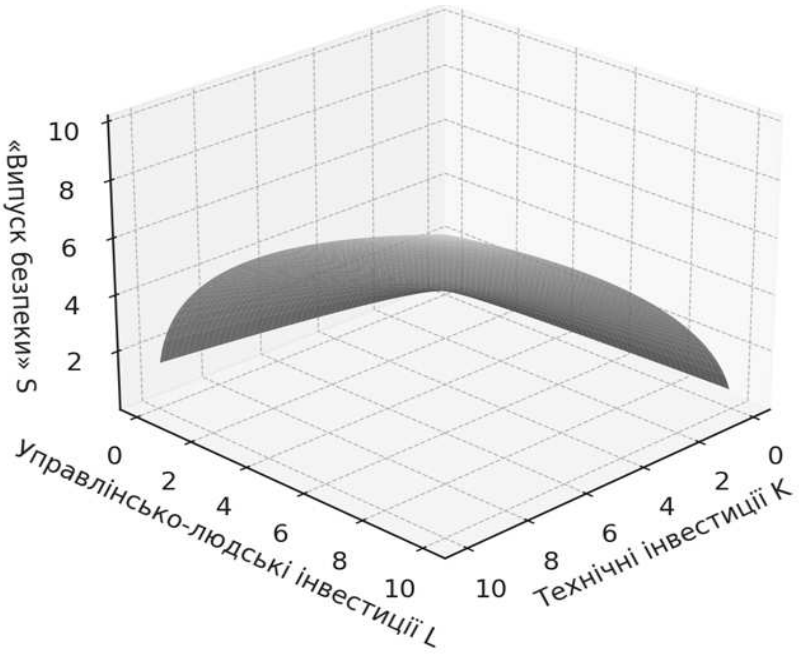

Рис. 2.13. Поверхня «випуску безпеки» (функція кіберстійкості) за функцією Кобба-Дугласа *(побудовано автором на основі власних розрахунків)*

Дослідження функції кіберстійкості підводить до поняття «плато технічних інвестицій». Під цим терміном доцільно розуміти ситуацію, коли після досягнення певного обсягу інвестицій у технічні засоби $K_p(L)$ додаткове інвестування не призводить до істотного зниження ризику. У математичному вигляді цей поріг визначається як значення змінної K, для якого гранична віддача функції $\frac{\partial S(K,L)}{\partial K}$ стає близькою до нуля за фіксованого рівня організаційних інвестицій L.

Запропонована концепція дозволяє відрізнити «ефективну зону» інвестування від зони перевитрат, коли кошти витрачаються без суттєвого впливу на рівень безпеки.

Водночас показано ефект зсуву плато: збільшення управлінсько-людських інвестицій підвищує ефективність технічних, що відображається у зміщенні порогового значення $K_p(L)$ праворуч. Вказана ситуація означає, що підприємство (наприклад, об’єкт критичної інфраструктури) здатне досягати вищого рівня безпеки без надмірних витрат, якщо водночас інвестує у навчання персоналу, організаційні процедури та управлінські процеси.

Для оцінки кінцевого результату впроваджених заходів необхідно враховувати одночасно кількісні та якісні показники. Якісні показники охоплюють рівень адаптивності системи управління до нових загроз, ступінь залучення персоналу до процесів кібербезпеки та підвищення загальної культури безпеки в організації. Більш детально в проведеному дослідженні вони розглядатимуться в процесі визначення організаційного та інституційного забезпечення інноваційних перетворень в управлінні кіберзахистом критичної інфраструктури.

В той же час кількісні показники включають зменшення кількості успішних кібератак, скорочення часу реагування на інциденти та зниження фінансових втрат від кіберінцидентів. Наприклад, впровадження автоматизованих систем моніторингу може скоротити час виявлення загрози з днів до хвилин, що безпосередньо впливає на мінімізацію шкоди. Тобто оцінка

ефективності управлінських інновацій повинна включати аналіз витрат на їхнє впровадження у порівнянні з потенційними втратами від кібератак. Це передбачає, насамперед, розрахунок коефіцієнту повернення інвестицій (ROI) у кібербезпеку.

На підставі звітів провідних аналітичних компаній сформовано узагальнену картину інвестицій у кіберзахист за 2022-2025 рр. (табл. 2.8). Зведені дані дають змогу простежити динаміку змін у структурі витрат і їхній вплив на середній рівень окупності інвестицій (ROI) [151, 181, 208, 214, 172].

Таблиця 2.8

Узагальнені результати здійснення інвестицій у кіберзахист (2022–2025рр.)

Рік	Інвестиції в кіберзахист, % IT-бюджету	Технічна частка, %	Організаційна частка, %	ROI (середній)	Джерела
2022	9,9	70	30	2,0	Cisco (2022)
2023	10,7	68	32	2,5	PwC (2023)
2024	11,4	65	35	3,0	IBM (2024); Secureworks (2024)
2025	12,2	60	40	3,5	WEF (2025); Verizon DBIR (2025)

Джерело: *складено автором на основі аналітичних звітів [151, 181, 208, 214]*

Отримані узагальнені результати демонструють стійку тенденцію до зростання ролі організаційно-управлінських інвестицій у системах кіберзахисту. Збільшення їхньої частки з 30 % до 40 % упродовж досліджуваного періоду супроводжується підвищенням середнього рівня окупності інвестицій, що свідчить про зростання ефективності комплексних управлінських рішень у сфері захисту інформаційних систем.

Зазначені емпіричні спостереження узгоджуються з теоретичними положеннями щодо комплементарності технічних і організаційних заходів захисту та підтверджують доцільність використання економіко-математичних моделей, у яких різні напрями інвестування розглядаються як взаємодіючі

фактори, що спільно визначають рівень кіберстійкості організаційно-економічних систем.

Аналіз відкритих аналітичних звітів міжнародних консалтингових та галузевих організацій у сфері кібербезпеки свідчить про поступову зміну підходів до структурування інвестицій у кіберзахист упродовж 2022-2025 рр. У зазначених матеріалах фіксується зростання ролі організаційно-управлінських та людських чинників у забезпеченні кіберстійкості на тлі обмеженої ефективності подальшого нарощування суто технічних заходів захисту.

Узагальнені дані, наведені в таблиці 2.9, дозволяють порівняти результативність різних напрямів інвестування з позицій управлінської ефективності. Технічні інвестиції демонструють нижчі показники граничної віддачі після досягнення певного рівня витрат, тоді як організаційно-управлінські заходи забезпечують більш стійкий ефект навіть за помірних обсягів фінансування. Найвищі показники результативності спостерігаються у випадку комбінованого підходу, що поєднує технічні та організаційні інвестиції, що узгоджується з концепцією комплементарності управлінських рішень у сфері кіберзахисту.

Таблиця 2.9

Розподіл інвестицій у кіберзахист за напрямами (2022–2025 рр.)

Тип інвестицій	Обсяг витрат, дол. США/рік	Результативність, %	Гранична віддача після порогу	Джерела
Технічні (K)	1500–2500	25–40	<1 % після ≈ 2000 дол. США	NIST (2014). IBM (2024)
Організаційно-управлінські (L)	500–1200	40–60	2–3 % навіть після ≈ 1000 дол. США	SANS (2025). PwC (2023)
Комбіновані (K+L)	2000–3500	65–80	ROI 3,0–4,0	Secureworks (2024). Verizon DBIR (2025)

Джерело: *складено автором за [181, 208, 172, 187, 214]*

Отримані узагальнені оцінки можуть використовуватися як емпіричне підґрунтя для подальшого економіко-математичного моделювання взаємодії різних напрямів інвестування та обґрунтовують доцільність розгляду технічних і

організаційно-управлінських ресурсів як взаємодіючих факторів формування кіберстійкості.

Виявлені закономірності підтверджують доцільність моделювання кіберстійкості як результату взаємодії технічних та організаційно-управлінських інвестицій із урахуванням ефектів спадної граничної віддачі.

Все вищевказане створює можливість для визначення граничної ефективності інвестицій, тобто співвідношення між додатковими витратами та приростом рівня кіберстійкості. Отримані результати дозволяють чітко простежити закономірність спадної віддачі у технічному каналі інвестицій. Якщо на початкових етапах додаткові витрати забезпечують значні зміни зниження ризику (до 10%), то після досягнення приблизно 1,5 тис. дол. на одного працівника ефект додаткових витрат стає мінімальним. Це підтверджує гіпотезу про існування «плато», після якого інвестиції у нові технології не забезпечують істотного підвищення рівня кіберстійкості.

Організаційні інвестиції демонструють більш тривалий позитивний ефект. Навіть після перевищення порогу у 0,8-1 тис. дол. на одного працівника вони продовжують давати суттєвий приріст, що свідчить про їх довгострокову ефективність. Це пояснюється тим, що навчання персоналу, розвиток культури безпеки та формування ефективних процедур реагування сприяють стабільному підвищенню стійкості системи, навіть коли технологічна складова досягла межі своєї результативності.

Комбіновані програми, у яких технічні та організаційні витрати поєднуються у співвідношенні близько 60/40, забезпечують найвищий інтегральний ефект. За умов загальних витрат у межах 2–3 тис. дол. на одного працівника рівень зниження ризику сягає 70–80 %, що значно перевищує результати при одноканальному фінансуванні.

Таким чином, можна стверджувати, що з погляду розподілу витрат доцільною є їхня збалансованість за технічним та організаційним напрямами. Зі свого боку, в межах організаційного напряму менеджмент об’єктів критичної інфраструктури обирає найбільш доцільні та ефективні управлінські підходи

залежно від поточної ситуації. Для порівняльної оцінки традиційних та інноваційних управлінських підходів (конкретними проявами останніх якраз є управлінські інновації) доцільно використати дані таблиці 2.10. Вона відображає ключові показники ефективності в межах традиційних та інноваційних підходів, а також пояснює вплив кожного показника на мінімізацію кіберзагроз.

Таблиця 2.10

Ключові метрики ефективності традиційних та інноваційних підходів до управління кібербезпекою

Показник ефективності	Традиційні підходи	Інноваційні підходи	Вплив на мінімізацію кіберзагроз
Час реагування на кіберінцидент	Середній. Залежить від досвіду та реакції фахівців.	Мінімальний. Застосовуються автоматизовані системи з використанням ШІ	Швидке реагування зменшує шкоду від атаки, запобігаючи поширенню загрози та мінімізуючи час простою систем.
Своєчасність виявлення загроз	Вища за середню на основі базових сигнатурних методів	Максимально висока за умов використання машинного навчання та поведінкового аналізу.	Дозволяє вчасно ідентифікувати нові загрози, а також ті, що еволюціонують, знижуючи ймовірність успішних проникнень.
Адаптивність до нових загроз	Обмежена наявними політиками та процедурами.	Висока. Використовуються динамічні моделі з самонавчанням.	Забезпечує захист від емерджентних загроз, таких як zero-day атаки, підтримується актуальність системи безпеки.
Залучення персоналу	Середнє. Обмежується періодичними тренінгами	Високе. Використовується постійне навчання з симуляціями.	Персонал допомагає зменшити ризики соціальної інженерії та внутрішніх помилок.
Відповідність стандартам	Базове дотримання.	Повна інтеграція з ISO, NIST тощо.	Повна відповідність підвищує довіру стейкхолдерів, полегшує аудит та забезпечує системний підхід до ризиків.

Джерело: *складено за [14, 56, 86, 55]*

Інноваційні управлінські підходи значно переважають традиційні за швидкістю реагування, ефективністю виявлення загроз та рівнем автоматизації. Наприклад, використання аналітики на основі штучного інтелекту дозволяє

прогнозувати потенційні атаки з точністю до 95%, що суттєво знижує ймовірність успішного проникнення зловмисників. Крім того, інноваційні підходи сприяють формуванню проактивної культури безпеки, де персонал регулярно проходить навчання з використанням симуляцій кібератак, що підвищує загальну стійкість організації.

Інтеграцію інноваційних управлінських підходів в діяльність об'єктів критичної інфраструктури з мінімізації кіберзагроз доцільно розглядати в межах циклу безперервного вдосконалення управлінських процесів (рис. 2.14).

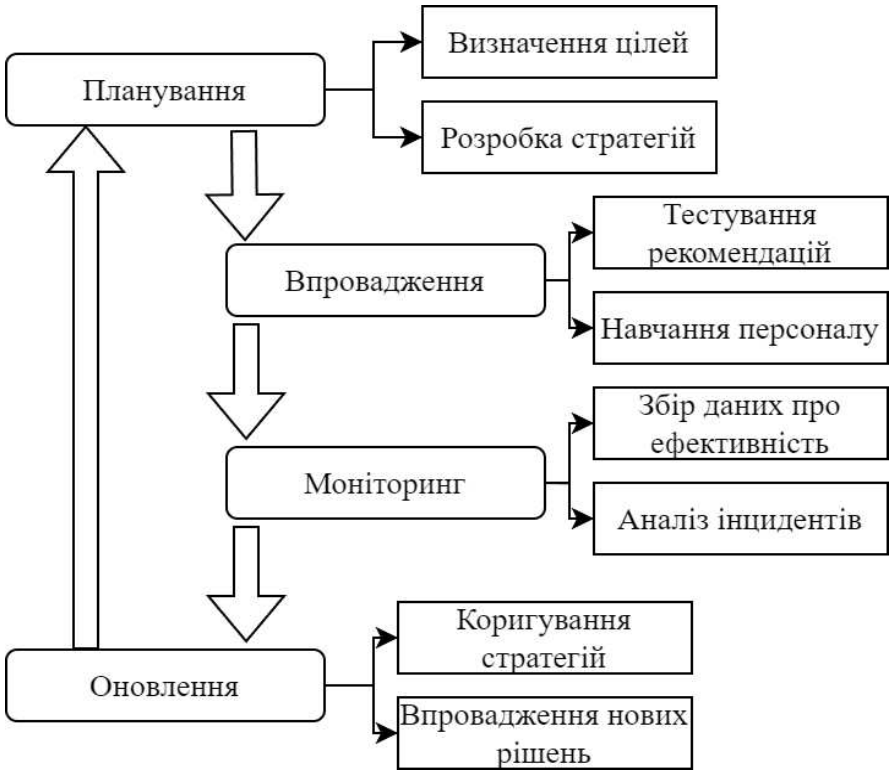

Рис. 2.14. Цикл вдосконалення управлінських процесів *(складено автором)*

Він відображає ітераційний підхід до вдосконалення управлінських процесів, що базується на циклі PDCA, який вже згадувався в теоретичній частині дослідження. На етапі планування визначаються цілі та розробляються стратегії, які враховують специфіку кіберзагроз для критичної інфраструктури. Етап впровадження включає тестування управлінських інновацій і навчання персоналу, що забезпечує їх практичну реалізацію. Моніторинг передбачає збір даних про ефективність впроваджених управлінських рішень і аналіз

кіберінцидентів для виявлення слабких місць. На етапі оновлення коригуються стратегії та впроваджуються нові рішення, після чого цикл повертається до планування для забезпечення безперервного вдосконалення. Такий підхід дозволить керівництву об’єктів критичної інфраструктури адаптуватися до динамічних кіберзагроз і підтримувати високий рівень безпеки.

Крім того, інноваційні управлінські підходи дозволяють інтегрувати національні стратегії кібербезпеки з локальними управлінськими рішеннями, забезпечуючи багатошаровий захист. Слід додати, що вже існують кейси успішного впровадження управлінських інновацій (здебільшого у вигляді інноваційних управлінських рішень про застосування сучасних цифрових технологій) для вирішення завдань кібербезпеки, в тому числі й на об’єктах критичної інфраструктури). Так, у США енергетична компанія Southern Company використовує системи штучного інтелекту для моніторингу електромереж, що дозволило скоротити кількість кіберінцидентів на 25% за останні три роки шляхом раннього виявлення загроз [197]. У фінансовому секторі банк Barclays використовує технологію блокчейн для захисту транзакцій і верифікації клієнтських даних, що підвищило безпеку операцій і знизило ризики шахрайства [168]. У Сінгапурі ініціатива Smart Nation використовує інтегровані системи управління безпекою на основі ШІ для захисту транспортної інфраструктури, що забезпечує швидке реагування на загрози, такі як спроби зламу систем управління дорожнім рухом [191].

Однак, незважаючи на наявний успішний іноземний досвід, поточна ефективність управлінських інновацій у завданнях протидії кіберзагрозам в Україні обмежена низкою структурних проблем. Насамперед, це стосується недостатньої узгодженості між різними інституціями, нестачі ресурсів та відсутності єдиного інформаційного простору для обміну загрозами й реагування. Для подолання зазначених проблем необхідна реформа управлінських підходів із фокусом на централізоване стратегічне планування та децентралізовану оперативну реалізацію.

Наприклад, задля управлінської підтримки на рівні вищого керівництва заслуговує уваги наявна практика призначення великими корпораціями спеціального члена правління, а саме директора з інформаційної безпеки (CISO) для нагляду за стратегією управління кібербезпекою. Серед його основних завдань можна відзначити нагляд за первинною архітектурою безпеки, а також оцінку будь-яких нових послуг на предмет потенційної вразливості; керівництво рішеннями зі змін в IT-інфраструктурі; організація навчання користувачів найкращих практик кіберзахисту тощо. Крім того, CISO повинен займатися організаційними питаннями подібно до інших виконавчих лідерів. Це означає збалансування бюджету департаменту та роботу з іншими керівниками над розробкою бізнес-стратегії [137].

Непрямий вплив на впровадження управлінських інновацій здійснює також розвиток міжнародного співробітництва у сфері кібербезпеки. Оскільки кібератаки дедалі частіше мають транскордонний характер, жодна держава не здатна самостійно протидіяти всьому спектру загроз. У цьому контексті набуває ваги участь у спільних ініціативах, таких як Європейський центр компетенцій з кібербезпеки, Глобальний форум з кіберекспертизи чи партнерства НАТО в межах програми Cooperative Cyber Defence Centre of Excellence.

Таким чином, можна стверджувати, що ефективність діяльності з протидії кіберзагрозам безпосередньо залежить від управлінських підходів, що застосовуються і може збільшуватися за рахунок впровадження управлінських інновацій. Успішність впровадження управлінських інновацій залежить від низки внутрішніх та зовнішніх факторів. До внутрішніх факторів належать організаційна структура окремих об’єктів критичної інфраструктури, рівень підготовки персоналу та доступність ресурсів. Зовнішні фактори включають характер кіберзагроз, регуляторні вимоги, міжнародні стандарти та міжнародну співпрацю.

Висновки до 2-го розділу

1. Управління захистом критичної інфраструктури від кіберзагроз відбувається на основі наявного технологічного підґрунтя та нормативно-правових обмежень. Використання технологічних інструментів відбувається на основі управлінських підходів, наприклад, Zero Trust Architecture, при цьому акцент поступово зміщується від кіберзахисту до кіберстійкості, тобто здатності не тільки запобігати кібератакам, але і відновлюватися після них з мінімальними втратами. До нормативно-правового забезпечення управлінських рішень у сфері протидії кіберзагрозам потрібно віднести, насамперед, «Стратегію кібербезпеки України», Закон України «Про основні засади забезпечення кібербезпеки України», а також низку міжнародних стандартів (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework тощо).

2. Вирішення управлінських альтернатив при побудові системи кіберзахисту передбачає наявність та доступність на ринку готових безпекових рішень. Світовий ринок продуктів і послуг кібербезпеки знаходиться у фазі стабільного зростання, а його обсяг у 2024 році становив 245,6 млрд дол. США. В Україні вказаний ринок також розвивається, насамперед, завдяки збільшенню внутрішнього попиту та можливостей для експорту рішень, перевірених в умовах гібридної війни. Проведений методом найменших квадратів аналіз ринку став основою для кон’юнктурного прогнозу з високим рівнем достовірності (коефіцієнт детермінації $R^2 = 0{,}9821$), згідно з яким найбільшого значення у 167,7 млн дол. США обсяг ринку досягне у 2027 році. Цей прогноз також було верифіковано за допомогою методу експоненційного згладжування. Відтак у процесі прийняття управлінських рішень, спрямованих на забезпечення кіберзахисту, керівництво об’єктів критичної інфраструктури може орієнтуватися як на власні розробки, так і на безпекові рішення, що присутні на ринку.

3. Проведений аналіз можливостей розширення моделі Гордона–Льоба з урахуванням двоканального інвестування, що передбачає одночасний облік

технічних та організаційно-управлінських заходів, надав змогу перейти від одновимірної оцінки інвестицій до аналізу структурної взаємодії. Отримані результати підтвердили, що економічна ефективність заходів кіберзахисту визначається не лише сукупним обсягом вкладень, а й пропорційністю їх розподілу між каналами. Порушення балансу призводить до зниження граничної віддачі та поступового вичерпання економічного ефекту. Запропонований підхід дозволив кількісно інтерпретувати комплементарність технічних і організаційно-управлінських інвестицій та обґрунтувати наявність граничного рівня їх ефективності. Введення «точки плато» окреслює межі доцільного нарощування інвестицій за одним напрямом без синхронного посилення іншого.

РОЗДІЛ 3. ОПТИМІЗАЦІЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ НА ОСНОВІ УПРАВЛІНСЬКИХ ІННОВАЦІЙ

3.1. Організаційно-інституційне забезпечення управлінських інновацій в процесі захисту критичної інфраструктури від кіберзагроз

Актуалізація процесів управління захистом об’єктів критичної інфраструктури відбувається, насамперед, під впливом ризиків та загроз, пов’язаних із впливом кіберсередовища. Для окремих об’єктів з вагомою інформаційною складовою навіть термін «безпека» використовується здебільшого у контексті «кібербезпека». Відтак і ефективне вирішення питань протидії кіберзагрозам має відбуватися за допомогою не окремих заходів, а цілого комплексу управлінських методів, підходів, інструментів та технологій, які доцільно об’єднати в загальну категорію – «менеджмент кібербезпеки» [17].

Як управлінська практика менеджмент кібербезпеки все ще залишається достатньо новим явищем для вітчизняних бізнес-структур. З урахуванням фокусування на критичній інфраструктурі в проведеному дослідженні пропонується визначити його як цілеспрямований процес розробки, впровадження та управління комплексом організаційних та технічних заходів, спрямованих на забезпечення сталого та безпечного функціонування життєво важливих об’єктів, а також їхній захист від актуальних і потенційних кіберзагроз.

В процесі дослідження впливу менеджменту кібербезпеки на критичну інфраструктуру важливим моментом є державна підтримка організаційних перетворень, створення науково-інноваційного фундаменту для технологічних змін, посилення кадрового потенціалу, збільшення професіоналізації менеджменту тощо. На рівні окремих об’єктів критичної інфраструктури менеджмент кібербезпеки спрямовується на впровадження ефективних

управлінських рішень із застосуванням методів, заходів та інструментів, необхідних для забезпечення кіберзахисту.

Серед найважливіших складових менеджменту кібербезпеки можна відзначити ідентифікацію та оцінку фізичних, технічних, кадрових, інформаційних та інших ризиків; розробку політик безпеки, які включаються до загальної стратегії об'єкта критичної інфраструктури; трансформацію організаційної структури для ефективної протидії кіберзагрозам; розробку та впровадження механізмів реагування на кіберінциденти; інвестування у продукти та послуги кібербезпеки; навчання працівників з питань безпеки; встановлення та модернізацію систем безпеки та контролю; сприяння виконанню національних та міжнародних стандартів безпеки; періодичний аудит та оцінку системи безпеки з метою виявлення слабких місць, зокрема з використанням «білого хакінгу».

Деякі з вказаних складових вже де-факто інтегровано в поточну діяльність окремих об'єктів критичної інфраструктури, але вказана інтеграція відбувається без належної управлінської підтримки і стосується майже виключно технічних працівників.

Формування системи менеджменту кібербезпеки в межах окремого об'єкта критичної інфраструктури відбувається за логікою побудови управлінського циклу та складається з певної послідовності етапів (табл. 3.1).

Таблиця 3.1

Етапи впровадження системи менеджменту кібербезпеки

Назва етапу	Характеристика етапу
Формування управлінського підґрунтя	Ідентифікація зацікавлених сторін, встановлення конкретних цілей кібербезпеки, затвердження рішення керівництвом щодо впровадження системи менеджменту кібербезпеки.
Розробка політики кібербезпеки	Визначення принципів, ролей, повноважень і відповідальності, вимог до захисту інформаційних ресурсів та загального підходу до управління кіберризиками.
Оцінка ризиків кібербезпеки	Ідентифікація активів, загроз і вразливостей, оцінка ризиків із використанням методології ISO/IEC 27005, OCTAVE, ранжування ризиків. Визначення способів реагування на ризики (зниження, прийняття, уникнення, передача) з формуванням відповідних управлінських рішень.

Продовження таблиці 3.1

Назва етапу	Характеристика етапу
Вибір та проєктування заходів забезпечення кібербезпеки	Визначення технічних та організаційних заходів кібербезпеки з формуванням їхнього переліку відповідно до обраного стандарту (наприклад, ISO/IEC 27002). Планування ресурсного, фінансового та кадрового забезпечення.
Розробка управлінських процедур та регламентів кібербезпеки	Розробка внутрішніх нормативних документів, що регламентують порядок управління доступом, реагування на інциденти, резервного копіювання, управління змінами, навчання персоналу тощо. Визначення порядку інформування та взаємодії з Національним координаційним центром кібербезпеки та CERT-UA.
Впровадження системи менеджменту кібербезпеки	Реалізація визначених заходів та процедур, впровадження технічних інструментів захисту, проведення навчання персоналу, інтеграція вимог кібербезпеки у бізнес-процеси та управлінські рішення.
Моніторинг, аудит, вдосконалення	Встановлення показників ефективності, проведення внутрішніх аудитів, аналіз з боку керівництва, коригування політик і процедур відповідно до змін зовнішнього середовища та характеру загроз.

Джерело: *складено автором*

Незважаючи на різнорідність об’єктів критичної інфраструктури (зокрема й за рівнем інформаційної складової), можна стверджувати, що вказана послідовність етапів буде адекватною для кожного з них. Зі свого боку, інтеграція менеджменту кібербезпеки впливає й на всю управлінську діяльність в межах об’єктів критичної інфраструктури. Для демонстрації вказаного впливу запропоновано використовувати схему, яка наочно відображає основні етапи формування стратегій оптимізації управлінських процесів. (рис. 3.1).

Вказана схема демонструє послідовний процес, який дозволяє керівництву об’єктів критичної інфраструктури систематично підійти до оптимізації управлінських процесів. На першому етапі проводиться аналіз поточного стану, що включає аудит організаційної структури та оцінку ефективності наявних процедур. Другий етап передбачає визначення пріоритетів на основі аналізу ключових загроз і критичних активів, що потребують захисту. На третьому етапі розробляються конкретні рекомендації, які включають впровадження автоматизованих систем і аналітики великих даних для прогнозування загроз. Четвертий етап зосереджений на оцінці економічної доцільності, зокрема шляхом розрахунку показника Return on Security Investment (ROSI). Останній,

п’ятий етап, передбачає пілотне впровадження рекомендацій і їх постійний моніторинг для забезпечення стійкості системи.

Рис. 3.1. Оптимізація управлінських процесів під впливом менеджменту кібербезпеки *(складено автором)*

Ефективність впровадження менеджменту кібербезпеки залежить від низки внутрішніх та зовнішніх чинників. Серед внутрішніх чинників можна відзначити такі. По-перше, оцінку ризиків, яка дозволяє визначити, які активи об’єкти критичної інфраструктури піддаються кібератакам і яким ризикам вони піддаються. По-друге, розробку політик та процедур кібербезпеки. Вони мають

визначити, як саме об’єкт критичної інфраструктури має захищатися від кібератак. По-третє, для реалізації політики та процедур кібербезпеки необхідно впроваджувати технології кібербезпеки, а саме встановлення брандмауерів, антивірусного програмного забезпечення та систем виявлення вторгнень. По-четверте, персонал повинен бути обізнаний про кібербезпеку та вміти запобігати кібератакам [191].

На останньому блоці доцільно зупинитися більш детально. Адже, як вже неодноразово зазначалося в дослідженні, людський чинник – це один із найуразливіших аспектів вітчизняного кіберпростору.

З погляду організації ефективної системи захисту від кіберзагроз, весь персонал об’єктів критичної інфраструктури доцільно поділити на 3 групи: управлінський персонал, технічні працівники та інші співробітники, які мають доступ до інформаційних систем. Для кожної групи необхідно розробити індивідуальні програми навчання, які враховують специфіку ролей, рівень ризиків та потреби об’єкта. Загальні принципи таких програм включають: регулярність (щонайменше раз на квартал), комбінацію теоретичних та практичних елементів (наприклад, симуляції атак), сертифікацію за міжнародними стандартами (як ISO 27001 чи NIST) та інтеграцію з національними ініціативами, такими як програми ДССЗЗІ чи партнерства з університетами (Додаток Д).

Для управлінського персоналу акцент робиться на стратегічному мисленні та прийнятті рішень. Зокрема, пропонується створення щорічного курсу з кіберризикового менеджменту, на якому керівники різних ланок вивчають сценарії криз та вчаться координувати подальше реагування. Додатково важливо впроваджувати семінари з етики та юридичних аспектів кібербезпеки, щоб розуміти відповідальність за витоки даних.

Технічні працівники, як адміністратори мереж чи розробники, потребують глибоких технічних знань. Рекомендується модульне навчання з хмарної безпеки, криптографії та інструментів моніторингу (наприклад, SIEM-системи). Практичні воркшопи з етичного хакінгу дозволять тестувати вразливості в

контрольованому середовищі, а сертифікація CompTIA Security+ забезпечить стандартизацію.

Для інших співробітників (насамперед, офісних, які мають доступ до інформаційних ресурсів) фокус потрібно зробити на базовій обізнаності: тренінги з розпізнавання фішингу, безпечного використання гаджетів та політики паролів. Гарний результат можуть демонструвати гейміфіковані онлайн-курси (наприклад, на платформі Coursera), що роблять навчання доступним, а завдяки періодичному тестуванню можна перевіряти фіксацію знань.

Крім навчання та підвищення кваліфікації кожної з категорій персоналу, організація ефективного захисту критичної інфраструктури потребує використання командного підходу. Формування команд є однією з ключових управлінських інновацій, оскільки командна діяльність виступає потужним інструментом створення синергії, що сприяє досягненню максимальної продуктивності під час виконання управлінських завдань.

Застосування командного принципу в менеджменті кібербезпеки ґрунтується на ідеї, що ефективний захист інформаційних систем потребує скоординованих зусиль фахівців різного профілю та рівнів відповідальності. І, хоча оперативні завдання (наприклад, перевірка мережевого трафіку або реагування на кіберінциденти) виконують майже виключно технічні спеціалісти, надійний кіберзахист можливий лише за умови, що дії всіх працівників незалежно від їхньої посади взаємодоповнюють одна одну.

Крім того, командний підхід сприяє обміну знаннями та досвідом, що є особливо важливим у сфері кібербезпеки, де швидкість реакції на інциденти та якість рішень можуть визначати успіх у захисті критичної інфраструктури. Такий підхід не лише підвищує ефективність управління, але й створює умови для постійного професійного розвитку учасників команди, що є критично важливим у динамічному середовищі кіберзагроз [67].

Ефективність управлінських команд ґрунтується на тому, що в процесі їхнього функціонування «групове мислення» протиставляється «командному

мисленню». І якщо групове мислення зазвичай базується на прихильності до вибору однієї думки (лінійний підхід), то «командне» націлене на виявлення різних, навіть конфліктуючих між собою думок (нелінійний підхід, що обґрунтовує множинність рішень). Коли спрацьовує синдром «групового мислення», сумарний ефект інтелектуальних зусиль членів команди нижчий, ніж в окремих її членів. У разі «командного мислення» люди, не відчуваючи тиску з боку керівників або колег, вільно висловлюють думки і створюють ефект синергії [19].

Враховуючи специфіку завдань протидії кіберзагрозам, формування та функціонування управлінських команд передбачає й певні складнощі. Так, кадровий резерв при формуванні управлінської команди майже завжди є обмеженим, особливо тоді, коли забезпечення кіберзахисту потребує специфічних компетенцій від менеджерів. Успішність кожного менеджера в межах однієї команди не гарантує такий самий результат при переході в іншу, оскільки в ній вже діють зовсім інші організаційні умови діяльності. З іншого боку, менеджер не має все життя працювати у комфортних умовах однієї й тієї ж самої команди. Крім того, кіберзагрози теж постійно еволюціонують, відтак ефективність команд може погіршуватися із часом. В цьому сенсі важливо, щоб команди створювалися лише на якийсь визначений заздалегідь період. І, нарешті, відсутність формальної підлеглості може призвести й до негативних наслідків, особливо коли керівник команди не має належних лідерських якостей, а для деяких об’єктів критичної інфраструктури формальне підпорядкування є обов’язковим.

При застосуванні командного підходу центральну роль у моделі управління кіберзахистом відіграє менеджер з кібербезпеки, який здійснює стратегічне планування, координацію діяльності команди та інтеграцію управлінських і технічних рішень (рис. 3.2). Аналітичний блок забезпечує інформаційно-аналітичну підтримку управлінських рішень шляхом моніторингу загроз, аналізу кіберінцидентів та оцінки рівня захищеності організації. Комунікаційно-маркетинговий блок спрямований на формування культури

кібербезпеки, ефективну взаємодію з персоналом та дослідження ринку відповідних продуктів і послуг. Включення цього блоку дозволяє обґрунтовувати управлінські рішення щодо впровадження нових технологій та інвестування в засоби кіберзахисту.

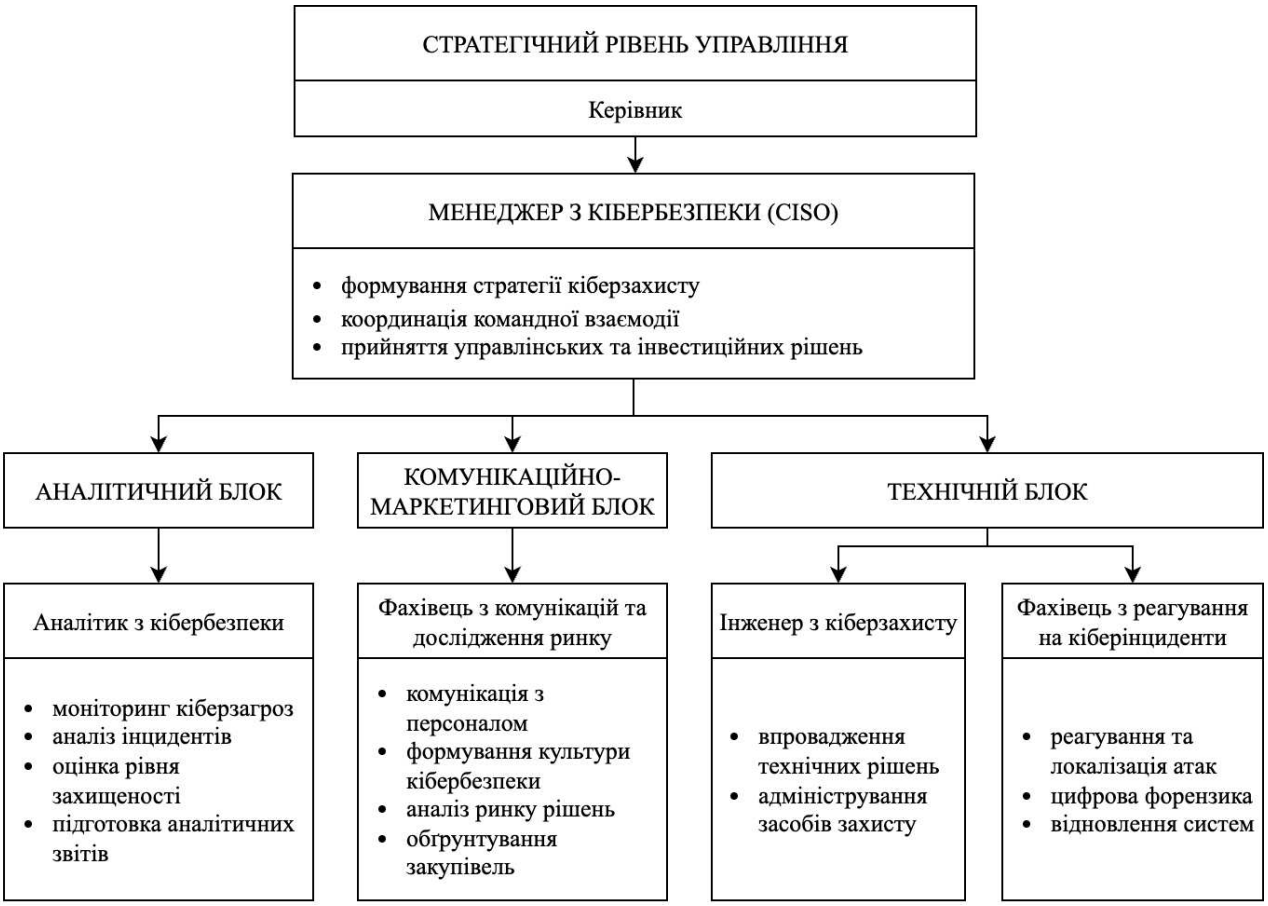

Рис. 3.2. Модель управління кіберзахистом на основі використання командного підходу *(створено автором)*

Технічний блок виконує функції практичної реалізації прийнятих рішень та забезпечує оперативне реагування на кіберінциденти. Взаємодія між блоками має циклічний характер, що забезпечує постійний зворотний зв’язок і коригування загальної стратегії кіберзахисту.

У випадку застосування запропонованої моделі на об’єктах критичної інфраструктури ефект командної співпраці проявлятиметься на всіх етапах управлінського процесу: від аналізу загроз і планування до реалізації та моніторингу заходів із кіберзахисту. Завдяки взаємодії між фахівцями із різними

досвідом, компетенціями та ментальними характеристиками, така команда здатна швидко адаптуватися до нових викликів, генерувати інноваційні рішення та ефективно розподіляти ресурси для протидії кіберзагрозам. Відтак запропонована модель сприятиме підвищенню узгодженості дій учасників команди та зменшенню фрагментарності управління кібербезпекою.

В результаті інноваційних перетворень в роботі з персоналом, на об'єктах критичної інфраструктури має сформуватися відповідна особиста культура кібербезпеки, здатна забезпечити мультиплікативний ефект, коли підвищення компетентності персоналу зменшує потребу у додаткових технічних витратах і підвищує ефективність уже наявних технологічних рішень.

Культура кібербезпеки формується під впливом відразу декількох аспектів. Когнітивний аспект передбачає, що кожен співробітник повинен мати усі необхідні знання та доступ до додаткової інформації, щоб в межах власної сфери відповідальності розуміти та оцінити рівень кіберзагроз, а також забезпечити їхнє попередження. Поведінковий аспект, який важливий, насамперед, для управлінського персоналу, передбачає вміння приймати адекватні рішення в умовах потенційної небезпеки, демонструвати лідерські якості та стресостійкість. Мотиваційний аспект стосується кожного окремого працівника і передбачає внутрішнє емоційне розуміння ним важливості нормального функціонування критичної інфраструктури, її залежності від надійного кіберзахисту і власної відповідальності за забезпечення зазначеного захисту.

Зовнішні чинники передбачають побудову ефективної взаємодії між державою та бізнесом задля протидії кіберзагрозам. Під пріоритетними завданнями державно-приватного партнерства в сфері кібербезпеки, як правило, розуміють розширення взаємодії державних структур з приватними науковими установами, громадськими об'єднаннями та волонтерським організаціями, зокрема в підготовці кадрів, а також підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі [100].

Слід зауважити, що в Україні вже існують ініціативи стосовно кроссекторальної співпраці між державою, приватним сектором і громадськими організаціями. Зокрема, у 2024 році в Україні створено 5 публічно-приватних партнерств у сфері кібербезпеки, які об'єднали комерційні підприємства (наприклад, Lifecell, Vodafone) та державні установи (наприклад, Держспецзв'язок). В результаті подібного партнерства відбувалась розробка систем моніторингу кіберзагроз у реальному часі, які, зі свого боку, зменшили кількість успішних атак на телекомунікаційні мережі. Громадські організації, такі як Cyber Volunteers Ukraine, залучають волонтерів до моніторингу кіберінцидентів. Так, у 2024 році волонтери виявили 277 потенційних загроз для державних сервісів [35].

В цьому контексті доцільно розглянути перспективи впровадження такої управлінської інновації, як створення в Україні кластеру кібербезпеки. Сама по собі ідея кластеру не є новою, однак як у науковій літературі, так і при практичному застосуванні термін «кластер» здебільшого використовувався в економічній, інноваційній або регіональній політиці.

Стосовно поняття «кластер кібербезпеки» можна стверджувати, що воно дотепер не має чітко визначеного понятійно-категоріального статусу. Зазначене поняття використовується фрагментарно і здебільшого у прикладному сенсі, наприклад, коли мова йде про співробітництво IT-компаній з державними структурами або закладами вищої освіти. В той же час відсутній системний опис функцій кластеру як в контексті управління ризиками, так і з точки зору залучення інвестицій з можливістю подальшої комерціалізації продукту діяльності кластеру.

Вищевказана ситуація створила умови для формування авторської пропозиції щодо впровадження кластерної форми забезпечення кібербезпеки (рис. 3.3). Слід зауважити, що в Україні вже функціонують «Національний Кластер Кібербезпеки» [188] та «Український Кластер Кібербезпеки» [74]. Однак перший – це координаційна платформа, спрямована на сталий розвиток сектору національної кібербезпеки України та організацію регулярних подій:

координаційних зустрічей, форумів, самітів, освітніх конференцій. Другий – це Громадська спілка, яка займається правовими, процедурними та технічними питаннями комплексного захисту та безпеки інформаційних активів даних. Її основним завданням є просвітницька діяльність з підвищення обізнаності у сфері кібербезпеки для всіх рівнів і сфер бізнес-середовища. Вказана спілка може також ефективно інтегруватися у структуру запропонованого кластеру як важливий учасник ком'юніті кібербезпеки.

Тобто жодна з вищевказаних структур не передбачає розробку та комерціалізацію кінцевого продукту, їхня діяльність із забезпечення кіберзахисту носить виключно підтримувальний та дорадчий характер і не фокусується на проблемах критичної інфраструктури.

Можна стверджувати і про наявність іноземного досвіду застосування кластерного підходу в сфері кібербезпеки (табл. 3.2). Наприклад, ще з 1990-х років функціонує кластер SFBA (Сан-Франциско, США), до якого, зокрема, входять компанії McAfee та Symantec.

Таблиця 3.2

Основні аспекти іноземного досвіду для інтеграції в Кластер кібербезпеки в Україні

Аспект	Кластер кібербезпеки (авторська пропозиція)	Кластер SFBA (США)	Кластер «Cyber Nation» (Ізраїль)	Кластер Північного Рейну-Вестфалії (Німеччина)	Кластер Вашингтон (США)
Структура управління	Координаційний хаб з інтеграцією державних органів, бізнесу та науки	Автономні компанії з венчурним капіталом, близькість до Кремнієвої долини	Військово-стартапна екосистема з державним фінансуванням	Регіональна спеціаліза-ція з понад 400 IT-компаніями, урядова співпраця	Фокус на державних контрактах з урядовими установами
Запозичені риси	Трикутник «влада-бізнес-наука», R&D-проєкти, комерціалізація	Інновації та венчурний капітал - адаптовано до грантів	Військові технології для реального тестування - адаптовано до критичної інфраструктури	Співпраця з урядом для контрактів адаптовано до національної безпеки	Державні контракти - адаптовано до гібридних загроз

Продовження таблиці 3.2

Аспект	Кластер кібербезпеки (авторська пропозиція)	Кластер SFBA (США)	Кластер «Cyber Nation» (Ізраїль)	Кластер Північного Рейну-Вестфалії (Німеччина)	Кластер Вашингтон (США)
Специфіка, що обумовлює привабливість для України	Пріоритет захисту критичної інфраструктури, інтеграція волонтерів та інших кластерів, фокус на грантах в умовах війни	Відсутній акцент на державному домінуванні	Адаптація до гібридних загроз, а не лише військових	Регіональна адаптація до обмежених ресурсів	Швидке реагування в реальному часі
Управлін-ський вплив	Посилення державної ролі для стійкості, рефінансування через продукти	Автономний розвиток для глобальної конкуренто-спроможності	Інтеграція для швидкої адаптації	Регіональна спеціалізація для ефективності	Державне регулювання для контрактів

Джерело: *систематизовано автором*

Кластер кібербезпеки Вашингтон, округ Колумбія (США) тісно пов’язаний з урядовими установами, в ньому зосереджені компанії, орієнтовані на державні контракти з кібербезпеки. За межами США можна відзначити кластер «Кібер Нація», (Тель-Авів/Беер-Шева, Ізраїль), який сформувався завдяки військовим технологіям та стартапам. В ЄС ключовим центром кібербезпеки є кластер у Північному Рейні-Вестфалії (Німеччина), до якого входять понад 400 IT-компаній, що спеціалізуються на захисті від кіберзлочинності.

Запозичені з міжнародної практики характеристики включають трикутник «влада-бізнес-наука», який є основою ізраїльського кластеру «Cyber Nation», де військові технології та стартапи стимулюють інновації через державне фінансування та венчурний капітал. У запропонованій моделі цей елемент трансформується в акцент на R&D-проєкти, де об’єкти критичної інфраструктури виступають не лише замовниками, але й тестувальниками рішень подібно до ізраїльського підходу, де військові структури інтегрують стартапи для реального застосування. Специфічним для українських умов є

інтеграція наявних ініціатив, таких як Національний Кластер Кібербезпеки та Український Кластер Кібербезпеки, які фокусуються на освітніх і правових аспектах, але не на комерціалізації, що дозволяє моделі заповнити цю прогалину через державне регулювання в умовах обмежених ресурсів та зовнішніх загроз. Таке рішення посилює роль держави як регулятора, на відміну від американських кластерів, таких як SFBA у Сан-Франциско, де венчурний капітал і близькість до Кремнієвої долини стимулюють автономний розвиток компаній на кшталт McAfee та Symantec, без домінуючого державного втручання.

У німецькому кластері Північного Рейну-Вестфалії основною рисою є регіональна спеціалізація та співпраця з урядовими установами для контрактів, що запозичено в українську модель через залучення об'єктів критичної інфраструктури як стейкхолдерів для ЗВО та інвесторів стартапів. Але український варіант адаптує це до поствоєнних реалій, де пріоритет віддається грантовому фінансуванню та інтеграції волонтерських мереж, як Cyber Volunteers Ukraine, що відсутнє в німецькій моделі з її стабільним економічним середовищем. Аналогічно кластер у Вашингтоні орієнтований на державні контракти, резонує з українським акцентом на співпрацю з РНБО та CERT-UA, але в Україні це доповнюється необхідністю швидкої адаптації до гібридних війн, що робить модель більш динамічною та орієнтованою на реагування в реальному часі.

Таким чином, з огляду на вітчизняний та іноземний досвід можна зазначити, що запропонований в дисертації кластер (рис. 3.3) крім традиційної функції платформи кооперації бізнесу, держави та науки виступатиме також ініціатором інноваційних проєктів в сфері кібербезпеки, а також надаватиме комплекс послуг, орієнтованих на практичні потреби. Серед них:

– консультаційні послуги з оцінки ризиків, наприклад, експертні аудити на основі стандартів ISO 27001 або NIST;

– семінари для менеджменту з персоналізованими рекомендаціями;

– модульні курси для персоналу з отриманням сертифікатів на кшталт CompTIA Security+, з фокусом на симуляціях атак;

– моніторинг та реагування на інциденти з використанням SIEM-систем.

Також в межах кластеру відбуватиметься розробка та тестування інноваційних продуктів, наприклад, організація пілотних проєктів для ШІ-систем виявлення аномалій з доступом до тестових середовищ.

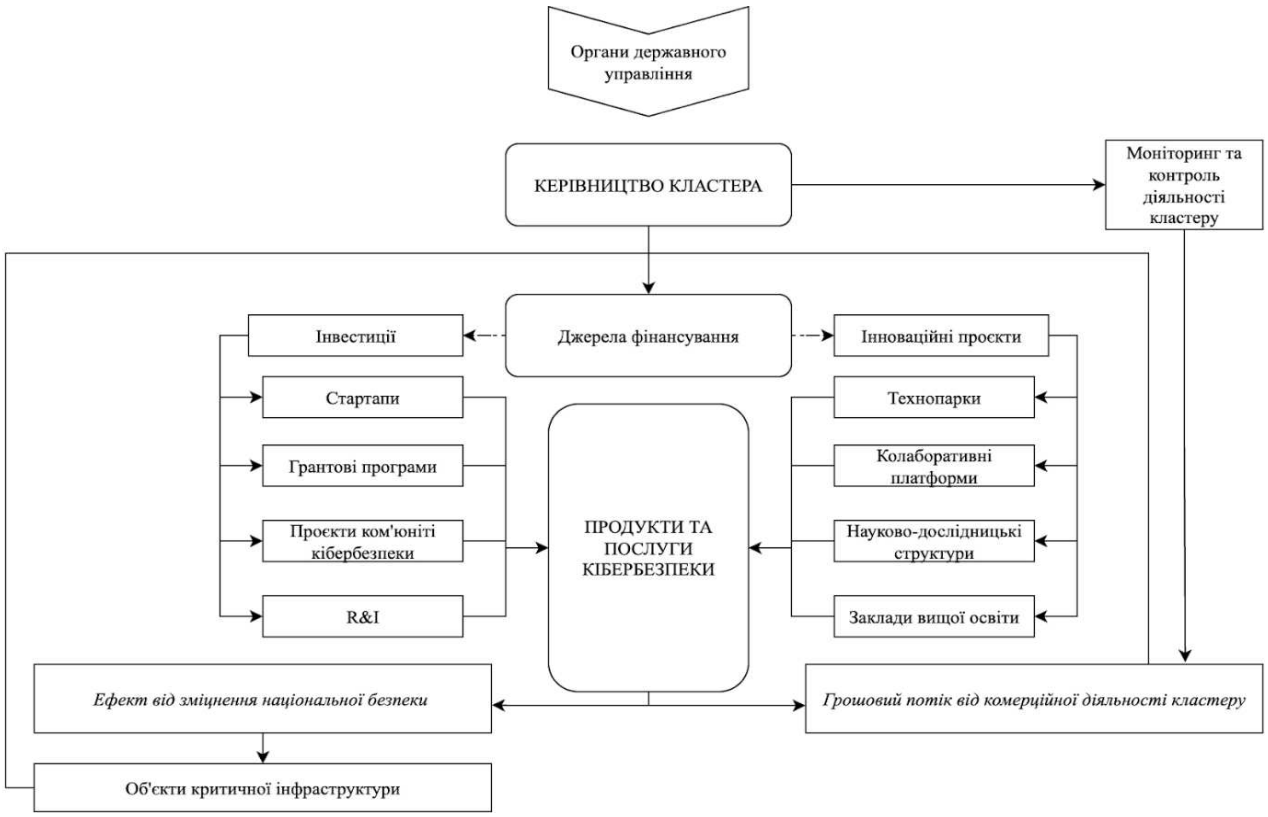

Рис. 3.3. Кластер кібербезпеки *(складено автором)*

Враховуючи важливість питань кіберзахисту в підтримці національної безпеки України, у ролі головного регулятора вказаної сфери (в тому числі й на рівні кластеру) повинні виступати державні структури, що зберігають за собою особливі функції захисту інтересів особистості, суспільства, держави. В запропонованій авторській схемі серед органів державного управління, що опікуються питаннями кібербезпеки і можуть здійснювати вплив на функціонування кластеру, насамперед, потрібно виділити Державну службу спеціального зв'язку та захисту інформації (Держспецзв'язок), Міністерство цифрової трансформації та Урядову команду реагування на комп'ютерні надзвичайні події CERT-UA.

Центральним елементом кластеру виступає координаційний хаб, який функціонує за принципом консенсусного прийняття рішень і має забезпечити як стратегічне планування, так і операційне управління. До його конкретних функцій можна віднести такі:

– моніторинг та контроль, включно з аудитом проєктів з використанням дашбордів для метрик ефективності;

– розвиток партнерських відносин, насамперед, на міжнародному рівні;

– сприяння комерціалізації результатів діяльності учасників кластеру;

– ризик-менеджмент та комплаєнс.

Крім безпосередньо управлінських функцій в межах власних повноважень, моніторингу та контролю за діяльністю кластеру, учасниками координаційного хабу може здійснюватися взаємне консультування, допомога в комерціалізації готових продуктів, інформаційна підтримка, аналіз проєктів нормативно-правових актів, підготовка пропозицій трансформації державної політики в кіберпросторі, інтеграція міжнародного досвіду тощо. Зважаючи на це, до керівництва кластером обов'язково мають долучитися представники РНБО, Держспецзв'язку, Міністерства цифрової трансформації, наукової спільноти, профільних бізнес-структур (наприклад, «EPAM» чи «Sigma Software Group»).

Основним напрямом діяльності кластеру має стати реалізація інноваційних проєктів в межах трикутника «влада-бізнес-наука». З огляду на застосування в сфері кіберзахисту та кібербезпеки термін «інноваційний проєкт» має використовуватися як комплекс взаємопов'язаних та неповторних робіт (на основі оригінальних ідей та технологій), які відбуваються в умовах обмежень в часі та ресурсах і спрямовуються на досягнення визначеного заздалегідь результату. Серед чинників, що здійснюють найбільший вплив на реалізацію інноваційних проєктів у сфері кібербезпеки, можна відзначити підвищений рівень впливу з боку держави, складність стадії ініціації проєкту, критичне значення термінів реалізації проєкту, значну диференціацію окремих проєктів за бюджетом, високий рівень персоніфікації, складність у розрахунках показників ефективності [209].

Реалізація інноваційних проєктів у сфері кібербезпеки в Україні ускладнена декількома чинниками. Як вже зазначалося в 2-му розділі, на ринку продуктів та послуг кібербезпеки переважають системні інтегратори – сервісні компанії з кібербезпеки повного циклу, які спеціалізуються на інтеграції різних технологій безпеки в єдину систему. Найбільші з них «IT-Solutions», «SIBIS», «LANTEC», «CBIT IT» надають комплексні послуги для забезпечення повного захисту бізнесу від кіберзагроз. Звісно, більшість з них покладаються на вже наявні рішення, а не розробляють власні інноваційні продукти.

На противагу системним інтеграторам, важливу роль у сфері кібербезпеки намагаються відігравати технопарки. В ролі екосистем вони об’єднують стартапи, дослідницькі центри, університети та великі компанії для створення нових технологій і продуктів. Технопарки створюють сприятливі умови для співпраці між розробниками, інвесторами та експертами, що сприяє появі інноваційних рішень, адаптованих до потреб ринку. Наприклад, у Києві технопарк UNIT.City став осередком для компаній із кібербезпеки, у Львові Lviv IT Park об’єднує компанії, які працюють над системами ШІ для виявлення кіберзагроз і тестування вразливостей, співпрацюючи з локальними університетами для підготовки фахівців, Kharkiv IT Cluster підтримує стартапи в галузі кібербезпеки через хакатони та програми менторства, сприяючи розробці нових продуктів, таких як системи моніторингу кібератак [124]. Таким чином, технопарки виступають каталізаторами інновацій, зменшуючи залежність від імпортованих рішень і сприяючи розвитку локальних технологій у сфері кібербезпеки. Але в Україні вони зараз здебільшого надають інформаційну підтримку і не є інвесторами при розробці інноваційних продуктів.

В умовах, коли у бізнесу недостатньо стимулів для інноваційної діяльності у сфері кіберзахисту, джерелом інновацій в теорії мають стати науково-дослідницькі структури, на кшталт Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації [200]. Однак на практиці в Україні майже відсутні і потужні наукові центри, здатні створювати інноваційні продукти та забезпечувати їхню подальшу комерціалізацію.

В розвинутих країнах важливим джерелом генерації інновацій є сфера вищої освіти. Станом на 01.09.2025 р. в Україні понад 50 державних та приватних ЗВО пропонували освітні програми на бакалаврському, магістерському та освітньо-науковому рівнях за спеціальністю F5 «Кібербезпека та захист інформації». Зокрема, мова йде про Київський політехнічний інститут імені Ігоря Сікорського, Національний університет «Львівська політехніка», Харківський національний університет радіоелектроніки, Національний університет «Одеська юридична академія» [26]. Крім того, окремі спеціалізовані курси чи програми за напрямом «кібербезпека» є в більшості ІТ-шкіл.

Однак низка проблем, на кшталт переважної спрямованості навчання на теорію, а не практику, слабкої координації освітніх програм або обмежених фінансових і технічних ресурсів для навчання, перешкоджає повноцінному розвитку системи підготовки фахівців з кібербезпеки [26]. Адже у підсумку, переважна більшість профільних випускників після отримання диплому працює на загальних ІТ-ролях, таких як, наприклад, фронтенд або бекенд розробка. У зв’язку з цим важливим кроком є створення національної моделі підготовки фахівців із кібербезпеки, яка включає профільну вищу освіту, післядипломне навчання, підвищення кваліфікації, сертифікацію та участь у міжнародних програмах.

ЗВО через програми дуальної освіти, дослідницькі центри та лабораторії мають активніше співпрацювати з приватним сектором та державними структурами для утримання балансу між теоретичними напрацюваннями та їх практичним застосуванням. В ролі прикладу для формату подібної взаємодії можна відзначити спеціалізовану лабораторію «Кіберполігон» Національного університету «Одеська юридична академія». Мета її діяльності полягає не тільки в підвищенні якості освітнього процесу та посиленні його прикладної складової, а й у розвитку наукових та прикладних досліджень у сфері кібербезпеки [25].

Крім того, ЗВО можуть відігравати важливішу роль і у сприянні комерціалізації розробок в сфері кібербезпеки в межах формування інноваційної екосистеми і виступати менторами для міждисциплінарних проєктних груп. Така

співпраця може бути ефективною, а теоретична підготовка як викладачів, так і студентів – стати важливою конкурентною перевагою [51].

Відтак у ситуації відсутності окремого домінуючого сектора з розробки та впровадження інновацій слід максимально використовувати потенціал професійної колаборації. Наприклад, CyberTech Committee при IT Ukraine Association координує обмін досвідом між експертами та співпрацю з урядом і міжнародними партнерами і прагне позиціонувати Україну як надійний кіберхаб у глобальному просторі [89]. Зі свого боку, Kyiv International Cyber Resilience Forum (KICRF 2024), організований NSDC спільно з CRDF Global, став майданчиком для донорів (CRDF, USAID, DAI, EU4Digital, Deloitte) і українських фахівців для обміну планами, аналітикою та налагодження співпраці [207]. Але знов-таки, саме за допомогою кластеру вказані структури мають отримати доступ для інвестиційних ресурсів для реалізації інноваційних проєктів.

Щодо комерціалізації результатів діяльності кластеру, слід відразу зауважити, що галузь кібербезпеки сприймається більшістю інвесторів як високотехнічна і водночас складна, яка вимагає спеціалізованих знань та профільних команд. Відтак важливим джерелом грошових надходжень і основою комерційного успіху (що має перетворитися на повноцінні інвестиційні ресурси для фінансування інноваційних проєктів у майбутньому) стануть продукти та послуги кібербезпеки, які можуть розроблятися в межах реалізації державно-приватного партнерства на основі контрактів на виконання визначених робіт і надання послуг (в межах, наприклад, співпраці з ЗСУ), а також у вигляді суто комерційних розробок, де результат є об’єктом купівлі-продажу). Зі свого боку, розробка та впровадження зазначених продуктів та послуг потребує інвестиційних ресурсів.

Як довів проведений в межах дослідження кон’юнктурний аналіз ринку продуктів та послуг кібербезпеки, в останні роки сфера кібербезпеки України розвивалася, насамперед, за рахунок грантового фінансування. USAID, наприклад, крім прямого виділення коштів за проєктом «Кібербезпека критично

важливої інфраструктури України». Наприклад, у 2024 році Київський політехнічний інститут за підтримки USAID відкрив першу в Україні лабораторію ICS-кібербезпеки, яка готує фахівців для роботи з промисловими системами критичної інфраструктури [166]. Відтак, в умовах потенційного скорочення чи навіть припинення реалізації проєктів після 2024 р., зокрема за програмами USAID, розробникам потрібно шукати та опановувати нові джерела фінансування та форми взаємодії.

Коли мова йде про форми залучення інвестицій, насамперед, потрібно згадати стартапи, адже тільки European Innovation Council (EIC) у 2025 р. виділив 20 млн євро для українських стартапів у сфері кібербезпеки [167]. Більшість вітчизняних стартапів спеціалізується на наданні рішень з кіберзахисту для малого та середнього бізнесу, сфери освіти, громадських організацій, особливо тих, що мають обмежені внутрішні ресурси. Зокрема, «SOC Prime» – заснований українцями стартап у вигляді маркетплейсу рішень для ідентифікації загроз, що дозволяє організаціям знаходити та впроваджувати необхідні захисні механізми. Завдяки цьому стартапу розробники можуть монетизувати власний контент, а клієнти отримують доступ до інноваційних продуктів [196]. Інший приклад, «Osavul» – стартап сектору «information/narrative security», створений як платформа, що аналізує текстові, відео- та аудіодані на вебсайтах і в соціальних мережах для виявлення онлайн-загроз [205].

Але найбільш перспективним форматом виглядає R&D (research and development, «дослідження та розвиток»), що скерований якраз на пошук інноваційних рішень. На відміну від наукової сфери, процес R&D має прикладну та комерційну природу, що якраз відповідає завданням кластеру. Наприклад, компанія «Swarmer» (розробник дронів із кіберзахистом), отримує гранти для інтеграції квантово-стійкого шифрування, обмінюючись даними з Держспецзв’язком для тестування на реальних мережах ЗСУ [44].

Що стосується безпосередньо об’єктів критичної інфраструктури, в межах запропонованого кластеру вони мають виконувати відразу декілька функцій: замовники окремих продуктів та послуг кібербезпеки; стейкхолдери для ЗВО, які

готують фахівців за спеціальністю F5 «Кібербезпека та захист інформації»; тестувальники нових розробок у сфері кіберзахисту; інвестори в стартапи за напрямом кібербезпеки. Дорожня карта реалізації зазначеної пропозиції складається з кількох етапів, починаючи з етапу підготовки протягом перших 6 місяців, коли проводиться аналіз стейкхолдерів, формується хаб та залучається фінансування. Далі йде запуск 6-12 місяців з організацією перших проєктів та інтеграцією 30 учасників. Потім від 12-24 місяців розгортається комерціалізація 5-10 продуктів та інвестиціями. Наступний етап – масштабування, охоплюваний період якого 12-36 місяців з створенням регіональних філій та інтеграцією з міжнародними кластерами. І нарешті, стабілізація після 36 місяців зі щорічним аудитом та самофінансуванням.

Таким чином, спираючись на іноземний досвід, запропонований кластер кібербезпеки виступає як концептуально нова для України форма організації системи управління кіберзахистом, яка об’єднує державні, науково-освітні, громадські та бізнес-структури в єдину екосистему мережевої взаємодії. Крім основної діяльності із забезпечення протидії кіберзагрозам, результатом діяльності кластеру та джерелом отримання доходів має стати розробка та впровадження/комерціалізація продуктів та послуг кібербезпеки.

3.2. Прикладні аспекти інтеграції штучного інтелекту в процеси прийняття управлінських рішень для кіберзахисту критичної інфраструктури

В сучасних системах кіберзахисту ШІ вже відіграє важливу роль при ідентифікації кіберзагроз та автоматизації реагування та них. Він все частіше використовується і в управлінській діяльності, наприклад, в ситуаціях, коли потрібно швидко підібрати та проаналізувати різні варіанти для прийняття управлінського рішення, провести порівняльну оцінку за кількісними показниками, створити оптимальну модель тощо. Відтак доцільно розглянути й можливість впровадження ШІ-інструментів в процеси управління критичною

інфраструктурою, а саме в розрізі її захисту від кіберзагроз (наприклад, прийняття стратегічних та оперативних управлінських рішень щодо кібербезпеки на основі ШІ-аналітики, а не виключно експертної інтуїції керівництва).

Враховуючи внутрішню різнорідність критичної інфраструктури України доцільно сконцентрувати дослідження на одному з її сегментів, а саме – енергетичній інфраструктурі. Основою енергетичної інфраструктури є 367 найбільших підприємств енергетичної сфери. З них у складі 61 (16,6%) присутні іноземні засновники або кінцеві бенефіціари. Найбільша кількість підприємств де-юре має власників з Кіпру (23), Німеччини (6), Китаю (5) та Латвії (5). Однак де-факто більша частина з вказаних підприємств підконтрольна вітчизняним олігархічним структурам [95].

Зосередження уваги саме на енергетичній інфраструктурі зумовлене низкою об'єктивних чинників. Насамперед, це високий рівень її критичності, адже сучасне урбанізоване суспільство повністю залежить від стабільного енергозабезпечення. В цьому сенсі надійність генерації, передачі та розподілу електроенергії є основою стабільності всієї критичної інфраструктури.

Також зазначимо, що енергетична інфраструктура знаходиться серед лідерів за кількістю кібератак (Додаток Е). Дійсно, кіберзлочинні групи навмисно націлюються на енергетичні системи та прагнуть паралізувати чи взагалі вивести з ладу електростанції, мережі розподілу або системи керування технологічними процесами. Наприклад, внаслідок кібератаки на «Прикарпаттяобленерго» у 2015 році понад 225 тис. споживачів залишилися без електропостачання. У 2016 році аналогічна атака була здійснена на Національну енергетичну компанію «Укренерго» [117].

З початком повномасштабного вторгнення кількість кібератак на енергетичну інфраструктуру почала стрімко зростати. Протягом 2022 року кількість кіберінцидентів в енергетичній сфері майже утричі перевищила показники 2021 року [203]. Одним із показових прикладів є спроба атаки у квітні 2022 року з використанням модифікованої версії Industroyer, відомої як

Industroyer2. Завдяки оперативній реакції українських спеціалістів, атаку вдалося нейтралізувати, що свідчить про зростання рівня кіберзахисту об’єктів критичної інфраструктури [60].

Відтак керівництво окремих підприємств (як державних, так і приватних) та енергетичної галузі в цілому знаходиться в постійному пошуку ефективних управлінських рішень для налагодження ситуації. Інноваційні перетворення в сфері управління енергетичною критичною інфраструктурою передбачають, насамперед, перехід до концепції «5D» (децентралізація, декарбонізація, дигіталізація, дерегуляція та демократизація), яка виступає теоретичною й практичною основою для формування гнучких, стійких та орієнтованих на користувача енергетичних екосистем [10]. В межах вказаної концепції децентралізація передбачає розвиток локальних джерел енергії та зменшення залежності від централізованої генерації; декарбонізація спрямована на зниження викидів парникових газів через використання відновлюваних джерел; дигіталізація забезпечує інтеграцію смарт-технологій для управління системами в реальному часі; дерегуляція відкриває ринки для конкуренції та інновацій; демократизація означає залучення споживачів як активних учасників енергетичних процесів.

На об’єктах енергетичної інфраструктури вже активно застосовуються окремі інструменти ШІ (табл. 3.3), які дозволяють здійснювати оперативний моніторинг і точне прогнозування пікових навантажень, забезпечують підвищену ефективність управління енергоспоживанням завдяки здатності до автоматизованого балансування навантажень і інтеграції децентралізованих джерел енергії в єдину систему. Зі свого боку, це дає змогу уникати перевантаження мереж і підвищує ефективність функціонування енергетичної інфраструктури. Такий підхід сприяє зміцненню надійності енергосистеми та пришвидшує її відновлення після аварійних ситуацій чи цілеспрямованих кіберінцидентів.

Крім того, системи накопичення енергії, особливо на основі літій-іонних акумуляторів, відіграють ключову роль у згладжуванні пікових навантажень і забезпеченні безперебійного енергопостачання в умовах нестабільності.

Таблиця 3.3

Інструменти ШІ, що застосовуються при кіберзахисті енергетичної інфраструктури

Категорія застосування	Назва інструменту / технології	Функціональність
Виявлення аномалій	Darktrace	Самонавчання мережевих моделей для виявлення підозрілих дій у реальному часі.
Автоматизоване реагування	SOAR (IBM Resilient, Palo Alto Cortex XSOAR)	Автоматичне реагування на інциденти, координація дій без участі людини.
Прогнозування енергоспоживання	Azure Machine Learning	Побудова моделей прогнозу навантаження та споживання енергії.
Ідентифікація загроз	VirusTotal + ШІ-модулі Google	Аналіз шкідливих файлів та сайтів за допомогою машинного навчання.
Моделювання кібератак	MITRE CALDERA, ATT&CK + ШІ	Симуляція поведінки хакера для тестування стійкості систем.
Когнітивний аналіз логів	Splunk + ШІ-модулі	Автоматичний аналіз логів для виявлення інцидентів безпеки.

Джерело: *складено за [171, 162, 163, 170, 139]*

Застосування ШІ та технологій обробки великих даних у сфері енергетичної безпеки дає змогу не лише ідентифікувати аномальні відхилення в роботі енергосистем, але й здійснювати прогностичну аналітику потенційних кіберзагроз. Такий підхід підвищує рівень проактивного реагування на кіберінциденти та підвищує ефективність управлінських рішень.

Для обґрунтованого і цілеспрямованого впровадження ШІ-інструментів у сфері кіберзахисту енергетичної інфраструктури надзвичайно важливим є попередній аналіз і кількісна оцінка потенціалу окремих підприємств з огляду на їхню спроможність до інтеграції інновацій [146]. Адже саме рівень економічного, технічного та організаційного потенціалу значною мірою визначає здатність підприємств ефективно впроваджувати інновації, забезпечувати їхнє

масштабування та підтримувати стійке функціонування в умовах нових кіберзагроз.

Якщо мова йде про управлінські інновації, можна стверджувати, що вони формують концептуальну основу для модернізації систем управління. Саме через управлінські інновації відбувається перехід до дано-орієнтованих моделей управління, які передбачають використання цифрових технологій для підвищення ефективності та стійкості. В цьому сенсі оцінка потенціалу впровадження ШІ виступає діагностичним інструментом, що дозволяє визначити рівень готовності підприємства до реалізації інноваційних управлінських рішень, враховуючи фінансовий, організаційний, технологічний та комунікаційний блоки.

За допомогою алгоритму графоаналітичного методу «Квадрат потенціалу» [16] та отриманих експертних оцінок (за п’ятибальною шкалою, де 5 бал означає найкращий результат, а 1 бал – найгірший) (Додаток Ж) в дослідженні визначено потенціал управлінських рішень про впровадження інструментів ШІ у кіберзахист на прикладі холдингу «ДТЕК», ПрАТ «НЕК «Укренерго», НАЕК «Енергоатом», ПрАТ «Укргідроенерго», ТОВ «Елементум Енерджі (Україна)». Вказані підприємства відносяться до критичної інфраструктури і охоплюють основні напрями генерації та передачі електроенергії в Україні, що дозволить отримати карту даних з графічним описом впровадження.

Використання графоаналітичного методу «Квадрат потенціалу» дає змогу наочно проілюструвати ступінь готовності вітчизняних енергетичних підприємств до цифрової трансформації систем управління безпекою**,** виявити внутрішні резерви розвитку та визначити пріоритетні напрями інноваційної модернізації. Також він дає можливість системно встановити кількісні та якісні зв’язки між окремими елементами потенціалу і на підставі цього обґрунтувати та своєчасно реалізувати управлінські рішення, спрямовані на підвищення ефективності інноваційних заходів.

Оцінка потенціалу впровадження систем ШІ має відбуватися з урахуванням технічних, організаційних, комунікаційних та управлінських аспектів. А отже, й

чотири вектори «Квадрата потенціалу» побудовані на базі системи показників за тими ж самими функціональними блоками. Обґрунтування вибору функціональних блоків базується на методології управлінських інновацій, що передбачає системне поєднання технологічних, фінансових, комунікаційних та управлінських аспектів.

Такий підхід забезпечує комплексну оцінку потенціалу впровадження систем ШІ у кіберзахист енергетичних компаній, спрямовану на підвищення їхньої ефективності та стійкості в умовах цифрових трансформацій.

Технологічний блок відображає рівень цифрової інфраструктури та готовність до її модернізації, управлінський – здатність керівництва інтегрувати інновації у стратегію розвитку та регуляторні вимоги, комунікаційний – ефективність інформаційних потоків і взаємодії з внутрішніми та зовнішніми стейкґолдерами, фінансовий – інвестиційні можливості та перспективи окупності рішень. У комплексі вони формують цілісну модель оцінювання готовності підприємства до використання інструментів ШІ у сфері управління кіберзахистом.

Алгоритм графоаналітичного методу «Квадрат потенціалу» передбачає подання вихідних даних у вигляді матриці (a_{ij}), де в рядках записані номери показників $(i=1,2,3,\ldots,n)$, а в стовпцях – назви підприємств, потенціал яких аналізують підприємства «Квадрат потенціалу» $(j = 1, 2, 3, \ldots, m)$. Для кожного підприємства знаходять суму місць (P_j), отриманих у процесі ранжирування за формулою:

$$P_j = \sum_{i=1}^{n} a_{ij} \tag{3.1}$$

Довжину вектору, що створює квадрат потенціалу підприємства (Bk, де k = 1, 2, 3, 4), знаходимо за допомогою формули [96]:

$$Bk = 100 - (P_j - n)\ \frac{100}{n(m-1)} \tag{3.2}$$

Ранжування експертної оцінки підприємств наведено за 4 блоками у таблиці Додатку И. Воно здійснювалося за шкалою від 1 до 5 балів, де 1 відповідає найвищій якості (найкращій оцінці), а 5 – найнижчій.

Форма «Квадрату потенціалу» для впровадження ШІ у кіберзахист енергетичної інфраструктури може мати два типи. Перший тип характеризується правильною формою квадрата, коли всі вектори (технологічний, управлінський, комунікаційний та фінансовий) є приблизно однаковими або наближеними за значенням. Такий варіант свідчить про збалансований потенціал компанії**,** що забезпечує успішність упровадження інноваційних інструментів ШІ для зміцнення кібербезпеки енергосистеми. Другий тип відображає викривлену форму квадрата. Це може бути зумовлено як надмірним розвитком одного з напрямів («проблемний» вектор), так і нерівномірністю розвитку всіх векторів, що створює дисгармонію між складовими потенціалу. Наближення квадрата до другого типу означає потребу у термінових трансформаціях для підвищення збалансованості елементів потенціалу й гармонізації процесів трансформації системи кіберзахисту.

Детальний розрахунок суми місць та довжина векторів холдингу «ДТЕК», ПрАТ «НЕК «Укренерго», НАЕК «Енергоатом», ПрАТ «Укргідроенерго», ТОВ «Елементум Енерджі (Україна)» наведено у Додатку К, де В1, В2, В3, В4 – довжина векторів відповідно для технологічного, управлінського, комунікаційного та фінансового блоків. Графічно результат розрахунків наведено на рисунку 3.4 у вигляді чотирикутників потенціалу впровадження інструментів ШІ у кіберзахист енергетичних компаній.

Перше підприємство, яке представлено на рисунку – холдинг «ДТЕК». При аналізі було з’ясовано, що найбільшим вектором є комунікаційний , який складає 95,83 у.о., що свідчить про сильний розвиток комунікаційних процесів. Технологічний (В1) та управлінський (В2) блоки займають проміжні позиції, демонструючи стабільний рівень розвитку відповідних напрямків. Фінансовий блок (В4) має досить високий показник, що підкреслює фінансову стійкість підприємства. Отже, перевага холдингу «ДТЕК» у комунікаційному блоці

забезпечує ефективну взаємодію між структурними підрозділами та сприяє успішному функціонуванню всіх бізнес-процесів.

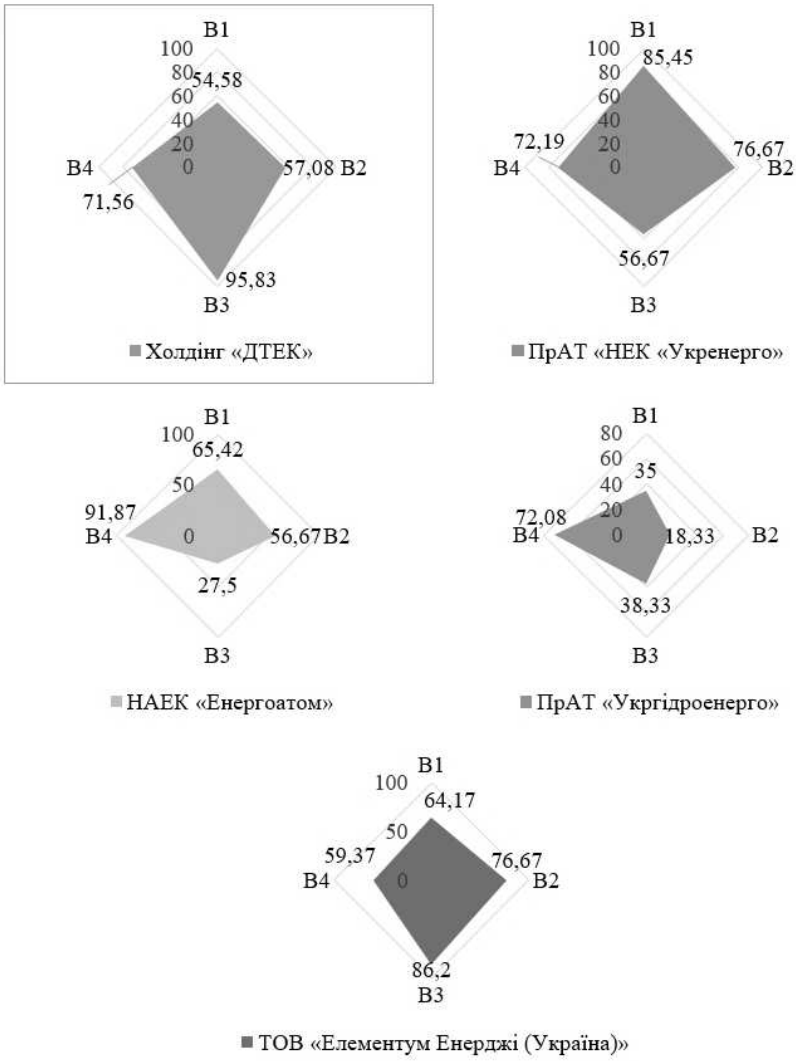

Рис. 3.4. Чотирикутники потенціалу впровадження інструментів ШІ у кіберзахист енергетичних компаній в 2024 р. *(розроблено автором)*

Дослідження потенціалу впровадження інструментів ШІ у кіберзахист ПрАТ «НЕК «Укренерго» призвело до отримання таких даних: В1=85,45у.о., В2=76,67у.о, В3=56,67 у.о., В4=72,19 у.о. Тобто найбільш розвиненим у ПрАТ «НЕК «Укренерго» є технологічний блок, тоді як найменш розвиненим – комунікаційний.

Показники НАЕК «Енергоатом» також є доволі високими. Так, вектори становлять відповідно: В1=85,45 у.о., В2=76,67 у.о, В3=56,67 у.о, В4=72,19у.о.

Серед поданих векторів найбільшу довжину має В1=85,45 у.о., що свідчить про його домінування за значенням у порівнянні з іншими. Найменшою довжиною характеризується В3=56,67 у.о.

Вектори ПрАТ «Укргідроенерго» складають: В1=35у.о., В2=18,33у.о., В3=38,33у.о., В4=72,08у.о. Серед зазначених векторів найбільшу довжину має фінансовий блок (В4), що свідчить про його домінування у структурі підприємства. Найменш розвиненим є управлінський блок (В2), який потребує підвищеної уваги до можливої оптимізації, зокрема й за допомогою інноваційних підходів. Технологічний та комунікаційний блоки мають проміжні значення.

І нарешті, вектори ТОВ «Елементум Енерджі (Україна)» складають: В1=64,17у.о., В2=76,67 у.о.. В3=86,2 у.о., В4=59,37 у.о. Серед зазначених векторів найбільший показник має комунікаційний блок (В3), а найменш розвиненим – фінансовий блок (В4), який потребує додаткової уваги для підвищення ефективності.

Отже, жодне підприємство не виявилося одночасно найсильнішим за всіма блоками. Однак, хоча ключові переваги кожного суб'єкта проявляються у різних напрямках, за іншими рівними умовами, визначальним для оцінки загальної стабільності підприємств є фінансовий блок. Серед проаналізованих підприємств найвищий показник фінансового потенціалу демонструє ПрАТ «НЕК «Укренерго» та ПрАТ «Укргідроенерго», що свідчить про їхню фінансову стійкість і спроможність до інвестування та розвитку. Холдинг «ДТЕК» та ТОВ «Елементум Енерджі (Україна)» мають проміжні значення фінансового блоку, демонструючи стабільний рівень управління фінансами. Найгірший показник спостерігається у НАЕК «Енергоатом», що вказує на потребу додаткової уваги до фінансового планування та оптимізації ресурсів.

Найвищий рівень організаційного, технологічного та інтелектуального потенціалу демонструє НЕК «Укренерго». Саме зазначене підприємство може стати національним полігоном для тестування ШІ-інструментів кіберзахисту енергетичної інфраструктури. «ДТЕК» та «Елементум Енерджі» демонструють високий рівень готовності до швидкої цифрової трансформації завдяки гнучкій

корпоративній структурі, сучасним системам моніторингу та управління, а також відкритості до інноваційних рішень. Вони можуть стати рушіями ринку у впровадженні розподілених рішень з кіберзахисту на базі штучного інтелекту, зокрема у напрямі прогнозування ризиків, аналітики подій і реагування в реальному часі. НАЕК «Енергоатом» має середній рівень потенціалу, що зумовлений високими вимогами до безпеки атомних об'єктів і складною ієрархічною структурою управління.

Проте ключовою слабкою ланкою залишається комунікаційний блок, який потребує глибокої модернізації. ПАТ «Укргідроенерго» демонструє низький рівень готовності до впровадження інтелектуальних технологій, що пов'язано з обмеженим інвестиційним ресурсом і застарілою технічною базою, а отже, потребує модернізації виробничо-управлінських процесів та інституційної підтримки для залучення технологічних партнерів і фінансових інструментів розвитку.

Можна зробити висновок про наявність потенціалу для інтеграції ШІ в управління кіберзахистом об'єктів енергетичної інфраструктури та переходу від реактивної до проактивної моделі управління кіберризиками, що дає можливість перейти від декларативних рекомендацій щодо застосування ШІ до диференційованих управлінських рішень, адаптованих до реальних можливостей конкретних підприємств. Результати аналізу потенціалу можуть стати підґрунтям для визначення пріоритетності, послідовності впровадження ШІ-інструментів у сфері кіберзахисту підприємств енергетичної галузі.

Таким чином, використання графоаналітичного методу «Квадрат потенціалу» забезпечує узгодження стратегічних цілей цифрової трансформації з фактичною управлінською спроможністю енергетичних підприємств (рис. 3.5).

Центральним елементом у запропонованій схемі є контролінг, який в енергоменеджменті забезпечує системне управління енергетичними ресурсами, витратами та ризиками в умовах зростання цін на енергоносії, декарбонізації та цифрової трансформації. Впровадження інструментів ШІ в управління кіберзахистом енергетичних підприємств потребує наявності контролінгу як

інструменту координації технологічних, економічних і ризик-орієнтованих процесів.

Рис. 3.5. Схема впровадження ШІ в управління кіберзахистом енергетичної інфраструктури (*розроблено автором)*

Контролінг забезпечує обґрунтування інвестицій у ШІ-рішення шляхом оцінки їх економічної ефективності та впливу на зниження кіберризиків. Він дозволяє системно ідентифікувати нові загрози, пов'язані з використанням ШІ, зокрема ризики помилкових рішень, деградації моделей і компрометації даних. Через встановлення ключових показників ефективності контролінг оцінює результативність ШІ в кіберзахисті, зокрема скорочення часу виявлення та реагування на інциденти. Важливою функцією контролінгу є забезпечення відповідності ШІ-рішень вимогам регуляторів і міжнародних стандартів кібербезпеки критичної інфраструктури. В цьому сенсі він сприяє інтеграції ШІ в загальну систему управління енергетичним підприємством, узгоджуючи дії підрозділів ІТ, операційної безпеки та менеджменту.

Наявні міжнародні стандарти забезпечують етичність, безпеку та ефективність ШІ-рішень. Зокрема, NIST безпосередньо впливає на логіку підходу, дозволяючи використовувати ШІ для автоматизації виявлення (наприклад, через машинне навчання для аналізу аномалій у мережах), що корелює з технологічним блоком «Квадрату потенціалу». Зі свого боку, ISO 31000 інтегрує ризик-менеджмент у процес оцінки готовності, де ШІ може моделювати сценарії ризиків на основі наявних даних, зменшуючи суб'єктивність ранжування та підвищуючи точність розрахунку сум місць та векторів. NIS2, як регуляторний стандарт, наголошує на обов'язковому включенні ШІ в системи моніторингу інцидентів для операторів суттєвих послуг, що посилює управлінський блок підходу, вимагаючи сертифікації ШІ-інструментів та навчання персоналу (через симуляції атак). Внаслідок вищевказаного стандарти перетворюють ШІ з технічного інструменту на інтегровану частину управлінської інновації, забезпечуючи комплаєнс і мінімізацію етичних ризиків, таких як упередженість алгоритмів.

З погляду конкретного напряму управлінських інновацій, можна виокремити децентралізацію енергопостачання та розвиток локальної розподіленої генерації. Основою децентралізованих систем стають відновлювані джерела енергії, зокрема сонячна, вітрова, біоенергетика та малі гідроресурси, що дозволяють формувати сталу, екологічно безпечну та економічно ефективну енергетику на місцевому рівні.

Основним завданням на управлінському рівні при цьому є перехід від централізованих рішень до локальних управлінських осередків (громади, підприємства, мікромережі), де ШІ підтримує автономне прийняття рішень і «острівний режим» роботи, а кінцевий результат – формування мікросмартґрід, тобто інноваційної моделі локальної енергетичної інфраструктури, що поєднує розподілену генерацію, системи зберігання енергії та інтелектуальні технології управління. Ключовою особливістю мікросмартґрід є здатність функціонувати як у складі централізованої мережі, так і в автономному «острівному» режимі, що підвищує рівень енергетичної стійкості [80]. Вказана особливість позитивно

впливає на кіберзахист за рахунок сегментації системи та локалізації можливих загроз, крім того, використання децентралізованих протоколів аутентифікації та шифрування знижує ймовірність несанкціонованого доступу до критичних вузлів.

Мікромережі різного масштабу демонструють відмінний рівень стійкості до кіберзагроз залежно від кількості користувачів, архітектури та цільового призначення. У громадах та населених пунктах ключовим захисним фактором є сегментація та здатність до автономного функціонування, що дозволяє мінімізувати ризики масштабних кібератак та ракетних ударів та атак дронів [135].

У мережах котеджних містечок децентралізація і невелика кількість вузлів знижує привабливість для зловмисників, хоча слабкі місця можуть виникати через недостатній рівень кіберграмотності користувачів. Внутрішні мережі ОСББ мають відносно просту структуру, що полегшує контроль за безпекою, проте обмежені фінансові ресурси ускладнюють запровадження комплексних рішень.

Мережі підприємств відзначаються найвищим рівнем уваги до кіберзахисту, оскільки атаки на них можуть призвести до значних економічних збитків і зупинки виробництва.

Залежно від конфігурації та функціонального призначення можна виділити три основні типи мікромереж. Дистанційні мікромережі (автономні мікромережі), які характеризуються повною ізоляцією від загальної електричної мережі. Такі системи функціонують виключно в автономному (острівному) режимі, що робить їх придатними для застосування в регіонах із відсутньою або недоступною передавальною та розподільною інфраструктурою [118]. Мікромережі, підключені до централізованої мережі, мають фізичне з’єднання з комунальною енергосистемою через точку загального підключення. Водночас за необхідності вони здатні від’єднуватися для автономної роботи з подальшим повторним приєднанням до основної мережі [157]. Мікромережі, що об’єднані у мережу (мережеві мікромережі), відомі також як інтегровані мікромережі.

Вказані структури об’єднують декілька локальних мікромереж, що мають спільні розподілені енергетичні ресурси та функціонують у межах єдиного енергетичного сегмента. Такі системи охоплюють великі географічні території та сприяють підвищенню надійності регіонального енергопостачання [121].

На відміну від традиційних енергетичних мереж, мікромережі характеризуються вищою гнучкістю до інтеграції відновлюваних джерел енергії з нестабільним виробітком у загальну енергетичну інфраструктуру. Але внаслідок цифровізації зростає кількість взаємопов’язаних елементів – від смарт-лічильників до автономних систем управління, що відкриває нові точки входу для кіберзлочинців. Отже, мікросмартґрід постає як перспективний напрям розвитку енергетичних систем у рамках цифровізації та посилення вимог до кібербезпеки.

Використання інструментів ШІ у мікромережах є комплексним процесом, який інтегрує людський контроль та автоматизовані алгоритми, забезпечуючи швидку, ефективну та надійну протидію кіберзагрозам у реальному часі. Вказане якраз і є основою для формування інноваційного управлінського підходу, що охоплює усі аспекти протидії кіберзагрозам.

Насамперед, сценарне моделювання кібератак (наприклад, на основі згадуваного в 1-му розділі дослідження MITRE ATT&CK та ШІ-інструментів) повинно перетворитися на обов’язковий елемент стратегічного менеджменту енергетичних компаній.

На рівні окремих бізнес-структур має бути запроваджена посада менеджера кібербезпеки (аналог директора з інформаційної безпеки – CISO у великих корпораціях). Серед його завдань слід виокремити: консультування співробітників з питань захисту інформації, моніторинг рівня ризиків та безпеки, формування механізмів реагування на інциденти, налаштування окремих елементів системи безпеки, створення команд безпеки, керування технічними фахівцями, забезпечення відповідності стандартам NIST, ISO 31000, NIS2. В цьому сенсі менеджер кібербезпеки виступає своєрідним куратором цифрового

інтелекту, здатним ефективно координувати процеси та забезпечувати стратегічну інтеграцію технологій у управлінські практики.

Крім безпосередньо менеджерів, до управління кіберзахистом енергетичної інфраструктури на рівні громад долучаються оператори системи – інженери та фахівці з енергетики, які використовують ШІ-інструменти для моніторингу стану мережі, виявлення аномалій та прийняття оперативних рішень про перенаправлення потоків енергії або ізоляції уражених компонентів, зберігаючи при цьому контроль над критичними процесами. Так, фахівці з кібербезпеки розробляють і налаштовують алгоритми ШІ для виявлення та протидії кібератакам, проводять аудит безпеки та аналізують потенційні загрози системі.

Паралельно із цим використовуються автоматизовані системи контролю та реагування виступають як підсистеми, що самостійно опрацьовують великі обсяги даних від сенсорів і керуючих пристроїв та приймають рішення у реальному часі з метою блокування атак, активації резервів або зміни режимів роботи. Об’єднання технічних можливостей та людського потенціалу може відбуватися на основі ШІ-платформи для координації дій між керівництвом, інженерами, фахівцями з кібербезпеки та зовнішніми стейкґолдерами в режимі реального часу.

Зазначена платформа має виконувати функцію інтегрованого аналітично-управлінського середовища, що забезпечує збір, консолідацію та обробку даних з енергетичних об’єктів, мереж та інформаційних систем у режимі реального часу. Використання алгоритмів машинного навчання дозволить здійснювати виявлення аномалій, прогнозування кіберзагроз, оцінювання рівня кіберризику та формування сценаріїв реагування. Водночас принциповим є збереження людиноцентричної моделі управління, за якої остаточне рішення приймається технічним диспетчером за участю менеджера ШІ та фахівця з енергетики. Платформа виступатиме інструментом підтримки прийняття управлінських рішень, а не їхнім автономним замінником, забезпечуючи прозорість, контрольованість та обґрунтованість процесу управління.

Вказана пропозиція передбачає не лише автоматизацію окремих процесів, а і, передусім, переосмислення роль менеджерів та усієї системи управління у вирішенні завдань кібербезпеки. Кінцевим результатом при цьому є створення ефективного, адаптивного та прозорого механізму прийняття рішень, який поєднує людський досвід і можливості аналітичних алгоритмів через систему контролінгу.

Особливе значення має поєднання принципів децентралізації та цифровізації. Децентралізоване управління дозволяє впроваджувати інтелектуальні системи на рівні окремих громад, підприємств та об’єктів, формуючи розподілену «розумну екосистему». Водночас цифрова інтеграція забезпечує узгодженість локальних рішень із загальнонаціональними стратегіями безпеки та сталого розвитку. Адже децентралізоване управління забезпечує впровадження інтелектуальних систем на рівні окремих вузлів (громад, підприємств, будинків), формуючи «розумну екосистему». У цій системі рішення приймаються локально, але узгоджено з загальними стратегічними цілями, що підвищує гнучкість та ефективність управлінських процесів.

Інтеграція інституційного, процесного та технологічного рівнів управління в єдину системну модель, буде враховувати сучасні виклики декарбонізації, цифрової трансформації та децентралізації. Інтеграція штучного інтелекту посилює функцію стратегічного контролінгу, забезпечує своєчасне виявлення відхилень та формування обґрунтованих управлінських дій, що переводить систему з фрагментарного реагування до комплексного ризик-менеджменту. Управління набуває адаптивного характеру завдяки можливості сценарного моделювання, швидкого коригування стратегії та оптимізації ресурсів громади відповідно до пріоритетів кіберзахисту та енергетичної безпеки. Зі свого боку, поєднання централізованого стратегічного бачення із децентралізованою реалізацією рішень забезпечує баланс між автономністю громад і відповідністю національним стандартам, підвищує прозорість, підзвітність і ефективність управлінських процесів.

Таким чином, поєднання розподіленої архітектури з можливостями ШІ за умов застосування інноваційних управлінських підходів дозволяє не лише виявляти загрози в реальному часі, а й прогнозувати потенційні сценарії атак на різних рівнях мережі. Це підвищує кіберстійкість системи, оскільки атака на одну точку не гарантує порушення роботи всієї мережі, а автоматизовані алгоритми ШІ забезпечують швидку локалізацію проблеми та адаптивне реагування. Відтак, управлінські інновації спрямовані на інтеграцію ШІ у мікросмартґрід забезпечують перехід від фрагментарного використання окремих інструментів ШІ до системної трансформації процесів прийняття управлінських рішень у сфері кіберзахисту енергетичної критичної інфраструктури.

3.3. Моделювання впливу управлінських інновацій на ефективність захисту критичної інфраструктури від кіберзагроз

В процесі комплексної оцінки можливостей мінімізації кіберзагроз критичній інфраструктурі, проведеної в 2-му розділі, було доведено, що ефективність забезпечення кіберстійкості об’єктів критичної інфраструктури визначається не лише рівнем впровадження сучасних технічних рішень, але й відповідними управлінськими заходами. Серед останніх найбільший вплив мають здійснювати управлінські інновації.

Критична інфраструктура України є достатньо неоднорідною, а отже, управлінські інновації мають спрямовуватися, насамперед, на об’єкти з найбільшою критичною значимістю та водночас з підвищеним рівнем кіберзагроз. Задля їхньої ідентифікації в проведеному дослідженні запропоновано двовимірну модель, яка забезпечує кількісну оцінку пріоритетів захисту шляхом поєднання показників критичності та рівня інформатизації. Її новизна полягає в структуруванні об’єктів критичної інфраструктури одночасно за рівнем критичності та вагомістю ІТ-складової з використанням бальної оцінки, що дозволяє встановити диференційовані вимоги до забезпечення

кіберзахисту зазначених об’єктів з урахуванням, зокрема, ступеня потенційної небезпеки здійснення акту незаконного втручання та його можливих наслідків.

Об’єкти критичної інфраструктури, відібрані для моделювання, охоплюють енергетичний сектор, інформаційно-комунікаційні технології, транспорт, водопостачання та водовідведення, охорону здоров’я, фінансовий сектор, промисловість, оборонний сектор, харчову промисловість, хімічну промисловість, сектор надзвичайних ситуацій і сектор державного управління.

Критичність секторів оцінено за категоріями, визначеними Постановою № 1109: I категорія охоплює об’єкти, порушення яких спричиняє кризові ситуації державного значення – 4 бали; II категорія: життєво важливі об’єкти, криза регіонального значення – 3 бали; III категорія стосується об’єктів із регіональним впливом – 2 бали; IV категорія включає об’єкти з локальними наслідками – 1 бал [28].

Наприклад, енергетичний сектор віднесено до першої категорії через його здатність спричинити відключення електроенергії для понад 100 тис. осіб, економічні втрати, що перевищують 1% валового внутрішнього продукту та значний вплив на національну безпеку через каскадний збій в інших секторах. Сектор харчової промисловості віднесено до четвертої категорії через обмежений масштаб наслідків його порушення.

Під рівнем інформатизації розуміється ступень залежності окремих секторів від інформаційно-комунікаційних технологій, зокрема автоматизованих систем управління технологічними процесами, хмарних технологій, Інтернету речей тощо. В дослідженні пропонується виокремити високий рівень інформатизації (80–100% залежності від ІКТ), якому присвоєно 3 бали; середній (40–79% залежності) – 2 бали; низький (0–39% залежності) – 1 бал.

Зазначене ранжування базується на аналізі технологічної структури секторів. Наприклад, енергетичний сектор отримав 3 бали (95% інформатизації) через широке використання АСУ ТП і SCADA-систем, що підтверджується звітом NIST SP 800-82, який вказує на високу залежність енергосистем від цифрових технологій. Сектор інформаційно-комунікаційних технологій також

отримав 3 бали (90%) через повну залежність від цифрових мереж. Водночас сектор водопостачання оцінено в 1 бал (30%), оскільки він переважно залежить від фізичної інфраструктури, а інформаційні технології відіграють виключно допоміжну роль. Модель пріоритетності, наведена в Додатку Л, відображає оцінку всіх секторів критичної інфраструктури за критичністю та рівнем інформатизації.

Для кількісного визначення пріоритетності окремих складових критичної інфраструктури використано інтегральний індекс пріоритетності, який дозволяє формалізувати узагальнену оцінку рівня ризику на основі поєднання показника критичності об’єкта та рівня його інформатизації. Формування такого індексу ґрунтується на ризик-орієнтованому підході, відповідно до якого рівень ризику визначається як функція ймовірності реалізації загрози та масштабу потенційних наслідків її реалізації.

У цьому контексті коефіцієнт критичності відображає величину можливих соціально-економічних втрат у разі порушення функціонування об’єкта, тоді як показник рівня інформатизації характеризує ступінь технологічної залежності об’єкта від інформаційно-комунікаційних систем і, відповідно, його експозицію до кіберзагроз. З урахуванням зазначеного інтегральний індекс пріоритетності визначається у вигляді зваженої лінійної комбінації нормованих показників:

$$IP_i = 0{,}6\,K_i + 0{,}4\,R_i, (0{,}6 + 0{,}4 = 1), \qquad (3.3)$$

де K_i – показник критичності об’єкта, який залежить від категорії його значущості та відображає масштаб потенційних наслідків при порушенні нормального функціонування; R_i – показник поточного рівня інформатизації об’єкта, який характеризує ступінь цифрової залежності об’єкта та його потенційну вразливість до кіберінцидентів.

Вибір вагових коефіцієнтів $0{,}6$ та $0{,}4$ зумовлений економічною природою ризику та базується на принципі домінування компоненти наслідків у структурі інтегральної оцінки. Оскільки саме масштаб можливих соціально-економічних втрат визначає системну важливість об’єкта та пріоритетність його захисту,

відповідному показнику критичності надано більшу вагу. Водночас показник рівня інформатизації визначає ступінь технологічної експозиції об’єкта до кіберзагроз і також суттєво впливає на рівень ризику, що обґрунтовує його включення до інтегрального індексу з відповідною ваговою часткою. Використання нормованих вагових коефіцієнтів забезпечує коректну інтерпретацію інтегрального індексу як узагальненого показника пріоритетності та дозволяє обґрунтовано здійснювати ранжування об’єктів критичної інфраструктури за рівнем необхідності впровадження заходів кіберзахисту.

З метою перевірки стійкості отриманих результатів до вибору вагових коефіцієнтів було проведено аналіз чутливості індексу пріоритетності до їхньої варіації в допустимих межах. Розгляд альтернативних комбінацій ваг за умови збереження загального рівня впливу показників засвідчив, що помірні зміни значень коефіцієнтів не призводять до істотних змін у відносному ранжуванні секторів критичної інфраструктури. Це свідчить про стійкість результатів запропонованого індексу та можливість його використання як надійного інструменту підтримки управлінських рішень за умов обмеженої визначеності щодо точних параметрів моделі.

Отримані значення індексу пріоритетності застосовуються для формування впорядкованого переліку секторів і об’єктів за рівнем доцільності першочергового впровадження заходів кіберзахисту, що використовується в подальшому аналізі в межах досліджуваної моделі (рис. 3.6).

Однак, крім визначення пріоритетності захисту, важливо розуміти наскільки в межах того чи іншого сектору критичної структури може бути створене сприятливе середовище для впровадження управлінських інновацій. Наприклад, сектор безпеки та оборони характеризується нульовою схильністю до інновацій через жорстку ієрархічну структуру, хоча окремі організаційні зміни, такі як перехід Збройних Сил України до корпусної структури у жовтні 2025 року [98], є винятками.

Суб’єкти господарювання державної та комунальної форми власності мають низьку схильність до інновацій, оскільки їхня готовність до змін залежить

від політичної волі, наприклад, від ініціатив Міністерства цифрової трансформації України, яке сприяло впровадженню цифрових рішень у сфері освіти, охорони здоров'я та надання державних послуг [8]. Проте ці технологічні інновації не завжди супроводжуються управлінськими змінами.

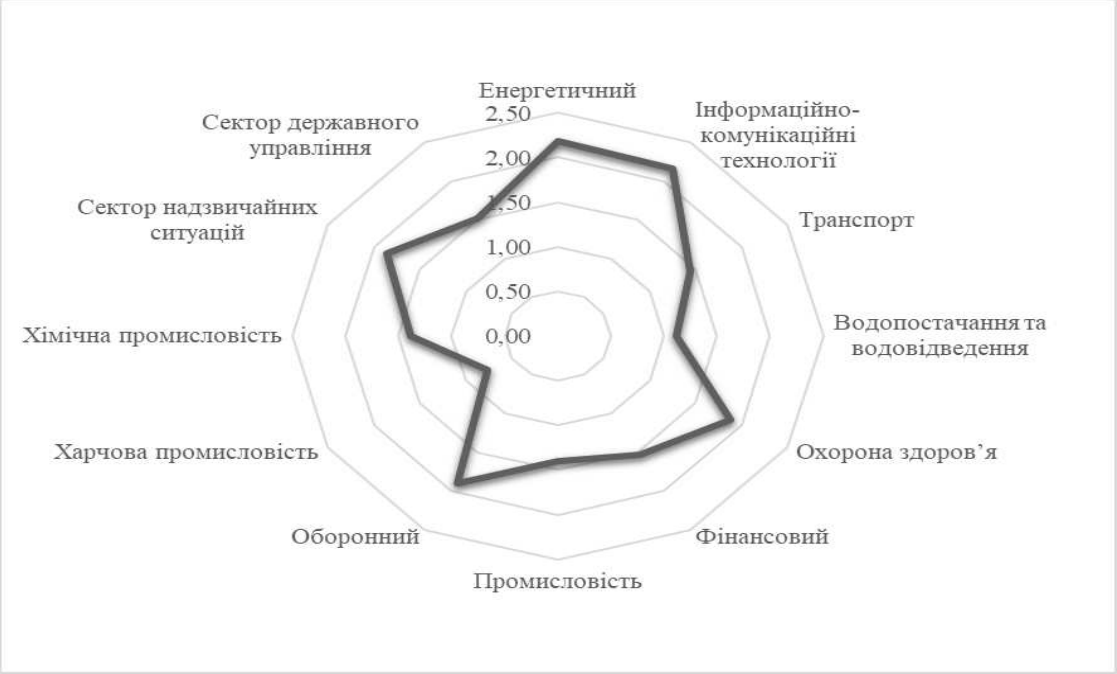

Рис. 3.6. Матриця пріоритету захисту критичної інфраструктури за видами об'єктів *(складено автором)*

Консервативні бізнес-структури (енергетичний, транспортний і фінансовий сектори) демонструють середню схильність до інновацій. Вказана ситуація зумовлена високим рівнем регуляторної визначеності, значною капіталомісткістю діяльності та підвищеними вимогами до надійності й безперервності функціонування. За таких умов оновлення управлінських підходів відбувається переважно шляхом селективного запозичення апробованих управлінських практик, адаптованих до галузевої специфіки, або через залучення зовнішніх консультантів і експертних організацій, що дозволяє мінімізувати управлінські та операційні ризики, не порушуючи стабільності ключових бізнес-процесів.

Інноваційно орієнтовані бізнес-структури, які функціонують здебільшого в сфері інформаційно-комунікаційних технологій, мають високу схильність до управлінських інновацій (Agile, Scrum, Kanban тощо). Це зумовлено динамічністю цифрового середовища, високим рівнем технологічної невизначеності, необхідністю швидкої адаптації до змін ринкової кон'юнктури та орієнтацією на безперервне вдосконалення бізнес-процесів, що в сукупності формує попит на децентралізовані моделі прийняття управлінських рішень і міждисциплінарні командні підходи.

Ранжування проводилося на основі експертних оцінок: висока схильність до управлінських інновацій, характерна для інноваційно орієнтованих бізнес-структур, оцінювалася в 3 бали; середня схильність, притаманна консервативним бізнес-структурам, які запозичують управлінські практики, оцінювалася в 2 бали; низька схильність, характерна, наприклад, для державних і комунальних підприємств із залежністю від політичної волі, оцінена в 1 бал; нульова схильність, притаманна сектору безпеки та оборони, оцінювалася в 0 балів. Наприклад, енергетичний сектор отримав 2 бали через обережне ставлення до управлінських інновацій, але відкритість до співпраці з консультантами, тоді як сектор інформаційно-комунікаційних технологій отримав 3 бали через активне впровадження інноваційних підходів.

Для більш повного врахування впливу управлінських інновацій на рівень кіберстійкості доцільно розширити базову функціональну залежність шляхом введення змінної, що характеризує людський капітал як ключовий елемент системи управління кібербезпекою. Такий підхід зумовлений тим, що ефективність технічних засобів захисту та організаційних процедур значною мірою визначається рівнем професійної підготовки персоналу, якістю управлінських рішень та здатністю організації адаптуватися до змін у кіберзагрозовому середовищі. У цьому контексті функцію кіберстійкості доцільно подати у вигляді розширеної мультиплікативної залежності типу Кобба-Дугласа:

$$S(T, O, H) = \theta \cdot T^{\alpha} \cdot O^{\beta} \cdot H^{\gamma}, \alpha + \beta + \gamma = 1, \quad (3.4)$$

де T характеризує рівень розвитку технічних засобів кіберзахисту; O – рівень розвитку організаційних процесів управління кібербезпекою, включаючи політики, процедури та управлінські механізми; H – показник людського капіталу, який відображає рівень професійної компетентності персоналу, ефективність управлінської взаємодії та здатність організації впроваджувати управлінські інновації. Параметри α, βта γ визначають еластичність функції кіберстійкості за відповідними напрямами та характеризують відносний внесок технічної, організаційної та кадрової складових у формування загального рівня захищеності.

Умова $\alpha + \beta + \gamma = 1$ відображає властивість постійної віддачі від масштабу, відповідно до якої пропорційне збільшення рівня розвитку всіх складових системи кіберзахисту забезпечує пропорційне зростання рівня кіберстійкості. Така властивість відповідає економічній природі функціонування систем кібербезпеки, у яких ефективність визначається збалансованим розвитком технічних засобів, організаційних механізмів та людського капіталу.

Якщо $\alpha + \beta + \gamma < 1$, спостерігається спадна віддача від масштабу, що відповідає реаліям систем кіберзахисту, де збільшення витрат на технічні засоби не забезпечує пропорційного зростання ефективності без супровідних управлінських інновацій. Показник рентабельності інвестицій у безпеку може бути поданий у двох формах, які є математично еквівалентними, але відображають різні рівні деталізації розрахунку. У базовій моделі, що використовується для аналізу ефективності окремих організацій або заходів, показник визначається за формулою яку, як правило, використовують для одного сценарію або окремої організації і є класичною формулою, яка відповідає підходу IBM Security [151] і використовується в економіко-математичних моделях для оцінки рентабельності конкретного заходу:

$$\text{ROSI} = \frac{A \times R \times P - C}{C} \quad (3.5)$$

де A – вартість активів, що підлягають ризику, R – ймовірність реалізації загрози, P – ефективність заходів безпеки (включно з кадровими і командними параметрами), C – інвестиції у безпеку.

Для задач управління кіберзахистом на рівні окремих складових критичної інфраструктури, що знайшли відображення в проведеному дослідженні, використання параметрів A, R і P в їхньому первісному вигляді є методологічно ускладненим через обмежену доступність деталізованих даних за окремими активами і сценаріями загроз. У зв'язку з цим у межах дослідження здійснено перехід від мікрорівневої інтерпретації показника ROSI до агрегованого подання, яке дозволяє узагальнювати результати для секторів критичної інфраструктури та порівнювати альтернативні управлінські рішення за умов неповної визначеності параметрів ризику.

Водночас у макроекономічних і галузевих узагальненнях для агрегованого оцінювання використовується еквівалентне подання:

$$\text{ROSI} = \frac{EAL \times \Delta - C}{C}, \tag{3.6}$$

де EAL– очікувані щорічні втрати (Expected Annual Loss), а Δ – частка зниження цих втрат після впровадження заходів (Risk Reduction Factor).

У межах запропонованої адаптації приймається, що очікувані річні втрати EAL відповідають добутку вартості активів під ризиком та ймовірності реалізації загрози (EAL = A × R), тоді як параметр Δ інтерпретується як інтегральний показник ефективності впроваджених заходів безпеки, включно з управлінськими та кадровими складовими (Δ = P).

Така інтерпретація дозволяє безпосередньо пов'язати економічну ефективність інвестицій у кіберзахист з управлінськими інноваціями та рівнем розвитку людського капіталу, що є принципово важливим для подальших емпіричних розрахунків у межах розробленої моделі.

В результаті отримано агреговану форму тієї ж самої залежності, де $A \times R$ замінено на інтегральний показник очікуваних річних втрат. Вона зручна, коли

робиться зведення за секторами або середні оцінки для різних галузей, тобто коли неможливо розділити дані на окремі параметри A, R, P.

Для подальших розрахунків приймаємо EAL – очікувані річні втрати від кіберінцидентів; Δ – очікуване зниження втрат, C – вартість навчальних заходів, тоді:

$$AL = EAL \cdot \Delta,\ NE = AL - C,\ ROSI = \frac{NE}{C},\ PB = \frac{C}{AL},\ \Delta^* = \frac{C}{EAL}. \quad (3.7)$$

Для агрегованих галузевих показників з метою деталізації використовується формула такого вигляду:

$$\mathrm{ROSI}_{\text{галузі}} = \frac{\sum_i (EAL_i \times \Delta_i - C_i)}{\sum_i C_i} = \frac{\sum_i EAL_i \times \Delta_i}{\sum_i C_i} - 1, \quad (3.8)$$

Вказану формулу можна застосовувати для узагальнення результатів за окремими об’єктами або їх групами (наприклад, енергетика, телекомунікації, державний сектор). Подібну методику галузевого рівня використовує Verizon DBIR при побудові індексів економічного ефекту [208].

Емпірична перевірка запропонованої моделі кіберстійкості здійснювалася у 2023–2025 рр. на основі даних підприємств критичної інфраструктури Одеської області. Оцінювався вплив навчальних програм трьох типів – базової кіберобізнаності (A), управлінських тренінгів (B) і технічних курсів (C) – на показники ризику, економічну віддачу та інтегральну ефективність P у реальних умовах.

Дизайном дослідження став кластеризований stepped-wedge із трьома хвилями інтервенцій, що охопили енергетичний, телекомунікаційний і державний сектори. Кожен кластер включав два підприємства й дозволяв здійснювати як міжчасові (T_0–T_1–T_2–T_3), так і міжкластерні порівняння. Загалом у програмі взяли участь 382 особи (55% – енергетика, 25% – телекомунікації, 20% – держсектор). Навчальні пакети реалізовувалися послідовно:

1. A (Mass Awareness) – онлайн-курс кібергігієни тривалістю 6 годин;

2. B (Managerial Training) – семінари з ризик-менеджменту та управління інцидентами (8 годин);

3. C (Technical Courses) – 24-годинний практикум із роботи SOC, SIEM і інструментів реагування.

Горизонт спостереження – 18 місяців (листопад 2023 – травень 2025 рр.). Для кожного етапу проводилися контрольні вимірювання технічної ефективності $P_{te}c_h$, організаційного потенціалу I, кадрової синергії S та розрахунок ROSI. Дані отримувалися через SOC-журнали, анкетування та інтегровані панелі Microsoft Sentinel.

В дослідженні застосовувалися міжнародні стандарти ISO 31000 для кількісної оцінки ризиків та калібрування параметрів моделі (частота інцидентів, збитки, час реагування) через стандартизовані методи, такі як матриці ризиків, що корелює зі зниженням очікуваних втрат і визначенням «зони виправданого інвестування», а також NIST Cybersecurity Framework, як інструмент для секторальних пріоритетів, де функція «відновлення» дозволяє моделювати пост-інцидентну стійкість.

Як наслідок, зокрема, з’явилася можливість кількісно оцінити ефект навчальних програм на динаміку S і ROSI у секторальному розрізі. Проведені розрахунки підтвердили спадну віддачу технічних інвестицій після певного порогу $z_{te}c_h$ та зростання ролі організаційно-кадрових чинників. Найвищу економічну ефективність продемонстрували базові програми кіберобізнаності (A), середній ROSI яких перевищив 200% при строку окупності 0,3–0,5 року; управлінські тренінги (B) дали 150–180%; технічні курси (C) 60–80%, але забезпечили довгострокове підвищення точності виявлення інцидентів.

Для оцінювання ефективності інвестицій у кіберзахист використано параметричну модель, у межах якої ключовим параметром є коефіцієнт зниження ризику Δ, що характеризує ефективність відповідних заходів кібербезпеки та визначає частку очікуваних втрат, якої вдається уникнути внаслідок їхньої реалізації. На основі цього коефіцієнта визначається обсяг

уникнених втрат, чистий економічний ефект, рентабельність інвестицій, а також термін їхньої окупності.

Такий підхід дозволяє кількісно оцінити економічну доцільність інвестицій у кіберзахист та порівняти ефективність різних напрямів інвестування. Результати відповідних розрахунків наведено у таблиці 3.4.

Таблиця 3.4

Порівняльна оцінка економічного ефекту від управлінських та технічних заходів

Сфера	EAL, тис. грн	Δ	C, тис. грн	AL, тис. грн	NE, тис. грн	ROSI, %	PB, років
Енергетика (управлінський персонал)	3 000	0,20	180	600	420	233	0,30
Енергетика (технічний персонал)	2 200	0,18	250	396	146	58	0,63
Енергетика (інші співробітники)	1 200	0,25	80	300	220	275	0,27
Телекомунікації (управлінський персонал)	1 800	0,18	150	324	174	116	0,46
Телекомунікації (технічний персонал)	1 500	0,15	200	225	25	12,5	0,89
Телекомунікації (інші співробітники)	900	0,22	70	198	128	183	0,35
Державний сектор (управлінський персонал)	1 000	0,15	100	150	50	50	0,67
Державний сектор (технічний персонал)	800	0,15	120	120	0	0	1,00
Державний сектор (інші співробітники)	600	0,20	50	120	70	140	0,42

Джерело: *розраховано автором на основі даних [151, 208, 214].*

Примітка: EAL – очікувані середньорічні втрати; Δ – відносне зниження ризику; C – витрати на реалізацію заходів; AL – уникнені втрати; NE – чистий економічний ефект; ROSI – рентабельність інвестицій у безпеку; RB – коефіцієнт зниження ризику.

Аналіз отриманих результатів свідчить, що ефективність інвестицій у кіберзахист істотно залежить від напряму інвестування та галузевої специфіки. Найвищі значення рентабельності інвестицій спостерігаються у випадку організаційно-управлінських заходів та заходів розвитку кіберобізнаності персоналу, що підтверджує визначальну роль людського чинника у забезпеченні кіберстійкості.

Водночас технічні заходи характеризуються більшими початковими інвестиціями та довшим строком окупності. Отримані результати підтверджують доцільність комплексного підходу до управління кібербезпекою, що передбачає поєднання технічних, організаційних та кадрових заходів з метою максимізації економічного ефекту та підвищення рівня кіберстійкості системи. Крім того, емпіричні оцінки узгоджуються з результатами економіко-математичного моделювання, наведеного у попередніх підрозділах, та підтверджують наявність ефекту комплементарності між різними напрямами інвестування у кіберзахист.

Середній рівень рентабельності інвестицій у базові програми кіберобізнаності перевищує 200%, а термін окупності становить менше 6 місяців, що підтверджує перевагу управлінських заходів над суто технічними інвестиціями на зрілих етапах розвитку систем кіберзахисту.

Згідно зі звітом IBM Security. Cost of a Data Breach Report 2025, середня частка інцидентів, спричинених людським фактором, становить 74%, а середнє скорочення збитків у бізнес-структур, які впровадили програми підвищення кіберобізнаності, досягає 1,49 млн дол. США на рік [151]. Подібні результати наводить World Economic Forum. Global Cybersecurity Outlook 2025, де підкреслено, що кожен долар, інвестований у підготовку персоналу, знижує середню тривалість реагування на інцидент на 28% і окупається менш ніж за 6 місяців [214]. За даними IBM Cost of a Data Breach Report 2025, лише близько 26% інцидентів мають людський фактор як первинну причину – Root Cause, проте частка інцидентів із залученням людського елемента на будь-якому етапі становить понад 70 %. Таким чином, використане в моделі значення 74 %

відповідає узагальненій оцінці рівня Human Involvement, а не лише показнику root cause [151].

В енергетичному секторі найефективнішими виявились базові програми кіберобізнаності для лінійного персоналу, які охоплювали фішинг-тестування, короткі онлайн-курси та внутрішні симуляції кризових сценаріїв. За результатами узагальнених розрахунків, виконаних на основі даних Verizon. Data Breach Investigations Report 2025 [208] та IBM Security [151], середній показник ROSI для таких програм становить близько 275%, а термін окупності інвестицій складає 3-4 місяці. При цьому прямий економічний ефект проявляється у зменшенні людських інцидентів на 50 % та скороченні часу реагування на 25–30%. Енергетичні компанії, які впровадили комбіновані програми (технічні + поведінкові тренінги), отримали додатковий ефект підвищення точності виявлення аномалій на 15–20%. Це повністю корелює з висновками SANS Institute. Security Awareness Report 2025, який визначає, що основні переваги навчання полягають не стільки у знаннях, скільки у зміні поведінкових патернів співробітників [186].

Сукупний аналіз свідчить, що найвищий економічний ефект мають базові освітні ініціативи з кібергігієни, які охоплюють майже увесь контингент працівників. Середній ROSI таких програм перевищує 200%, а строк окупності становить 0,3–0,5 року, що узгоджується з аналітичними висновками World Economic Forum [214]. Управлінські тренінги дають 150–180 % ефекту завдяки зменшенню часу реагування та кращій координації команд, тоді як технічні курси, хоч і мають нижчу короткострокову віддачу (до 60%), формують довгострокову основу для підвищення точності виявлення інцидентів та стійкості IT-інфраструктури.

З метою деталізації впливу людського чинника на економічну ефективність заходів кіберзахисту здійснено порівняльний аналіз навчальних програм за галузями та категоріями персоналу. Розрахунок показників ефективності виконано на основі економіко-математичної моделі, наведеної у таблиці 3.4, із використанням параметра зниження ризику Δ, що відображає

частку очікуваних втрат, якої вдається уникнути внаслідок реалізації відповідного навчального заходу. На основі вказаного параметра визначено обсяг уникнених втрат, чистий економічний ефект, рентабельність інвестицій та строк їх окупності. Результати розрахунків наведено у таблиці 3.5.

Таблиця 3.5

Порівняльна ефективність навчальних заходів за галузями та категоріями персоналу

Галузь	Категорія персоналу	Тип навчальних заходів	Середній ROSI, %	Термін окупності, років	Найбільший ефект за показником
Енергетика	Управлінський	Кризові симуляції, семінари з ризик-менеджменту	233	0,30	Зменшення часу реагування на 25-30 %
Енергетика	Технічний	Курси з безпечного коду, IDS/IPS моніторинг	58	0,63	Поліпшення точності виявлення інцидентів
Енергетика	Інші	Програми кіберобізнаності, фішинг-тестування	275	0,27	Зменшення людських інцидентів на 50 %
Телекомунікації	Управлінський	Семінари з управління ризиками	116	0,46	Підвищення узгодженості рішень
Телекомунікації	Технічний	Хмарна безпека, мережевий моніторинг	12,5	0,89	Висока вартість, низька віддача
Телекомунікації	Інші	Онлайн-курси з кібергігієни	183	0,35	Скорочення фішингу на 35-40 %
Державний сектор	Управлінський	Тренінги NIST CSF 2.0	50	0,67	Скорочення часу прийняття рішень
Державний сектор	Технічний	Курси з аудиту та адміністрування	0	1,00	Ефект переважно репутаційний
Державний сектор	Інші	Курс з цифрової грамотності	140	0,42	Скорочення інцидентів на 30 %

Джерело: *розраховано автором за [208, 172]*

Аналіз результатів, наведених у таблиці 3.5, свідчить про суттєву диференціацію економічної ефективності навчальних заходів. Так, найвищу рентабельність інвестицій у навчання демонструють базові програми

кіберобізнаності (ROSI понад 200%). Їхня вартість є найнижчою, а ефект – безпосереднім, оскільки усуває найпоширеніші людські помилки. Усі три галузі підтверджують, що людський чинник є домінантним джерелом ризику, але водночас – основним резервом підвищення стійкості.

Наведені значення ROSI є результатом узагальнених авторських розрахунків за методологією, запропонованою у звітах IBM 2025, SANS 2025, і мають ілюстративний характер. Офіційні звіти не містять універсальних констант ROSI, проте підтверджують тенденцію зростання ефективності інвестицій у навчальні програми з кібербезпеки.

Управлінські тренінги мають стабільну ефективність (ROSI ≈ 150–200%), створюючи мультиплікативний ефект через підвищення готовності до кризових ситуацій і зменшення середнього часу реагування на інциденти. Для технічного персоналу ефект проявляється повільніше, але формує довгострокову базу безпеки.

Таким чином, оптимальна структура інвестицій у навчальні програми для персоналу об’єктів критичної інфраструктури повинна мати таке співвідношення: 40% – базові програми; 35% – управлінські тренінги, 25% – технічні тренінги**.** Вказана структура здатна забезпечити максимальне зростання показника кіберстійкості.

Позитивний вплив від впровадження запропонованих рішень проявлятиметься через посилення ролі людського чинника, чому сприятиме підготовка персоналу, розвиток організаційної культури безпеки та оптимізація процесів управління. Подальше посилення цифровізації може призвести до формування нової HR-моделі, де за допомогою ШІ буде провадитися об’єктивна оцінка кіберграмотності персоналу, моделювання впливу людського чинника при аналізі ризиків та персоналізоване навчання окремих категорій персоналу через симуляції атак.

Все це безпосередньо відповідає соціальному компоненту ESG (Environmental, Social, Governance), спрямованому на захист стейкхолдерів, включно з працівниками, громадами та суспільством в цілому. Тобто

запропоновані заходи сприяють ефективному розподілу ресурсів, зниженню ризиків для навколишнього середовища та вдосконаленню корпоративного управління шляхом впровадження прозорих, інноваційних механізмів прийняття рішень.

Відтак результати дослідження набувають ширшої релевантності, виходячи за межі вузької сфери кібербезпеки та вносячи вклад у глобальну дискусію про сталий розвиток, де кіберстійкість критичної інфраструктури стає елементом забезпечення соціальної справедливості, економічної стабільності та захисту прав людини в цифрову еру. Акцентування на цих аспектах підкреслює актуальність дослідження в контексті міжнародних стандартів, таких як Цілі сталого розвитку ООН, та дозволяє позиціонувати запропоновані рішення як інструмент для досягнення комплексної стійкості суспільства до гібридних загроз.

Висновки до 3-го розділу

1. Задля досягнення максимальної ефективності управління кіберзахистом критичної інфраструктури в її діяльність доцільно імплементувати механізми менеджменту кібербезпеки, що є цілеспрямованим процесом розробки та впровадження комплексу організаційних і технічних заходів. Вказані заходи спрямовані на забезпечення сталого функціонування життєво важливих об’єктів та їхній захист від актуальних і потенційних кіберзагроз. Фундаментальним елементом кіберзахисту, окрім застосування передових технологій, визначено персонал об’єктів критичної інфраструктури: управлінців, технічних фахівців та інших співробітників, що мають доступ до інформаційних систем. Інноваційний підхід в управлінні для кожної категорії передбачає розробку індивідуалізованих навчальних програм, які враховують специфіку функціональних ролей, рівень асоційованих ризиків і конкретні потреби об’єкта. Додатковий синергетичний ефект у процесі управління кіберзахистом досягається через забезпечення командної взаємодії. Організаційне забезпечення необхідних управлінських трансформацій передбачає створення в Україні кластеру кібербезпеки.

2. Серед технологічних інновацій, рекомендованих до інтеграції у процеси управління захистом критичної інфраструктури (зокрема, її енергетичного сегмента), пріоритетним є застосування інструментів штучного інтелекту. Рівень готовності підприємств енергетичної галузі до цієї інтеграції визначено за допомогою алгоритму графоаналітичного методу оцінки потенціалу підприємства «Квадрат потенціалу». Впровадження управлінських інновацій має здійснюватися в контексті децентралізації енергетики, що передбачає перехід від централізованих систем до формування локальних енергетичних осередків, керованих на рівні територіальних громад. Зокрема, це стосується мікросмартгрідів – інноваційної моделі локальної енергетичної інфраструктури, яка об'єднує розподілену генерацію, системи накопичення енергії та інтелектуальні технології управління. Запропонований підхід до управління кіберзахистом енергетичної інфраструктури на рівні громад із використанням

інструментів ШІ дозволить не лише автоматизувати окремі операційні процеси, а й суттєво переосмислити роль менеджменту у вирішенні завдань кібербезпеки. Кінцевим результатом такої імплементації стане створення ефективного, адаптивного та прозорого механізму прийняття управлінських рішень, що інтегрує людський досвід та можливості аналітичних алгоритмів через систему контролінгу.

3. Запропонована економіко-математична модель забезпечує опис взаємозв'язку між технічними, організаційними та кадровими компонентами системи кіберзахисту. У рамках такої моделі модифікована функція кіберстійкості відображає інтегральний вплив управлінських інновацій на здатність організації ефективно протидіяти кіберзагрозам. Такий методологічний підхід дозволяє здійснити кількісну оцінку внеску людського чинника та організаційних процесів у загальний рівень стійкості, який раніше характеризувався недостатньою формалізацією. Управлінські інновації, орієнтовані на формування та розвиток культури інформаційної безпеки, генерують мультиплікативний ефект: підвищення рівня компетентності персоналу знижує потребу в додаткових технічних інвестиціях і водночас підвищує ефективність застосованих технологічних рішень. Результати економіко-математичного моделювання підтверджують доцільність переорієнтації акцентів державної політики та корпоративних стратегій кіберзахисту в бік інвестування в кадрові й організаційні ініціативи. Це, зі свого боку, дає змогу підвищити інтегральний рівень кіберстійкості без пропорційного зростання фінансових витрат і створює надійну основу для подальшого використання розробленої моделі у прогнозних сценаріях та практичних проєктах.

ВИСНОВКИ

1. Науковий фундамент вирішення проблем безпеки інтегрує положення теорії систем, кібернетики, менеджменту, права, економіки та інформаційних технологій, формуючи основу для всебічного аналізу загроз і створення ефективних механізмів їхньої нейтралізації. Він ґрунтується на закономірностях функціонування складних соціально-економічних і технічних систем, методах управління ризиками, принципах стійкості та адаптивності, що дає змогу забезпечувати збалансоване поєднання превентивних, реактивних і відновлювальних заходів для гарантування безпеки на всіх рівнях – від індивідуального до державного. У межах цього фундаменту управлінські інновації дозволяють підвищити ефективність використання людського капіталу, створюють сприятливі умови для розробки та поширення технологічних інновацій, скорочують час реагування й формують більш гнучку систему протидії загрозам. При цьому впровадження таких рішень потребує не тільки фінансових ресурсів, а й організаційної готовності до змін: гнучкої структури управління, відкритості до експериментів, пілотних проєктів та співпраці з науковими установами та бізнес-структурами.

2. Сучасна критична інфраструктура охоплює не тільки енергетичні системи, транспортні вузли та об’єкти водопостачання, а й складні цифрові мережі, які ними керують. У добу цифрової трансформації майже всі процеси життєзабезпечення суспільства спираються на інформаційні технології: від автоматизованих систем управління на електростанціях до мереж сенсорів у комунальному господарстві міста. Цифровізація водночас значно підвищує ефективність роботи критичної інфраструктури, але робить її вкрай вразливою до кіберзагроз. У разі успішної кібератаки зловмисники отримують можливість впливати не лише на інформацію, а й на реальні фізичні процеси: зупинення виробництва, виведення з ладу енергомереж чи компрометація систем водопостачання здатні спричинити катастрофічні наслідки для економіки та національної безпеки держави.

3. Поточний рівень кіберзагроз критичній інфраструктурі України потребує системних і комплексних трансформацій управлінських систем, а також ухвалення національних стратегій захисту критичної інфраструктури, забезпечення її стійкості та ефективного функціонування. Особливу роль у вдосконаленні управлінських процесів відіграють інновації, зокрема впровадження автоматизованих систем управління інцидентами, технологій штучного інтелекту, адаптивних механізмів захисту та блокчейн-технологій для верифікації цілісності даних. У довгостроковій перспективі вдосконалення організаційно-управлінських механізмів має базуватися на ключових стратегічних принципах: системності, інтегрованості, багаторівневого управління, прозорості й адаптивності. Саме ці принципи дадуть змогу сформувати стійку до загроз модель, яка не лише реагуватиме на інциденти, а й проактивно протидіятиме кіберризикам. Особливо важливо інтегрувати зазначені підходи в загальну архітектуру національної безпеки, щоб кіберзахист не сприймався як ізольована сфера, а став невід'ємною складовою сучасного державного управління та ключовою умовою сталого розвитку країни.

4. Ефективний захист критичної інфраструктури України від кіберзагроз вимагає наявності нормативно-правової бази та застосування сучасних технологічних інструментів. До нормативно-правового забезпечення належать «Стратегія кібербезпеки України», Закони України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про національну безпеку України», а також низка спеціалізованих постанов Кабінету Міністрів України. Не менш важливим є впровадження міжнародних стандартів, таких як ISO/IEC 27001, ISO/IEC 27002 та NIST Cybersecurity Framework. Використання технологічних інструментів базується на підходах Zero Trust Architecture, Defense-in-Depth та Cyber Threat Intelligence. При цьому в управлінських процесах акцент поступово зміщується від традиційного кіберзахисту до концепції кіберстійкості, яка передбачає здатність не тільки запобігати кібератакам, а й оперативно відновлюватися після них.

5. Глобальний ринок продуктів і послуг кібербезпеки (обсяг якого у 2024 році становив 245,6 млрд дол. США) останніми роками перейшов до фази стабільного зростання переважно під впливом технологічних факторів, зокрема стрімкого розвитку штучного інтелекту. Водночас український ринок розвивається як завдяки реалізації внутрішнього потенціалу для забезпечення кіберзахисту вітчизняних підприємств та організацій, так і на основі накопиченого досвіду протидії кібератакам в умовах гібридної війни, а також можливостей експорту готових рішень. Проведений методом найменших квадратів аналіз ринку став основою для кон'юнктурного прогнозу з високим рівнем достовірності (коефіцієнт детермінації $R^2 = 0{,}9821$), згідно з яким найбільшого значення у 167,7 млн дол. США обсяг ринку досягне у 2027 році. Цей прогноз також було верифіковано за допомогою методу експоненційного згладжування.

6. Проведене розширення моделі Гордона-Льоба на двоканальне інвестування (технічне та організаційно-управлінське) продемонструвало, що ефективність захисних заходів значною мірою залежить від їхньої комплементарності. Жоден із цих напрямів не є самодостатнім: порушення балансу веде до швидкого падіння граничної віддачі від додаткових інвестицій. Використання виробничої функції Кобба-Дугласа дозволило кількісно змоделювати взаємодію між технічними та організаційно-управлінськими заходами. Така специфікація дає змогу визначати оптимальне співвідношення витрат з урахуванням як їхнього абсолютного обсягу, так і еластичності впливу кожного каналу на загальний рівень безпеки. Запроваджено поняття «точки плато» – моменту, коли додаткові інвестиції в один канал стають економічно неефективними без відповідного зростання вкладень в інший. Це підкреслює необхідність гнучкого перерозподілу ресурсів і недопущення концентрації витрат виключно в одному напрямі. Застосування розширеної моделі не тільки формалізує процес прийняття інвестиційних рішень, а й надає менеджменту практичні рекомендації щодо визначення меж доцільних витрат, вибору

оптимальної структури інвестицій та створення прикладних сценаріїв на основі реальних емпіричних даних.

7. Задля максимізації ефективності управління кіберзахистом критичної інфраструктури воно має здійснюватися на основі менеджменту кібербезпеки – цілеспрямованого процесу розробки та впровадження комплексу організаційних і технічних заходів, спрямованих на забезпечення сталого й безпечного функціонування життєво важливих об’єктів, а також їхнього захисту від актуальних і потенційних кіберзагроз. Основою кіберзахисту поряд із застосуванням сучасних технологій має стати персонал об’єктів критичної інфраструктури. Пропонується поділити його на три групи: управлінський персонал, технічних фахівців та інших співробітників, які мають доступ до інформаційних систем. Для кожної з цих груп доцільно розробляти індивідуальні програми навчання, що враховують специфіку ролей, рівень пов’язаних ризиків і потреби конкретного об’єкта. Додатковий синергетичний ефект забезпечуватиме командна взаємодія в процесі управління кіберзахистом. Організаційне забезпечення управлінських трансформацій передбачає створення в Україні кластера кібербезпеки під егідою координаційного хабу, до складу якого мають увійти представники РНБО, Держспецзв’язку, Міністерства цифрової трансформації, наукової спільноти, профільних бізнес-структур та інших зацікавлених сторін.

8. Серед технологічних інновацій, які доцільно інтегрувати в процеси управління захистом критичної інфраструктури (зокрема її енергетичної складової), обрано інструменти штучного інтелекту. За допомогою алгоритму графоаналітичного методу оцінки потенціалу підприємства «Квадрат потенціалу» визначено рівень готовності підприємств енергетичної сфери до такої інтеграції. Впровадження управлінських інновацій має відбуватися в межах процесу децентралізації енергетики, який передбачає перехід від централізованих систем до локальних енергетичних осередків, керованих на рівні територіальних громад. Йдеться, зокрема, про мікросмартгріди — інноваційну модель локальної енергетичної інфраструктури, що поєднує

розподілену генерацію, системи накопичення енергії та інтелектуальні технології управління. Запропонований підхід до управління кіберзахистом енергетичної інфраструктури на рівні громад із використанням інструментів ШІ дасть змогу не лише автоматизувати окремі процеси, а й переосмислити роль менеджменту в розв’язанні завдань кібербезпеки. Кінцевим результатом стане створення ефективного, адаптивного та прозорого механізму прийняття управлінських рішень, який поєднує людський досвід і можливості аналітичних алгоритмів через систему контролінгу.

9. Запропонована економіко-математична модель описує взаємозв’язок між технічними, організаційними та кадровими складовими системи кіберзахисту. У межах цієї моделі модифікована функція кіберстійкості відображає інтегральний вплив управлінських інновацій на здатність організації протидіяти кіберзагрозам. Такий підхід дає змогу кількісно оцінювати внесок людського чинника та організаційних процесів у загальний рівень стійкості, що раніше залишалося недостатньо формалізованим. Управлінські інновації, спрямовані на розвиток культури інформаційної безпеки, створюють мультиплікативний ефект: зростання компетентності персоналу зменшує потребу в додаткових технічних інвестиціях і одночасно підвищує ефективність уже впроваджених технологічних рішень. Результати економіко-математичного моделювання підтверджують доцільність зміщення акцентів державної політики та корпоративних стратегій кіберзахисту в бік інвестування в кадрові й організаційні ініціативи. Це дозволяє підвищити інтегральний рівень кіберстійкості без пропорційного зростання витрат і створює основу для подальшого використання розробленої моделі в прогнозних сценаріях та практичних проєктах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абібулаєв А. Р., Піскозуб А. З. Аналіз можливостей покращення стану безпеки хмарної інфраструктури за допомогою NLP та ML. *Сучасний захист інформації. 2025*. № 2. С. 124-140. DOI: 10.31673/2409-7292.2025.026884.

2. Августин Р. Р., Деміків І. О. Управлінські інновації як чинник підвищення конкурентоспроможності підприємств. *Ефективна економіка*. 2020. № 4. DOI: https://doi.org/10.32702/2307-2105-2020.4.14.

3. Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. Forbes.ua. 2023. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення: 10.03.2026).

4. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47-59. DOI: https://doi.org/10.31617/2.2022(43)04.

5. Близнюкова І. О., Тесленко П. О., Малахова Д. О. Особливості формування команди управління ІТ-проєктом. *Вісник Національного технічного університету «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами*. 2022. № 2(6). С. 14-20. DOI: https://doi.org/10.20998/2413-3000.2022.6.3.

6. Богдан Б. В. Вплив цифровізації критичної інфраструктури на економічну стійкість держави: виклики та можливості. *Право та державне управління*. 2024. С. 546-551. DOI: https://doi.org/10.32782/pdu.2024.4.75.

7. Божанова О., Грицина О. Управлінські інновації: сутність, види, класифікація та етапи впровадження. *Аграрна економіка.* 2021. Т. 14, № 1-2. С. 43-49. DOI: https://doi.org/10.31734/agrarecon2021.01-02.043.

8. В Україні завершили перехід ЗСУ на корпусну систему. Рубрика. URL: https://rubryka.com/2025/10/01/perehid-zsu-na-korpusnu-systemu/ (дата звернення: 10.03.2026).

9. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення : монографія. Львів : Арал, 2008. 384 с.

10. Величко В. EnergyTech для України: як сучасні технології можуть допомогти побудувати захищену та сучасну енергосистему ProIT. 2024. URL: https://proit.ua/energytech-dlia-ukrayini-iak-suchasni-tiekhnologhiyi-mozhut-dopomoghti-pobuduvati-zakhishchienu-ta-suchasnu-ienierghosistiemu/ (дата звернення: 10.03.2026).

11. Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни : дис. ... д-ра юрид. наук : 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Одеський держ. ун-т внутр. справ. – Одеса, 2021. 500 с.

12. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. *Цифрова трансформація кібербезпеки*: наук.-практ. інтернет-конф., м. Київ, 20 квітн. 2022 р. Державний університет телекомунікацій Навчальнонаукового інституту захисту інформації. Київ. 2022. С. 31-33.

13. Газдайка-Васильшин І. Б. Основні терміни проекту Закону України «Про критичну інфраструктуру та її захист». *Право і суспільство*. 2019. № 9. С. 15-20.

14. Гайдученко А. В. Економічні аспекти цифрової трансформації: інноваційні технології безпеки та автоматизації в ІТ-індустрії. *Здобутки економіки: перспективи та інновації*. 2025. № 19. DOI: https://doi.org/10.5281/zenodo.15747486.

15. Гончаренко Г. А. Управління сектором безпеки: поняття й сутність. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: юридичні науки. 2020. Том 31 (70) Ч. 2 № 2. С. 40-46. DOI https://doi.org/10.32838/2707-0581/2020.2-2/08.

16. Гончарук О. В., Бузовська Г. О. Методичні положення графоаналітичної оцінки економічного потенціалу підприємства. *Глобальні та національні проблеми економіки*. 2016. № 10. С. 302-307.

17. Горбаченко С. А. Місце менеджменту кібербезпеки у сучасній управлінській науці та практиці. *Сталий розвиток економік*и. 2024. № 1(48). С. 144-149. DOI: https://doi.org/10.32782/2308-1988/2024-48-19.

18. Горбаченко С. А. Особливості рекламних кампаній продуктів та послуг у сфері кібербезпеки. *Конкурентоспроможна модель інноваційного розвитку економіки України*: матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 7-8 листоп. 2024 р. Кропивницький. 2024. С. 52-54.

19. Горбаченко С. А. Перспективи використання командних форм управління у морегосподарському комплексі. *International Scientific Conference (Warsaw, March 22-23, 2018).* Warsaw: BMT Eridia Sp. Wydawnictwo Erida, 2018. PP. 348-351.

20. Горбаченко С. А. Управлінські інновації як економічна категорія. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*: міжнар. наук. Інтернет-конф., м. Тернопіль, 13 вересн. 2019 р. Тернопіль. Одеського національного університету імені І. І. Мечникова. 2019. № 41. С. 52-54.

21. Горбаченко С. А. Управлінські передумови інноваційно-інвестиційного розвитку морегосподарського комплексу України : монографія. Одеса : Фенікс, 2019. 314 с.

22. Горбаченко С. А., Саврацький О. О. Transformation of the innovative component of management processes in the context of digitalization. *Приазовський економічний вісник.* 2025. № 2(42). DOI: https://doi.org/10.32782/2522-4263/2025-3-11.

23. Гречанінов В. Моделі та технології інтелектуального захисту інформаційних систем критичної інфраструктури для підвищення стійкості. *Кібербезпека: освіта, наука, техніка.* 2025. № 1(29). С. 877-896. DOI: https://doi.org/10.28925/2663-4023.2025.29.948.

24. Дацків Р. М. Економічна безпека держави в умовах глобальної конкуренції. Львів : Центр Європи, 2006. 160 с.

25. Делембовський М. М., Ткаченко В. А., Мельник Д. В. Навчання та сертифікація спеціалістів з кібербезпеки в Україні. *Grail of Science*. 2024. № 41. С. 282-286. DOI: http://dx.doi.org/10.36074/grail-of-science.05.07.2024.044.

26. Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації. URL: https://csi.cip.gov.ua/ (дата звернення: 08.09.2025).

27. Державний стандарт України 2293:2014 «Охорона праці. Терміни та визначення основних понять». Національний стандарт України, МінЕкономРозвитку України. 2015. URL: https://surl.li/xvxfeg (дата звернення: 08.09.2025).

28. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету міністрів України від 09.10.2020 р. № 1109. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (дата звернення: 08.03.2026).

29. Деякі питання паспортизації об'єктів критичної інфраструктури: Постанова КМУ від 04.08.2023 року № 818. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#n9 (дата звернення: 08.03.2026).

30. Діордіца І. В. Поняття та зміст кібершпигунства. *Наукові праці Національного університету "Одеська юридична академія"*. 2020. № 26. С. 49-55. DOI https://doi.org/10.32837/npnuola.v26i0.660.

31. Домарацький М. Б. Державне управління забезпеченням безпеки критичної інфраструктури в Україні : дис. … канд. наук з держ. упр. : 25.00.05 / Національний університет цивільного захисту України. Харків, 2022. 259 с.

32. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепцій «глибинного захисту». *Підприємництво і торгівля*. 2019. № 25. С. 116-121. DOI: https://doi.org/10.36477/2522-1256-2019-25-17.

33. Єрменчук О. П. Поняття критична інфраструктура. *Інформаційна безпека людини, суспільства, держави*. 2018. № 1. С. 20-28.

34. Завадський Й. С., Осовська Т. В., Юшкевич О. О. Економічний словник. Київ : Кондор, 2006. 355 с.

35. Заскока Ю. В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи*. 2021. № 9(15). С. 85-98. DOI: https://doi.org/10.52058/2708-7530-2021-9(15)-85-98.

36. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с.

37. Зянько В. В. Інноваційне підприємництво: сутність, механізми і форми розвитку: монографія. Вінниця: УНІВЕРСУМ-Вінниця, 2008. 397 с.

38. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ. 2023. № 7. 270 с.

39. Клименко Н. Г. Еволюція змісту концепту «безпека» за різних історичних епох та політичних систем. *Державне управління: удосконалення та розвиток.* 2019. DOI: http://dx.doi.org/10.32702/2307-2156-2019.8.20.

40. Кожедуб Ю. В. Концептуальна модель захисту інформації об'єктів критичної інформаційної інфраструктури України. *Information Technology and Security.* 2021. № 9(2). PP. 151–164. DOI: https://doi.org/10.20535/2411-1031.2021.9.2.249889.

41. Козачок В., Драпатий М. Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 2. №. 26. С. 374-391. DOI: https://doi.org/10.28925/2663-4023.2024.26.699.

42. Коломієць Б. С. Еволюція поняття безпеки: від класичних теорій до сучасних підходів. *Economics: time realities*. 2024. № 6(76). DOI: http://dx.doi.org/10.5281/zenodo.14549644.

43. Комаров М. Ю., Гончар С. Ф. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури. *Моделювання та інформаційні технології*. 2017. № 81. С. 12-19.

44. Компанія Osavul отримала три мільйони доларів інвестицій для впровадження технологій інформаційної безпеки в бізнес-сектор. Interfax

Україна. 2024. URL: https://interfax.com.ua/news/press-release/1013354.html (дата звернення: 08.03.2026).

45. Кому належить енергетична інфраструктура України. YouControl. URL: https://youcontrol.com.ua/data-research/komu-nalezhyt-enerhetychna-infrastruktura-ukrayiny/ (дата звернення: 15.03.2026).

46. Копитко М. І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств. Навчально-методичний посібник. Львів: Ліга-Прес, 2016. 172 с.

47. Корж І. Безпека: медотологічні підходи до поняття. *National law journal: teory and practice*. 2019. С. 68-72.

48. Король О. Г., Лаптєва Т. О. Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці Mitre Att&ck. *Сучасний захист інформації*. 2024. № 3. С. 69-74. DOI: https://doi.org/10.31673/2409-7292.2024.030007.

49. Корсун К. Кібербезпека, захист персональних даних і інтеграція України до Єдиного цифрового ринку ЄС. *European Media Platform*. 2021. С. 27-36. URL: https://eump.org/media/2021/Materialy.pdf (дата звернення: 15.02.2026).

50. Котелевець Д. О. Сутність інфраструктури та її вплив на розвиток економічних систем. *Науково-освітній інноваційний центр суспільних трансформацій*. 2022. С. 64-66.

51. Котлубай В. О., Рединa Є. В., Блатін С. Д. Напрями розвитку стартап-екосистеми в Україні. *Наукові інновації та передові технології*. 2024. № 6(34). С. 825-836. DOI: https://doi.org/10.52058/2786-5274-2024-6(34)-825-836

52. Краліч Є. Р. Штучний інтелект в інноваційному менеджменті: переваги та виклики. *Наукова весна 2025*: матеріали XV Міжнар. наук.-техн. конф. аспірант. та молод. вчен. НТУ»ДП». 2025. С. 241-242.

53. Криворучко О. М. Інтегрований підхід до удосконалення бізнес-процесів підприємства. *Економіка трансп. комплексу* : зб. наук. пр. М-во освіти і науки України, Харків. нац. автомоб.-дор. ун-т. Харків, 2018. № 32. С. 17-29. DOI: http://dx.doi.org/10.30977/ETK.2225-2304.2018.32.0.17.

54. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. № 44. С. 15-19. DOI: https://doi.org/10.32782/2524-0072/2022-44-21.

55. Лисенко С.М. Метод виявлення кібер-загроз на основі еволюційних алгоритмів. *Вісник Хмельницького національного університету. Технічні науки*. 2017. № 6. С. 81-88.

56. Лисецький Ю. М., Калбазов Д. Й. Підходи до забезпечення інформаційної безпеки. *Математичні машини і системи*. 2023. №4. С. 26-32.

57. Литюга Є., Яценко В. Перспективи розвитку хактивізму та хакерських атак в сфері фінансових послуг: виклики та шляхи протидії. *Виклики кібербезпеки індустрії фінансових послуг* : матеріали наук. онлайн-конф., м. Суми, 07 вересн. 2023. За загальною редакцією доц. Койбічук В.В. Суми : Сумський державний університет, 2023. С. 67-70.

58. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

59. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. Економіко-правові засади забезпечення захисту критичної інфраструктури. *Фінансово-кредитна діяльність: проблеми теорії і практики.* 2020. № 4. С. 426-438. DOI: https://doi.org/10.18371/fcaptp.v4i35.222453.

60. Мануїлов Я. С. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. № 1(44). С. 154-167. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287780.

61. Міністерство цифрової трансформації України. Офіційний веб-сайт. URL: https://thedigital.gov.ua/projects (дата звернення: 15.02.2026).

62. Музика В. В. До питання про відсутність поняття «критична інфраструктура» в міжнародному праві. 2021. С. 359-362. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/ed69690e-0042-4b0b-8440-298bcd1be77b/content (дата звернення: 15.02.2026).

63. Новик І. В. Менеджмент безпеки як невід'ємний складник інтегрованої системи менеджменту підприємства. *Економіка та управління підприємствами*. 2019. Т. 30. С. 191-196.

64. Огляд ринку кібербезпеки в Україні. DataDriven 2025. 43 с. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 21.02.2026).

65. Оніщенко С., Глушко А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Науковий журнал «Економіка і регіон».* 2022. №1(84). С. 13-20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540.

66. Осокіна А. В., Сергієнко Н. С. Управлінські інновації: сутність, різновиди, механізм розробки. *Молодий вчений*. 2017. № 10. С. 973–977. DOI: https://doi.org/10.31734/agrarecon2021.01-02.043.

67. Павук І. В., Кобилкін Д. С. Особливості формування концепції управління проєктними ризиками на об’єктах критичної інфраструктури. *Інновінг сучасних трендів в менеджменті безпеки* : матеріали всеукр. наук.-практ. конф., м. Львів. 26 травня 2023 року. Львів, 2023. С. 59-60.

68. Панченко В. Вплив військових дій на фінансову стійкість підприємства. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки*. 2024. № 1. С. 175-191. DOI: http://doi.org/10.34025/2310-8185-2024-1.93.13.

69. Полторак А. С., Сухорукова А. Л., Бурковська А. І. Кібербезпека в системі трансформації управління бізнес-організацією. *Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики* : колективна монографія/ за заг. ред. Сагайдака М. П., Соболєвої Т. О., 2021. С 158-176.

70. Пономарьов С.П. Поняття та сутність сектору безпеки. *Право.ua.* 2015. № 3. С. 69-72.

71. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури : Закон України від 26.09.2023 № 857. *Верховна Рада України.* № 23. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#n10 (дата звернення: 21.02.2026).

72. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : Закон України № 90/26535 від 28.01.2015 р. *Верховна Рада України*. 2024. URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text (дата звернення: 21.02.2026).

73. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : Постанова КМУ від 22.07.2022 р. № 821-2022-п. *Верховна Рада України*. 2023. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#n8 (дата звернення: 21.02.2026).

74. Про кластер. Національний Кластер Кібербезпеки. URL: https://cybersecuritycluster.org.ua/about/ (дата звернення: 25.01.2026).

75. Про критичну інфраструктуру : Закон України від 21.09.2024 р. № 1882-IX. *Відомості Верховної Ради.* 2024. № 52. Ст. 303.

76. Про національну безпеку України : Закон України від 24.01.2026 р. № 2469-VIII. *Відомості Верховної Ради.* 2026. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 21.02.2026).

77. Про основні засади забезпечення кібербезпеки України: Закон України від 19.10.2025 р. № 2163-VIII. *Відомості Верховної Ради.* 2025. № 35. Ст. 134.

78. Проблеми кон'юнктурних досліджень ринків товарів та послуг в Україні : монографія / під наук. кер. д.е.н., проф. Ковальова А.І. Одеса : Атлант, 2010. 266 с.

79. Прохорчук С. В. Функціонування інноваційного кластеру в регіоні. *Науковий вісник Ужгородського національного університету*. 2016. № 6(3). С. 12-15.

80. Рєпіна І. М. Підприємницький потенціал: методологія оцінки та управління. *Вісник Української академії державного управління при Президентові України*. 1998. №2. С. 262-271.

81. Саврацький О. О. Адаптація системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів. *Трансформаційна економіка*. 2024. №1(06). С. 53–57. DOI: https://doi.org/10.32782/2786-8141/2024-6-10.

82. Саврацький О. О. Аналіз кон'юнктури ринку продуктів та послуг кібербезпеки. *Науково-виробничий журнал «Бізнес-навігатор».* 2025. №1. С. 443-449. DOI: https://doi.org/10.32782/business-navigator.78-74.

83. Саврацький О. О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. *Актуальні питання економічних наук.* 2025. № 13. DOI: https://doi.org/10.5281/zenodo.16885042.

84. Саврацький О. О., Слатвінська В. М. Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень. *Наука і техніка сьогодні.* 2025. № 8 (49). С. 1704-1716. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716.

85. Саврацький О. О., Чепурна О. Є. Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних системах з урахуванням спадної віддачі інвестицій. *Успіхи і досягнення у науці*. 2026. № 1(23). С. 1305-1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317.

86. Сахарова О., Близнюк І. Виявлення та реагування на кіберінциденти і кібератаки як заходи запобігання кіберзлочинності. *Наука і правоохорона.* 2023. № 2(60). С. 220-231. DOI: https://doi.org/10.36486/np.2023.2(60).

87. Свердлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук.* 2022. №10. С.175-188. DOI: https://doi.org/10.31866/2616-7654.10.2022.269495.

88. Соколов А. В., Кілко В. В., Трофименко О. Г., Саврацький О. О. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об'єктах критичної інфраструктури. *Вісті вищих учбових закладів. Радіоелектроніка*. 2026. DOI: https://doi.org/10.20535/S0021347025040028.

89. Спеціалізована лабораторія «Кіберполігон». Факультет кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія». URL: https://www.fcit.od.ua/cyberpoligon/ (дата звернення: 21.02.2026).

90. Стратегія кібербезпеки України : Указ президента України від 15.08.2016 р. № 96/2016. *Офіційне інтернет-представництво Президента України.* URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 01.03.2026).

91. Стратегія кібербезпеки України : Указ президента України від 26.08.2021 р. № 44/2021. *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 01.03.2026).

92. Субач І., Власенко О. Інформаційні технології захисту баз даних від кібератак в інформаційних системах військового призначення. *Information Technology and Security.* 2022. № 10(2). С. 177-193. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270412.

93. Талеб. Н. Антикрихкість. Про (не)вразливе у реальному житті. Київ: Наш формат. 2021. 392 с.

94. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Херсон: Видавничий дім «Гельветика», 2020. 601 с.

95. Український Кластер Кібербезпеки. Офіційний веб-сайт. URL: https://www.cybercluster.org.ua/ (дата звернення: 03.12.2025).

96. Федонін О. С., Репіна І. М., Олексюк, О. І. Потенціал підприємства: формування та оцінка: навч. посібник. 2004. Київ: КНЕУ. 316 с.

97. Федорова А. М. Компаративний аналіз дефініції «безпека». *Інвестиції: практика та досвід*. 2018. № 11. С. 144–148.

98. Федосеєнко О. М. Керування та управління мікромережевими кластерами: розвиток та майбутні дослідження. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність.* 2023. № 2(7). С. 66-71. DOI: https://doi.org/10.20998/2224-0349.2023.02.02

99. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії*. 2021. № 3. С. 142-148.

100. Хитра О. В. Синергетичні аспекти створення та функціонування управлінської команди. *Науковий вісник Міжнародного гуманітарного університету.* Серія : Економіка і менеджмент. 2016. №18. С. 118-126.

101. Циганов В. В. Національна безпека України. / Нац. акад. внутр. справ України. Київ, 2004. 100 с.

102. Шевченко В. Дослідження та програмна реалізація системи доступу до хмарних сервісів з використанням технології PKI. *Збірник праць молодих науковців ЦНТУ.* Кропивницький. 2022. № 13. С. 206-219.

103. Штангрет А. М., Котляревський Я. В., Караїм М. М. Економічна безпека підприємства в умовах антикризового управління: концептуальне визначення та механізм забезпечення : монографія. Львів : Укр. акад. друкарства. 2012. 288 с.

104. Шумпетер Й. Теорія економічного розвитку: Дослідження прибутків, капіталу, кредиту, відсотка та економічного циклу / Пер. з англ. В. Старка. - Київ: Видавничий дім «Києво-Могилянська академія», 2011. 242 с.

105. Ящук В. І. Принципи проєктування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури. *Львівський державний університет безпеки життєдіяльності.* 2021. URL: http://surl.li/stkfad (дата звернення: 16.12.2025).

106. Adeniran I. A., Efunniyi C. P., Osundare O. S., Abhulimen A. O. Enhancing security and risk management with predictive analytics: A proactive approach. *International Journal of Management & Entrepreneurship Research*. 2024. № 04(01). PP. 32-40. DOI: https://doi.org/10.56781/ijsret.2024.4.1.0021.

107. Agyepong E. et al. A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security*. 2023. № 124. DOI: https://doi.org/10.1016/j.cose.2022.102959.

108. Ainslie S., Thompson D., Maynard S., Ahmad A. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security.* 2023. №132. DOI: https://doi.org/10.1016/j.cose.2023.103352.

109. Alberts C. J., Dorofee A. J. OCTAVE Method Implementation Guide Version 2.0. Volume 1: Introduction. № 1. 2001. DOI: http://dx.doi.org/10.21236/ADA634140

110. Alelyani S., GR H. K. Overview of cyberattack on saudi organizations. *Journal of Information Security and Cybercrimes Research.* 2018. № 1(1). С. 32-39. DOI: 10.26735/16587790.2018.004.

111. Almadani M. S., Alotaibi S., Alsobhi H., Hussain O. K., Hussain F. K. Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*. 2023. № 23. DOI: https://doi.org/10.1016/j.iot.2023.100844.

112. Alomari M. A., et al. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. *Energies.* 2025. № 18(1), 141. DOI: https://doi.org/10.3390/en18010141.

113. Analysis of security configuration for IDS/IPS. Trisolino A. Politecnico di Torino. 2023. 92 p.

114. Anderson R., Moore T. The Economics of Information Security. *Science*. 2006. № 314(5799). PP. 610-613. DOI: http://dx.doi.org/10.1126/science.1130992.

115. Balleste R. Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity. *Emory Corporate Governance and Accountability Review*. 2021. № 8(1). 24 p. URL: https://scholarlycommons.law.emory.edu/ecgar/vol8/iss1/1 (дата звернення: 06.12.2025).

116. Barik K. et al. RONSI: a framework for calculating return on network security investment. *Telecommunication Systems*. 2023. Т. 84. №. 4. PP. 533-548. DOI: https://doi.org/10.1007/s11235-023-01039-9.

117. Beerman J., Berent D., Falter Z., Bhunia S. A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW),* Bangalore, India. 2023. PP. 8-15. DOI: http://dx.doi.org/10.1109/CCGridW59191.2023.00017.

118. Billanes J. D., Jørgensen B. N., Ma Z. A Framework for Resilient Community Microgrids: Review of Operational Strategies and Performance Metrics. *Energies.* 2025. № 18(2). PP. 405-444. DOI: https://doi.org/10.3390/en18020405.

119. Birkinshaw J. How Management Innovation Happens. *MIT Sloan Management Review*. 2006. P. 302-324.

120. Black D. Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences. The International Institute for Strategic Studies. 2023. URL: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf (дата звернення: 21.12.2025).

121. Bordbari M. J., Nasiri F. Networked Microgrids: A Review on Configuration, Operation, and Control Strategies. *Energies.* 2024. № 17(3). PP. 715-743. DOI: https://doi.org/10.3390/en17030715.

122. Brittain J. S. Threading the Needle. The Center for Creative Leadership. 25 p. DOI: https://doi.org/10.35613/ccl.2025.2067.

123. Bronk C., Tikk-Ringas E. The cyber attack on Saudi Aramco. *Survival*. 2013. № 55(2). PP. 81-96. DOI: https://doi.org/10.1080/00396338.2013.784468.

124. Bunkovsky V., Ilichev I. Y. Theoretical Research of the Concepts Innovative Project and Competitiveness of an Innovative Project. *Advances in Economics, Business and Management Research*. 2018. № 47. PP. 12-15. URL: https://ssrn.com/abstract=3372854 (дата звернення: 05.02.2026).

125. Caballero A. Information security essentials for IT managers: protecting mission-critical systems. Chapter 1. Managing information security. *Elsevier.* 2013. PP. 1-46. URL: https://booksite.elsevier.com/samplechapters/9781597495332/02~Chapter_1.pdf (дата звернення: 05.02.2026).

126. Capano D. E. Throwback attack: Lessons from the Aurora vulnerability: A government-sponsored test a cyberattack's real-world physical damage reverberates today. See eight steps on how to mitigate risk of a cyberattack. *Control Engineering*. 2021. № 68(6). PP. 36-38.

127. Chowdhury R. H., Prince N. U., Abdullah S. M., Mim L. A. The role of predictive analytics in cybersecurity: Detecting and preventing threats. *World Journal of Advanced Research and Reviews*. 2024. № 23(02). PP. 1615-1623. DOI: https://doi.org/10.30574/wjarr.2024.23.2.2494.

128. Collins S., McCombie S. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*. 2012. № 7(1). PP. 80-91. DOI: https://doi.org/10.1080/18335330.2012.653198.

129. Critical Infrastructure Sector. CIPedia. URL: https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector#cite_note-54 (дата звернення: 17.11.2025).

130. Cyber and Information warfare in the Ukrainian conflict. CSS cyber defense project. Center for Security Studies (CSS), ETH Zürich. 2018. 54 p. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf (дата звернення: 17.11.2025).

131. Cyber Security Market (2025 - 2030). Grand View Research. 2025. URL: https://www.grandviewresearch.com/industry-analysis/cyber-security-market (дата звернення: 17.11.2025).

132. Cyber Security Market Size, Share, Competitive Landscape and Trend Analysis Report, by Component (Solution, Service), by Deployment Model (On-premise, Cloud), by Enterprise Size (Large Enterprises, Small and Medium-sized Enterprise), by Industry Vertical (IT and Telecom, Automotive, BFSI, Government, Healthcare, Energy and Utilities, Manufacturing, Retail, Others): Global Opportunity Analysis and Industry Forecast, 2023 – 2033. Allied Market Research. 2024. 300 p. URL: https://www.alliedmarketresearch.com/cyber-security-market (дата звернення: 17.02.2026).

133. Cyberaccelerator. Social Boost. 2023. URL: https://www.socialboost.ua/projects/cyberaccelerator (дата звернення: 17.02.2026).

134. Cybersecurity: market data & analysis. Statista Market Insights. 2023. URL: https://live.handelsblatt.com/wp-content/uploads/2023/10/study_id124913_cybersecurity-report.pdf (дата звернення: 17.02.2026).

135. Dawn S., et al. Integration of Renewable Energy in Microgrids and Smart Grids in Deregulated Power Systems: A Comparative Exploration. *Adv. Energy Sustainability Res.* 2024. №5. DOI: https://doi.org/10.1002/aesr.202400088.

136. Degtiareva O., Shyriaieva N., Kuklinova T. Artificial Intelligence Solutions for Cybersecurity in Energy Systems. *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense).* Naples, Italy. 2024. PP. 177-182. DOI: http://dx.doi.org/10.1109/TechDefense63521.2024.10863745.

137. Easttom C., Butler W. A Modified McCumber Cube as a Basis for a Taxonomy of Cyber Attacks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. Las Vegas, NV, USA. 2019. PP. 943-949. DOI: http://dx.doi.org/10.1109/CCWC.2019.8666559.

138. Fayi S. Y. A. What Petya/NotPetya ransomware is and what its remidiations are. *Information technology-new generations* : 15th international conference on information technology. Cham: Springer International Publishing. 2018. PP. 93-100. DOI: https://doi.org/10.1007/978-3-319-77028-4_15.

139. Felix A. Enhancing Digital Forensics Investigations Using AI Driven Anomaly Detection and Log Correlation: A Mixed Methods Approach. *International Journal of Future Engineering Innovations*. 2025. № 2. PP. 71-84. DOI: http://dx.doi.org/10.54660/IJFEI.2025.2.4.71-84.

140. Freg. J. Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments. *National Security Agency, Information Assurance Solutions Grou*p – STE 6737. URL: https://www.academia.edu/29548467/Defense_in_Depth (дата звернення: 17.02.2026).

141. German legislation. IT Security Acts of 2015 and 2021. Legal basis. URL: https://surl.li/msnsjw (дата звернення: 17.02.2026).

142. Ghazo A. T. A., Kumar R. Andvi: Automated network device and vulnerability identification in scada/ics by passive monitoring. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2024. № 54(4). PP. 2539-2550. DOI: http://dx.doi.org/10.1109/TSMC.2023.3345254.

143. González-Granadillo G., González-Zarzosa S., Diaz R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*. 2021. № 21(14). PP. 4759-4787. DOI: https://doi.org/10.3390/s21144759.

144. Gordon L. A., Loeb M. P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*. 2002. № 5(4). P. 438-457. DOI: https://doi.org/10.1145/581271.58127.

145. Gücüyener A. Understanding the vulnerabilities of critical energy infrastructure to cyber terrorism and threats: How to secure our energy systems. Strategic Cyber Defense. *IOS Press*. 2017. PP. 74-85. DOI: http://dx.doi.org/10.3233/978-1-61499-771-9-74.

146. Guduru S. AI-Driven Threat Hunting: Sigma Rules, Elastic EQL, and MITRE CAR Analytics in Splunk UBA. *Journal of Scientific and Engineering Research*. 2021. № 8(12). PP. 239-243.

147. Hamel G. The Why, What and How of Management Innovation. Harvard Business Review. 2006. 16 p.

148. Hausken K. Returns to information security investment: The effect of alternative breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*. 2006. № 8(5). P. 329-341. DOI: http://dx.doi.org/10.1007/s10796-006-9001-y.

149. Hausken K., Welburn J.W., Zhuang J. A Review of Attacker–Defender Games and Cyber Security. *Games*. 2024. № 15(4). PP. 28-55. DOI: https://doi.org/10.3390/g1504002.

150. Hunziker S. Modern Approaches to Balancing Risk and Reward. Enterprise Risk Management The second edition. Springer Gabler Wiesbaden. 2021. 236 p. DOI: https://doi.org/10.1007/978-3-658-33523-6.

151. IBM. Cost of a Data Breach Report 2024. Armonk, NY : IBM Security, 2024. URL: https://www.ibm.com/reports/data-breach (дата звернення: 13.09.2025).

152. Instruction Generale Interministerielle Relative a la securite des activites d'Imprortance vitale N°6600/SGDSN/PSE/PSN du 7 janvier 2014. Direction Protection et Sécurité de l'Etat N° NOR: PRMD1400503J. URL:

http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf (дата звернення: 13.09.2025).

153. ISO/IEC 27001:2022. ISO. Офіційний веб-сайт. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 13.09.2025).

154. ISO/IEC 27002:2022. ISO. Офіційний веб-сайт. URL: https://www.iso.org/ru/standard/75652.html (дата звернення: 13.09.2025).

155. Jena J. Building resilience against modern cyber threats the importance of bcp and dr strategies. *International journal of computer engineering & technology*. 2023. №14. PP. 279-292. DOI: https://doi.org/10.34218/IJCET_14_02_026.

156. Joshi C. et al. Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus expected utility theory. *Computers & Security*. 2025. T. 154. DOI: https://doi.org/10.1016/j.cose.2025.104450.

157. Khai V. Emerging trends in microgrids technology and prospects for their implementation in Ukraine. *Computational problems of electrical engineering.* 2024. №14(1). PP. 6-11. DOI: https://doi.org/10.23939/jcpee2024/01/006/.

158. Khan F. B., Asad A., Durad H., Mohsin S. M., Kazmi S. N. Dragonfly cyber threats: A case study of malware attacks targeting power grids. *Journal of Computing & Biomedical Informatics.* 2023. № 4(02). PP. 172-185. DOI: https://doi.org/10.56979/402/2023.

159. Kholimtaeva I., Shamshieva B. Analysis on Risk Management Methods and Tools. *2024 5th International Conference on Image Processing and Capsule Networks*. IEEE. 2024. PP. 276-279. DOI: http://dx.doi.org/10.1109/ICIPCN63822.2024.00052.

160. Kibik O., et al. Managing sustainable development projects through a risk-oriented framework. *International journal*. 2025. № 14. PP. 95-106. DOI: http://dx.doi.org/10.33844/ijol.2025.60462.

161. Kibik O. et al. Strategic vectors for enterprise development in the context of the digitalization of the economy. *Postmodern Openings*. 2022. № 13(2). PP. 384-395. DOI: https://doi.org/10.18662/po/13.2/460.

162. Kim S., Hwang C., Lee T. Anomaly Based Unknown Intrusion Detection in Endpoint Environments. *Electronics.* 2020. № 9(6). 1022. 19 p. DOI: https://doi.org/10.3390/electronics9061022.

163. Kinyua J., Awuah L. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing. 2021*. № 28(2). P. 527-545. DOI: http://dx.doi.org/10.32604/iasc.2021.016240.

164. Kitsoft Secures EU Grant to Build Cyber Defense Hub for Ukraine's Public Sector. Digital State UA. 2025. URL: https://digitalstate.gov.ua/news/govtech/kitsoft-zapuskaye-tsentr-kiberzakhystu-dlia-derzavnykh-saytiv (дата звернення: 13.09.2025).

165. Kobozeva A.A., Sokolov A.V. Efficient Coding of the Embedded Signal in Steganographic Systems with Multiple Access. *Problemele energeticii regionale.* 2021. № 2(50). P. 101-113. DOI: https://doi.org/10.52254/1857-0070.2021.2-50.09.

166. Kyiv international cyber resilience forum 2024. Resilience at the Cyber War. Офіційний веб-сайт. URL: https://cyberforumkyiv.org/2024/en/ (дата звернення: 12.02.2026).

167. Kyiv Polytechnic, USAID, and Partners Strengthen Ukraine's Cyber Resilience. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". URL: https://kpi.ua/en/2024-08-20 (дата звернення: 12.02.2026).

168. Less hype and more collaboration: how Barclays is exploring blockchain technology. Barclays. 2019. URL: https://home.barclays/news/2019/7/less-hype-and-more-collaboration--how-barclays-is-exploring-bloc (дата звернення: 12.02.2026).

169. Lysenko, S., Bobro N., Korsunova K., Vasylchyshyn O., Tatarchenko Y. The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*. 2024. № 69. PP. 43-51. DOI: http://dx.doi.org/10.46852/0424-2513.1.2024.6.

170. Mathumitha R., Rathika P., Manimala K. Intelligent deep learning techniques for energy consumption forecasting in smart buildings: a review. *Artif Intell Rev*. 2024. № 57(35). DOI: https://doi.org/10.1007/s10462-023-10660-8.

171. Moghaddam M. P., Nasiri S., Yousefian M. 5D giga trends in future power systems. Decentralized frameworks for future power systems. *Academic Press.* 2022. PP. 19-50. DOI: https://doi.org/10.1016/B978-0-323-91698-1.00015-7.

172. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. Gaithersburg : NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

173. Ning X., Jiang J. Defense-in-depth against insider attacks in cyber-physical systems. *Internet of Things and Cyber-Physical Systems*. 2022. № 2. PP. 203-211. DOI: https://doi.org/10.1016/j.iotcps.2022.12.001.

174. North D. C. Institutions, institutional change and economic performance. Cambridge university press. 1990. 152 p.

175. Núñez-Merino M., Maqueira-Marín H. M., Moyano-Fuentes J., Castaño-Moraga C. A. Quantum-inspired computing technology in operations and logistics management. *International Journal of Physical Distribution & Logistics Management.* 2024. № 54(3). PP. 247-274. DOI: https://doi.org/10.1108/IJPDLM-02-2023-0065.

176. Nurov A. Software development for rapid response to information security incidents. *Вісник науки*. 2025. Т. 1. №. 6 (87). PP. 1323-1332. DOI: 10.24412/2712-8849-2025-687-1323-1332.

177. Open Data Bot. Офіційний веб-сайт. URL: https://opendatabot.ua (дата звернення: 11.01.2026).

178. Overview of the 9 Distinct Data Wipers Used in the Ukraine War. Insikt Group. 2022. URL: https://go.recordedfuture.com/hubfs/reports/mtp-2022-0512.pdf (дата звернення: 12.02.2026).

179. Özker U. Critical Infrastructure and Cyber Security in Türkiye. Konrad-Adenauer-Stiftung Türkiye. 2022. URL: https://surl.li/iyjzsg (дата звернення: 12.03.2026).

180. Project Management in the Digital economy: Textbook. Britchenko I., Chukurna O., Tardaskina T., Gordeeva Y., Olvinska Y. Sofia: Professor Marin Drinov Publishing House of Bulgarian Academy of Sciences, 2025. 241 p.

181. PwC. Global Digital Trust Insights Survey 2023. PwC, 2023. URL: https://www.pwc.com/gx/en/services/consulting/cybersecurity/digital-trust-insights.html (дата звернення: 12.03.2026).

182. Reilly J., et al. FY2021 Isolated Grids and Grid-Connected Turbine Reference Systems. *National Renewable Energy Laboratory*. 2022. № INL/RPT-22-67108-Rev000. URL: https://docs.nrel.gov/docs/fy22osti/81792.pdf (дата звернення: 11.03.2026).

183. Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art / G.Giannopoulos, R.Filippini, M. Schimmer. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. 70 p.

184. Rosenstein-Rodan P. Notes on the Theory of the «Big Push». *Economic Development for Latin America.* 1961. № 4. PP. 57-81. DOI: https://doi.org/10.1007/978-1-349-08449-4_3.

185. Samuelson P. The pure theory of public expenditure. *Rev Econ Stat.* 1954. № 36(4). PP. 387–389. DOI: https://doi.org/10.2307/1925895.

186. SANS Institute. Security Awareness Report 2025. SANS Institute, 2025. URL: https://www.sans.org (дата звернення: 12.08.2025).

187. Secureworks. Boardroom Cybersecurity Report 2024. URL: https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024 (дата звернення: 12.08.2025).

188. Shkurak L. Ukrainian drone startup Swarmer secures nearly $50k grant from BRAVE1. AIN. 2024. URL: https://en.ain.ua/2024/08/27/ukrainian-drone-startup-swarmer-secures-nearly-50k-grant-from-brave1/ (дата звернення: 18.01.2026).

189. Simonenko M. Stuxnet and nuclear enrichment of the cyber security regime. *Security Index.* 2013. № 19(2). PP. 85-97. DOI: https://doi.org/10.1080/19934270.2013.779435.

190. Singh P. S., The Cyberwar Between Russia and Ukraine: Impacts and Implications. O.P. *Jindal Global University*. 2024. DOI: http://dx.doi.org/10.2139/ssrn.5019998.

191. Smart Nation 2.0 A Thriving Digital Future for All. Ministry of Digital Development and Information. 2024. URL: https://file.go.gov.sg/smartnation2-report.pdf (дата звернення: 12.03.2026).

192. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation.* 2021. № 11(3). P. 147-161. DOI: 10.15276/imms.v11.no3.147

193. Stafford V. Zero trust architecture. *NIST special publication*. 2020. №800 (207), 800-207. 50 p. DOI: https://doi.org/10.6028/NIST.SP.800-207.

194. Steen R., Haug O. J., Patriarca R. Business continuity and resilience management: A conceptual framework. *Journal of Contingencies and Crisis Management.* 2024. Т. 32. № 1. 13 p. DOI: https://doi.org/10.1111/1468-5973.12501.

195. Sullivan A., Sheffrin M. S. Economics: Principles in action. Upper Saddle River, New Jersey 07458: Pearson Prentice Hall. 2003. 474 p.

196. Support for Ukrainian tech SMEs and start-ups. European Commission. URL: https://eismea.ec.europa.eu/funding-opportunities/calls-proposals/support-ukrainian-tech-smes-and-start-ups_en (дата звернення: 21.01.2026).

197. Sustainability Summary. 2024. Southern Company Report. 2024. URL: https://www.southerncompany.com/content/dam/southerncompany/sustainability/pdfs/2024-sustainability-summary.pdf (дата звернення: 12.03.2026).

198. Tashatov N., Onarkulov M., Askarbekkizi A. Methods of analyzing and assessing information security risks. *Farg'ona davlat universiteti*. 2024. № 3. DOI: http://dx.doi.org/10.56292/SJFSU/vol30_iss3/a125.

199. Tech Behemoths. Офіційний веб-сайт. URL: https://techbehemoths.com/companies/cybersecurity/ukraine (дата звернення: 14.10.2025).

200. Tech ecosystem guide to Ukraine. 120 p. Unit City. URL: https://data.unit.city/tech-guide/Tech_Ecosystem_Guide_To_Ukraine_En-1.1.pdf (дата звернення: 12.03.2026).

201. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. The White house. Washington. 2003. 96 p.

202. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

203. The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector. International Centre for Defence and Security. 51 p. URL: https://icds.ee/wp-content/uploads/dlm_uploads/2025/05/ICDS_Report_The_Staying_Power_of_Ukrainian_Lights_Jermalavicius_Roigas_Sukhodolia_Teperik_May_2025.pdf (дата звернення: 11.02.2026).

204. The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). The white house. 2013. URL: https://fas.org/irp/offdocs/ppd/ppd-21.pdf (дата звернення: 12.03.2026).

205. Threat Detection Marketplace World's Largest Detection-as-Code Library of Rules & Real-Time CTI. SOC Prime. URL: https://socprime.com/wp-content/uploads/TDM_2025_data-sheets.pdf (дата звернення: 10.05.2025).

206. Ukraine's tech market: 2025 report. N-ix. 2025. 65 p. URL: https://src.n-ix.com/uploads/2025/02/25/d3f17988-8246-40ae-9703-3cd14f6163ad.pdf (дата звернення: 21.01.2026).

207. Ukrainian CyberTech Industry Navigator. IT Ukraine Association. 35 p. URL: https://itukraine.org.ua/files/Ukrainian_CyberTech_Industry_Navigator.pdf (дата звернення: 21.01.2026).

208. Verizon. 2025 Data Breach Investigations Report. Verizon, 2025. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 21.01.2026).

209. Vulnerability detection and cyber incident/cyber attack response system: 2024 annual report. State Service of Special Communications and Information Protection of Ukraine. URL: https://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3 (дата звернення: 21.01.2026).

210. Wang Y., Liu H., Li Z., Su Z., Li J. Combating advanced persistent threats: Challenges and solutions. *IEEE Network*. 2024. № 38(6). PP. 324-333. DOI: http://dx.doi.org/10.1109/MNET.2024.3389734.

211. Wang Z., et al. Business Innovation based on artificial intelligence and Blockchain technology. *Information Processing & Management*. № 59(1). 2022. DOI: https://doi.org/10.1016/j.ipm.2021.102759.

212. Williamson O. E. The economic institutions of capitalism. The political economy reader: Markets as institutions. 2008. № 27. 25 p.

213. Williamson O. E. Transaction-cost economics: the governance of contractual relations. *The journal of Law and Economics*. 1979. № 22(2). PP. 233-261. DOI: https://doi.org/10.1086/466942.

214. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva : WEF, 2025. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025 (дата звернення: 20.09.2025).

215. Xiaoshao M., Antwi-Afari M. F. The applications of Internet of Things (IoT) in industrial management: a science mapping review. *International Journal of Production Research.* 2024. PP. № 62(5). PP. 1928-1952. DOI: https://doi.org/10.1080/00207543.2023.2290229.

ДОДАТКИ

ДОДАТОК А

Таблиця А.1

Визначення поняття «критична інфраструктура» та розподіл об'єктів за досвідом інших країн

Джерело	Визначення поняття	Об'єкти
ЄС	Сукупність фізичних і кібернетичних систем, які забезпечують основні функції суспільства, включаючи економічну стабільність, безпеку, охорону здоров'я, енергопостачання, транспорт, комунікації тощо.	електростанції, газопроводи, нафтопроводи, водоочисні станції, каналізаційні системи, інтернет-мережі, телекомунікаційні радіомовні станції, аеропорти, морські порти, залізниці, автостради, лікарні, медичні центри, центри лабораторій, банки, фондові біржі, виробництво та розподіл продуктів харчування, силіконові долини, хмарні платформи, державні будинки, системи урбанізації.
Німеччина	Фізичні та нематеріальні активи, що забезпечують функціонування суспільства.	
Туреччина	Об'єкти, що забезпечують ключові функції держави.	
Бельгія	Об'єкти, що підтримують основні суспільні функції.	
Норвегія	Об'єкти, що мають стратегічне значення для національного контексту.	
Франція	Об'єкти, діяльність яких пов'язана з виробництвом і розподілом товарів чи послуг, необхідних для основних потреб населення, державних повноважень, економіки, оборони чи безпеки.	
США	Фізичні та віртуальні системи і ресурси, недієздатність яких може серйозно вплинути на національну безпеку, економіку чи громадське здоров'я.	електростанції, нафто та газопроводи, водоочисні станції, каналізаційні системи, інтернет-мережі, телекомунікаційні радіомовні станції, аеропорти, морські порти, залізниці, автостради, лікарні, медичні центри, центри лабораторій, банки, фондові біржі, виробництво та розподіл продуктів харчування, хмарні платформи.

Продовження таблиці А.1

Джерело	Визначення поняття	Об’єкти
Сальвадор	Об’єкти, що забезпечують життєдіяльність суспільства.	залізниці, порти, аеропорти, телекомунікації, електрогенерація, кордони, морська інфраструктура, транспортні мережі, енергетичні об'єкти.
Індія та Індонезія	Системи, що підтримують технологічний і суспільний розвиток.	енергетичні об'єкти, транспортні мережі, фінансові установи, банківські системи, телекомунікаційні мережі, оборонні споруди, правоохоронні органи, служби безпеки, медичні заклади, питне водопостачання, електронне урядування, критична промисловість.

Джерело: *складено автором за [201, 72, 209, 141, 179, 62, 129, 204, 152]*

ДОДАТОК Б

	США	Європейський Союз	Велика Британія	Японія	Україна	Канада	Сінгапур
Енергетика	електростанції, газопроводи, нафтові платформи.	електричні та газові мережі, нафтові термінали.	електростанції, газопроводи, нафтопереробні заводи.	атомні та гідроелектростанції, газопроводи.	атомні електростанції, вугільні та гідроелектростанції.	гідроелектростанції, нафтові платформи, газопроводи.	електростанції, нафтові термінали.
Водопостачання та водовідведення	водоочисні станції, каналізаційні системи.	водоочисні та водорозподільні системи.	системи очищення та розподілу води.	водоочисні споруди, водорозподільні системи.	водоканали, системи очищення води.	водоочисні споруди, системи каналізації.	водоочисні споруди, системи дистрибуції води.
Телекомунікації	інтернет-мережі, телефонні станції, радіомовні станції.	інтернет та телефонні мережі.	мобільні та стаціонарні телефонні мережі, інтернет.	інтернет-мережі, телефонні системи.	інтернет-провайдери, мобільні оператори.	інтернет-провайдери, телефонні мережі, радіомовні станції.	інтернет-мережі, мобільні оператори, телекомунікаційні хаби.
Транспорт	аеропорти, морські порти, залізниці, автостради.	аеропорти, порти, залізничні та дорожні мережі.	мережі громадського транспорту, порти, аеропорти.	швидкісні залізниці (шінкансен), порти, аеропорти.	порти, залізниці, аеропорти.	аеропорти, залізничні мережі, морські порти, автостради.	порти, аеропорти, міські транспортні системи
Охорона здоров'я	лікарні, медичні центри, лабораторії.	лікарні, аптеки, медичні установи.	Національна служба охорони здоров'я (NHS), лікарні.	лікарні, медичні клініки.	лікарні, медичні заклади.	лікарні, клініки, медичні установи.	лікарні, клініки, медичні установи.
Фінансовий сектор	банки, фондові біржі.	банки, страхові компанії.	Лондонський фінансовий центр, банки, біржі.	банки, Токійська фондова біржа.	банки, Національний банк України.	банки, фондові біржі.	банки, Сінгапурська фондова біржа.
Харчова промисловість	виробництво та розподіл продуктів харчування.	банки, страхові компанії.	Лондонський фінансовий центр, банки, біржі.	риболовля, сільське господарство.	агропромислові комплекси, продовольчі компанії.	виробництво та постачання продуктів харчування.	імпорт та переробка продуктів харчування.
Інформаційні технології		сільськогосподарське виробництво, харчові підприємства.		виробництво електроніки, дата-центри.	IT-компанії, дата-центри.		дата-центри, IT-компанії.
Урядові установи	державні будівлі, системи управління.		продовольчі компанії, логістика.			державні будівлі, системи управління, безпека.	

Рис. Б.1. Розподіл критичної інфраструктури за закордонним досвідом *(сформовано автором за [201, 72, 209, 141, 179, 62, 129, 204, 152])*

ДОДАТОК В

Таблиця В.1

Законодавчий базіс управління захистом критичної інфраструктури від кіберзагроз

Назва документа	Основний зміст	Ключові положення
Закон України «Про критичну інфраструктуру»	Визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури.	- Визначення термінів критичної інфраструктури. - Засади державної політики у сфері захисту критичної інфраструктури. - Порядок віднесення об'єктів до критичної інфраструктури (сектори, категоризація, реєстр, паспортизація). - Суб'єкти національної системи захистукритичної інфраструктури . - Режими функціонування системи. - Повноваження уповноваженого органу. - Завдання, права та обов'язки операторів критичної інфраструктури.
Постанова КМУ «Деякі питання об'єктів критичної інфраструктури»	Визначає механізм віднесення об'єктів до критичної інфраструктури та їх категоризації.	- Порядок віднесення об'єктів до критичної інфраструктури. - Секторіальний перелік об'єктів критичної інфраструктури. - Перелік секторів критичної інфраструктури. - Методика категоризації об'єктів критичної інфраструктури (секторальні та міжсекторальні критерії).
Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури»	Визначає механізм та періодичність моніторингу рівня безпеки об'єктів критичної інфраструктури.	- Мета: перевірка відповідності стану захищеності вимогам законодавства. - Надання методичної допомоги операторам критичної інфраструктури. - Удосконалення системи захисту критичної інфраструктури.
Постанова КМУ «Деякі питання паспортизації об'єктів критичної інфраструктури»	Визначає вимоги до розроблення та погодження паспорта безпеки об'єктів критичної інфраструктури.	- Паспорт безпеки розробляється оператором на кожен об'єкт критичної інфраструктури. - Складові паспорта: титульний аркуш, характеристика об'єкта, плани захисту, акти оцінки стану захищеності.

Джерело: *складено за [75, 29, 73, 28]*

ДОДАТОК Г

Таблиця Г.1

Хронологія ключових подій у розвитку ринку кібербезпеки в Україні

Назва етапу	Період	Ключові події	Наслідки
Перші значні кіберінциденти	2010–2013	Перші значні атаки на фінансові системи Зростання попиту на базові антивіруси. Імпорт іноземних рішень, таких як Kaspersky, Symantec тощо.	Введення фаєрволів у корпоративних мережах. Впровадження базового шифрування (SSL/TLS) для захисту транзакцій. Формування перших команд кібербезпеки в банківському секторі.
Початок гібридної війни	2014	Анексія Криму Росією, початок гібридної війни. Ескалація цільових кібератак на державні та комерційні установи. Створення CERT-UA для реагування на інциденти.	Розвиток систем моніторингу мереж у державному секторі. Перші спроби локалізації кіберзахисту. Залучення міжнародних експертів для консультацій.
Перші кібератаки на критичну інфраструктуру	2015	Атака BlackEnergy на енергосистему України Перша у світі підтверджена кібератака на критичну інфраструктуру.	Впровадження резервних систем живлення та даних у критичній інфраструктурі. Розгортання систем виявлення вторгнень (IDS). Початок тренінгів для персоналу.
Формалізація кібербезпеки	2016	Ухвалення Національної стратегії кібербезпеки України. Формалізація політики кіберзахисту на державному рівні. Залучення міжнародних інвестицій від США та ЄС	Стандартизація захисту даних. Розробка перших національних стандартів кібербезпеки. Зростання локальних стартапів у сфері.
Глобальна кіберкриза	2017	Атака NotPetya. Ринок кібербезпеки в Україні зріс удвічі через терміновий попит. Фокус на швидкому відновленні після атак.	Розвиток ШІ-систем для виявлення ransomware у реальному часі. Впровадження процедур швидкого відновлення даних. Міжнародна співпраця з Interpol та NATO.
Захист промислових систем	2018	Спроба атаки на хлорну станцію. Посилення захисту SCADA-систем у промислових об’єктах. Гранти від ЄС на модернізацію безпеки критичної інфраструктури.	Інтеграція OT-безпеки з IT-системами. Впровадження сегментації мереж у промислових об’єктах. Розвиток локальних рішень для OT-захисту.
Підготовка до війни	2021	Дефейс урядових сайтів. Зростання інвестицій у захист вебресурсів. Активна підготовка до повномасштабної війни через розвіддані про кіберзагрози.	Впровадження автоматизованих систем аудиту безпеки. Розгортання вебфаєрволів для захисту державних порталів. Навчання кіберфахівців за підтримки НАТО.
Кібервійна	2022	Початок повномасштабної війни, атаки WhisperGate і DDoS на держустанови та банки. Міграція критичних систем до хмарних платформ. Ринок кібербезпеки зріс на 50%. Міжнародна допомога від США, ЄС, Starlink.	Впровадження моделі нульової довіри (Zero Trust). Розвиток систем моніторингу в реальному часі. Створення кіберкоманд для швидкого реагування на атаки.

Продовження таблиці Г.1

Назва етапу	Період	Ключові події	Наслідки
Технологічний прорив	2023–2024	Зростання атак на енергетичний сектор. Ринок кібербезпеки досяг 1 млрд дол. Запуск освітніх програм із кібербезпеки в університетах.	Дослідження квантових технологій для шифрування. Використання Big Data та ШІ для прогнозування атак. Розвиток міжнародних партнерств для експорту технологій.

Джерело: *складено за [64, 130, 190, 178, 120, 206]*

ДОДАТОК Д

Таблиця Д.1

Пропозиції з навчання персоналу об'єктів критичної інфраструктури

Блок персоналу	Тип навчання/ освіти	Основний контент	Частота та тривалість	Рекомендовані ресурси
Управлінський персонал	Стратегічні семінари та курси з кіберризикового менеджменту	Аналіз загроз, кризове планування, бюджетування на безпеку, етичні та юридичні аспекти	Щорічно, 2-3 дні (24-40 годин) + щоквартальні вебінари (2 години)	Курси NIST Cybersecurity Framework, партнерства з ДССЗЗІ, платформа edX
	Симуляції криз та рольові ігри	Моделювання атак, координація з правоохоронцями	Раз на півроку, 1 день (8 годин)	Інструменти як Cyber Range від CERT-UA, ISO 22301
Технічні працівники	Модульні курси з технічної безпеки	Хмарна безпека (AWS/Azure), криптографія, моніторинг мереж (IDS/IPS), програмування безпечного коду	Щоквартально, 4-6 модулів по 4 години	Платформи Udemy, Coursera; бібліотеки як OWASP
	Воркшопи з етичного хакінгу	Penetration testing, аналіз логів, інструменти (Metasploit, Wireshark)	Раз на квартал, 1-2 дні (16 годин)	Сертифікація CEH (Certified Ethical Hacker), інструменти від SANS Institute
Інші співробітники	Базові онлайн-курси з обізнаності	Розпізнавання фішингу, безпечне використання email/гаджетів, політика паролів (2FA)	Щомісяця, 1-2 години + щорічний повний курс (8 годин)	Безкоштовні ресурси KnowBe4, національні кампанії ДССЗЗІ
	Гейміфіковані тренінги та тести	Симуляції атак (фейкові email), базові принципи GDPR-подібних норм	Щотижня (короткі сесії по 15 хв)	Платформи як PhishingBox, інтеграція з MS Teams

Джерело: *складено автором*

ДОДАТОК Е

Таблиця Е.1

Найпотужніші кібератаки на енергетичні об’єкти

Рік	Назва атаки	Ціль / Країна	Опис
2003	David-Besse Nuclear Plant	США	Хробак Slammer ізолював моніторинг реактора на 5 годин.
2007	BTC Oil Pipeline	Туреччина	Ін'єкція фальшивих даних, вибух і розлив нафти.
2007	Aurora	США	Aurora спричинив вибух генератора через збої у системі.
2010	WinCC SCADA System	Німеччина	Stuxnet атакував SCADA-системи, вразливість виправлено.
2010	Natanz Nuclear Power Plant	Іран	Stuxnet вивів з ладу понад 1000 центрифуг.
2011	Aramco Oil & Gas	Саудівська Аравія	Shamoon стер 30 тис. комп’ютерів, збитки 15 млн. дол.
2011–2014	Dragonfly / Energetic Bear	Енергетичні компанії по всьому світу	Серія атак на інтелектуальні енергосистеми.
2012	RasGas	Катар	Disttrack знищив критичні дані, зупинив виробництво.
2012	Power Grid	Україна	BlackEnergy3 знеструмив 230 000 споживачів.
2015	Power Grid	Україна	Повторення атаки BlackEnergy3, відключення електроенергії.
2016–2018	Industroyer / CrashOverride	Israel Electric Corporation	Атаки на електромережі, масштабні збої.
2017	NotPetya Ransomware	Енергетичні компанії по всьому світу	Порушення систем управління, зв’язку та білінгу.
2019	Norsk Hydro Renewables	Норвегія	LockerGoga заблокував IT-інфраструктуру, збитки 71 млн. дол.
2021	Colonial Oil Pipeline	США	Darkside заблокував сервери, сплачено викуп 4.4 млн. дол
2022–2024	Sandworm / Industroyer2	Україна (ДТЕК, енергосистеми)	Складна серія атак на системи ОТ з новими методами впливу.

Джерело*: складено за [45, 112, 136, 128, 145, 126, 115, 189, 123, 158, 110, 138, 122]*

ДОДАТОК Ж

Таблиця Ж.1

Експертна оцінка доцільності впровадження ШІ в енергетичні компанії (бали), 2024 р.

№ п/п	Показник	Коефіцієнт чутливості	Холдінг «ДТЕК»	ПрАТ «НЕК «Укренерго»	НАЕК «Енергоатом»	ПрАТ «Укргідроенерго»	ТОВ «ЕЛЕМЕНТУМ ЕНЕРДЖІ (УКРАЇНА)»
Виробничий блок							
1	Оперативність ШІ у виявленні та реагуванні на кіберзагрози	1,2	4	5	5	2	4
2	Масштабованість управлінських ШІ рішень у кіберзахисті	1,25	3	5	4	3	3
3	Гнучкість та адаптивність ШІ в управлінні кібербезпекою	1,15	4	4	3	3	5
Управлінський блок							
1	Рівень готовності компанії до впровадження інструментів ШІ	1,2	4	5	3	3	5
2	Гнучкість управління впровадженням нових технологій	1,15	3	4	4	3	4
3	Партнерство з ШІ-стартапами та науковими установами	1,15	5	4	4	3	4
Комунікаційний блок							
1	Позиціонування компанії як цифрово стійкої	1,2	5	4	3	5	5
2	Освітні ініціативи для ринку та партнерів	1,15	5	2	1	1	3

Продовження таблиці Ж.1

№ п/п	Показник	Коефіцієнт чутливості	Холдінг «ДТЕК»	ПрАТ «НЕК «Укренерго»	НАЕК «Енергоатом»	ПрАТ «Укргідроенерго»	ТОВ «ЕЛЕМЕНТУМ ЕНЕРДЖІ (УКРАЇНА)»
Комунікаційний блок							
3	Рівень готовності компанії до впровадження ШІ-рішень	1,15	5	5	4	3	5
Фінансовий блок							
1	Економічна ефективність впровадження ШІ-рішень	1,05	4	3	3	2	4
2	Потенціал залучення інвестицій	1,1	4	5	5	5	5
3	Державне та міжнародне фінансування	1,05	3	3	4	4	2
4	Зниження витрат на ліквідацію наслідків атак	1,05	4	3	2	4	2

Джерело*: розраховано автором*

ДОДАТОК И

Таблиця И.1

Ранжування енергетичних компаній за рівнем впровадження штучного інтелекту у 2024 р. (за результатами експертної оцінки, бали)

№ п/п	Показник	Коефіцієнт чутливості	Холдінг «ДТЕК»	ПрАТ «НЕК «Укренерго»	НАЕК «Енергоатом»	ПрАТ «Укргідроенерго»	ТОВ «ЕЛЕМЕНТУМ ЕНЕРДЖІ (УКРАЇНА)»
Виробничий блок							
1	Оперативність ШІ у виявленні та реагуванні на кіберзагрози	1,2	2	1	1	3	2
2	Масштабованість управлінських ШІ рішень у кіберзахисті	1,25	3	1	2	3	3
3	Гнучкість та адаптивність ШІ в управлінні кібербезпекою	1,15	2	2	3	3	1
Управлінський блок							
1	Рівень готовності компанії до впровадження інструментів ШІ	1,2	2	1	3	3	1
2	Гнучкість управління впровадженням нових технологій	1,15	4	2	2	4	2
3	Партнерство з ШІ-стартапами та науковими установами	1,15	1	2	2	4	2

Продовження таблиці И.1

№ п/п	Показник	Коефіцієнт чутливості	Холдінг «ДТЕК»	ПрАТ «НЕК «Укренерго»	НАЕК «Енергоатом»	ПрАТ «Укргідроенерго»	ТОВ «ЕЛЕМЕНТУМ ЕНЕРДЖІ (УКРАЇНА)»
3	Партнерство з ШІ-стартапами та науковими установами	1,15	1	2	2	4	2
Комунікаційний блок							
1	Позиціонування компанії як цифрово стійкої	1,2	1	3	4	1	1
2	Освітні ініціативи для ринку та партнерів	1,15	1	3	4	4	2
3	Рівень готовності компанії до впровадження ШІ-рішень	1,15	1	1	2	4	1
Фінансовий блок							
1	Економічна ефективність впровадження ШІ-рішень	1,05	1	2	2	3	1
2	Потенціал залучення інвестицій	1,1	3	1	1	1	1
3	Державне та міжнародне фінансування	1,05	3	3	1	1	4
4	Зниження витрат на ліквідацію наслідків атак	1,05	1	2	3	1	3

Джерело: *розраховано автором*

ДОДАТОК К

Розрахунок суми місць та довжини векторів холдингу «ДТЕК», ПрАТ «НЕК «Укренерго», НАЕК «Енергоатом», ПрАТ «Укргідроенерго», ТОВ «Елементум Енерджі (Україна)».

Позначення:

– P1,P2,P3,P4 – сума місць відповідно для технологічного, управлінського, комунікаційного та фінансового блоків.

– B1, B2, B3, B4 – довжина векторів відповідно для технологічного, управлінського, комунікаційного та фінансового блоків.

1. Холдінг «ДТЕК»

Сума місць:

P1 = (1,2x2)+(1,25x3)+(1,15x2)= 8,45

P2 = (1,2x2)+(1.15x4)+(1,15x1)= 8,15

P3 = (1,2x1)+(1,15x1)+(1,15x1)= 3,5

P4=(1.05x1)+(1.1x3)+(1.05x3)+(1.05x1)= 8,55

Довжина вектору:

B1= 100-(8,45-3)x100/3(5-1)= 54,58 у.о.

B2=100-(8,15-3)x100/3(5-1)= 57,08у.о

B3= 100-(3,5-3)x100/3(5-1)= 95,83у.о

B4=100-(8,55-4)x100/4(5-1)= 71,56у.о

2. ПрАТ «НЕК «Укренерго»

Сума місць:

P1 = (1.2x1)+(1.25x1)+(1.15x2)=4,75

P2 = (1.2x1)+(1.15x2)+(1.15x2)=5,8

P3 = (1.2x3)+(1.15x3)+(1.15x1)=8,2

P4=(1.05x2)+(1.1x1)+(1.05x3)+(1.05x2)=8,45

Довжина вектору:

B1= 100-(4,75-3)x100/3(5-1)=85,45 у.о.

В2=100-(5,8-3) х100/3(5-1)= 76,67 у.о

В3=100-(8,2-3)х100/3(5-1)= 56,67 у.о

В4=100-(8,45-4)х100/4(5-1)= 72,19у.о

3. НАЕК «Енергоатом»

Сума місць:

Р1 = (1.2х1)+(1.25х2)+(1.15х3)=7,15

Р2 = (1.2х3)+(1.15х2)+(1.15х2)=8,2

Р3 = (1.2х4)+(1.15х4)+(1.15х2) =11,7

Р4=(1.05х2)+(1.1х1)+(1.05х1)+(1.05х1)=5,3

Довжина вектору:

В1= 100-(7,15-3)х100/3(5-1)= 65,42 у.о.

В2=100-(8,2-3) х100/3(5-1)= 56,67у.о

В3= 100-(11,7-3) х100/3(5-1)= 27,50 у.о

В4=100-(5,3-4) х100/4(5-1)= 91,87у.о

4. ПрАТ «Укргідроенерго»

Сума місць:

Р1 = (1.2х3)+(1.25х3)+(1.15х3)= 10,8

Р2 = (1.2х3)+(1.15х4)+(1.15х4)=12,8

Р3 = (1.2х1)+(1.15х4)+(1.15х4)=10,4

Р4=(1.05х3)+(1.1х1)+(1.05х1)+(1.05х1)=6,35

Довжина вектору:

В1= 100-(10,8-3)х100/3(5-1)= 35у.о.

В2=100-(12,8-3) х100/3(5-1)= 18,33у.о

В3= 100-(10,4-3) х100/3(5-1)= 38,33у.о

В4=100-(6,35-3) х100/3 (5-1)= 72,08у.о

5. ТОВ «Елементум Енерджі (Україна)»

Сума місць:

Р1 = (1.2х2)+(1.25х3)+(1.15х1)= 7,3

Р2 = (1.2х1)+(1.15х2)+(1.15х2)=5,8

Р3 = (1.2х1)+(1.15х2)+(1.15х1)=4,65

P4=(1.05x1)+(1.1x1)+(1.05x4)+(1.05x3)=9,5

Довжина вектору:

B1= 100-(7,3-3)x100/3(5-1)= 64,17у.о.

B2=100-(5,8-3) x100/3(5-1)= 76,67у.о

B3= 100-(4,65-3) x100/3(5-1)= 86,2у.о

B4=100-(9,5-3) x100/4(5-1)=59,37 у.о

ДОДАТОК Л

Таблиця Л.1

Модель пріоритетності об’єктів критичної інфраструктури за критичністю, рівнем інформатизації та схильності до інновацій

Сектор	Категорія критичності	Бали критичності	Бали інформатизації	Пріоритет кіберзахисту	Схильність до інновацій	Бали інновацій	Інноваційна пріоритетність
Енергетичний	I	4	3	2,38	Середня	2	2,78
Інформаційно-комунікаційні технології	I	4	3	2,36	Висока	3	2,96
Транспорт	II	3	2	1,74	Середня	2	2,14
Водо-постачання та водовідведення	II	3	1	1,62	Низька	1	1,82
Охорона здоров’я	I	4	2	2,28	Низька	1	2,48
Фінансовий	II	3	2	1,84	Середня	2	2,24
Промисловість	II	3	2	1,7	Низька	1	1,9
Оборонний	I	4	2	2,3	Нульова	0	2,3
Харчова промисловість	IV	1	1	0,66	Низька	1	0,86
Хімічна промисловість	II	3	1	1,68	Низька	1	1,88
Сектор надзвичайних ситуацій	I	4	2	2,26	Низька	1	2,46
Сектор державного управління	II	3	2	1,82	Низька	1	2,02

Джерело: *складено автором*

ДОДАТОК М

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Соколов А. В., Кілко В. В., Трофименко О. Г., Саврацький О. О. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об'єктах критичної інфраструктури. *Вісті вищих учбових закладів. Радіоелектроніка.* 2026. URL: https://radio.kpi.ua/article/view/S0021347025040028. DOI: https://doi.org/10.20535/S0021347025040028.

2. Саврацький О. О. Адаптація системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів. *Трансформаційна економіка*. 2024. №1(06). С. 53–57. DOI: https://doi.org/10.32782/2786-8141/2024-6-10.

3. Саврацький О. О. Аналіз кон'юнктури ринку продуктів та послуг кібербезпеки. *Науково-виробничий журнал «Бізнес-навігатор».* 2025. №1. С. 443-449. DOI: https://doi.org/10.32782/business-navigator.78-74.

4. Саврацький О. О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. *Актуальні питання економічних наук*. 2025. № 13. DOI: https://doi.org/10.5281/zenodo.16885042.

5. Горбаченко С. А., Саврацький О. О. Transformation of the innovative component of management processes in the context of digitalization. *Приазовський економічний вісник.* 2025. № 3 (43). С. 62-67. DOI: https://doi.org/10.32782/2522-4263/2025-3-11.

6. Саврацький О.О., Слатвінська В.М. Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень. *Наука і техніка сьогодні.* 2025. № 8 (49). С. 1704-1716. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716.

7. Саврацький О. О., Чепурна О. Є. Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних

системах з урахуванням спадної віддачі інвестицій. *Успіхи і досягнення у науці*. 2026. № 1(23). С. 1305-1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317.

наукові праці, які засвідчують апробацію матеріалів дисертації:

8. Саврацький О. О. Критична інфраструктура як об’єкт кіберзахисту. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика :* матеріали Міжнар. наук.-практ. конф., м. Одеса, 24 листопад. 2023 р. Одеса, 2023. С. 76-78.

9. Саврацький О. О. Особливості підготовки фахівців з кібербезпеки в умовах війни. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар. наук.-практ. конф., м. Одеса, 26 квітн. 2024 р. НУ "ОЮА" ; за заг. ред. С. В. Ківалова ; відп. за вип. М. Р. Аракелян. – Одеса : Фенікс, 2024. – С. 905-907.

10. Саврацький О.О. Нормативно-правовий фундамент управління кібербезпекою підприємства. *Конкурентоспроможна модель інноваційного розвитку економіки України :* матеріали VII Міжнар. наук.-практ. конф., м. Кропивницький, 7-8 листопад. 2024 р. Кропивницький, 2024. С. 116-118.

11. Саврацький О. О. Системний підхід при управління кіберризиками в умовах війни. *Кібербезпека в сучасному світі: актуальні виклики* : матеріали Міжнар. наук.-практ. конф., м. Одеса, 22 листопад. 2024 р. Одеса. 2024. С. 274-277.

12. Саврацький О. О. Current trends in security management. *Achievements of Science and Applied Research :* матеріали III Міжнар. наук.-практ. конф., м. Дублін 21-23 липн. 2025. С. 70-75. DOI: http://dx.doi.org/10.70286/EOSS-21.07.2025

ДОДАТОК Н

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

Положення та висновки дисертаційного дослідження обговорювались під час засідання кафедри кримінального процесу Національного університету «Одеська юридична академія». Основні результати наукового дослідження були висвітлені у доповідях на наукових, науково-практичних конференціях, зокрема на: Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.) – форма участі заочна; Міжнародна науково-практична конференція «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.) – форма участі заочна; VII Міжнародна науково-практична конференція «Конкурентоспроможна модель інноваційного розвитку економіки України» (м. Кропивницький, 7-8 листопада 2024 р.) – форма участі заочна; Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.) – форма участі заочна; III Міжнародна науково-практична конференція «Achievements of Science and Applied Research» (м. Дублін, 21-23 липня 2025) – форма участі заочна; Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.) – форма участі заочна.

ДОДАТОК П

ДОВІДКА

про використання результатів наукових досліджень
Саврацького Олександра Олександровича,
представлених у дисертації на здобуття наукового ступеня доктора філософії
за спеціальністю 073 «Менеджмент»

Довідка підтверджує, що наукові положення та прикладні рекомендації дисертаційної роботи Саврацького О.О. зокрема ті, що є результатами емпіричного дослідження, проведеного ГО «Кіберпростір», представляють практичний інтерес для учасників «Odesa IT Family», зокрема з точки зору їхнього застосування у діяльності регіональних IT-спільнот та підприємств критичної інфраструктури, а також покращенні інноваційного та технологічного іміджу регіону.

На основі представленого в додатках до дисертації Аналітичного звіту, одним з виконавців якого є Саврацький О.О., на 2026 р. заплановано впровадження постійних програм підвищення кіберобізнаності управлінського персоналу (Awareness Training) під егідою «Odesa IT Family», а також проведення круглого столу «Управлінські аспекти протидії кіберзагрозам в сучасному світі».

Крім того за результатами дослідження Саврацького О.О. для окремих підприємств-учасників «Odesa IT Family» також надана низка слушних управлінських рекомендацій: створення внутрішніх координаційних груп із управління інцидентами; удосконалення процедур контролю доступу та впровадження внутрішнього аудиту SOC (Security Operations Center); моніторинг ROSI (окупності інвестицій у кіберзахист) за кожним напрямом витрат.

Таким чином практичне застосування інструментів та підходів, описаних у дисертаційній роботі Саврацького О.О., здійснює позитивний вплив на створення нових бізнес-можливостей в Одеському регіоні, реалізацію потенціалу фахівців та забезпечення управлінського підґрунтя впровадження технологічних ініціатив.

Директор ГС “Айті фемілі Одеса”
Катерина Соловей

УКРАЇНА ГРОМАДСЬКА СПІЛКА “АЙТІ ФЕМІЛІ ОДЕСА” 43880859 Одеська область, місто Одеса

ДОДАТОК Р

ОДЕСКАБЕЛЬ
ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО

ДОВІДКА

Про використання результатів наукових досліджень
Саврацького Олександра Олександровича
представлених в дисертації на здобуття наукового ступеня доктора філософії
за спеціальністю 073 «Менеджмент»
«Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз»

Керівництво ПАТ «ОДЕСКАБЕЛЬ» ознайомилося та прийняло до використання у практичній діяльності пропозиції Саврацького О.О. щодо шляхів зміцнення ефективності кіберзахисту за рахунок впровадження управлінських інновацій.

В контексті специфіки діяльності підприємства, як об'єкта критичної інфраструктури, особливої уваги заслуговує запропонований в дисертації науково-практичний підхід до оптимізації інвестицій в кібербезпеку на основі моделі Гордона-Льоба та функції кіберстійкості. Адже він дозволяє верифікувати межу ефективності – «зону виправданого інвестування». Це, у свою чергу, допомагає підприємству досягти необхідного рівня кіберзахисту без надмірного фінансового навантаження.

Означений підхід вже використовується в поточній діяльності ПАТ «ОДЕСКАБЕЛЬ», на його основі формується та структурується бюджет на забезпечення кіберзахисту підприємства. Зокрема, отримала підтвердження викладена в дисертації гіпотеза, що комбіновані програми, у яких технічні та організаційні витрати поєднуються у співвідношенні близько 60/40, забезпечують найвищий інтегральний ефект. Адже підприємство стикнулося із ситуацією «плато технічних інвестицій», коли додаткове інвестування в технічні засоби кібербезпеки вже не призводило до істотного зниження ризику.

В результаті в 2025 році основний фокус у витратах змістився на розвиток навчальних програм, а також оптимізацію процедур управління доступом та покращення організаційної культури безпеки. І можна стверджувати, що вказані напрями посприяли стабільному підвищенню стійкості системи, навіть коли технологічна складова досягла межі своєї результативності.

Генеральний директор Вадим ІОРГАЧОВ

Миколаївська дорога, 144,
Одеса, 65102,
Україна

Тел.: +38 048 716 11 23
+38 048 716 14 04
Факс: +38 048 716 14 01

www.odeskabel.com
office@odeskabel.com

ДОДАТОК С

ОДЕСЬКА МІСЬКА РАДА
Комунальне підприємство
«ТЕПЛОПОСТАЧАННЯ міста ОДЕСИ»
вул. Балківська, 1-Б, м.Одеса, Україна. 65029,ЄДРПОУ 34674102
тел.: (048) 705-62-18, факс: (048) 705-62-48, email: office@teplo.od.ua; www.teplo.od.ua

22.12.25 01-18/1534

ДОВІДКА

про використання результатів наукових досліджень Саврацького Олександра Олександровича, представлених в дисертації на здобуття наукового ступеня доктора філософії

Наукові положення та прикладні рекомендації дисертаційної роботи Саврацького О.О. «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз» представляють практичний інтерес для КП «Теплопостачання міста Одеси» в контексті оптимізації власних управлінських рішень, адже в умовах повномасштабного вторгнення критична інфраструктура виступає головним об'єктом не тільки фізичних атак, а й кіберзагроз.

Обґрунтованими постають пропозиції щодо структурування персоналу підприємства для вирішення питань кібербезпеки на такі групи як управлінський персонал, технічні працівники та інші співробітники, які мають доступ до інформаційних систем. Метою зазначеного структурування, яке вже впроваджується у КП «Теплопостачання міста Одеси», є подальша розробка індивідуальних програм навчання, які враховують специфіку ролей з огляду кібербезпекових питань, рівень ризиків та локальні потреби об'єктів. В подальшому посилити ефект від роботи з персоналом планується за рахунок запропонованого у дисертації командного підходу в управлінні кіберзахистом на основі координації зусиль фахівців різного профілю та рівнів відповідальності.

Пропозиції викладені в дисертації знайшли відображення у наступних наукових працях:

Саврацький О.О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. DOI: https://doi.org/10.5281/zenodo.16885042

Саврацький О.О., Слатвінська В.М. Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716

Використання керівництвом КП «Теплопостачання міста Одеси» зазначених пропозицій не тільки сприяє збільшенню ефективності протидії кіберзагрозам, але й забезпечує загальне зміцнення інноваційної культури та конкурентоспроможності менеджменту підприємства.

Заступник директор з економічних та фінансових питань КП «Теплопостачання міста Одеси» ЄВГЕНІЙ Колопенюк

ДОДАТОК Т

ДОВІДКА

Про використання результатів наукових досліджень

Саврацького Олександра Олександровича

представлених в дисертації на здобуття наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент» на тему:

«Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз»

Комерційна діяльність ТОВ «КІПСОЛІД УКРАЇНА» пов'язана з експлуатацією складних цифрових рішень, інтегрованих інформаційних систем та хмарних сервісів, що зумовлює підвищений рівень кіберризиків і потребує системного управлінського підходу до забезпечення стійкості бізнес-процесів. У цьому контексті тематика дисертаційного дослідження Саврацького О.О. є стратегічно релевантною потребам компанії, оскільки орієнтована на впровадження саме управлінських інновацій, а не виключно технічних засобів захисту.

Результати дослідження дисертанта пройшли практичну апробацію в діяльності ТОВ «КІПСОЛІД УКРАЇНА». Зокрема, в компанії впроваджено методику двоканального інвестування в кіберстійкість у процесі стратегічного та операційного бюджетування, що дозволило:

- структурувати витрати компанії на забезпечення кіберзахисту за технологічним та організаційним напрямами;
- встановити економічно обґрунтовану межу доцільності додаткових інвестицій у продукти та послуги кібербезпеки;
- підвищити прозорість управлінських рішень у сфері розподілу ресурсів на протидію кіберзагрозам.

Використання встановленої автором «точки плато» забезпечило менеджменту компанії оптимізацію інвестиційного портфеля у сфері кібербезпеки та запобігло неефективному нарощуванню витрат на програмно-технічні засоби без синхронного розвитку людського капіталу.

У межах реалізації положень дисертації в компанії впроваджено диференційовану систему професіоналізації персоналу у сфері інформаційної безпеки. Розроблено та інтегровано в корпоративну систему навчання три контури підготовки: базовий (для всіх працівників), управлінський (для керівного складу) та спеціалізований технічний (для ІТ-фахівців). У контексті розподілу ресурсів застосовано запропоновану структуру інвестицій у навчальні програми у співвідношенні 40% — базові програми, 35% — управлінські тренінги, 25% — технічні курси. Як елемент системи внутрішнього контролю ризиків зазначена модель підтвердила свою спроможність впливати на зменшення кількості інцидентів, пов'язаних із людським фактором.

Апробація наукових положень дисертації Саврацького О.О. підтвердила їхню прикладну цінність для підвищення ефективності управління кіберризиками, зміцнення культури інформаційної безпеки та забезпечення безперервності діяльності ТОВ «КІПСОЛІД УКРАЇНА». Запропоновані управлінські інновації інтегровані в систему стратегічного планування та використовуються під час формування середньострокових програм розвитку компанії.

Керівник громадської організації
«ОСВІТНІЙ ФОНД КІПСОЛІД»; Віктор ЯЦЕНКО

ДОДАТОК Ф

Прим. № 1

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ
УПРАВЛІННЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ
ІНФОРМАЦІЇ УКРАЇНИ В ОДЕСЬКІЙ ОБЛАСТІ
Управління Держспецзв'язку в Одеській області

вул. Єврейська, 43, м. Одеса, 65045, тел. (048)722-71-57,
e-mail: odesa@cip.gov.ua, web: cip.gov.ua
Код ЄДРПОУ 34800034

від 02.03.2026 р. № 40-30 На № _____ від _____20___ р.

ДОВІДКА

про використання результатів дисертаційного дослідження
Саврацького Олександра Олександровича на тему:
«Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз»

Ефективне управління захистом критичної інфраструктури України передбачає, насамперед, мінімізацію ризиків та загроз, пов'язаних із впливом цифрового середовища. Фахівці Управління Державної служби спеціального зв'язку та захисту інформації України в Одеській області ознайомилися з дослідженням Саврацького О.О. і погоджуються з висновками автора щодо неможливості забезпечення ефективного кіберзахисту виключно за рахунок технологічних рішень. Аналітичні звіти також підтверджують, що під час кібератак на критичну інфраструктуру зловмисники здебільшого намагаються використовувати організаційні прогалини та людський фактор.

В дисертації автором вдало застосовується економіко-математичне моделювання, зокрема проведено розширення моделі Гордона-Льоба до двоканального (технічного та організаційного) інвестування в кібербезпеку та визначено граничну ефективність інвестицій за кожним напрямом. Отримані результати дозволяють чітко простежити закономірність спадної віддачі за технічним напрямом, адже, якщо на початкових етапах додаткові витрати забезпечують значний приріст зниження ризику, то після досягнення приблизно 1,5 тис дол на одного працівника ефект додаткових витрат стає мінімальним. Тобто, існує «плато», після якого інвестиції у нові технології не забезпечують істотного підвищення рівня кіберстійкості. Організаційні інвестиції демонструють більш тривалий позитивний ефект. Навіть після перевищення порогу у 0,8–1 тис дол на працівника вони продовжують давати суттєвий

приріст, що свідчить про їх довгострокову ефективність. Вказана ситуація пояснюється тим, що навчання персоналу або розвиток культури безпеки сприяють стабільному підвищенню кіберстійкості, навіть коли технологічна складова досягла межі. Комбіновані програми, у яких технічні та організаційні витрати поєднуються у співвідношенні близько 60/40, забезпечують найвищий інтегральний ефект, а, отже, їхнє впровадження наразі має знаходитися у пріоритеті.

Окремої уваги заслуговують пропозиції автора щодо формування в Україні кластеру кібербезпеки. Зокрема пропонується, щоб до керівництва цим кластером, у вигляді координаційного хабу, що функціонує за принципом консенсусного прийняття рішень, долучилися представники РНБО, Держспецзв'язку, Міністерства цифрової трансформації, наукової спільноти, профільних бізнес-структур.

Враховуючи викладене вище, можна дійти висновку, що напрацювання автора заслуговують на практичне застосування у діяльності Управління Державної служби спеціального зв'язку та захисту інформації України в Одеській області.

Начальник
Управління Державної служби спеціального зв'язку
та захисту інформації України
в Одеській області **Володимир ДЯТЛОВСЬКИЙ**

ДОДАТОК Х

«ЗАТВЕРДЖУЮ»
Ректор
Національного університету
«Одеська юридична академія»
_____ проф. Олег ТОДОЩАК
«22» грудня 2023 р.

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційного дослідження
Саврацького Олександра Олександровича
«Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз»

Комісія у складі: проректора з навчальної роботи, доктора юридичних наук, професора Галини УЛЬЯНОВОЇ, завідувача кафедри кібербезпеки, доктора економічних наук, професора Станіслава ГОРБАЧЕНКА, доцента кафедри кібербезпеки, кандидата фізико-математичних наук, доцента Олени ЧЕПУРНОЇ засвідчує, що результати дослідження аспіранта Саврацького Олександра Олександровича, представленого на здобуття наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент» використовуються в навчальному процесі Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «Менеджмент та маркетинг інновацій», «Проєктний менеджмент», «Інноваційний менеджмент», «Управління та організаційне забезпечення кібербезпеки», «Прогнозування кон'юнктури ринку», «Цифрові технології в бізнесі, а також під час виконання кваліфікаційних робіт та в науково-дослідній роботі здобувачів.

Необхідність впровадження результатів дослідження зумовлена важливістю нормального функціонування та розвитку критичної інфраструктури України в умовах викликів цифрового середовища, а також доцільністю інтеграції інноваційних підходів, заходів, інструментів в управлінські процеси на рівні окремих об'єктів критичної інфраструктури. Адже в сучасних умовах питання кібербезпеки все частіше переходять від суто технічної площини до комплексної проблематики з домінуванням людського чиннику, яка потребує відповідних управлінських рішень.

Впровадження результатів дисертації в навчальний процес здійснюється через:

- видання колективної монографії «Безпека інформації та інфраструктури інформаційно-комунікаційних систем: міждисциплінарний підхід» з наявністю авторського розділу (Горбаченко С. А. Саврацький О. О.

Управлінські аспекти забезпечення кіберзахисту об'єктів критичної інфраструктури (https://doi.org/10.36059/978-966-397-537-5-1);

- використання наукових публікацій дисертанта як додаткових джерел в силабусах освітніх компонентів «Прогнозування кон'юнктури ринку» (Саврацький О. О. Аналіз кон'юнктури ринку продуктів та послуг кібербезпеки. Науково-виробничий журнал «Бізнес-навігатор». 2025. №1. С. 443-449), «Проєктний менеджмент» (Саврацький О.О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. Актуальні питання економічних наук. 2025 № 13. URL: https://a-economics.com.ua/index.php/home/article/view/717/713), «Інноваційний менеджмент» (Горбаченко С.А., Саврацький О.О. Transformation of the innovative component of management processes in the context of digitalization. Приазовський економічний вісник. 2025. № 2 (42). URL: http://www.pev.kpu.zp.ua/vypusk-2-42);
- інтеграцію запропонованих методів економіко-математичного моделювання в практичну частину курсових та дипломних робіт, зокрема, при вирішенні завдань ефективності інвестицій в кібербезпеку.

Результати дослідження планується і надалі використовувати при підготовці бакалаврів, магістрів та докторів філософії на факультеті кібербезпеки та інформаційних технологій. Це сприятиме формуванню у студентів системного розуміння процесів впровадження управлінських інновацій в умовах актуальних безпекових викликів цифрового середовища.

Члени комісії:

Проректор з навчальної роботи,
доктор юридичних наук, професор Галина УЛЬЯНОВА

Завідувач кафедри кібербезпеки,
доктор економічних наук, професор Станіслав ГОРБАЧЕНКО

Доцент кафедри кібербезпеки,
кандидат фізико-математичних наук, доцент Олена ЧЕПУРНА