КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1060
УДК 004.056.5:005.334

Легомінова Світлана Володимирівна
д.е.н., професор,
завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Примаченко Діана Володимирівна
асистент
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

РОЛЬ РИЗИК-МЕНЕДЖМЕНТУ В ПІДВИЩЕННІ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЇ ЗА УМОВ ГІБРИДНИХ ЗАГРОЗ

Анотація. У статті здійснено комплексне дослідження ролі ризик-менеджменту в забезпеченні кіберстійкості організації в умовах інтенсифікації гібридних загроз, які поєднують кібернетичні, інформаційно-психологічні, організаційні та технологічні впливи. Актуальність дослідження зумовлена зростанням складності сучасного безпекового середовища, у якому традиційні підходи до кібербезпеки виявляються недостатньо ефективними без урахування системних ризиків та невизначеностей. У роботі проведено аналіз сутності гібридних загроз та гібридних впливів, визначено їхні ключові характеристики, механізми реалізації та наслідки для функціонування інформаційної інфраструктури організацій. Особливу увагу приділено впливу таких загроз на критичні інформаційні ресурси, бізнес-процеси та безперервність діяльності. Узагальнено сучасні наукові підходи до управління кіберризиками, зокрема стандартизовані та адаптивні моделі, що використовуються в міжнародній практиці. Розглянуто основні елементи ризик-орієнтованого підходу до забезпечення кіберстійкості, включаючи ідентифікацію загроз, оцінювання ймовірності та потенційних наслідків ризиків, визначення пріоритетів реагування, а також моніторинг і перегляд ризикового профілю організації. Проаналізовано можливості інтеграції ризик-менеджменту в загальну систему управління кібербезпекою, корпоративного управління та стратегічного планування. Показано переваги застосування ризик-орієнтованого підходу порівняно з фрагментарними або реактивними заходами захисту. У статті запропоновано модель підвищення кіберстійкості організації шляхом оптимізації процесів ризик-менеджменту, яка передбачає узгодження технічних, організаційних і управлінських заходів, підвищення рівня обізнаності персоналу та формування культури управління ризиками. Результати дослідження свідчать, що ефективна та системна реалізація ризик-менеджменту є базовою умовою формування стійкої до гібридних загроз організаційної структури, забезпечення захищеності критичних інформаційних ресурсів і підвищення адаптивності організацій до динамічних викликів сучасного кіберпростору.

Ключові слова: кібербезпека; кіберстійкість; гібридні загрози; ризик-менеджмент; управління ризиками; інформаційна безпека.

ВСТУП

Цифрова трансформація всіх сфер діяльності організацій зумовлює стрімке зростання залежності бізнес-процесів, комунікацій і систем управління від інформаційних технологій. Паралельно з цим підвищується рівень кіберзагроз, які все

частіше мають гібридний характер — поєднання технічних атак, психологічного впливу, інформаційних операцій, маніпулятивних дій та соціальної інженерії. Гібридні загрози відзначаються непередбачуваністю, багатокомпонентністю та здатністю впливати не лише на ІТ-інфраструктуру, а й на управлінські процеси та репутацію організації.

Постановка проблеми. Організації все частіше стикаються з різноманітними загрозами, які виникають на перетині інформаційних технологій, соціальних мереж та політичних процесів. Гібридні загрози, що поєднують кібернетичні атаки, дезінформацію та психологічний вплив на персонал, створюють складне середовище для функціонування будь-якої організації. Традиційні підходи до інформаційної безпеки, що зосереджуються лише на технічних засобах захисту, виявляються недостатніми для забезпечення стійкості до цих комплексних впливів, тому ризик-менеджмент набуває особливої актуальності, оскільки дозволяє системно оцінювати потенційні загрози, їхні наслідки та визначати ефективні заходи для мінімізації шкоди. Формування кіберстійкості організації стає неможливим без інтегрованого підходу, що поєднує технічні, організаційні та стратегічні аспекти управління ризиками.

Аналіз останніх досліджень і публікацій. Jawhar та співавтоори зазначають, що застосування технологій штучного інтелекту в процесах оцінювання кіберризиків відкриває можливість суттєво підвищити точність прогнозування потенційних інцидентів та оптимізувати механізми реагування організацій на загрози [6]. На думку авторів, алгоритми машинного навчання дають змогу виявляти приховані кореляції в масивах даних безпеки, формувати адаптивні моделі загроз та автоматично визначати аномалії, що значно знижує імовірність пропуску критичних подій. Використання таких підходів є особливо актуальним у динамічному середовищі гібридних загроз, де поведінка нападників є нестабільною та важко прогнозованою традиційними методами.

У дослідженні Jazairy та співавторів підкреслюється стратегічна важливість інтеграції методів кіберризик-менеджменту у структуру ланцюгів постачання для забезпечення їхньої стійкості, надійності та захищеності від комбінованих впливів [5]. Автори наголошують, що атаки на постачальників, логістичні центри або суміжних партнерів можуть мати cascading effect — ефект «ланцюгової реакції», який паралізує діяльність всієї екосистеми. Тому управління кіберризиками має здійснюватися не ізольовано в межах окремої організації, а в рамках ширшої мережевої взаємодії, включаючи аудит постачальників, безперервний моніторинг та спільні протоколи реагування.

Поряд із технологічними аспектами вагоме місце посідає людський фактор. Mer акцентує увагу на потенціалі штучного інтелекту в управлінні персоналом, зокрема у процесах оцінювання компетентності працівників, аналізі поведінкових ризиків та підтримці прийняття управлінських рішень [7]. Науковець доводить, що використання моделей поведінкової аналітики (UBA/UEBA) дозволяє ідентифікувати небезпечні або нехарактерні дії користувачів, виявляти схильність до порушення політик безпеки та прогнозувати ризик інсайдерських загроз.

Millot у своїх дослідженнях наголошує на значущості кооперативних організаційних структур, які забезпечують підвищення рівня ситуаційної обізнаності, прозорість комунікації та швидкість реагування на інциденти [8]. Автор підкреслює, що ефективна взаємодія між командами, підрозділами та зовнішніми партнерами дозволяє створити інтегровану систему підтримки рішень, що є критично важливою за умов гібридних атак, коли швидкість і точність інформаційного обміну визначають результативність протидії загрозам.

Мета статті. Метою цієї статті є дослідження ролі ризик-менеджменту в підвищенні кіберстійкості організації за умов гібридних загроз. Основна задача полягає у визначенні ключових принципів та механізмів управління ризиками, які забезпечують комплексну захищеність організації, з урахуванням технічних, організаційних та стратегічних аспектів кібербезпеки. У статті також прагнеться окреслити практичні підходи до інтеграції ризик-менеджменту у внутрішню політику організації та забезпечення її готовності до різнопланових загроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз сучасних концепцій та підходів до ризик-менеджменту у сфері кібербезпеки засвідчує, що його інтеграція в організаційну структуру суттєво підвищує здатність підприємств та установ протидіяти багатовекторним гібридним загрозам. Ризик-менеджмент у цьому контексті виступає не лише інструментом оцінювання технічних вразливостей, а й комплексним механізмом управління, що охоплює стратегічні, організаційні та поведінкові аспекти безпеки. Одним із ключових результатів узагальнення наукових джерел є підтвердження того, що систематичне, циклічне й методологічно виважене оцінювання ризиків дозволяє своєчасно виявляти структурні та процесні слабкі місця в інформаційній інфраструктурі, корпоративних технологічних ланцюгах, системах доступу й комунікаційних потоках [2]. Це, у свою чергу, істотно знижує ймовірність успішної реалізації атак, зменшує можливість неконтрольованого поширення загроз і забезпечує більш раціональне формування захисних контрзаходів.

Важливим компонентом ефективного ризик-менеджменту є запровадження процедур постійного моніторингу, аналізу та кореляції подій безпеки. У сучасних умовах гібридної війни традиційні реактивні моделі захисту виявляються недостатніми, оскільки загрози характеризуються високою динамічністю, адаптивністю та синхронізованістю з інформаційними чи психологічними впливами. Безперервний моніторинг із використанням інструментів SIEM, SOAR, EDR та UEBA дає можливість виявляти аномалії на ранніх стадіях, оцінювати їх критичність та здійснювати автоматизоване або напівавтоматизоване реагування, що значно зменшує масштаб потенційних збитків. Таким чином, ризик-менеджмент стає основою для переходу від реактивних стратегій захисту до проактивних, адаптивних та прогностичних моделей.

KPMG Ukraine може слугувати як приклад української консалтингової/аудиторської фірми, яка допомагає бізнесу реалізувати risk-менеджмент кіберзагроз в умовах гібридних загроз. За інформацією KPMG Ukraine, багато українських компаній зараз сприймають кібербезпеку як стратегічний пріоритет — і в умовах війни та зростання загроз, бізнес дедалі активніше інвестує у захист IT-інфраструктури. Компанія рекомендує підприємствам будувати системи управління інформаційною безпекою, формувати політики, створювати центри реагування, проводити оцінку ризиків та впроваджувати стандарти безпеки [8].

Також PwC є професійною структурою, що реалізує risk-менеджмент кібербезпеки та допомагає компаніям підвищити їхню кіберстійкість. У публікації «Розбудова кібербезпеки завдяки співпраці топменеджменту» PwC описує, як у регіоні Центральної та Східної Європи компанії зміцнюють кіберстійкість. Зокрема, там зазначено, що дедалі частіше залучають директорів з інформаційної безпеки до стратегічного планування компаній, що є частиною risk-менеджменту в IT [9]. PwC надає послуги з кібербезпеки, допомагає оцінювати ризики, проводити аудит безпеки, тестування, планування політик

реагування на інциденти тощо. Це – приклад професійної консалтингової організації, яка допомагає «іншій» організації впровадити risk-менеджмент кіберзагроз і підвищити її кіберстійкість.

Наукові дослідження підтверджують, що формування корпоративної культури кібербезпеки, яка передбачає усвідомлення персоналом важливості дотримання політик безпеки, регулярне проходження тренінгів, підвищення цифрової грамотності й відпрацювання сценаріїв реагування, є критичним фактором у зменшенні впливу людського чинника. Людський фактор, відповідальний за значну частку інцидентів, може бути ефективно мінімізований у разі впровадження системи постійного навчання, моделювання інцидентів, проведення тестових атак соціальної інженерії та формування особистої відповідальності співробітників за дії в інформаційному середовищі.

Окрему увагу слід приділити тому, що ризик-менеджмент сприяє не лише підвищенню рівня безпеки, а й оптимізації витрат на кіберзахист. Завдяки системному аналізу ризиків організації можуть більш обґрунтовано розподіляти фінансові та людські ресурси між превентивними заходами, інструментами моніторингу, підсистемами резервування, методами реагування та заходами з відновлення. Це дає змогу зменшити надлишкові інвестиції у другорядні процеси та сконцентрувати ресурси на критичних напрямах, що безпосередньо впливають на безперервність діяльності. Якщо узагальнити ключові етапи ризик-менеджменту [1], можна подати їх у вигляді схеми, зображеної на рис. 1.

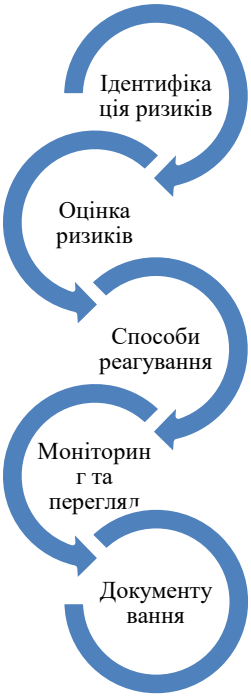

Рис. 1. Етапи процесу ризик-менеджменту підприємств

Сучасні гібридні загрози вирізняються комплексністю, оскільки поєднують кібератаки, інформаційно-психологічний тиск, маніпуляції довірою, підривні операції у медіапросторі та, в окремих випадках, фізичний вплив на інфраструктуру. За таких умов організації, що впроваджують системний ризик-менеджмент, здатні формувати гнучкі, багаторівневі й адаптивні механізми захисту, які відповідають реальній динаміці загрозового середовища. Стратегічне планування на основі ризик-орієнтованого підходу

дозволяє створювати сценарні моделі можливих атак, визначати індикатори раннього попередження та формувати довгострокові програми модернізації систем захисту.

Інтеграція ризик-менеджменту з управлінням бізнес-процесами, системами планування безперервності діяльності (BCP/DRP), внутрішнім аудитом і корпоративним управлінням сприяє створенню цілісної екосистеми кіберстійкості. Такий підхід дозволяє не лише уніфікувати процеси управління ризиками, а й забезпечити їх узгодженість на всіх рівнях — від тактичного до стратегічного [3].

Дуже важливим напрямом є оцінювання та розвиток людського потенціалу. Ризик-менеджмент у сфері кібербезпеки передбачає впровадження систем класифікації компетентностей, аналіз поведінкових ризиків, мотиваційних механізмів і процедур контролю доступу, що дозволяють формувати персонал, здатний діяти ефективно та своєчасно в умовах кризових ситуацій. Досвід практичних впроваджень підтверджує, що навіть найбільш технічно оснащені організації зазнають поразок у разі недооцінювання ролі персоналу в підтримці безпеки.

Роль ризик-менеджменту в підвищенні кіберстійкості організації є комплексною, системною та багаторівневою. Вона охоплює технічні, стратегічні, організаційні, економічні та поведінкові аспекти захисту. Інтеграція ризик-менеджменту у всі рівні управління забезпечує не лише зменшення ймовірності успішних атак чи мінімізацію шкоди від інцидентів, але й створює умови для оперативного відновлення бізнес-процесів, збереження репутаційної стійкості та підвищення конкурентоспроможності організації в довгостроковій перспективі.

Модель підвищення кіберстійкості організації на основі ризик-орієнтованого підходу відображає взаємозв'язки між ключовими елементами системи управління кіберризиками [4]. Вона включає послідовні етапи ідентифікації загроз, оцінювання ризиків, визначення пріоритетів, впровадження технічних та організаційних заходів, а також постійного моніторингу та вдосконалення політик безпеки. Особливістю моделі є інтеграція технічних механізмів (SIEM, EDR, SOAR), управлінських процесів (аудит, планування безперервності діяльності), а також оцінювання людського фактору як ключового елемента кіберстійкості. Структура моделі представлена на рис. 2.

Рис. 2. Модель підвищення кіберстійкості організації в умовах гібридних загроз на основі ризик-орієнтованого підходу (розробка автора)

Наведена модель підкреслює, що ефективність ризик-менеджменту у сфері кібербезпеки визначається не лише наявністю окремих технологічних рішень чи

регламентів, а узгодженістю та взаємодією всіх її компонентів. Успішні організації використовують ризик-орієнтований підхід як основу для формування цілісної системи кіберзахисту, у якій кожен елемент — від технічної інфраструктури до компетентностей персоналу — підсилює інші. Завдяки цьому забезпечується здатність не лише протидіяти актуальним загрозам, а й швидко адаптуватися до нових форм кібернетичного та інформаційного впливу.

Інтеграція ризик-менеджменту в загальну систему корпоративного управління створює умови для формування стійкої, адаптивної та прогнозованої моделі кіберзахисту, що відповідає викликам сучасного гібридного середовища. Такий підхід дозволяє організаціям підтримувати безперервність діяльності, захищати критичні ресурси, підвищувати рівень довіри з боку партнерів і клієнтів та зміцнювати власні позиції на ринку. Саме тому ризик-менеджмент виступає не допоміжним, а стратегічним компонентом розвитку кіберстійкості, визначаючи довгострокову конкурентоспроможність і здатність організації ефективно діяти в умовах постійно зростаючої складності кіберзагроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Системний підхід до управління ризиками дозволяє ідентифікувати потенційні загрози, оцінити їх вплив на критичні активи та сформувати ефективні стратегії реагування. Інтеграція ризик-менеджменту у внутрішні процеси організації підвищує готовність до кібератак, оптимізує витрати на кіберзахист та сприяє формуванню корпоративної культури кібербезпеки.

Отже, ризик-менеджмент виступає не лише інструментом оцінки і контролю загроз, але й стратегічним механізмом забезпечення стійкості організації у складному гібридному середовищі. Його впровадження дозволяє організаціям адаптуватися до нових викликів, зменшувати негативні наслідки інцидентів та забезпечувати безперервність функціонування бізнес-процесів. В умовах гібридних загроз ефективне управління ризиками стає ключовою складовою національної та корпоративної безпеки, що робить його невід'ємною частиною стратегії кіберзахисту будь-якої організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Visure Solutions. (2025). *Top 10+ best risk management software solutions and tools for 2025*. https://visuresolutions.com/uk/alm-guide/найкраще-програмне-забезпечення-для-управління-ризиками-а/
2. Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., & Thalassinos, E. (2023). Cyber incident response managerial approaches for enhancing small- and medium-sized enterprises' cyber maturity. In *Digital transformation, strategic resilience, cyber security and risk management* (pp. 175–190). Emerald Publishing Limited. https://doi.org/10.1108/s1569-37592023000111a012
3. OECD. (2017). Growing cyber risk and the contribution of insurance to cyber risk management. In *Enhancing the role of insurance in cyber risk management* (pp. 11–17). https://doi.org/10.1787/9789264282148-3-en
4. Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cybersecurity resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems, 34*(1). https://doi.org/10.1080/12460125.2025.2479546

5. Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: Toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management*, *54*(11), 1–29. https://doi.org/10.1108/IJPDLM-12-2023-0445
6. Lazebnyk, I. O., & Arnautova, Y. A. (2020). The methodological foundations of statistical analysis of the labor market in Ukraine and the role of HR management in improving the quality of human resources. *Business Inform*, *10*(513), 220–227. https://doi.org/10.32983/2222-4459-2020-10-220-227
7. Mer, A. (2023). Artificial intelligence in human resource management: Recent trends and research agenda. In *Digital transformation, strategic resilience, cyber security and risk management* (pp. 31–56). Emerald Publishing Limited. https://doi.org/10.1108/s1569-37592023000111b003
8. KPMG. (2025). *Cybersecurity and IT risk management*. https://kpmg.com/ua/uk/home/services/consulting/technology/information-protection-and-cyber-security.html
9. PwC. (2025). *Building cybersecurity through top management collaboration*. https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Svitlana Lehominova
Doctor of Sciences, professor, head of the department of information and cyber security management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Diana Prymachenko
Assisant
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID 0009-0003-2386-7440
primachenkodiana08@gmail.com

THE ROLE OF RISK MANAGEMENT IN IMPROVING THE CYBER RESILIENCE OF AN ORGANISATION IN THE CONTEXT OF HYBRID THREATS

Анотація. The article provides a comprehensive study of the role of risk management in ensuring the cyber resilience of an organisation in the context of intensifying hybrid threats that combine cybernetic, informational-psychological, organisational and technological influences. The relevance of the study is due to the increasing complexity of the modern security environment, in which traditional approaches to cybersecurity are proving insufficiently effective without taking into account systemic risks and uncertainties. The paper analyses the essence of hybrid threats and hybrid influences, identifies their key characteristics, mechanisms of implementation and consequences for the functioning of the information infrastructure of organisations. Particular attention is paid to the impact of such threats on critical information resources, business processes and business continuity. It summarises current scientific approaches to cyber risk management, including standardised and adaptive models used in international practice. The main elements of a risk-oriented approach to ensuring cyber resilience are considered, including threat identification, assessment of the probability and potential consequences of risks, prioritisation of responses, and monitoring and review of the organisation's risk profile. The possibilities of integrating risk management into the overall system of cybersecurity management, corporate governance, and strategic planning are analysed. The advantages of applying a risk-oriented approach compared to fragmented or reactive protection measures are demonstrated. The article proposes a model for improving the cyber resilience of an organisation by optimising risk management processes, which involves coordinating technical, organisational and managerial measures, raising staff awareness and developing a risk management culture. The results of the study show that effective and systematic implementation of risk management is a basic condition for forming an organisational structure that is resistant to hybrid threats, ensuring the security of critical information resources and increasing the adaptability of organisations to the dynamic challenges of the modern cyberspace.

Ключові слова: cybersecurity; cyber resilience; hybrid threats; risk management; risk control; information security.

REFERENCES

1. Visure Solutions. (2025). *Top 10+ best risk management software solutions and tools for 2025*. https://visuresolutions.com/uk/alm-guide/найкраще-програмне-забезпечення-для-управління-ризиками-а/
2. Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., & Thalassinos, E. (2023). Cyber incident response managerial approaches for enhancing small- and medium-sized enterprises' cyber maturity. In *Digital transformation, strategic resilience, cyber security and risk management* (pp. 175–190). Emerald Publishing Limited. https://doi.org/10.1108/s1569-37592023000111a012
3. OECD. (2017). Growing cyber risk and the contribution of insurance to cyber risk management. In *Enhancing the role of insurance in cyber risk management* (pp. 11–17). https://doi.org/10.1787/9789264282148-3-en

4. Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cybersecurity resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems, 34*(1). https://doi.org/10.1080/12460125.2025.2479546
5. Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: Toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management, 54*(11), 1–29. https://doi.org/10.1108/IJPDLM-12-2023-0445
6. Lazebnyk, I. O., & Arnautova, Y. A. (2020). The methodological foundations of statistical analysis of the labor market in Ukraine and the role of HR management in improving the quality of human resources. *Business Inform, 10*(513), 220–227. https://doi.org/10.32983/2222-4459-2020-10-220-227
7. Mer, A. (2023). Artificial intelligence in human resource management: Recent trends and research agenda. In *Digital transformation, strategic resilience, cyber security and risk management* (pp. 31–56). Emerald Publishing Limited. https://doi.org/10.1108/s1569-37592023000111b003
8. KPMG. (2025). *Cybersecurity and IT risk management*. https://kpmg.com/ua/uk/home/services/consulting/technology/information-protection-and-cyber-security.html
9. PwC. (2025). *Building cybersecurity through top management collaboration*. https://www.pwc.com/ua/uk/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey.html