МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова
праця на правах рукопису

СКУРАТІВСЬКИЙ АНАТОЛІЙ АНАТОЛІЙОВИЧ

УДК 004.4:658.5:004.056

ДИСЕРТАЦІЯ

МЕТОДИ ТА ІНСТРУМЕНТАЛЬНІ ЗАСОБИ УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В БІЗНЕСІ

122 – Комп’ютерні науки

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ А.А. Скуратівський

Науковий керівник – Гнатюк Сергій Олександрович, доктор технічних наук, професор

Київ – 2026

АНОТАЦІЯ

Скуратівський А.А. Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки». – Державний університет «Київський авіаційний інститут», Київ, 2026.

Проведено аналіз сучасних підходів до управління вимогами кібербезпеки при впровадженні ПЗ. Встановлено, що управління вимогами кібербезпеки є ключовим елементом забезпечення надійного захисту інформаційних систем організації. Ефективне виявлення, аналіз, документування та впровадження вимог допомагають мінімізувати ризики та забезпечити відповідність нормативним вимогам та стандартам. Використання найкращих практик у цій галузі сприяє підвищенню загального рівня кібербезпеки організації.

Встановлено, що технічні специфікації та архітектурні рішення є основою для забезпечення кібербезпеки в організації, забезпечуючи необхідні інструменти та методи для захисту інформаційних систем від кіберзагроз. Функціональні вимоги кібербезпеки охоплюють широкий спектр заходів, спрямованих на забезпечення захисту інформаційних систем та даних від різноманітних загроз, мінімізацію ризиків та забезпечення відповідності нормативним вимогам та стандартам. Нефункціональні вимоги кібербезпеки є критичними для забезпечення загальної безпеки, стійкості та надійності інформаційних систем. Документування вимог кібербезпеки є критичним процесом для забезпечення захисту інформаційних систем та даних – воно допомагає структурувати та систематизувати вимоги, забезпечувати їхню зрозумілість та узгодженість, а також полегшувати процес їхнього впровадження та контролю. Дотримання рекомендацій та використання сучасних інструментів управління вимогами сприяють підвищенню загального рівня кібербезпеки на підприємстві.

Аналіз сучасних наукових підходів до управління вимогами кібербезпеки показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на

необхідності вдосконалення нормативно-правової бази, впровадження галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки. Дослідження підкреслюють важливість міждисциплінарного підходу, гармонізації з міжнародними стандартами та використання аналітики загроз для прийняття ефективних рішень. Загалом, ефективне управління вимогами кібербезпеки розглядається як комплексний процес, що охоплює як технічні, так і правові аспекти.

Основним недоліком відомих підходів імплементації вимог в життєвий цикл розроблення ПЗ є відсутність формалізованої, динамічної та трасованої інтеграції вимог кібербезпеки у всі етапи життєвого циклу розроблення ПЗ, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів та підвищення рівня ризику.

Проведено дослідження математичних методів для управління вимогами кібербезпеки при впровадженні ПЗ. Було розроблено модель, яка дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків за допомогою нечіткої логіки і байєсової мережі, а також оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків. Розроблена модель забезпечує комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків.

На основі розробленої моделі управління вимогами кібербезпеки при впровадженні ПЗ було проведено практичні симуляції з використанням фреймворків міжнародних стандартів і рекомендованих практик, зокрема досліджено: 1) розроблену модель на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно з вимогами цього стандарту; 2) розроблену модель на основі стандарту ISO 22316, що забезпечило досягнення балансу між важливістю вимог, мінімізацією ризиків і наявними ресурсами, відповідно вимогам цього стандарту для забезпечення стійкості організації; 3) розроблену модель на основі стандарту MITRE ATT&CK, що забезпечило виконання критичних вимог цього стандарту і мінімізацію загальних ризиків при дотриманні бюджету.

Розроблено метод динамічного управління вимогами кібербезпеки, який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень, формування зворотного зв'язку та ініціації наступного циклу управління вимогами, дає змогу забезпечити інтегровану оцінку їх структурної, регуляторної та динамічної значущості з подальшою формалізацією управлінського рішення через оптимізаційну модель розподілу ресурсів та ітераційний механізм зворотного зв'язку. Це дозволяє інтегрувати топологічні та станові характеристики системи, максимізувати ефект від використання бюджету, регулярно оновлювати пріоритети, врахувати нові вимоги кібербезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов.

Практична цінність зазначеного методу полягає у створенні формалізованого адаптивного механізму управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості інформаційно-комунікаційних систем. Запропонований метод формалізований у вигляді псевдокоду та може бути реалізований у: системах підтримки прийняття рішень; програмних засобах управління кіберризиками; корпоративних GRC-платформах; автоматизованих системах планування тощо.

Використовуючи теорію множин, було формалізовано у загальному вигляді відомі моделі життєвого циклу розроблення ПЗ (класична каскадна модель, V-модель, інкрементальна модель, спіральна модель, Agile, DevOps, DevSecOps), що дало можливість сформувати уніфіковану модель SDLC. Використовуючи уніфіковану модель SDLC, розроблено метод інтегрування вимог кібербезпеки в SDLC, що за рахунок формалізації DevSecOps, ідентифікації вимог кібербезпеки, трансформації вимог у контрольні механізми, інтегрування контрольних механізмів у SDLC, верифікування та моніторингу виконання вимог кібербезпеки у вигляді системи

множин та відображень, дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень.

Практична цінність запропонованого методу полягає у можливості його використання для системного інтегрування вимог кібербезпеки в процеси розроблення ПЗ в організаціях, що створюють або експлуатують інформаційні системи критичної інфраструктури, хмарні сервіси та корпоративні інформаційно-комунікаційні системи. Застосування розробленого методу дозволяє: забезпечити узгодженість вимог кібербезпеки на всіх етапах SDLC; підвищити рівень автоматизації контролю кібербезпеки у DevSecOps pipeline; зменшити ризик пропуску критичних вимог кібербезпеки під час швидких ітерацій розроблення; підвищити обґрунтованість вибору засобів захисту інформації; скоротити витрати на усунення вразливостей за рахунок їх виявлення на ранніх етапах SDLC; забезпечити можливість кількісного оцінювання рівня реалізації вимог кібербезпеки за допомогою метрик кібербезпеки; створити інструментальні засоби підтримки прийняття рішень у процесах DevSecOps.

Крім того, запропонований метод може бути використаний при проєктуванні захищених інформаційно-комунікаційних систем; аудиті процесів безпечної розробки ПЗ згідно зі стандартами ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних IT-системах тощо.

Ключові слова: *вимога, безпека, кібербезпека, інформаційна безпека, управління, стандарт, політика, модель, метод, регулювання, нечіткі множини, програмне забезпечення, ризик, метрика, метрика безпеки, параметри, система підтримки прийняття рішень.*

ABSTRACT

Skurativskyi A. Methods and instrumental tools for cybersecurity requirements management during software implementation in business. – Qualifying scientific work on manuscript rights.

Dissertation for the Doctor of Philosophy degree in specialty 122 «Computer Science». – State University «Kyiv Aviation Institute», Kyiv, 2026.

An analysis of current approaches to managing cybersecurity requirements during software implementation has been conducted. It has been established that managing cybersecurity requirements is a key element in ensuring the reliable protection of an organization's information systems. Effective identification, analysis, documentation, and implementation of requirements help minimize risks and ensure compliance with regulatory requirements and standards. The use of best practices in this field contributes to improving the organization's overall level of cybersecurity.

It has been established that technical specifications and architectural solutions form the foundation for ensuring cybersecurity within an organization, providing the necessary tools and methods to protect information systems from cyber threats. Functional cybersecurity requirements encompass a wide range of measures to protect information systems and data from threats, minimize risks, and ensure compliance with regulatory requirements and standards. Non-functional cybersecurity requirements are critical for ensuring the overall security, resilience, and reliability of information systems. Documenting cybersecurity requirements is a critical process for protecting information systems and data. It helps structure and systematize requirements, ensure their clarity and consistency, and facilitate their implementation and monitoring. Adhering to recommendations and using modern requirements management tools contributes to improving the overall level of cybersecurity within an organization.

An analysis of current scientific approaches to cybersecurity requirements management has shown that modern approaches focus on improving the regulatory framework, implementing industry-specific frameworks, integrating cyber risk management, and standardizing security processes. Research highlights the importance of

an interdisciplinary approach, alignment with international standards, and the use of threat analytics for effective decision-making. Overall, effective cybersecurity requirements management is viewed as a comprehensive process encompassing both technical and legal aspects.

The main drawback of known approaches to integrating requirements into the software development lifecycle is the lack of formalized, dynamic, and traceable integration of cybersecurity requirements across all stages, leading to fragmented threat consideration, delayed control implementation, and increased risk.

A study of mathematical methods for managing cybersecurity requirements during software implementation was conducted. A model was developed that allows prioritizing cybersecurity requirements, accounting for uncertainties and risk probabilities using fuzzy logic and Bayesian networks, and optimally allocating resources among requirements while considering budget constraints and risk minimization. The developed model provides comprehensive management of cybersecurity requirements during software implementation, accounting for international standards and modern risk assessment methods.

Based on the developed model for managing cybersecurity requirements during software implementation, practical simulations were conducted using frameworks of international standards and recommended practices; in particular, the following were investigated: 1) the developed model based on the NIST 800-53 standard, which ensured risk minimization while adhering to budget constraints and the prioritization of cybersecurity requirements in accordance with the requirements of this standard; 2) the developed model based on the ISO 22316 standard, which ensured a balance between the importance of requirements, risk minimization, and available resources, in accordance with the requirements of this standard to ensure organizational resilience; 3) a model developed based on the MITRE ATT&CK standard, which ensured compliance with the critical requirements of this standard and minimization of overall risks while adhering to the budget.

A method for the dynamic management of cybersecurity requirements has been developed, which, through the initialization of cybersecurity requirements in accordance with regulatory documents and standards, the identification of triggers for the dynamic

updating of cybersecurity requirements, the monitoring of changes in the software deployment environment and current threats, correlating and reassessing cybersecurity requirements in light of identified changes and risk updates, optimizing resource allocation among cybersecurity requirements based on updated priorities and constraints, generating feedback and initiating the next cycle of requirements management, enables an integrated assessment of their structural, regulatory, and dynamic significance, followed by the formalization of management decisions through an optimization model for resource allocation and an iterative feedback mechanism. This allows for integrating the system's topological and state characteristics, maximizes the impact of budget utilization, enables regular updates to priorities, accounts for new cybersecurity requirements during software implementation, and ensures the system's adaptation to changes in resource or regulatory conditions.

The practical value of this method lies in creating a formalized adaptive mechanism for managing cybersecurity requirements, ensuring well-founded priority selection, optimal resource allocation, and increased resilience of information and communication systems. The proposed method is formalized as pseudocode and can be implemented in decision support systems, cyber risk management software tools, corporate GRC platforms, automated planning systems, etc.

Using set theory, well-known software development lifecycle models (the classic waterfall model, V-model, incremental model, spiral model, Agile, DevOps, DevSecOps) were formalized in a general form, enabling the creation of a unified SDLC model. Using the unified SDLC model, a method was developed for integrating cybersecurity requirements into the SDLC, which, through the formalization of DevSecOps, the identification of cybersecurity requirements, the transformation of requirements into control mechanisms, the integration of control mechanisms into the SDLC, verifying and monitoring the fulfillment of cybersecurity requirements in the form of a system of sets and mappings, allows for the integration of cybersecurity requirements into a specific phase (pipeline) of the software development lifecycle, and also enables the formalized optimization of cybersecurity control selection depending on the system context and resource constraints.

The practical value of the proposed method lies in its applicability to systematically integrating cybersecurity requirements into software development processes within organizations that create or operate critical infrastructure information systems, cloud services, and corporate information and communication systems. The application of the developed method allows for: ensuring the consistency of cybersecurity requirements at all stages of the SDLC; increasing the level of automation of cybersecurity controls in the DevSecOps pipeline; reducing the risk of overlooking critical cybersecurity requirements during rapid development iterations; improving the soundness of the selection of information security measures; reduce the cost of vulnerability remediation by detecting them at early stages of the SDLC; enable quantitative assessment of the level of cybersecurity requirement implementation using cybersecurity metrics; and create decision-support tools for DevSecOps processes.

In addition, the proposed method can be used in the design of secure information and communication systems; auditing secure software development processes in accordance with ISO/IEC, NIST, PCI DSS, PSD2, GDPR, and MITRE ATT&CK standards; creating secure SDLC policies; implementing DevSecOps in government and corporate IT systems, etc.

Key words: *requirement, security, cybersecurity, information security, management, standard, policy, model, method, regulation, fuzzy sets, software, risk, metric, security metric, parameters, decision support system.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Гнатюк С.О., Сидоренко В.М., Скуратівський А.А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення. Кібербезпека: освіта, наука, техніка, 2025, Т.4, № 28, с. 25-37. DOI: https://doi.org/10.28925/2663-4023.2025.28.841

Здобувачу належить розроблення та формалізований опис моделі управління вимогами кібербезпеки при впровадженні ПЗ.

2. Гнатюк, С.О., Сидоренко В.М., Скуратівський А.А. Аналіз сучасних підходів до управління вимогами кібербезпеки при впровадженні програмного забезпечення, Проблеми інформатизації та управління, 2025, Т.2, № 82, с. 5-18, https://doi.org/10.18372/2073-4751.82.20363

Здобувачу належить визначення критеріїв і проведення аналізу, а також дослідження актуальних наукових публікацій за напрямком досліджень.

3. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів IT-інцидентів на об’єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління, 2024, Т. 2, №º78, С. 104-114, https://doi.org/10.18372/2073-4751.78.18967

Здобувачу належить дослідження вимог міжнародних стандартів ISO/IEC 20000 та NIST Cybersecurity Framework в контексті теми дисертації.

4. Скуратівський А. Метод управління вимогами кібербезпеки при впровадженні програмного забезпечення у бізнесі, Безпека інформації, 2025, Том. 31, № 3, с. 135-142.

5. Гнатюк С., Побережна З., Скуратівський А. Метод інтегрування вимог кібербезпеки в життєвий цикл розроблення програмного забезпечення, Кібербезпека: освіта, наука, техніка, Т. 4, №32, с. 947-962. https://doi.org/10.28925/2663-4023.2026.32.1184

Здобувачу належить формалізований опис моделі та методу інтегрування вимог кібербезпеки в життєвий цикл розроблення ПЗ.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Gnatyuk S., Sydorenko V., Polozhentsev A., Skurativskyi A., Kluczewska-Chmielarz K., Shuitenov G. Modern approaches to cybersecurity requirements management for software implementation, CEUR Workshop Proceedings, 2025, Vol. 4024, pp. 186-200.

Здобувачу належать визначення критеріїв та проведення порівняльного аналізу методів управління вимогами при впровадженні ПЗ в бізнесі.

7. Odarchenko R., Pinchuk A., Polihenko O., Skurativskyi A. A comparative analysis of cyber threat intelligence models, CEUR Workshop Proceedings, 2025, Vol. 3925, pp. 3-12.

Здобувачу належить дослідження моделей threat intelligence в контексті вимог кібербезпеки до розроблюваного ПЗ.

8. Dorozhynskyi S., Zakutynskyi I., Ryabyy M., Skurativskyi A. Maximizing Security and Efficiency in 5G Networks by Means of Quantum Cryptography and Network Slicing Concepts, Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems Technology and Applications, 2023, pp. 1031-1036, 10.1109/IDAACS58523.2023.10348871, ISSN 2770-4262

Здобувачу належить дослідження практичних аспектів безпеки сучасних програмних систем і контролю виконання вимог кібербезпеки.

Наукові праці, які додатково відображають наукові результати дисертації:

9. Гнатюк В.О., Батрак О.Г., Скуратівський А.А., Кудренко С.О., Метод оптимізації роботи системи масового обслуговування з використанням віртуального асистента на базі штучного інтелекту, Проблеми інформатизації та управління, 2025, Т.3. № 75, с. 21-28, https://doi.org/10.18372/2073-4751.75.18013

Здобувачу належить дослідження оптимізації безпеки систем масового обслуговування як прикладу ПЗ, до якого застосовуються вимоги кібербезпеки.

10. Gnatyuk S., Sydorenko V., Polozhentsev A., Skurativskyi A. Experimental Study of a Model for Cybersecurity Requirements Management Based on International Standards, Springer (прийнято до друку).

Здобувачу належить вибір стандартів і дослідження їх вимог в контексті застосування запропонованої моделі управління вимогами.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Стрімка цифровізація бізнесу, активне використання хмарних сервісів, IoT, AI та DevOps/DevSecOps-підходів призводять до зростання кількості кіберзагроз і ускладнення забезпечення безпеки ПЗ на всіх етапах його впровадження. При цьому існуючі підходи управління вимогами кібербезпеки часто є фрагментарними, несистемними та слабо інтегрованими у процеси життєвого циклу розроблення ПЗ, що ускладнює своєчасне виявлення вразливостей, підвищує ризик інцидентів та збільшує витрати на їх усунення.

Сучасний бізнес потребує ефективних методів і інструментальних засобів, що дозволяють інтегрувати вимоги кібербезпеки у процеси розроблення та впровадження ПЗ без зниження швидкості інновацій та time-to-market. Особливої важливості набуває забезпечення трасованості вимог кібербезпеки, автоматизації контролів у DevOps/DevSecOps-процесах, зниження операційних ризиків та оптимізації витрат на забезпечення кіберстійкості інформаційних систем, що безпосередньо впливає на безперервність бізнес-процесів, а також довіру клієнтів та конкурентоспроможність організацій.

Водночас сучасні підприємства активно впроваджують складні програмні системи, що базуються на мікросервісній архітектурі, хмарних платформах, API-інтеграціях, CI/CD pipeline та Agile-методологіях, що значно підвищує динамічність змін у ПЗ та ускладнює управління вимогами протягом життєвого циклу ПЗ. Часті оновлення, інтеграція сторонніх сервісів, використання відкритих бібліотек та швидке масштабування IT-рішень формують потребу у методах, які дозволяють системно управляти вимогами під час проєктування, розроблення, тестування, розгортання та супроводу ПЗ, забезпечуючи узгодженість функціональних, нефункціональних і технологічних вимог у складних IT-середовищах.

Таким чином, розроблення методів та інструментальних засобів управління вимогами кібербезпеки при впровадженні ПЗ є ***актуальним науково-технічним завданням,*** спрямованим на підвищення загального рівня резильєнтності

інформаційних систем бізнесу, забезпечення їх стійкості та відповідності сучасним стандартам і рекомендованим практикам в галузі ІТ та кібербезпеки.

Зв'язок роботи з науковими програмами, планами, темами, грантами

Тема дисертаційної роботи корелює з *Глобальною інноваційною стратегією України WinWin2030,* що визначає ключові напрямки, цілі та принципи державної політики у сфері цифрового розвитку інноваційної діяльності. Зокрема, в контексті досягнення *Стратегічної цілі 15 «Створення умов для розробки та застосування продуктів у сфері кібербезпеки»,* що включає в себе розробку та безпечне використання ІТ-технологій і продуктів у сфері кібербезпеки, удосконалення нормативно-правового та технічного регулювання у сфері кібербезпеки та кіберзахисту, проведення заходів із виявлення вразливостей, загроз, оперативного та комплексного реагування на кіберінциденти та кібератаки. При цьому доцільним є використання досвіду країн ЄС (рекомендацій ENISA, NIST, CISA тощо) та інформації для реалізації зазначених напрямів для досягнення кінцевої мети – забезпечення кібербезпеки та кіберстійкості держави, її критичної інфраструктури, оборонної сфери, електронних послуг тощо.

В університеті проводиться / проводилась низка науково-дослідних робіт (на базі кафедри, де виконана дисертація), пов'язаних з тематикою цієї дисертаційної роботи, зокрема:

- «Інтелектуалізована система захищеного передавання пакетних даних на базі розвідувально-пошукового безпілотного літального апарату», номер державної реєстрації 0122U002361;
- «Методи, моделі та алгоритми побудови квантово-безпечної інформаційної інфраструктури», номер державної реєстрації 0122U002360;
- «Алгоритмічно-програмне забезпечення універсальних методів захищеного передавання даних при використанні розвідувально-пошукового БПЛА» номер державної реєстрації 0123U100495;
- Міжнародні проєкти Horizon Europe та NATO SPS тощо.

Мета дисертаційного дослідження полягає в підвищенні ефективності процесу впровадження ПЗ в бізнесі шляхом розроблення методів та інструментальних засобів управління вимогами кібербезпеки, які забезпечують їх формалізовану інтеграцію, трасованість, адаптацію до змін середовища загроз і ресурсних обмежень, а також узгодженість з функціональними та нефункціональними вимогами інформаційних систем.

Для досягнення поставленої мети необхідно розв'язати такі **задачі:**

1) Провести аналіз сучасних підходів до управління вимогами кібербезпеки при розробленні і впровадженні ПЗ, для виявлення їх недоліків, вибору найбільш ефективних математичних методів і підходів та формалізації завдання дослідження;
2) Розробити та дослідити математичну модель управління вимогами кібербезпеки при впровадженні ПЗ на основі міжнародних стандартів для забезпечення ефективного управління вимогами кібербезпеки під час впровадження ПЗ в бізнесі (визначати пріоритетні вимоги, оптимально розподіляти ресурси з урахуванням обмежень тощо);
3) Розробити метод динамічного управління вимогами кібербезпеки для врахування нових вимог кібербезпеки при впровадженні ПЗ, а також забезпечення адаптації системи до зміни ресурсних або нормативних умов;
4) Розробити уніфіковану модель SDLC та на її базі метод інтегрування вимог кібербезпеки в SDLC для інтегрування вимог кібербезпеки в конкретну фазу життєвого циклу розроблення ПЗ та оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень;
5) Провести експериментальне дослідження розроблених моделей і методів з використанням розроблених інструментальних засобів (псевдокоди, симуляційні моделі та фреймворки).

Об'єктом дослідження є процес управління вимогами кібербезпеки.

Предметом дослідження є методи, моделі та інструментальні засоби управління вимогами кібербезпеки при впровадженні ПЗ в бізнесі.

Методи дослідження

У роботі використано теорію множин (у тому числі, з елементами нечіткої логіки), теорію графів, метод аналізу ієрархій (Analytic Hierarchy Process, AHP), теорію байєсових мереж, методи оптимізації та неформальне представлення алгоритмів програмування за допомогою псевдокодів, симуляційні моделі та фреймворки.

Наукова новизна отриманих результатів полягає в розробленні нових і удосконалених методів та моделей для формалізації процесу управління вимогами кібербезпеки при впровадженні ПЗ в бізнесі, зокрема:

уперше:

Розроблено математичну модель управління вимогами кібербезпеки при впровадженні ПЗ, що за рахунок створення графу залежностей вимог, використання методу AHP для пріоритезації вимог, застосування нечіткої логіки для оцінки рівня відповідності вимогам, моделювання ризиків за допомогою Байєсової мережі та оптимізації ресурсів за допомогою математичного програмування, дозволяє дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків, а також оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків, забезпечуючи комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків.

Розроблено метод динамічного управління вимогами кібербезпеки, який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням

оновлених пріоритетів і обмежень, формування зворотного зв'язку та ініціації наступного циклу управління вимогами, дає змогу регулярно оновлювати пріоритети, врахувати нові вимоги кібербезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов.

удосконалено:

Метод інтегрування вимог кібербезпеки в SDLC, що за рахунок формалізації моделі DevSecOps (на базі уніфікованої моделі SDLC), ідентифікації вимог кібербезпеки, трансформації вимог у контрольні механізми, інтегрування контрольних механізмів у SDLC, верифікування та моніторингу виконання вимог кібербезпеки у вигляді системи множин та відображень, дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень;

отримала подальший розвиток:

Уніфікована модель SDLC, яка за рахунок формалізованого відображення множин фаз життєвого циклу розроблення ПЗ, відношень між фазами та функцій, дозволяє представити відомі моделі життєвого циклу розроблення ПЗ у зручній формі для інтегрування й імплементування вимог.

Практичне значення отриманих результатів:

1) на основі розробленої моделі управління вимогами кібербезпеки при впровадженні ПЗ було проведено практичні симуляції з використанням фреймворків міжнародних стандартів і рекомендованих практик, зокрема досліджено:

- розроблену модель на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно з вимогами стандарту NIST;
- розроблену модель на основі стандарту ISO 22316, що забезпечило досягнення балансу між важливістю вимог, мінімізацією ризиків і наявними ресурсами, відповідно вимогам ISO 22316 для забезпечення стійкості організації;

- розроблену модель на основі стандарту MITRE ATT&CK, що забезпечило виконання критичних вимог MITRE ATT&CK і мінімізацію загальних ризиків при дотриманні бюджету.

2) формалізовано адаптивний механізм управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості ІКС у вигляді псевдокоду, що та може бути реалізований у системах підтримки прийняття рішень; програмних засобах управління кіберризиками; корпоративних GRC-платформах; автоматизованих системах планування тощо;

3) на основі уніфікованої моделі SDLC було формалізовано відомі моделі життєвого циклу розроблення ПЗ, зокрема класичну каскадну модель, V-модель, інкрементальну модель, спіральну модель, Agile, DevOps та DevSecOps, що може бути використано при проєктуванні захищених ІКС; аудиті процесів безпечної розробки ПЗ згідно стандартів ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних IT-системах тощо;

4) практична цінність методу інтегрування вимог кібербезпеки в SDLC полягає у можливості його використання для системного інтегрування вимог кібербезпеки в процеси розроблення ПЗ в організаціях, що створюють або експлуатують інформаційні системи критичної інфраструктури, хмарні сервіси та корпоративні ІКС. Застосування цього методу дозволяє: забезпечити узгодженість вимог кібербезпеки на всіх етапах SDLC; підвищити рівень автоматизації контролю кібербезпеки у DevSecOps pipeline; зменшити ризик пропуску критичних вимог кібербезпеки під час швидких ітерацій розроблення; підвищити обґрунтованість вибору засобів захисту інформації; скоротити витрати на усунення вразливостей за рахунок їх виявлення на ранніх етапах SDLC; забезпечити можливість кількісного оцінювання рівня реалізації вимог кібербезпеки за допомогою метрик кібербезпеки; створити інструментальні засоби підтримки прийняття рішень у процесах DevSecOps;

5) результати роботи впроваджені у навчальний процес кафедри комп’ютерних інформаційних технологій Факультету комп’ютерних наук та

технологій Державного університету «Київський авіаційний інститут» і діяльність Наукової асоціації кібербезпеки України, що підтверджено відповідними актами впровадження.

Апробація матеріалів дисертації. Основні результати дисертаційної роботи доповідались і обговорювались на семінарі кафедри комп'ютерних інформаційних технологій КАІ та на низці міжнародних наукових конференцій, серед яких зокрема:

- IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, Dortmund, Germany, 07-09.09.2023;
- Cyber Hygiene and Conflict Management in Global Information Networks, Kyiv, Ukraine, 24-27.01.2024;
- Workshop on Advanced Technologies in Cyber Resilience, Kyiv, Ukraine, 20-22.06.2025.

Особистий внесок здобувача. Дисертаційне дослідження виконане автором самостійно. У дисертації наукові ідеї та розробки співавторів не використовувалися. Усі сформульовані положення, висновки та пропозиції обґрунтовані на основі особистих досліджень автора.

Публікації. Основні результати дослідження викладено в 10 наукових працях, серед яких 6 статей, опублікованих у наукових фахових виданнях України, 1 розділ у закордонній колективній монографії та 3 публікації у збірниках міжнародних наукових конференцій. Зокрема, 3 публікації автора проіндексовані в наукометричній базі Scopus (з них 2 у періодичних виданнях).

Структура та обсяг дисертації. Дисертація складається з основної частини (анотації, вступу, чотирьох розділів та висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 121 сторінку, з яких 102 сторінки основного тексту. Список використаних джерел складається з 101 найменування і займає 15 сторінок, додатки викладено на 2 сторінках.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ

У сучасному цифровому світі кібербезпека стала критичним аспектом функціонування будь-якої організації. Забезпечення кібербезпеки вимагає систематичного підходу до управління вимогами, що охоплює виявлення, аналіз, документування та впровадження необхідних заходів безпеки. У цьому дослідженні представлені основні процеси управління вимогами кібербезпеки, визначаються ключові етапи та методи, а також обговорюються найкращі практики в цій галузі.

Стрімкий розвиток цифрових технологій, зростання кіберзагроз та посилення нормативних вимог створюють нові виклики для забезпечення надійної кібербезпеки в інформаційних системах. Одним із ключових елементів побудови ефективної системи захисту є управління вимогами до кібербезпеки – процес, що охоплює визначення, формалізацію, документування, впровадження та контроль виконання вимог. У сучасних умовах, коли інформаційна безпека стає критичним компонентом стратегічної стійкості організацій, якісне управління вимогами має вирішальне значення для мінімізації ризиків та відповідності регуляторним нормам.

На практиці організації часто стикаються з проблемами у сфері управління вимогами до кібербезпеки: відсутністю чітких критеріїв виявлення вимог, розбіжностями у нормативних джерелах, складністю інтеграції вимог у процеси розробки програмного забезпечення (ПЗ), а також нестачею компетентного супроводу на етапах моніторингу та підтримки. Крім того, міжнародна і вітчизняна практика демонструє значну варіативність підходів – від формалізованих методологій, таких як NIST RMF або ISO/IEC 27001, до гнучких адаптивних моделей, що застосовуються в окремих галузях. Відсутність системного узагальнення наукових напрацювань у цій сфері ускладнює вибір оптимальних рішень для різних типів організацій.

З огляду на зазначене, виникає потреба в комплексному аналізі сучасних підходів до управління вимогами кібербезпеки з метою виявлення найбільш ефективних практик і рекомендацій. Такий аналіз є особливо актуальним у контексті впровадження ПЗ, коли вимоги до кібербезпеки мають бути не лише технічно обґрунтованими, але й інтегрованими у всі фази життєвого циклу системи.

1.1. Визначення вимог кібербезпеки

Вимоги кібербезпеки можна визначити як набір умов та обмежень, що повинні бути виконані для забезпечення захисту інформаційних систем від несанкціонованого доступу, модифікації, розкриття або знищення. Визначення вимог кібербезпеки є першим і найважливішим етапом у забезпеченні безпеки організації.

Для формального представлення вимог можуть бути використані математичні методи та алгоритми, представлені в роботах [1-10].

Джерела вимог

Вимоги кібербезпеки можуть походити з різних джерел, включаючи:

Законодавчі та регуляторні акти України:

- *Закон України "Про основні засади забезпечення кібербезпеки України".* Закон, що встановлює основні принципи, завдання та напрями державної політики у сфері кібербезпеки.
- *Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".* Закон, що визначає основи забезпечення захисту інформації в інформаційно-телекомунікаційних системах.
- *ДСТУ ISO/IEC 27001.* Національний стандарт України, що відповідає міжнародному стандарту ISO/IEC 27001 і встановлює вимоги до системи управління інформаційною безпекою.

Стандарти та найкращі практики

- *ISO/IEC 27001.* Міжнародний стандарт, що визначає вимоги до системи управління інформаційною безпекою (ISMS). Він містить вимоги щодо створення, впровадження, підтримки та постійного вдосконалення ISMS [11].
- *GDPR (General Data Protection Regulation).* Загальний регламент про захист даних Європейського Союзу, що встановлює вимоги щодо захисту особистих даних і конфіденційності для всіх організацій, що обробляють дані резидентів ЄС [12].
- *NIST (National Institute of Standards and Technology) Cybersecurity Framework.* Структура кібербезпеки, розроблена NIST, що надає рекомендації щодо управління кіберризиками. Широко використовується у США та за їх межами [13].

▪*CISA (Cybersecurity Information Sharing Act).* Закон, що заохочує обмін інформацією про кіберзагрози між урядом та приватним сектором для покращення кібербезпеки [14].

▪*HIPAA (Health Insurance Portability and Accountability Act).* Закон, що визначає вимоги щодо захисту конфіденційності та безпеки медичної інформації в електронному вигляді [15].

▪*FISMA (Federal Information Security Management Act).* Закон, що встановлює вимоги щодо захисту інформаційних систем федеральних агентств США [16].

▪*NIS Directive (Directive on Security of Network and Information Systems).* Директива ЄС, що встановлює заходи для досягнення високого спільного рівня безпеки мереж та інформаційних систем в усьому Союзі [17].

▪*ePrivacy Directive.* Директива, що регулює обробку особистих даних і захист конфіденційності в секторі електронних комунікацій [18].

Політики та процедури організації

Політики та процедури організації відіграють ключову роль у визначенні та забезпеченні вимог кібербезпеки. Вони створюють рамки для управління кіберризиками, забезпечення відповідності нормативним вимогам та впровадження ефективних заходів безпеки. Нижче наведено основні політики та процедури, які можуть бути впроваджені в організації для забезпечення кібербезпеки.

Політика інформаційної безпеки. Ця політика визначає загальні принципи та підходи до захисту інформаційних ресурсів організації. Вона охоплює такі аспекти, як конфіденційність, цілісність і доступність інформації [11]. Основні елементи:

▪Визначення відповідальності за забезпечення інформаційної безпеки

▪Класифікація інформаційних ресурсів та визначення рівнів доступу

▪Забезпечення безпеки мережі та систем

▪Захист від шкідливого ПЗ

Політика управління ризиками. Ця політика спрямована на ідентифікацію, оцінку та управління ризиками, пов'язаними з кібербезпекою [13]. Основні елементи:

▪Процедури оцінки ризиків

▪Визначення та впровадження заходів для зниження ризиків

▪Регулярний перегляд та оновлення оцінок ризиків

Політика управління доступом. Ця політика регулює доступ до інформаційних систем та даних організації, забезпечуючи, що доступ мають лише авторизовані користувачі. Основні елементи:

- Вимоги до автентифікації та авторизації
- Управління ролями та дозволами
- Процедури моніторингу та аудиту доступу

Політика реагування на інциденти. Ця політика визначає процедури реагування на інциденти інформаційної безпеки, такі як кібератаки, витоки даних або інші порушення безпеки. Основні елементи:

- Визначення типів інцидентів та критеріїв їх класифікації
- Процедури повідомлення про інциденти
- Дії у відповідь на інциденти та процедури відновлення

Політика управління змінами. Ця політика забезпечує контроль над змінами в інформаційних системах, щоб гарантувати їх безпеку та стабільність. Основні елементи:

- Процедури запиту та затвердження змін
- Оцінка впливу змін на безпеку
- Тестування та документування змін

Політика навчання та підвищення обізнаності. Ця політика спрямована на підвищення рівня обізнаності працівників щодо кібербезпеки та їх підготовку до виконання політик і процедур безпеки. Основні елементи:

- Регулярні тренінги з кібербезпеки
- Кампанії з підвищення обізнаності про загрози
- Оцінка ефективності навчальних програм

Політика збереження та видалення даних. Ця політика визначає вимоги щодо збереження та видалення даних, забезпечуючи захист конфіденційної інформації протягом всього її життєвого циклу [12]. Основні елементи:

- Визначення періодів зберігання даних
- Процедури безпечного видалення даних
- Вимоги до зберігання резервних копій

Технічні специфікації та архітектурні рішення

Технічні специфікації та архітектурні рішення відіграють ключову роль у забезпеченні кібербезпеки, оскільки вони визначають конкретні технічні заходи, які повинні бути впроваджені для захисту інформаційних систем та даних. Нижче наведено огляд основних технічних специфікацій та архітектурних рішень, які можуть бути застосовані для задоволення вимог кібербезпеки.

1) Технічні специфікації

Шифрування даних

Шифрування є одним з основних методів захисту конфіденційності даних як під час зберігання, так і під час передачі.

– AES (Advanced Encryption Standard): Стандарт шифрування, що забезпечує високу безпеку даних.

– TLS (Transport Layer Security): Протокол забезпечення захищених комунікацій через мережу Інтернет.

Аутентифікація та авторизація

Аутентифікація та авторизація гарантують, що доступ до систем та даних мають лише авторизовані користувачі.

– MFA (Multi-Factor Authentication): Використання кількох факторів для аутентифікації користувачів.

– OAuth: Протокол авторизації, що дозволяє надавати доступ до ресурсів без розкриття паролів.

Управління уразливостями

Виявлення та усунення уразливостей в ПЗ та інфраструктурі є критично важливими для забезпечення безпеки.

– CVSS (Common Vulnerability Scoring System): Стандартизована система оцінки уразливостей.

– Nessus: Інструмент для сканування уразливостей і перевірки безпеки систем.

2) Архітектурні рішення

Мережева безпека. Архітектурні рішення для захисту мережевих комунікацій включають використання брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), а також сегментацію мережі.

– DMZ (Demilitarized Zone): Сегмент мережі, що забезпечує додатковий рівень захисту між внутрішньою мережею та зовнішніми загрозами.

– VPN (Virtual Private Network): Технологія для створення захищених тунелів для передачі даних через незахищені мережі.

Захист кінцевих точок включає впровадження рішень для захисту робочих станцій, серверів та мобільних пристроїв.

– EDR (Endpoint Detection and Response): Інструменти для виявлення, розслідування та реагування на загрози на кінцевих точках.

– Антивірусне ПЗ: Захист від шкідливого ПЗ.

Безпека додатків включає впровадження практик безпечного розроблення ПЗ та тестування на безпеку.

– OWASP (Open Web Application Security Project): Рекомендації та інструменти для забезпечення безпеки веб-додатків.

– SAST (Static Application Security Testing): Інструменти для статичного аналізу коду з метою виявлення уразливостей.

Моніторинг та логування. Ефективний моніторинг та логування дозволяють вчасно виявляти та реагувати на інциденти безпеки.

– SIEM (Security Information and Event Management): Системи для збору, аналізу та кореляції логів з різних джерел.

– Syslog: Протокол для централізованого збору та зберігання логів.

Хмарні рішення для кібербезпеки. З розвитком хмарних технологій важливість забезпечення безпеки в хмарних середовищах зростає.

– CASB (Cloud Access Security Broker): Інструменти для забезпечення безпеки доступу до хмарних сервісів.

– Керовані сервіси безпеки (MSS): Послуги, що надаються третіми сторонами для забезпечення безпеки хмарних середовищ.

Виявлення вимог

Виявлення вимог включає взаємодію з усіма зацікавленими сторонами для збору інформації про їх потреби та очікування. Це може бути здійснено через інтерв'ю, анкети, семінари та аналіз існуючої документації.

1.2. Аналіз та документування вимог

Після виявлення вимог необхідно їх ретельно проаналізувати для виявлення можливих конфліктів, дублювань та прогалин. Аналіз вимог включає оцінку їх доцільності, зрозумілості, можливості перевірки та пріоритетності.

Категоризація вимог

Вимоги можуть бути класифіковані за різними категоріями, такими як:

Функціональні вимоги: визначають конкретні функції системи, які забезпечують кібербезпеку.

Функціональні вимоги кібербезпеки визначають конкретні функції та можливості, які повинні бути реалізовані в системах для забезпечення безпеки. Ці вимоги охоплюють широкий спектр заходів, спрямованих на захист конфіденційності, цілісності та доступності. Нижче наведено основні функціональні вимоги кібербезпеки [19].

Аутентифікація та авторизація

1) Аутентифікація

– Багатофакторна аутентифікація (MFA): Вимога використання кількох методів аутентифікації (наприклад, пароль + біометричні дані або токен) для підтвердження особи користувача.

– Єдина точка входу (SSO): Можливість одного входу для доступу до кількох систем, що знижує кількість паролів і підвищує зручність для користувача.

2) Авторизація

– Рольова модель доступу (RBAC): Надання доступу до ресурсів на основі ролей користувачів.

– Контроль доступу на основі атрибутів (ABAC): Надання доступу на основі атрибутів користувача, таких як місце розташування, час доби та інші фактори.

Захист даних

1) Шифрування

– Шифрування даних під час зберігання (Data at Rest): Захист даних, що зберігаються, шляхом їх шифрування.

– Шифрування даних під час передачі (Data in Transit): Захист даних під час передачі через мережу, використовуючи протоколи шифрування, такі як TLS.

2) Маскування даних

– Маскування конфіденційних даних: Забезпечення доступу до даних без розкриття конфіденційної інформації шляхом маскування або псевдонімізації даних.

Виявлення та реагування на інциденти

1) Системи виявлення вторгнень (IDS)

– Мережева IDS (NIDS): Виявлення аномальної активності та потенційних загроз у мережевому трафіку.

– Хостова IDS (HIDS): Виявлення підозрілої активності та змін у системних файлах на окремих хостах.

2) Системи запобігання вторгнень (IPS)

– Мережева IPS (NIPS): Запобігання шкідливій активності в реальному часі шляхом блокування небезпечного трафіку.

– Хостова IPS (HIPS): Запобігання шкідливим діям на окремих хостах, таким, як виконання шкідливого коду.

Управління доступом

1) Управління ідентифікацією

– Життєвий цикл ідентифікації: Управління створенням, зміною та видаленням ідентифікаційних даних користувачів.

– Аудит доступу: ведення журналу дій користувачів для забезпечення прозорості та відстеження несанкціонованого доступу.

2) Політики паролів

– Складність паролів: вимоги до складності паролів, такі як мінімальна довжина, наявність цифр, спеціальних символів тощо.

– Політики зміни паролів: вимоги до регулярної зміни паролів та уникнення повторного використання старих паролів.

Захист кінцевих точок

1) Антивірусний захист

– Антивірусне ПЗ: Встановлення антивірусного ПЗ на кінцевих пристроях для виявлення та видалення шкідливого ПЗ.

2) Захист від шкідливого ПЗ

– Антиспам-фільтри: Захист від спаму та фішингових листів шляхом фільтрації електронної пошти.

– Фаєрволи: Використання фаєрволів для захисту кінцевих пристроїв від несанкціонованого доступу.

Безпека додатків

1) Безпечне розроблення ПЗ

– Вбудована безпека: Інтеграція заходів безпеки на всіх етапах розроблення ПЗ.

– Тестування безпеки: Регулярне проведення тестів на проникнення та аналізу коду для виявлення уразливостей.

2) Захист веб-додатків

– Веб-фаєрволи (WAF): Захист веб-додатків від атак, таких як SQL-ін'єкції, XSS.

Управління конфігурацією та змінами

Управління конфігурацією

– Відстеження конфігураційних змін: ведення журналу всіх змін конфігураційних параметрів системи.

– Забезпечення відповідності конфігурацій: Впровадження політик для підтримки конфігурацій відповідно до стандартів безпеки.

Управління змінами

– Процедури зміни: Визначення процедур для ініціювання, оцінки та впровадження змін у системах.

– Оцінка впливу змін на безпеку: Аналіз впливу запланованих змін на безпеку системи перед їх впровадженням.

Нефункціональні вимоги: включають характеристики, такі як продуктивність, масштабованість, надійність та зручність використання.

Нефункціональні вимоги кібербезпеки описують характеристики та атрибути системи, які не пов'язані безпосередньо з її функціональністю, але є критичними для забезпечення загальної безпеки, надійності, продуктивності та зручності використання. Вони визначають, як система повинна виконувати свої функції з точки зору безпеки. Нижче наведено основні нефункціональні вимоги кібербезпеки. [19]

Продуктивність і масштабованість

1) Продуктивність

– Час відгуку: Система повинна забезпечувати швидкий відгук на запити користувачів навіть під час атак, таких як DDoS.

– Пропускна здатність: Система повинна мати достатню пропускну здатність для обробки великої кількості запитів, зберігаючи високий рівень безпеки.

2) Масштабованість

– Горизонтальна та вертикальна масштабованість: Система повинна бути здатна до масштабування як горизонтально (додавання нових серверів), так і вертикально (покращення потужності існуючих серверів) без зниження рівня безпеки.

Надійність і відновлюваність

1) Надійність

– Стійкість до збоїв: Система повинна бути стійкою до збоїв і продовжувати функціонувати навіть у разі виникнення часткових відмов.

– Безперервність роботи: Забезпечення безперервності роботи системи під час і після інцидентів безпеки.

2) Відновлюваність

– Процедури відновлення: Наявність документованих процедур для швидкого відновлення роботи системи після інциденту.

– Резервне копіювання та відновлення: Регулярне резервне копіювання даних і можливість швидкого відновлення з резервних копій.

Захищеність

1) Конфіденційність

– Шифрування даних: Використання надійних алгоритмів шифрування для захисту конфіденційних даних як під час зберігання, так і під час передачі.

2) Цілісність

– Контроль цілісності даних: Впровадження механізмів для перевірки цілісності даних і виявлення несанкціонованих змін.

3) Доступність

– Захист від DDoS-атак: Впровадження заходів для захисту системи від розподілених атак на відмову в обслуговуванні.

– Висока доступність: Забезпечення високого рівня доступності системи шляхом використання резервування та балансування навантаження.

Зручність використання

1) Простота використання

– Інтуїтивний інтерфейс: Забезпечення простого та інтуїтивно зрозумілого інтерфейсу для користувачів та адміністраторів системи.

– Документація та навчання: Наявність детальної документації та програм навчання для користувачів та адміністраторів щодо безпечного використання системи.

2) Автоматизація

– Автоматичне оновлення: Автоматизація процесу оновлення ПЗ та патчів безпеки.

– Автоматичне виявлення та реагування: Впровадження автоматизованих систем виявлення та реагування на інциденти безпеки.

Документування вимог

Документування вимог є критичним для забезпечення їхньої зрозумілості та подальшого впровадження. Вимоги зазвичай документуються у вигляді специфікацій, що включають опис, критерії прийняття та пріоритетність.

Документування вимог кібербезпеки є важливим етапом у забезпеченні безпеки інформаційних систем підприємства. Це дозволяє систематизувати та структурувати вимоги, забезпечити їхню зрозумілість для всіх зацікавлених сторін, а також полегшити процес впровадження та контролю відповідності. Нижче наведено кроки та рекомендації щодо документування вимог кібербезпеки на підприємстві.

Кроки документування вимог кібербезпеки

Крок 1. Збір вимог

Перший крок у документуванні вимог кібербезпеки полягає у зборі всіх релевантних вимог з різних джерел:

– Законодавчі та регуляторні акти: вимоги, встановлені державними органами та галузевими стандартами (наприклад, GDPR, ISO/IEC 27001).

– Політики та процедури підприємства: Внутрішні документи, що визначають підходи до управління інформаційною безпекою.

– Технічні специфікації та архітектурні рішення: Вимоги, що випливають з технічних рішень та архітектури інформаційних систем.

Крок 2. Аналіз та узгодження вимог

Після збору вимог необхідно їх проаналізувати та узгодити з усіма зацікавленими сторонами:

– Виявлення конфліктів та дублювань: Визначення та вирішення потенційних конфліктів між вимогами, уникнення дублювання.

– Пріоритезації вимог: Визначення пріоритетності вимог залежно від їх важливості та впливу на безпеку.

Крок 3. Структурування вимог

Вимоги кібербезпеки повинні бути структуровані для забезпечення їх зручності використання та управління:

– Категоризація: Розподіл вимог за категоріями (наприклад, аутентифікація, авторизація, шифрування, управління доступом).

– Ієрархічна структура: Визначення ієрархії вимог, що дозволяє відстежувати залежності між ними.

Крок 4. Документування вимог

Документування вимог включає створення детальних описів, які містять всю необхідну інформацію:

– Назва вимоги: коротка назва, що відображає суть вимоги.

– Опис вимоги: детальний опис вимоги, включаючи її призначення та очікуваний результат.

– Критерії прийняття: умови, за яких вимога вважається виконаною.

– Пріоритетність: визначення пріоритету вимоги (високий, середній, низький).

– Відповідальні особи: визначення відповідальних за виконання та моніторинг вимог.

Крок 5. Огляд та затвердження

Після документування вимог необхідно провести їх огляд та затвердження:

– Огляд з зацікавленими сторонами: узгодження документів з усіма зацікавленими сторонами, включаючи IT-відділ, керівництво та юридичний відділ.

– Затвердження: Офіційне затвердження документів керівництвом підприємства.

Рекомендації щодо документування вимог кібербезпеки

1. Використання стандартів та шаблонів

– Використовуйте стандартизовані шаблони для документування вимог, щоб забезпечити їх узгодженість та зрозумілість.

– Дотримуйтеся міжнародних стандартів, таких як ISO/IEC 27001, для забезпечення високої якості документування.

2. Прозорість та доступність

– Забезпечте доступність документів для всіх зацікавлених сторін.

– Ведіть централізоване сховище документів, що дозволяє легко знаходити та оновлювати вимоги.

3. Регулярне оновлення

– Регулярно переглядайте та оновлюйте вимоги кібербезпеки відповідно до змін у законодавстві, технологіях та бізнес-процесах.

– Забезпечте механізми для швидкого внесення змін у разі виявлення нових загроз або вразливостей.

4. Навчання та підвищення обізнаності

– Проведіть навчання для персоналу щодо важливості та змісту вимог кібербезпеки.

– Забезпечте, щоб всі працівники розуміли свої обов'язки щодо виконання вимог кібербезпеки.

5. Використання інструментів управління вимогами

– Використовуйте спеціалізовані інструменти для управління вимогами, які дозволяють ефективно відстежувати виконання, аналізувати та генерувати звіти.

1.3. Впровадження вимог кібербезпеки, моніторинг та підтримка

1) Впровадження вимог кібербезпеки включає розробку, тестування та інтеграцію заходів безпеки у інформаційні системи організації. Це включає в себе:

– Розробку технічних рішень, які відповідають визначеним вимогам

– Проведення тестування для верифікації виконання вимог

– Інтеграцію рішень у існуючі системи та процеси

2) Моніторинг та підтримка вимог кібербезпеки є постійним процесом, що включає:

– Безперервний моніторинг систем для виявлення та реагування на нові загрози

– Оновлення вимог та рішень у відповідь на зміни у технологічному середовищі та загрозах

– Проведення регулярних аудитів та оцінок безпеки

Впровадження вимог кібербезпеки є критично важливим етапом для забезпечення надійного захисту інформаційних систем і даних підприємства. Цей процес включає розробку та інтеграцію відповідних технічних та організаційних заходів для виконання задокументованих вимог. Нижче наведено ключові кроки та рекомендації щодо впровадження вимог кібербезпеки.

Рекомендації щодо впровадження вимог кібербезпеки

1. Інтеграція безпеки у всі етапи життєвого циклу системи

Варто забезпечити інтеграцію вимог кібербезпеки на всіх етапах розробки та експлуатації системи, від початкового планування до завершення її життєвого циклу.

2. Використання найкращих практик та стандартів

Потрібно дотримуватися найкращих практик та стандартів (наприклад, NIST, ISO/IEC 27001) для забезпечення високого рівня безпеки.

3. Регулярні оцінки та вдосконалення

Треба проводити регулярні оцінки ефективності впроваджених заходів та постійно вдосконалювати їх відповідно до нових загроз та технологій.

4. Залучення зацікавлених сторін

Необхідно залучати всі зацікавлені сторони до процесу впровадження вимог кібербезпеки, включаючи керівництво, IT-відділ та кінцевих користувачів.

5. Використання автоматизованих інструментів

Потрібно використовувати автоматизовані інструменти для моніторингу, аналізу та реагування на інциденти безпеки для підвищення ефективності та швидкості реагування.

1.4. Найкращі практики в управлінні вимогами кібербезпеки

Найкращі практики включають:

1) Використання стандартизованих методологій та інструментів для управління вимогами кібербезпеки є ключовим аспектом для забезпечення ефективності та узгодженості процесів в організації. Стандартизовані методології допомагають структурувати підхід до кібербезпеки, забезпечуючи систематичність, прозорість та відповідність нормативним вимогам. Інструменти, у свою чергу, автоматизують та оптимізують процеси, підвищуючи їх ефективність. Нижче наведено огляд основних стандартизованих методологій та інструментів для управління вимогами кібербезпеки [11-17].

Стандартизовані методології

- ISO/IEC 27001
- NIST Cybersecurity Framework (CSF)
- COBIT (Control Objectives for Information and Related Technologies)
- ITIL (Information Technology Infrastructure Library)

2) Активна взаємодія з усіма зацікавленими сторонами

3) Регулярне навчання та підвищення кваліфікації персоналу

4) Забезпечення прозорості та документованості всіх процесів

Огляд інструментів для управління вимогами кібербезпеки

1. Jira

Jira є популярним інструментом для управління проєктами та вимогами, що дозволяє ефективно відстежувати виконання завдань та вимог кібербезпеки.

Функціональність: відстеження завдань, управління проєктами, інтеграція з іншими інструментами. Переваги: гнучкість, можливість налаштування, підтримка Agile та Scrum-методологій.

2. Confluence

Confluence використовується для створення, обміну та управління документацією, включаючи вимоги кібербезпеки. Функціональність: спільна робота над документами, структуроване зберігання інформації, інтеграція з Jira. Переваги: зручність використання, можливість спільної роботи, централізоване зберігання документів.

3. ServiceNow

ServiceNow забезпечує управління IT-послугами, включаючи аспекти кібербезпеки та управління вимогами. Функціональність: управління інцидентами, управління змінами, управління конфігураціями. Переваги: інтеграція процесів, автоматизація, аналітика та звітність.

4. RSA Archer

RSA Archer є платформою для управління ризиками, що дозволяє організаціям управляти ризиками та відповідністю нормативним вимогам. Функціональність: управління ризиками, відповідністю, аудитами, інцидентами безпеки. Переваги: широка функціональність, масштабованість, інтеграція з іншими системами.

5. Tenable

Tenable пропонує інструменти для управління уразливостями та забезпечення відповідності вимогам безпеки. Функціональність: сканування уразливостей, моніторинг безпеки, звітність. Переваги: детальний аналіз уразливостей, інтеграція з іншими системами безпеки, регулярні оновлення баз даних загроз.

1.5. Аналіз сучасних наукових підходів до управління вимогами кібербезпеки

Розглянемо більш детально сучасний стан наукових досліджень за цим напрямком в Україні та світі .

У роботі Сироватченко О. [20] аналізуються правові аспекти забезпечення кібербезпеки в Україні, зокрема оцінка статистичних даних щодо ситуації в

кіберпросторі та роль національного та міжнародного законодавства у протидії кіберзагрозам. Автор підкреслює необхідність вдосконалення законодавчої бази та міжнародного співробітництва у сфері кібербезпеки.

Худолій А. в статті [21] розглядає сучасні виклики у сфері кібербезпеки України, включаючи загрози, що виникають у зв'язку з цифровізацією та гібридними війнами. Автор аналізує заходи, здійснені урядом України для поліпшення стану кібербезпеки, та пропонує рекомендації щодо подальшого вдосконалення системи захисту.

У [22] Цвілій О.О. розглядає систему сертифікації кібербезпеки інформаційних та комунікаційних технологій як ключовий елемент забезпечення безпеки цифрової економіки та державного управління. Автор аналізує існуючі стандарти та процедури сертифікації, а також пропонує шляхи їх вдосконалення.

У дослідженні Трофіменко О.Г., та ін. [23] визначено політичні, науково-технічні, організаційні та просвітницькі питання, вирішення яких є необхідним у рамках комплексної протидії кіберзагрозам. Автори аналізують сучасний стан кібербезпеки України та пропонують рекомендації щодо її покращення.

У [24] Admass W.S., Munaye Y.Y., Diro A.A. представлено огляд сучасного стану кібербезпеки, викликів та тактик, поточних умов і глобальних тенденцій у сфері кібербезпеки. Автори обговорюють нові загрози, такі як атаки з використанням глибоких підробок (deepfakes), та підкреслюють необхідність адаптації стратегій управління вимогами до кібербезпеки для ефективного реагування на ці виклики.

Інше дослідження [25] Kim H., Park J., Lee S. Демонструє систему управління вимогами до кібербезпеки (CRMS) як структуру аналізу вимог до безпеки, застосовувану в автомобільній промисловості. Ця система допомагає інженерам і експертам з безпеки ідентифікувати та впроваджувати вимоги до кібербезпеки на ранніх етапах розробки ПЗ.

У [26] Cremer S., Sheehan B., Smith J. аналізується наявна академічна та галузева література з питань кібербезпеки та управління кіберризиками з особливим акцентом на доступність даних. Автори виявили, що відсутність доступних даних про кіберризики ускладнює ефективне управління вимогами до кібербезпеки та розробку політик захисту.

У статті Nguyen T.T., Tran M.H., Le D.H. [27] представлено огляд кібербезпеки в новітніх технологіях. Автори висвітлюють перешкоди, з якими стикаються компанії при управлінні цими ризиками, та підкреслюють важливість інтеграції управління вимогами до кібербезпеки на ранніх етапах впровадження нових технологій.

Проведений в [28] аналіз публікацій показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на необхідності вдосконалення нормативно-правової бази, впровадження галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки. Як українські, так і іноземні дослідження підкреслюють важливість міждисциплінарного підходу, гармонізації з міжнародними стандартами та використання аналітики загроз для прийняття ефективних рішень. Загалом, ефективне управління вимогами кібербезпеки розглядається як комплексний процес, що охоплює як технічні, так і правові аспекти.

З іншого боку, в роботах [29-41] висвітлено спроби імплементації різноманітних вимог, включаючи вимоги кібербезпеки, в життєвий цикл розроблення ПЗ, зважаючи на різні моделі. Основний недолік – це відсутність формалізованої, динамічної та трасованої інтеграції вимог кібербезпеки на всіх етапах життєвого циклу розроблення ПЗ, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів та підвищення рівня ризику.

Саме це і визначає постановку завдання дисертації, а саме – розроблення ефективних моделей, методів та інструментальних засобів управління вимогами кібербезпеки при впровадженні ПЗ в бізнесі.

1.6. Висновки до першого розділу дисертації

Таким чином, у цьому розділі роботи проведено аналіз сучасних підходів до управління вимогами кібербезпеки при впровадженні ПЗ. Встановлено, що управління вимогами кібербезпеки є ключовим елементом забезпечення надійного захисту інформаційних систем організації. Ефективне виявлення, аналіз, документування та впровадження вимог допомагають мінімізувати ризики та забезпечити відповідність

нормативним вимогам та стандартам. Використання найкращих практик у цій галузі сприяє підвищенню загального рівня кібербезпеки організації.

Законодавчі та регуляторні акти, що визначають вимоги кібербезпеки, відіграють критичну роль у формуванні безпечного цифрового середовища. Вони забезпечують організаціям чіткі керівні принципи та зобов'язання, які спрямовані на захист даних та інформаційних систем від кіберзагроз. Виконання цих вимог допомагає знизити ризики та підвищити загальний рівень кібербезпеки.

Розробка та впровадження політик і процедур кібербезпеки є необхідними для забезпечення захисту інформаційних систем та даних організації. Вони створюють основу для ефективного управління кіберризиками та відповідають на вимоги законодавства і нормативних актів. Регулярний перегляд та оновлення цих політик і процедур дозволяють організації залишатися актуальною в умовах постійно змінюваних кіберзагроз.

Технічні специфікації та архітектурні рішення є основою для забезпечення кібербезпеки в організації. Вони забезпечують необхідні інструменти та методи для захисту інформаційних систем від різноманітних кіберзагроз. Постійний розвиток та вдосконалення цих рішень є необхідними для адаптації до змінних умов та нових викликів у сфері кібербезпеки.

Функціональні вимоги кібербезпеки охоплюють широкий спектр заходів, спрямованих на забезпечення захисту інформаційних систем та даних від різноманітних загроз. Впровадження цих вимог допомагає організаціям мінімізувати ризики, підвищити рівень безпеки та забезпечити відповідність нормативним вимогам та стандартам. Нефункціональні вимоги кібербезпеки є критичними для забезпечення загальної безпеки та надійності інформаційних систем. Вони визначають характеристики, які допомагають захистити систему від різноманітних загроз, забезпечити її стабільну роботу та відповідність нормативним вимогам. Впровадження цих вимог допомагає організаціям створити більш захищене та надійне цифрове середовище.

Документування вимог кібербезпеки є критичним процесом для забезпечення захисту інформаційних систем та даних підприємства. Воно допомагає структурувати та систематизувати вимоги, забезпечувати їхню зрозумілість та узгодженість, а також

полегшувати процес їхнього впровадження та контролю. Дотримання рекомендацій та використання сучасних інструментів управління вимогами сприяють підвищенню загального рівня кібербезпеки на підприємстві.

Впровадження вимог кібербезпеки є складним, але необхідним процесом для забезпечення надійного захисту інформаційних систем та даних підприємства. Це включає розробку та інтеграцію технічних рішень, тестування та верифікацію, навчання персоналу, а також постійний моніторинг та підтримку систем безпеки. Дотримання найкращих практик та регулярне вдосконалення заходів безпеки допоможуть організації ефективно захищатися від кіберзагроз та забезпечити високий рівень захищеності.

Аналіз сучасних наукових підходів до управління вимогами кібербезпеки показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на необхідності вдосконалення нормативно-правової бази, впровадження галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки. Дослідження підкреслюють важливість міждисциплінарного підходу, гармонізації з міжнародними стандартами та використання аналітики загроз для прийняття ефективних рішень. Загалом, ефективне управління вимогами кібербезпеки розглядається як комплексний процес, що охоплює як технічні, так і правові аспекти.

Основний недолік відомих підходів імплементації вимог в життєвий цикл розроблення ПЗ – це відсутність формалізованої, динамічної та трасованої інтеграції вимог кібербезпеки у всі етапи життєвого циклу розроблення ПЗ, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів та підвищення рівня ризику.

1.7. Список використаних джерел у другому розділі дисертації

1. L. Li et al., "LogicEdu: Enhancing Computational Logic Understanding through Web-Based Boolean Logic Simplification Tool," 2024 21st International SoC Design Conference (ISOCC), Sapporo, Japan, 2024, pp. 390-391, doi: 10.1109/ISOCC62682.2024.10762040.

2. S. Deepak, J. A. Shah, N. Chetan and H. Sharda, "New Decision-Making Process Based on Set Theory: Towards Application of Set Theory," 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2023, pp. 1-6, doi: 10.1109/ICTBIG59752.2023.10456045.

3. H. Wang, "Network Graph Theory and Organization Model Analysis based on Mathematical Modeling with the Dynamic Systematic Data Perspective," 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 915-919, doi: 10.1109/ICOEI53556.2022.9776767.

4. Q. Yu and Z. Li, "A Bayesian Model Averaging Method for Software Reliability Assessment," 2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM), Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/APARM49247.2020.9209504.

5. B. Yang et al., "A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges," in Protection and Control of Modern Power Systems, doi: 10.23919/PCMP.2024.000297.

6. Pratyush Shukla; Sanjay Kumar Singh; Aditya Khamparia; Anjali Goyal, "9 Nature-inspired optimization techniques," in Nature-Inspired Optimization Algorithms: Recent Advances in Natural Computing and Biomedical Applications , De Gruyter, pp.137-152.

7. R. Beniwal, V. Kumar and V. Sharma, "Metaheuristics Approaches Towards Secure and Optimized Routing in IoT: A Systematic Literature Review," 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), Greater Noida, India, 2024, pp. 1-6, doi: 10.1109/ICEECT61758.2024.10739076.

8. T. T. Zin, A. S. T. Moe, C. N. Phyo and P. Tin, "Fusion of Strategic Queueing Theory and AI for Smart City Telecommunication System," 2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS), Seoul, Korea, Republic of, 2024, pp. 653-657, doi: 10.1109/MASS62177.2024.00104.

9. N. Zhang, Y. Chen, W. Yang, Z. Zhang, Y. Liu and W. Mao, "Application of Fault Tree Analysis for Reliability Evaluation and Weak Link Identification of Stadium Power Supply System Using Monte Carlo Simulation," 2021 IEEE Sustainable Power and Energy Conference (iSPEC), Nanjing, China, 2021, pp. 4209-4214, doi: 10.1109/iSPEC53008.2021.9735815.

10. D. Kim, B. Jeon and K. C. Koo, "Addressing Timely AI Technology Standardization Challenges through a Hierarchical Analysis Approach," 2023 14th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2023, pp. 1431-1433, doi: 10.1109/ICTC58733.2023.10393654.

11. ISO/IEC, "Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements," ISO/IEC 27001:2022, International Organization for Standardization, Geneva, Switzerland, 2022, pp. 1–33. doi: 10.3403/30514785.

12. European Parliament and Council, "General Data Protection Regulation (GDPR)," Regulation (EU) 2016/679, Brussels, Belgium, 2016, pp. 1–88.

13. National Institute of Standards and Technology, "Cybersecurity Framework 2.0," NIST, Gaithersburg, MD, USA, 2024, pp. 1–58. doi: 10.6028/NIST.CSWP.02022024.

14. U.S. Congress, "Cybersecurity Information Sharing Act (CISA)," Public Law No: 114-113, Washington, DC, USA, 2015, pp. 1–13.

15. U.S. Department of Health and Human Services, "Health Insurance Portability and Accountability Act (HIPAA)," Washington, DC, USA, amended 2024, pp. 1–42.

16. U.S. Congress, "Federal Information Security Modernization Act (FISMA) of 2014," Washington, DC, USA, 2014, pp. 1–16.

17. European Parliament and Council, "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)," Directive (EU) 2022/2555, Brussels, Belgium, 2022, pp. 1–71.

18. European Parliament and Council, "Directive on Privacy and Electronic Communications (ePrivacy Directive)," Directive 2002/58/EC, Brussels, Belgium, 2002, consolidated 2009, pp. 1–10.

19. QATestLab. Нефункціональні вимоги: приклади, типи, підходи [Електронний ресурс]. – Режим доступу: https://training.qatestlab.com/blog/technical-articles/non-functional-requirements-examples-types-approaches/

20. Сироватченко, Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та перспективи, Юридичний вісник, № 4(41), с. 78–85, 2024.

21. А. Худолій, Кібербезпека: сучасні виклики перед Україною, Acta De Historia & Politica: Saeculum XXI, № 1, с. 138–146, 2019.

22. О. Цвілій, Система сертифікації кібербезпеки інформаційних та комунікаційних технологій, Наукові праці ОНАЗ ім. О.С. Попова, № 2, с. 121–126, 2020.

23. О.Г. Трофіменко, Ю.В. Прокоп, Н.І. Логінова та О.В. Задерейко, Кібербезпека України: аналіз сучасного стану, Захист інформації, т. 21, с. 3-12, 2019.

24. W. S. Admass, Y. Y. Munaye and A. A. Diro, Cyber Security: State of the Art, Challenges and Future Directions, Cyber Security and Applications, vol. 2, Article ID: 100031, 2024. Available: https://www.scirp.org/journal/paperinformation.aspx?paperid=129715

25. H. Kim, J. Park and S. Lee, "A Framework for Cybersecurity Requirements Management in the Automotive Industry," Sensors, vol. 23, no. 10, p. 4979, 2023, doi: 10.3390/s23104979.

26. S. Cremer, B. Sheehan and J. Smith, "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability," Global Policy and Public Risk, vol. 47, no. 3, pp. 123-139, 2022.

27. T. T. Nguyen, M. H. Tran and D. H. Le, "Managing Cybersecurity Risks in Emerging Technologies," Journal of Emerging Technologies, vol. 5, no. 2, pp. 89–102, 2023.

28. Гнатюк, С.О., Сидоренко В.М., Скуратівський А.А. Аналіз сучасних підходів до управління вимогами кібербезпеки при впровадженні програмного забезпечення, Проблеми інформатизації та управління, 2025, Т.2, №82, с. 5-18, https://doi.org/10.18372/2073-4751.82.20363

29. V. B. Manjeti, S. Penumajji, S. R. Patlolla, Y. S. Srinath Abburi, J. Teppala and S. G. Krishna Patro, "Enhancing Security in SDLC with DevOps Tools and Practices," *2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET)*, Gunupur, India, 2025, pp. 1-5, doi: 10.1109/GIET65294.2025.11234805.

30. N. H. Husin *et al*., "Investigating the Practicality of the Systems Engineering Process Approach as an Alternative to SDLC in Developing Health Information Systems," *2023 13th International Conference on Information Science and Technology (ICIST)*, Cairo, Egypt, 2023, pp. 54-58, doi: 10.1109/ICIST59754.2023.10367089.

31. A. A. A. Sen *et al*., "A New SDLC Model for Enhancing Privacy and Security in a Design-Based Approach," *2025 12th International Conference on Computing for Sustainable*

Global Development (INDIACom), Delhi, India, 2025, pp. 1-6, doi: 10.23919/INDIACom66777.2025.11115282.

32. P. R. P, T. M and C. Q. Jaslin, "SDLC AutoPilot AI: Agentic Automation of Software Development Life Cycle," *2025 International Conference on Intelligent Computing, Information and Control Systems (ICOIICS)*, Lalitpur, Nepal, 2025, pp. 1237-1242, doi: 10.1109/ICOIICS67115.2025.11390299.

33. V. K. Mavani, "Codebase Aware Generative Agents for the SDLC: Automating Documentation, Dependency Analysis and Test Generation," *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA, 2026, pp. 1-4, doi: 10.1109/ICAIC67076.2026.11395666.

34. A. Garg, R. Kumar Kaliyar and A. Goswami, "PDRSD-A systematic review on plan-driven SDLC models for software development," *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 2022, pp. 739-744, doi: 10.1109/ICACCS54159.2022.9785261.

35. R. Davila-Campos, M. Mora, P. Yuritzy Reyes Delgado, S. Galván-Cruz and G. Citlalli López Torres, "Design and Evaluation of AgileBPM SDLC–An Agile SDLC for Business Process Management Systems," in *IEEE Access*, vol. 13, pp. 142058-142088, 2025, doi: 10.1109/ACCESS.2025.3594684.

36. V. Aishwarya, S. Pediredla, B. Radhika, B. Vasanthi, k. Padmanaban and A. K. Velmurugan, "Incorporating of Security Methods into the Software Development Lifecycle Process (SDLC)," *2023 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128620.

37. O. Shokunbi, O. Uche, D. Akinwunmi, H. Akinwumi, O. Awodele and F. Ayankoya, "Emerging Security Threat in the SDLC and Mitigations," *2024 IEEE SmartBlock4Africa*, Accra, Ghana, 2024, pp. 1-11, doi: 10.1109/SmartBlock4Africa61928.2024.10779490.

38. S. Chahar and S. Singh, "Developing a Unified Framework Integrating Web Engineering and SDLC Methodologies," *2025 2nd International Conference on Computational Intelligence and Computing Applications (ICCICA)*, Samalkha, India, 2025, pp. 171-176, doi: 10.1109/ICCICA67008.2025.11337815.

39. Y. Shestak, S. Toliupa, A. Torchylo and O. J. Onyigwang, "Minimization of Information Losses in Data Centers as one of the Priority Areas of Information Security Technologies," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2022, pp. 227-230, doi: 10.1109/PICST57299.2022.10238649.

40. Saxena, S. Singh, S. Prakash, T. Yang and R. S. Rathore, "DevOps Automation Pipeline Deployment with IaC (Infrastructure as Code)," *2024 IEEE Silchar Subsection Conference (SILCON 2024)*, Agartala, India, 2024, pp. 1-6, doi: 10.1109/SILCON63976.2024.10910699.

41. S. Sudarsan, A. Mittal and A. S. Chandrasekaran, "Secure AI-SDLC for Critical Infrastructure: Operationalizing the NIST AI RMF with Evidence-Driven Controls," *2025 International Conference on Computer and Applications (ICCA)*, Bahrain, Bahrain, 2025, pp. 1-7, doi: 10.1109/ICCA66035.2025.11430939.

РОЗДІЛ 2. МОДЕЛІ УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Математичні методи для управління вимогами кібербезпеки при впровадженні програмного забезпечення

Для побудови моделі управління вимогами кібербезпеки при впровадженні програмного забезпечення (ПЗ) доцільно використовувати кілька математичних підходів та інструментів, кожен з яких дозволяє вирішувати різні завдання в управлінні вимогами кібербезпеки. Ось основні математичні методи, які можна застосувати [1-12]:

1) Логіка і теорія множин

- Булева логіка: Використовується для визначення відповідності між вимогами кібербезпеки та їхніми залежностями. Застосовується для опису умов або перевірки виконання вимог через логічні вирази та оператори [1].
- Теорія множин: Допомагає класифікувати та групувати вимоги кібербезпеки, аналізувати їх перетини, взаємозалежності та суперечності між вимогами. Наприклад, множини вимог можуть бути розбиті на обов'язкові, рекомендовані та додаткові [2].

2) Моделювання з використанням графів та мереж

- Графи залежностей: Для побудови моделі вимог можна використовувати графи, де вершини представляють окремі вимоги, а ребра – залежності між ними. Це дозволяє візуалізувати взаємозалежність вимог і визначити критичні шляхи [3].
- Петля Петрі: Використовується для моделювання та аналізу послідовності та умов виконання вимог. Петлі Петрі дозволяють формалізувати процес управління вимогами, особливо коли існує багато паралельних процесів або залежностей між вимогами [4].

3) Теорія нечіткої логіки

- Нечітка логіка (Fuzzy Logic): Часто застосовується для оцінки виконання вимог, коли критерії виконання вимоги не є чітко визначеними або мають ступінь

невизначеності. Це дозволяє моделювати рівень відповідності вимогам за допомогою нечітких множин і функцій належності [5].

- Нечіткі правила та висновки: Використовуються для прийняття рішень щодо пріоритезації вимог або оцінки рівня ризику з урахуванням можливих невизначеностей [5].

4) Ймовірнісні моделі та теорія ризиків

- Байєсові мережі: Можуть бути використані для моделювання ризиків, пов'язаних з вимогами кібербезпеки, враховуючи ймовірності виникнення певних загроз і їх вплив на вимоги. Байєсові мережі дозволяють визначити ймовірність невиконання вимог у залежності від певних умов [6].

- Теорія ігор: Застосовується для моделювання поведінки атакуючих та системи захисту, враховуючи можливі стратегії атак. Модель може бути корисною для прийняття рішень щодо пріоритетів вимог з точки зору кібербезпеки [7].

5) Математичне програмування та оптимізація

- Цільова функція та обмеження: Управління вимогами кібербезпеки часто потребує оптимізації обмежених ресурсів (часу, бюджету, людських ресурсів), тому корисно застосувати лінійне або нелінійне програмування для оптимізації виконання вимог [8].

- Метаевристичні алгоритми (генетичні алгоритми, алгоритми рою): Дозволяють розв'язувати завдання з пошуку оптимального набору вимог або визначення пріоритетів для виконання з урахуванням обмежень [9].

6) Теорія систем масового обслуговування

Моделі обслуговування запитів: Може використовуватися для побудови моделей обробки вимог у процесі розробки ПЗ. Наприклад, застосування теорії черг допоможе визначити, скільки ресурсів і часу знадобиться для впровадження кожної вимоги з кібербезпеки [10].

7) Динамічне моделювання та симуляції

- Моделі Монте-Карло: Для оцінки можливого впливу різних ризиків на виконання вимог, особливо коли вимоги є ресурсозатратними або ризики змінюються з часом [11].

▪ Агентно-орієнтоване моделювання: Використовується для моделювання взаємодії між учасниками процесу впровадження вимог кібербезпеки, зокрема для моделювання поведінки атакуючих.

8) Аналіз ієрархій та методу аналізу ієрархій (AHP)

Метод AHP: Застосовується для встановлення пріоритетів серед вимог кібербезпеки на основі їхньої важливості. Цей метод допомагає систематично зважувати та порівнювати різні вимоги, що особливо корисно при обмежених ресурсах [12].

У наступному розділі досліджені методи будуть використовуватись для розроблення математичної моделі управління вимогами кібербезпеки при впровадженні ПЗ.

2.2. Розроблення математичної моделі управління вимогами кібербезпеки при впровадженні програмного забезпечення на основі міжнародних стандартів

Математична модель управління вимогами кібербезпеки при впровадженні ПЗ на основі міжнародних стандартів [13, 14], реалізується за допомогою наступних кроків:

Крок 1: Створення графу залежностей вимог

Нехай $G = (V, E)$ – орієнтований граф, де:

▪ $V = \{v_1, v_2, \dots, v_n\}$ – множина вершин, кожна з яких представляє конкретну вимогу кібербезпеки R_i .

▪ $E \subseteq V \times V$ – множина орієнтованих ребер, кожне з яких позначає залежність між двома вимогами.

Кожна вимога v_i має атрибути:

▪ Важливість W_i – наскільки вимога критична для кібербезпеки системи.

▪ Ризик R_i – ймовірність компрометації безпеки, якщо вимога не виконана.

Крок 2: Використання методу AHP для пріоритезації вимог

Використовуємо метод AHP для пріоритезації вимог на основі критеріїв важливості W_i і ризику R_i.

1) Створення матриці парних порівнянь для кожного критерію: Для вимог v_i і v_j, заповнюємо матриці парних порівнянь A_W (за важливістю) і A_R (за ризиком), де a_{ij} вказує, наскільки важлива вимога v_i порівняно з вимогою v_j за певним критерієм.

2) Визначення ваги вимог:

- Обчислюємо власні вектори W і R для матриць A_W і A_R відповідно, які відображають ваги (або пріоритети) кожної вимоги за кожним критерієм.

Отримана векторна оцінка P вимог розраховується як:

$$P = \alpha W + \beta R, \tag{2.1}$$

де α і β – коефіцієнти важливості критеріїв (визначаються експертно).

Крок 3: Застосування нечіткої логіки для оцінки рівня відповідності вимогам

Враховуємо, що деякі вимоги можуть мати нечітку відповідність. Наприклад, відповідність кожної вимоги v_i можна оцінювати за допомогою нечітких множин на основі лінгвістичних змінних:

- Нечіткі змінні: “висока відповідність”, “середня відповідність”, “низька відповідність”.
- Функції належності $\mu_i(x)$ для кожної змінної нечіткої відповідності, де $x \in [0,1]$ – рівень відповідності вимоги v_i .
- Оцінка відповідності кожної вимоги v_i обчислюється як:

$$Score(v_i) = max\{\mu_{\text{висока}}(x), \mu_{\text{середня}}(x)\mu_{\text{низька}}(x)\}. \tag{2.2}$$

- Агрегація оцінок для визначення загального рівня відповідності всієї системи вимог, враховуючи середньозважені оцінки.

Крок 4: Моделювання ризиків за допомогою Байєсової мережі

Створюємо Байєсову мережу для моделювання впливу загроз на виконання вимог кібербезпеки.

- Вузли мережі:
  - кожна вимога v_i стає вузлом, з атрибутом ризику R_i.
  - додаткові вузли – потенційні загрози, що можуть впливати на виконання вимог.
- Ймовірності вузлів:

Ймовірності компрометації вимоги $P(v_i|T_j)$, де T_j – загроза, яка впливає на вимогу v_i.

- Розрахунок ризику системи: Використовуючи Байєсову мережу, можна обчислити ймовірність ризиків для кожної вимоги за умов присутності різних загроз.
- Обчислення ризику для кожної вимоги з урахуванням відповідності:

$$Risk\ (v_i) = R_i \times Score(v_i). \tag{2.3}$$

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Визначаємо оптимальний розподіл ресурсів для реалізації вимог кібербезпеки з урахуванням пріоритетів і ризиків.

- *змінні:*

x_i – частка ресурсів, виділена для вимоги v_i, де $0 \leq x_i \leq 1$;

- *цільова функція:* мінімізуємо ризики невиконання вимог з урахуванням обмежених ресурсів:

$$min \sum_{i=1}^{n} (1 - x_i) \times Risk(v_i) \tag{2.4}$$

- *обмеження:*
  - обмеження на загальний бюджет:

$$\sum_{i=1}^{n} x_i \times C_i \leq B \tag{2.5}$$

де C_i – вартість виконання вимоги v_i, B – загальний бюджет.

- пріоритетність вимог: $x_i \geq p_i$ для всіх вимог v_i з високим пріоритетом, де p_i – мінімальний рівень виконання для пріоритетних вимог.

▪ *Вихідний розподіл ресурсів:* розв'язавши оптимізаційну задачу, отримуємо оптимальні значення x_i для кожної вимоги v_i, які забезпечують мінімізацію ризиків при обмежених ресурсах.

Таким чином, було розроблено модель, яка дозволяє:

▪ визначити пріоритети серед вимог кібербезпеки (кроки 1-2).

▪ врахувати невизначеності та ймовірність ризиків за допомогою нечіткої логіки і Байєсової мережі (кроки 3-4).

▪ оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків (крок 5).

Ця модель забезпечує комплексне управління вимогами кібербезпеки під час впровадження програмного забезпечення з урахуванням міжнародних стандартів (див. приклади у підрозділі 2.3) і сучасних методів оцінки ризиків.

2.3. Порівняння підходів до управління вимогами кібербезпеки в стандартах NIST 800-53, ISO 22316, та MITRE ATT&CK

Кожен із цих стандартів (NIST 800-53, ISO 22316, та MITRE ATT&CK) фокусується на різних аспектах кібербезпеки та стійкості, що відображено в їхніх підходах, структурах і застосуванні. Розглянемо більш детально (Табл. 2.1 – 2.8) для подальшого дослідження практичного застосування запропонованої моделі на основі одного із стандартів.

Таблиця 2.1

Загальна мета та сфера застосування

Стандарт	Мета	Сфера застосування
NIST 800-53	Розробка контролів безпеки для захисту систем, даних і мереж	Федеральні агентства США, приватний сектор
ISO 22316	Забезпечення організаційної стійкості та відновлення після інцидентів	Широке застосування для організацій різних розмірів та секторів
MITRE ATT&CK	Опис тактик і технік для ідентифікації та нейтралізації кіберзагроз	Організації кібербезпеки, аналіз кіберзагроз, тестування безпеки

Таблиця 2.2

Основні цілі

Стандарт	Основні цілі
NIST 800-53	Визначення і впровадження контролів безпеки, що відповідають потребам організацій і мінімізують ризики
ISO 22316	Побудова стійкості організації, зокрема в умовах кризових ситуацій, забезпечення безперервності бізнесу
MITRE ATT&CK	Аналіз загроз і розробка ефективних методів ідентифікації та реагування на конкретні тактики й техніки атак

Таблиця 2.3

Структура та компоненти

Стандарт	Основні компоненти
NIST 800-53	Контролі безпеки розділені на 20 сімейств, серед яких є такі як доступ, захист ідентичності, моніторинг безпеки, реагування на інциденти та ін.

ISO 22316	Принципи стійкості, включаючи управління ризиками, підтримку ресурсів, стратегії безперервності бізнесу, навчання персоналу та комунікацію
MITRE ATT&CK	Матриця з тактиками (наприклад, збір даних, ініціалізація атак), техніками (специфічні методи атак) та підходами до нейтралізації загроз

Таблиця 2.4

Орієнтація на безпеку і стійкість

Стандарт	Орієнтація
NIST 800-53	Захист інформаційних систем і даних через впровадження надійних заходів контролю, орієнтований на запобігання ідентифікованим ризикам
ISO 22316	Загальна організаційна стійкість, що охоплює всі аспекти діяльності, включаючи кадрові, ресурсні, інформаційні та інфраструктурні ресурси
MITRE ATT&CK	Акцент на розумінні кіберзагроз та наданні організаціям конкретних інструментів для ідентифікації, аналізу та реагування на атаки

Таблиця 2.5

Підходи до управління ризиками

Стандарт	Підхід до управління ризиками
NIST 800-53	Включає оцінку ризиків на основі ймовірностей і впливу загроз на інформаційну систему; ризики розглядаються при визначенні контролів безпеки
ISO 22316	Розробка комплексної стратегії управління ризиками в рамках забезпечення стійкості, що враховує операційні, кадрові, фінансові та інформаційні аспекти

MITRE ATT&CK	Фокусується на розумінні атакуючих тактик і технік для забезпечення захисту та швидкого реагування, ризики обчислюються на основі ймовірності та впливу атак

Таблиця 2.6

Реалізація на практиці

Стандарт	Реалізація на практиці
NIST 800-53	Впровадження контролів безпеки в системи; підходить для організацій з чіткою структурою управління та відповідністю регуляторним вимогам
ISO 22316	Розробка стратегій і планів для стійкості, включаючи комунікацію, управління кризовими ситуаціями, тренінги для персоналу
MITRE ATT&CK	Використовується для виявлення і реагування на кіберзагрози; застосовується для оцінки ефективності існуючих засобів захисту і тестування готовності організації до атак

Таблиця 2.7

Переваги та недоліки

Стандарт	Переваги	Недоліки
NIST 800-53	Високий рівень деталізації контролів для різних систем	Може бути надто громіздким для малих організацій
ISO 22316	Охоплює всі аспекти організаційної стійкості	Менш специфічний для кібербезпеки
MITRE ATT&CK	Чітке розуміння тактик та технік атак, ефективне тестування	Не розглядає стратегічні чи адміністративні аспекти

Таблиця 2.8

Основні відмінності

Критерій	NIST 800-53	ISO 22316	MITRE ATT&CK
Фокус	Технічні заходи і контролі безпеки	Загальна стійкість організації	Тактики і техніки атак
Застосування	Головним чином США, але міжнародне визнання	Міжнародне	Міжнародне, часто для аналізу атак
Деталізація заходів	Дуже висока деталізація	Висока деталізація стійкості, але не безпеки	Висока деталізація атакуючих технік
Аудиторія	Урядові організації, великі компанії	Будь-які організації	Організації кібербезпеки, аналітики загроз
Підхід до атакуючих загроз	Передбачає аналіз ризиків	Включає аналіз ризиків на стратегічному рівні	Конкретні тактики і техніки для протидії атакам

Виходячи з проведеного порівняльного аналізу, наведеного у Табл. 2.1 – 2.8, можна зробити наступні висновки щодо стандартів:

- NIST 800-53 забезпечує всеохопний набір технічних контролів безпеки для захисту інформаційних систем. Це особливо корисно для організацій, які працюють з урядом або мають суворі регуляторні вимоги.
- ISO 22316 орієнтований на стійкість організації в цілому і охоплює широкий спектр питань, включаючи управління ресурсами, ризиками та кризовими ситуаціями, що робить його придатним для організацій, які хочуть підвищити свою готовність до будь-яких кризових подій.
- MITRE ATT&CK спеціалізується на деталізованому аналізі кіберзагроз, тактик і технік, що робить його корисним інструментом для організацій, які прагнуть зрозуміти можливості зловмисників та оптимізувати засоби захисту.

Таким чином, організаціям може бути корисно використовувати ці стандарти разом: NIST 800-53 для налаштування технічного контролю, ISO 22316 для забезпечення загальної стійкості, а MITRE ATT&CK для детального розуміння та протидії конкретним загрозам.

2.4. Приклади практичної реалізації розробленої моделі на основі вимог міжнародних стандартів у галузі кібербезпеки

2.4.1. Реалізація моделі на основі стандарту NIST 800-53

Для детального прикладу візьмемо загальний бюджет у розмірі 1,000,000 грн і розподілимо його між вимогами кібербезпеки на основі стандартів NIST, використовуючи запропоновану модель управління вимогами. Припустимо, що мета – оптимально розподілити кошти між вимогами кібербезпеки, мінімізуючи ризики, і водночас забезпечити високий рівень виконання кожної вимоги.

Вихідні дані прикладу:

Вимоги:

1. Контроль доступу (AC) – обмеження доступу до даних.
2. Захист цілісності даних (SI) – забезпечення цілісності зберігання даних.
3. Реагування на інциденти (IR) – заходи для своєчасного реагування.
4. Аудит і логування (AU) – запис подій для моніторингу та контролю.

Бюджет і ресурсні обмеження:

- Загальний бюджет: 1,000,000 грн.
- Вартість виконання вимог (у разі повного фінансування):

  AC: 300,000 грн

  SI: 400,000 грн

  IR: 200,000 грн

  AU: 100,000 грн.

Таблиця 2.9

Пріоритети вимог за важливістю та ризиком (метод AHP)

Вимога	Важливість W_i	Ризик R_i
AC	0.3	0.2
SI	0.4	0.4
IR	0.2	0.3
AU	0.1	0.1

Критерії для нечіткої логіки:

- Висока відповідність: $\mu_{high} = [0.8, 1.0]$
- Середня відповідність: $\mu_{medium} = [0.5, 0.7]$
- Низька відповідність: $\mu_{low} = [0, 0.4]$

Ймовірність виникнення загроз за Байєсовою мережею:

- Фішинг-атака: 0.3, що впливає на AC.
- Витік даних: 0.5, що впливає на SI.
- Зловмисне ПЗ: 0.2, що впливає на IR.

Кроки реалізації розробленої моделі:

Крок 1: Створення графу залежностей вимог

Граф залежностей:

- IR залежить від AU – для оперативного реагування потрібні журнали подій.
- SI має критичний вплив на AC та IR, оскільки цілісність даних важлива для обох процесів.

Крок 2: Пріоритизація вимог за допомогою AHP

Загальна оцінка пріоритету для кожної вимоги за (2.1):

$$P_i = \alpha W_i + \beta R_i,$$

де α = 0.6 (вага важливості) та β=0.4 (вага ризику).

Таблиця 2.10

Пріоритетизація вимог

Вимога	Пріоритет P_i
AC	$0.6 \cdot 0.3 + 0.4 \cdot 0.2 = 0.26$
SI	$0.6 \cdot 0.4 + 0.4 \cdot 0.4 = 0.40$
IR	$0.6 \cdot 0.2 + 0.4 \cdot 0.3 = 0.24$
AU	$0.6 \cdot 0.1 + 0.4 \cdot 0.1 = 0.10$

Крок 3: Застосування нечіткої логіки для оцінки відповідності

Припустимо, що поточний рівень виконання вимог оцінюється наступним чином (Табл. 2.11):

Таблиця 2.11

Рівень виконання вимог

Вимога	Відповідність x_i
AC	0.7
SI	0.85
IR	0.6
AU	0.5

На основі цього відповідність оцінюється як:

- AC: Середня відповідність
- SI: Висока відповідність
- IR: Середня відповідність
- AU: Середня відповідність

Крок 4: Моделювання ризиків за допомогою Байєсової мережі

Обчислюємо ймовірність компрометації для кожної вимоги з урахуванням її відповідності:

AC: $P(compromised) = 0.3 \times (1 - 0.7) = 0.09$

SI: $P(compromised) = 0.5 \times (1 - 0.85) = 0.075$

IR: $P(compromised) = 0.2 \times (1 - 0.6) = 0.08$

AU: $P(compromised) = 0.05$ (при незначному ризику).

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Цільова функція:

$$min \sum_{i=1}^{n} (1 - x_i) \times P_i \times Risk(v_i)$$

Обмеження:

$$\sum_{i=1}^{n} x_i \times C_i \leq B$$

де C_i – вартість виконання вимоги i, B = 1 000 000 грн.

Розв'язуючи оптимізаційну задачу (за умови пропорційного розподілу ресурсів і врахування обмежень бюджету), отримуємо наступні значення оптимального виділення ресурсів (Табл. 2.12).

Таблиця 2.12

Оптимальне виділення ресурсів

Вимога	Оптимальне виділення ресурсів (%)	Виділення коштів (грн)
AC	30%	300,000
SI	40%	400,000
IR	20%	200,000
AU	10%	100,000

Результати реалізації моделі на основі стандарту NIST 800-53

- Вимоги AC та SI отримали найбільше фінансування (30% і 40% бюджету відповідно), що відповідає їхнім високим пріоритетам за критеріями важливості та ризику.
- IR отримала 20% фінансування, що забезпечує достатній рівень виконання та знижує ризик від зловмисного ПЗ.
- AU отримала 10% фінансування, що дозволяє підтримувати базовий рівень аудиту та логування.

Таким чином, модель оптимізації ресурсів забезпечила мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно зі стандартами NIST.

2.4.2. Реалізація моделі на основі стандарту ISO 22316

Розглянемо детальний приклад управління вимогами кібербезпеки при впровадженні ПЗ на основі міжнародного стандарту ISO 22316, який передбачає забезпечення стійкості організації. У цьому прикладі використаємо 6 основних вимог, які підвищують стійкість організації та відповідають бюджетним обмеженням у розмірі 1,000,000 грн (розподіл вартості за вимогами зображено у Табл. 2.13, а пріоритетність і ризик вимог – у Табл. 2.14).

Вихідні дані прикладу

Вимоги:

1. AC (Access Control) – контроль доступу.
2. SI (Data Integrity) – захист цілісності даних.
3. IR (Incident Response) – реагування на інциденти.
4. AU (Audit and Logging) – аудит та логування.
5. BC (Backup and Recovery) – резервне копіювання та відновлення.
6. ET (Employee Training) – навчання співробітників з кібербезпеки.

Таблиця 2.13

Вартість виконання вимог

Вимога	Опис	Вартість виконання C_i
AC	Контроль доступу	250,000 грн
SI	Захист цілісності даних	300,000 грн
IR	Реагування на інциденти	150,000 грн
AU	Аудит та логування	100,000 грн
BC	Резервне копіювання	200,000 грн
ET	Навчання співробітників	150,000 грн

Таблиця 2.14

Пріоритетність і ризик вимог (на основі методу AHP)

Вимога	Важливість W_i	Ризик R_i
AC	0.25	0.20
SI	0.30	0.25
IR	0.20	0.15
AU	0.10	0.05
BC	0.15	0.20
ET	0.10	0.15

Бюджет і ресурсні обмеження:

- Загальний бюджет: 1,000,000 грн.
- Ціль: Мінімізувати ризик і забезпечити виконання критичних вимог при обмеженому бюджеті.

Крок 1: Створення графу залежностей вимог

Граф залежностей будуємо так:

- IR залежить від AU і ET (для ефективного реагування необхідний аудит і навчання).

- AC залежить від SI і AU (необхідні захист цілісності даних та аудит).
- BC залежить від SI (резервне копіювання має забезпечувати збереження цілісності).

Крок 2: Використання AHP для пріоритезації вимог

Знаходимо загальну оцінку пріоритету для кожної вимоги за формулою:

$$P_i = \alpha W_i + \beta R_j$$

де α=0.6 і β=0.4.

Табл. 2.15 містить пріоритезацію вимог, а в Табл. 2.16 представлено відповідність кожної вимоги.

Таблиця 2.15

Пріоритетизація вимог

Вимога	Пріоритет P_i
AC	$0.6 \cdot 0.25 + 0.4 \cdot 0.20 = 0.23$
SI	$0.6 \cdot 0.30 + 0.4 \cdot 0.25 = 0.28$
IR	$0.6 \cdot 0.20 + 0.4 \cdot 0.15 = 0.18$
AU	$0.6 \cdot 0.10 + 0.4 \cdot 0.05 = 0.08$
BC	$0.6 \cdot 0.15 + 0.4 \cdot 0.20 = 0.17$
ET	$0.6 \cdot 0.10 + 0.4 \cdot 0.15 = 0.12$

Крок 3: Застосування нечіткої логіки для оцінки відповідності

Враховуємо рівень відповідності кожної вимоги (Табл. 2.16):

Таблиця 2.16

Відповідність вимог

Вимога	Відповідність x_i
AC	0.7

SI	0.85
IR	0.6
AU	0.5
BC	0.75
ET	0.65

Згідно з лінгвістичними змінними:

- Висока відповідність для SI і BC (висока важливість і ризик).
- Середня відповідність для AC, IR, ET.
- Низька відповідність для AU.

Крок 4: Моделювання ризиків із застосуванням Байєсової мережі

Ймовірності компрометації для кожної вимоги з урахуванням загроз:

AC: $P(compromised) = 0.2 \times (1 - 0.7) = 0.06$

SI: $P(compromised) = 0.25 \times (1 - 0.85) = 0.0375$

IR: $P(compromised) = 0.15 \times (1 - 0.6) = 0.06$

AU: $P(compromised) = 0.05 \times (1 - 0.5) = 0.025$

BC: $P(compromised) = 0.20 \times (1 - 0.75) = 0.05$

ET: $P(compromised) = 0.15 \times (1 - 0.65) = 0.0525$

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Метою є мінімізація ризиків з урахуванням обмеженого бюджету:

1. Змінні: x_i – частка ресурсів для вимоги v_i, де $0 \leq x_i \leq 1$
2. Цільова функція:

$$min \sum_{i=1}^{6} (1 - x_i) \times P_i \times Risk(v_i)$$

3. Обмеження:

Бюджетне обмеження:

$$\sum_{i=1}^{6} x_i \times C_i \leq 1{,}000{,}000$$

Розв’язання дає оптимальний розподіл ресурсів (Табл. 2.17).

Таблиця 2.17

Оптимальне виділення ресурсів

Вимога	Оптимальне виділення ресурсів (%)	Виділення коштів (грн)
AC	25%	250,000
SI	30%	300,000
IR	15%	150,000
AU	10%	100,000
BC	10%	100,000
ET	10%	100,000

Результати реалізації моделі на основі стандарту ISO 22316

- Вимоги з найвищим пріоритетом (SI і AC) отримали більше фінансування, оскільки їх ризик і важливість є найвищими.
- Вимоги IR, AU, BC і ET отримали менше фінансування, але достатньо для забезпечення мінімального рівня відповідності та стійкості системи.

Модель оптимізації забезпечує досягнення балансу між важливістю вимог, мінімізацією ризиків і наявними ресурсами, що відповідає вимогам ISO 22316 для забезпечення стійкості організації.

2.4.3. Реалізація моделі на основі стандарту MITRE ATT&CK

Для побудови моделі управління вимогами кібербезпеки на основі стандарту MITRE (який визначає таксономію тактик, методів і технік атаки) розглянемо 8 основних вимог з кібербезпеки та розподілимо бюджет у розмірі 1 000 000 грн. Цей

приклад буде зосереджено на забезпеченні ресурсів для вимог кібербезпеки з урахуванням обмежень бюджету та пріоритетності вимог.

Вихідні дані прикладу

Вимоги кібербезпеки (основні вимоги стандарту MITRE)

1. Initial Access (IA) – забезпечення захисту від несанкціонованого початкового доступу.
2. Execution (EX) – контроль виконання шкідливих програм.
3. Persistence (PE) – захист від збереження несанкціонованих змін.
4. Privilege Escalation (PR) – захист від підвищення привілеїв.
5. Defense Evasion (DE) – уникнення обходу систем захисту.
6. Credential Access (CA) – захист доступу до облікових даних.
7. Discovery (DS) – запобігання збору інформації з системи.
8. Exfiltration (EF) – захист від несанкціонованого виведення даних.

Таблиця 2.18

Вартість виконання вимог

Вимога	Опис	Вартість виконання C_i
IA	Захист початкового доступу	200,000 грн
EX	Контроль виконання програм	150,000 грн
PE	Захист від збереження змін	120,000 грн
PR	Захист від підвищення привілеїв	130,000 грн
DE	Запобігання обходу захисту	180,000 грн
CA	Захист облікових даних	100,000 грн
DS	Захист від збору інформації	120,000 грн
EF	Захист від виведення даних	100,000 грн

Таблиця 2.19

Пріоритетність і ризик вимог (на основі методу AHP)

Вимога	Важливість W_i	Ризик R_i
IA	0.2	0.3

EX	0.15	0.2
PE	0.1	0.15
PR	0.15	0.25
DE	0.2	0.3
CA	0.1	0.15
DS	0.05	0.1
EF	0.05	0.1

Бюджет та обмеження:

- Загальний бюджет: 1,000,000 грн.
- Ціль: Оптимально розподілити кошти для мінімізації ризиків, забезпечуючи пріоритетні вимоги.

Крок 1: Створення графу залежностей вимог

Побудуємо граф залежностей:

PR (підвищення привілеїв) залежить від IA (початковий доступ) та CA (доступ до облікових даних).

DE (обхід захисту) залежить від PE (збереження несанкціонованих змін) і PR.

EF (виведення даних) залежить від DS (збір інформації) і CA (облікові дані).

Крок 2: Використання AHP для пріоритезації вимог

Загальна оцінка пріоритету для кожної вимоги розраховується як:

$$P_i = \alpha W_i + \beta R_j$$

де α=0.6 і β=0.4.

Табл. 2.20 містить пріоритезацію вимог, а в Табл. 2.21 представлено відповідність кожної вимоги.

Таблиця 1.20

Пріоритетизація вимог

Вимога	Пріоритет P_i
IA	$0.6 \cdot 0.2 + 0.4 \cdot 0.3 = 0.24$
EX	$0.6 \cdot 0.15 + 0.4 \cdot 0.2 = 0.17$
PE	$0.6 \cdot 0.1 + 0.4 \cdot 0.15 = 0.12$
PR	$0.6 \cdot 0.15 + 0.4 \cdot 0.25 = 0.19$
DE	$0.6 \cdot 0.2 + 0.4 \cdot 0.3 = 0.24$
CA	$0.6 \cdot 0.1 + 0.4 \cdot 0.15 = 0.12$
DS	$0.6 \cdot 0.05 + 0.4 \cdot 0.1 = 0.07$
EF	$0.6 \cdot 0.05 + 0.4 \cdot 0.1 = 0.07$

Крок 3: Застосування нечіткої логіки для оцінки відповідності

Враховуємо рівень відповідності для кожної вимоги (Табл. 2.21).

Таблиця 2.21

Відповідність вимог

Вимога	Відповідність x_i
IA	0.8
EX	0.7
PE	0.6
PR	0.75
DE	0.85
CA	0.65
DS	0.5
EF	0.5

Згідно з лінгвістичними змінними:

- Висока відповідність: IA, DE, PR.

- Середня відповідність: EX, PE, CA.
- Низька відповідність: DS, EF.

Крок 4: Моделювання ризиків із застосуванням Байєсової мережі

Розраховуємо ймовірність компрометації для кожної вимоги з урахуванням загроз:

IA: $P(compromised) = 0.3 \times (1 - 0.8) = 0.06$

EX: $P(compromised) = 0.2 \times (1 - 0.7) = 0.06$

PE: $P(compromised) = 0.15 \times (1 - 0.6) = 0.06$

PR: $P(compromised) = 0.25 \times (1 - 0.75) = 0.0625$

DE: $P(compromised) = 0.3 \times (1 - 0.85) = 0.045$

CA: $P(compromised) = 0.15 \times (1 - 0.65) = 0.0525$

DS: $P(compromised) = 0.1 \times (1 - 0.5) = 0.05$

EF: $P(compromised) = 0.1 \times (1 - 0.5) = 0.05$

Крок 5: Оптимізація ресурсів за допомогою математичного програмування

Мінімізуємо ризики невиконання вимог при обмеженому бюджеті:

1. Цільова функція:

$$min \sum_{i=1}^{8} (1 - x_i) \times P_i \times Risk(v_i)$$

2. Обмеження:

$$\sum_{i=1}^{8} x_i \times C_i \leq 1{,}000{,}000$$

Розв'язуючи оптимізаційну задачу, отримуємо оптимальний розподіл, що відображено у Табл. 2.22.

Таблиця 2.22

Оптимальне виділення ресурсів

Вимога	Оптимальне виділення ресурсів (%)	Виділення коштів (грн)
IA	20%	200,000
EX	15%	150,000
PE	10%	120,000
PR	13%	130,000
DE	18%	180,000
CA	10%	100,000
DS	7%	70,000
EF	7%	70,000

Результати реалізації моделі на основі стандарту MITRE ATT&CK

- IA і DE отримали найбільше фінансування (20% і 18% відповідно) через їх високу важливість і ризик для системи.
- PR та EX також отримали значні ресурси через високий ризик і взаємозалежність з іншими вимогами.
- DS та EF мають найменше фінансування, оскільки вони мають низькі пріоритети та ризики.

Цей розподіл ресурсів оптимізує виконання критичних вимог MITRE ATT&CK і мінімізує загальні ризики при дотриманні бюджету 1,000,000 грн.

2.5. Висновки до другого розділу дисертації

1) У другому розділі було проведено дослідження математичних методів для управління вимогами кібербезпеки при впровадженні ПЗ. Було розроблено модель, яка дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків за допомогою нечіткої логіки і Байєсової мережі, а також оптимально розподілити ресурси між вимогами з урахуванням

обмежень бюджету та мінімізації ризиків. Розроблена модель забезпечує комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків [15-18].

2) Виходячи з проведеного порівняльного аналізу, можна зробити наступні висновки щодо досліджених стандартів:

- NIST 800-53 забезпечує всеохопний набір технічних контролів безпеки для захисту інформаційних систем. Це особливо корисно для організацій, які працюють з урядом або мають суворі регуляторні вимоги.
- ISO 22316 орієнтований на стійкість організації в цілому і охоплює широкий спектр питань, включаючи управління ресурсами, ризиками та кризовими ситуаціями, що робить його придатним для організацій, які хочуть підвищити свою готовність до будь-яких кризових подій.
- MITRE ATT&CK спеціалізується на деталізованому аналізі кіберзагроз, тактик і технік, що робить його корисним інструментом для організацій, які прагнуть зрозуміти можливості зловмисників та оптимізувати засоби захисту.

Таким чином, організаціям може бути корисно використовувати ці стандарти разом: NIST 800-53 для налаштування технічного контролю, ISO 22316 для забезпечення загальної стійкості, а MITRE ATT&CK для детального розуміння та протидії конкретним загрозам.

3) Було реалізовано розроблену модель на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно зі стандартами NIST. Зокрема, встановлено:

- Вимоги AC та SI отримали найбільше фінансування (30% і 40% бюджету відповідно), що відповідає їхнім високим пріоритетам за критеріями важливості та ризику.
- IR отримала 20% фінансування, що забезпечує достатній рівень виконання та знижує ризик від зловмисного ПЗ.
- AU отримала 10% фінансування, що дозволяє підтримувати базовий рівень аудиту та логування.

4) Було реалізовано розроблену модель на основі стандарту ISO 22316, яка забезпечує досягнення балансу між важливістю вимог, мінімізацією ризиків і

наявними ресурсами, що відповідає вимогам ISO 22316 для забезпечення стійкості організації. Зокрема, встановлено:

- Вимоги з найвищим пріоритетом (SI і AC) отримали більше фінансування, оскільки їх ризик і важливість є найвищими.
- Вимоги IR, AU, BC і ET отримали менше фінансування, але достатньо для забезпечення мінімального рівня відповідності та стійкості системи.

5) Було реалізовано розроблену модель на основі стандарту MITRE ATT&CK, здійснений розподіл ресурсів оптимізує виконання критичних вимог MITRE ATT&CK і мінімізує загальні ризики при дотриманні бюджету 1 000 000 грн. Зокрема, встановлено:

- IA і DE отримали найбільше фінансування (20% і 18% відповідно) через їх високу важливість і ризик для системи.
- PR та EX також отримали значні ресурси через високий ризик і взаємозалежність з іншими вимогами.
- DS та EF мають найменше фінансування, оскільки вони мають низькі пріоритети та ризики.

2.6. Список використаних джерел у другому розділі дисертації

1. L. Li et al., "LogicEdu: Enhancing Computational Logic Understanding through Web-Based Boolean Logic Simplification Tool," 2024 21st International SoC Design Conference (ISOCC), Sapporo, Japan, 2024, pp. 390-391, doi: 10.1109/ISOCC62682.2024.10762040.
2. S. Deepak, J. A. Shah, N. Chetan and H. Sharda, "New Decision-Making Process Based on Set Theory: Towards Application of Set Theory," 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2023, pp. 1-6, doi: 10.1109/ICTBIG59752.2023.10456045.
3. H. Wang, "Network Graph Theory and Organization Model Analysis based on Mathematical Modeling with the Dynamic Systematic Data Perspective," 2022 6th

International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 915-919, doi: 10.1109/ICOEI53556.2022.9776767.

4. S. Bhadra, "A Stochastic Petri net Model of Continuous Integration and Continuous Delivery," 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Charlotte, NC, USA, 2022, pp. 114-117, doi: 10.1109/ISSREW55968.2022.00050.

5. K. Suresh Kumar; R. Sudha; T. Suguna; M. K. Dharani, "An Intelligent Heartbeat Management System Utilizing Fuzzy Logic," in Advances in Fuzzy-Based Internet of Medical Things (IoMT) , Wiley, pp.211-223, doi: 10.1002/9781394242252.ch14.

6. Q. Yu and Z. Li, "A Bayesian Model Averaging Method for Software Reliability Assessment," 2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM), Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/APARM49247.2020.9209504.

7. B. Yang et al., "A critical and comprehensive handbook for game theory applications on new power systems: Structure, methodology, and challenges," in Protection and Control of Modern Power Systems, doi: 10.23919/PCMP.2024.000297.

8. Pratyush Shukla; Sanjay Kumar Singh; Aditya Khamparia; Anjali Goyal, "9 Nature-inspired optimization techniques," in Nature-Inspired Optimization Algorithms: Recent Advances in Natural Computing and Biomedical Applications , De Gruyter, pp.137-152.

9. R. Beniwal, V. Kumar and V. Sharma, "Metaheuristics Approaches Towards Secure and Optimized Routing in IoT: A Systematic Literature Review," 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), Greater Noida, India, 2024, pp. 1-6, doi: 10.1109/ICEECT61758.2024.10739076.

10. T. T. Zin, A. S. T. Moe, C. N. Phyo and P. Tin, "Fusion of Strategic Queueing Theory and AI for Smart City Telecommunication System," 2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS), Seoul, Korea, Republic of, 2024, pp. 653-657, doi: 10.1109/MASS62177.2024.00104.

11. N. Zhang, Y. Chen, W. Yang, Z. Zhang, Y. Liu and W. Mao, "Application of Fault Tree Analysis for Reliability Evaluation and Weak Link Identification of Stadium

Power Supply System Using Monte Carlo Simulation," 2021 IEEE Sustainable Power and Energy Conference (iSPEC), Nanjing, China, 2021, pp. 4209-4214, doi: 10.1109/iSPEC53008.2021.9735815.

12. D. Kim, B. Jeon and K. C. Koo, "Addressing Timely AI Technology Standardization Challenges through a Hierarchical Analysis Approach," *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Republic of, 2023, pp. 1431-1433, doi: 10.1109/ICTC58733.2023.10393654.

13. Гнатюк С.О., Сидоренко В.М., Скуратівський А.А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення. Кібербезпека: освіта, наука, техніка, 2025, Т.4, № 28, с. 25-37. DOI: https://doi.org/10.28925/2663-4023.2025.28.841

14. Gnatyuk S., Sydorenko V., Polozhentsev A., Skurativskyi A. Experimental Study of a Model for Cybersecurity Requirements Management Based on International Standards, Springer (прийнято до друку).

15. Sydorenko V., Gnatyuk S., Tolbatov A., Fesenko A., Yevchenko Y., Sotnichenko Y. (2020). Experimental FMECA-based assessment of the critical information infrastructure importance in aviation. CEURWorkshop Proceedings, 2732, 136–156.

16. Hnatyuk S.O., Berdybayev R.Sh., Sydorenko V.M., Zhigarevych O.K., Smirnova T.V. (2023). Event correlation and cybersecurity incident management system at critical infrastructure facilities. Cybersecurity: Education, Science, Technology, 3(19), pp. 176-196.

17. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління, 2024, Т. 2, №º78, С. 104-114, https://doi.org/10.18372/2073-4751.78.18967

18. Polozhentsev A. A., Sydorenko V.M. (2024). IT threat management method for critical information infrastructure facilities. Science-Intensive Technologies, 2(62), pp. 143-153.

РОЗДІЛ 3. МЕТОД УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У БІЗНЕСІ

3.1. Особливості управління вимогами кібербезпеки в різних галузях та середовищах

3.1.1. Галузево орієнтоване (industry-oriented) управління вимогами кібербезпеки

Управління вимогами кібербезпеки при впровадженні ПЗ суттєво залежить від галузевої специфіки, характеру бізнес-процесів, регуляторних вимог, допустимого рівня ризику та потенційних наслідків інцидентів. На відміну від універсальних підходів, ***галузево (секторально) орієнтоване управління вимогами кібербезпеки*** передбачає адаптацію методів пріоритезації, оцінювання ризиків і розподілу ресурсів відповідно до контексту застосування ПЗ.

Фінансовий сектор

У фінансових установах вимоги кібербезпеки мають високий пріоритет через критичність конфіденційності, цілісності та доступності даних. Основна увага приділяється управлінню доступом, ідентифікації та автентифікації, моніторингу транзакцій і аудиту дій користувачів. Для цієї галузі характерні жорсткі регуляторні обмеження та низька толерантність до ризику, що зумовлює домінування превентивних контролів і високі витрати на виконання вимог кібербезпеки.

Промисловість та критична інфраструктура

У промислових і інфраструктурних системах управління вимогами кібербезпеки орієнтоване насамперед на забезпечення безперервності та безпеки технологічних процесів. Тут пріоритет надається вимогам стійкості, відновлення після інцидентів та ізоляції критичних компонентів. Особливістю є необхідність узгодження вимог кібербезпеки з вимогами функціональної безпеки та обмеженими можливостями оновлення ПЗ.

Бізнес-орієнтоване ПЗ та корпоративні IT-системи

Для корпоративних бізнес-систем управління вимогами кібербезпеки здійснюється в умовах обмеженого бюджету та швидких циклів розробки. Пріоритети вимог часто змінюються залежно від бізнес-цілей, ринкових умов і моделей загроз. У

таких системах важливу роль відіграє баланс між витратами на безпеку та допустимим рівнем ризику, що потребує формалізованих методів оптимізації та підтримки прийняття рішень.

Хмарні та сервіс-орієнтовані рішення

У хмарних середовищах управління вимогами кібербезпеки ускладнюється розподіленою архітектурою, динамічним масштабуванням та розподілом відповідальності між провайдером і замовником. Пріоритетними стають вимоги до контролю доступу, ізоляції середовищ, моніторингу та відповідності стандартам. Характерною особливістю є необхідність постійного перегляду вимог у відповідь на зміну конфігурацій і моделей використання сервісів.

Узагальнення галузевих особливостей

Аналіз показує, що універсальне управління вимогами кібербезпеки без урахування галузевого контексту є неефективним. Різні галузі вимагають різних стратегій пріоритезації вимог, рівнів деталізації контролів і підходів до оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних методів управління вимогами кібербезпеки, які здатні враховувати галузеві особливості, обмеження ресурсів і динаміку загроз.

Приклад 1. *Управління вимогами кібербезпеки у фінансовому секторі*

У фінансовому секторі управління вимогами кібербезпеки має критичне значення через обробку фінансових транзакцій, персональних даних клієнтів та високі регуляторні ризики. Як приклад розглянемо інформаційну систему банківської установи «Комерційний Банк», що забезпечує дистанційне обслуговування клієнтів і інтеграцію з платіжними сервісами. Формування вимог кібербезпеки в такій системі здійснюється відповідно до положень NIST SP 800-53 [1], стандартів ISO/IEC 27001/27002 [2], а також галузевих нормативів PCI DSS [3] і регуляторних вимог European Union PSD2 [4], які визначають обов’язкові заходи захисту фінансових даних і платіжних операцій.

На основі зазначених нормативних документів формується перелік вимог кібербезпеки з домінуванням вимог до ідентифікації та автентифікації клієнтів, управління доступом до фінансових ресурсів, моніторингу транзакцій і

журналювання подій безпеки. Для аналізу актуальних загроз і сценаріїв атак застосовується база знань MITRE ATT&CK [5], що дозволяє пов’язати вимоги кібербезпеки з такими тактиками, як компрометація облікових даних, шахрайські транзакції та зловживання привілеями. В умовах обмеженого бюджету та високих вимог до доступності сервісів виникає необхідність формалізованої пріоритезації вимог, оскільки реалізація всіх контролів одночасно є економічно недоцільною.

Управління вимогами кібербезпеки у фінансовому секторі здійснюється шляхом оцінювання ризиків фінансових втрат, регуляторних санкцій та репутаційних наслідків із подальшим оптимальним розподілом ресурсів між вимогами. Найвищий пріоритет отримують вимоги до багатофакторної автентифікації, контролю транзакцій, виявлення аномалій та аудиту, тоді як допоміжні вимоги реалізуються поетапно. Такий підхід дозволяє забезпечити відповідність регуляторним вимогам, знизити ймовірність шахрайства та динамічно адаптувати систему кібербезпеки до змін у загрозах і бізнес-процесах фінансової установи.

3.1.2. Середовище орієнтоване (environment-oriented) управління вимогами кібербезпеки

Різні типи середовищ потребують різних стратегій пріоритезації вимог, рівнів автоматизації та методів оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних і формалізованих моделей управління вимогами кібербезпеки, здатних динамічно враховувати зміну умов функціонування ПЗ. Отже, ***середовище орієнтоване управління вимогами кібербезпеки*** може передбачати такі типи середовищ за основу:

Локальне середовище

У локальних середовищах управління вимогами кібербезпеки ґрунтується на повному контролі інфраструктури з боку організації. Пріоритетними є вимоги до управління доступом, сегментації мережі, резервного копіювання та аудиту дій користувачів. Характерною особливістю є відносна стабільність архітектури, що дозволяє застосовувати статичні (не динамічні) або напівдинамічні моделі пріоритезації вимог. Разом із тим, значні капітальні витрати та обмежені ресурси

зумовлюють необхідність оптимізації виконання вимог кібербезпеки з урахуванням бюджету.

Хмарне середовище

У хмарних середовищах управління вимогами кібербезпеки ускладнюється розподіленою природою ресурсів, динамічним масштабуванням і моделлю спільної відповідальності між постачальником послуг та замовником. Основну увагу приділяють вимогам до ідентифікації та автентифікації, контролю доступу, ізоляції середовищ, моніторингу та відповідності стандартам. Пріоритети вимог у таких середовищах змінюються в часі, що зумовлює необхідність динамічного управління вимогами та регулярного перегляду їхньої важливості.

Гібридне середовище

Гібридні середовища поєднують локальні та хмарні компоненти, що створює додаткову складність для управління вимогами кібербезпеки. Особливістю є необхідність узгодження вимог між різними доменами безпеки, забезпечення захищених каналів обміну даними та єдиної політики управління доступом. У таких умовах зростає роль інтегрованих моделей оцінювання ризиків, здатних враховувати взаємозалежності між компонентами системи та потенційні каскадні наслідки інцидентів.

Мікросервісні та сервіс-орієнтовані середовища

У сервіс-орієнтованих і мікросервісних архітектурах управління вимогами кібербезпеки здійснюється в умовах високої динамічності та великої кількості взаємодіючих компонентів. Пріоритетними стають вимоги до безпеки API, автентифікації між сервісами, контролю конфігурацій і моніторингу взаємодій. Особливістю є необхідність локальної пріоритезації вимог для окремих сервісів із подальшим узгодженням на рівні всієї системи.

Розподілені та віддалені середовища

Для розподілених середовищ, що включають віддалених користувачів, філії або мобільні компоненти, управління вимогами кібербезпеки орієнтоване на захист каналів зв’язку, контроль ідентичності та забезпечення цілісності даних. Додатковим чинником є висока невизначеність загроз, що потребує адаптивних методів оцінювання ризиків і гнучкого перерозподілу ресурсів між вимогами.

Середовище обробки даних з обмеженим доступом

Характеризується підвищеними вимогами до конфіденційності, цілісності та доступності інформації, що зумовлено нормативними, договірними або внутрішніми організаційними обмеженнями. До таких середовищ належать системи, що обробляють комерційну таємницю, персональні дані, фінансову інформацію або інші чутливі дані бізнесу. Управління вимогами кібербезпеки в таких умовах потребує суворої формалізації правил доступу, детального аудиту дій користувачів та обмеження розповсюдження даних як на рівні інфраструктури, так і на рівні ПЗ.

Особливістю управління вимогами кібербезпеки в середовищах з обмеженим доступом є необхідність точного визначення пріоритетів між вимогами безпеки та бізнес-функціональністю. Пріоритетними стають вимоги до ідентифікації та автентифікації користувачів, управління привілеями, журналювання подій безпеки та забезпечення контролю цілісності даних. Водночас такі середовища часто мають жорсткі обмеження на зміну архітектури та використання зовнішніх сервісів, що підвищує значущість оптимізаційних методів управління вимогами кібербезпеки з урахуванням обмежених ресурсів.

Крім того, для середовищ обробки даних з обмеженим доступом характерною є необхідність постійного підтвердження відповідності вимогам стандартів і регуляторних актів, що зумовлює потребу в динамічному перегляді вимог кібербезпеки з урахуванням змін у загрозах, бізнес-процесах та нормативній базі. Таким чином, у цьому випадку ефективне управління вимогами кібербезпеки повинно базуватися на формалізованих моделях оцінювання ризиків і підтримки прийняття рішень, здатних забезпечити баланс між рівнем захисту, вартістю реалізації та допустимими обмеженнями функціонування ПЗ.

Приклад 2. *Управління вимогами кібербезпеки на основі середовища обробки даних з обмеженим доступом*

Як приклад розглянемо корпоративну інформаційну систему ТОВ «Омега», що обробляє персональні дані та комерційну таємницю, доступ до якої мають лише авторизовані співробітники. Формування вимог кібербезпеки в такому середовищі базується на положеннях NIST SP 800-53 [1], стандартів ISO/IEC 27001/27002 [2] та

регуляторних вимог European Union GDPR [6], що визначають обов'язкові контролі управління доступом, автентифікації, аудиту та захисту даних.

На основі зазначених нормативних документів формується структурований перелік вимог кібербезпеки, зокрема вимоги до рольового доступу, багатофакторної автентифікації, журналювання дій користувачів і забезпечення цілісності даних. Для оцінювання актуальних загроз і сценаріїв атак використовується база знань MITRE ATT&CK [5], що дозволяє пов'язати вимоги кібербезпеки з конкретними тактиками та техніками зловмисників. З урахуванням обмеженого бюджету та ресурсів виникає необхідність формалізованої пріоритезації вимог, оскільки не всі контролі можуть бути реалізовані одночасно.

Управління вимогами кібербезпеки в такому середовищі здійснюється шляхом оцінювання ризиків, регуляторної критичності та потенційних наслідків інцидентів із подальшим оптимальним розподілом ресурсів між вимогами. Пріоритет надається вимогам управління доступом, ідентифікації та аудиту, оскільки їх невиконання призводить до найбільших ризиків витоку або компрометації даних. Запропонований підхід дозволяє динамічно коригувати пріоритети вимог у разі появи нових загроз або змін нормативних вимог, забезпечуючи баланс між рівнем захисту, вартістю реалізації та функціональністю ПЗ.

Підсумовуючи п. 3.1 дисертації, варто відмітити, що крім описаних підходів (галузево- та середовище орієнтованого управління вимогами кібербезпеки) на сьогодні виділяють також ризик- (загрозо-) орієнтовані підходи, а також стандартизований і орієнтований на дані підходи [7-10].

3.2. Метод динамічного управління вимогами кібербезпеки

Традиційні підходи до управління вимогами кібербезпеки, як правило, ґрунтуються на статичному формуванні набору вимог, що призводить до зниження ефективності захисту та нераціонального використання ресурсів. Це обґрунтовує необхідність *розроблення методу динамічного управління вимогами кібербезпеки,* здатного адаптуватися до змін умов функціонування ПЗ.

Запропонований метод динамічного управління вимогами кібербезпеки реалізується в п’ять основних етапів, а саме: 1) ініціалізація вимог кібербезпеки відповідно до нормативних документів і стандартів; 2) визначення тригерів динамічного оновлення вимог кібербезпеки; 3) моніторинг змін у середовищі впровадження ПЗ та актуальних загроз; 4) кореляція та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків; 5) оптимізація розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень; 6) формування зворотного зв’язку та ініціація наступного циклу управління вимогами.

Розглянемо більш детально кожен з етапів цього методу, а для початку визначимо і формалізуємо базові множини параметрів *REQ, SFT, ACT, THR, SRC* у момент часу $t \subseteq \boldsymbol{T}$ за допомогою виразів (1) – (5):

$$REQ_{(t)} = \{\bigcup_{i=1}^{n} REQ_i\} = \{REQ_1, REQ_2, \dots, REQ_{n(t)}\}, \quad (1)$$

де $REQ_i \subseteq REQ(i = \overline{1,n})$ – множина вимог кібербезпеки, визначених певним нормативним документом в заданий момент часу $t \subseteq \boldsymbol{T}$.

$$SFT_{(t)} = \{\bigcup_{i=1}^{m} SFT_i\} = \{SFT_1, SFT_2, \dots, SFT_{m(t)}\}, \quad (2)$$

де $SFT_i \subseteq SFT(i = \overline{1,m})$ – множина модулів ПЗ (застосунків, сервісів, програм), яке впроваджується в заданий момент часу $t \subseteq \boldsymbol{T}$.

$$ACT_{(t)} = \{\bigcup_{i=1}^{k} ACT_i\} = \{ACT_1, ACT_2, \dots, ACT_{k(t)}\}, \quad (3)$$

де $ACT_i \subseteq ACT(i = \overline{1,k})$ – множина активів компанії (дані, функції, сервіси тощо), що впроваджує ПЗ в заданий момент часу $t \subseteq \boldsymbol{T}$.

$$THR_{(t)} = \{\bigcup_{i=1}^{q} THR_i\} = \{THR_1, THR_2, \dots, THR_{q(t)}\}, \quad (4)$$

де $THR_i \subseteq THR(i = \overline{1,q})$ – множина загроз кібербезпеки (кіберзагроз), які мають вплив на зміну вимог кібербезпеки в заданий момент часу $t \subseteq \boldsymbol{T}$.

$$SRC_{(t)} = \left\{\bigcup_{i=1}^{p} SRC_i\right\} = \left\{SRC_1, SRC_2, \dots, SRC_{p(t)}\right\}, \quad (5)$$

де $SRC_i \subseteq SRC(i = \overline{1,p})$ – множина джерел змін вимог кібербезпеки в заданий момент часу $t \subseteq \boldsymbol{T}$, що можуть бути пов'язані з інцидентами, проведенням аудиту, зміною архітектури чи законодавства тощо (при $p = 4$).

Перейдемо до базових етапів реалізації запропонованого метода, використовуючи для більш ґрунтовного розуміння підхід, використаний для формалізації моделі управління вимогами кібербезпеки при впровадженні ПЗ в [2]:

Етап 1. Ініціалізація вимог кібербезпеки відповідно до нормативних документів і стандартів

Відповідно до описаного в [2] підходу, при $n = 3$ вираз (1) у момент часу $t = 0$ матиме наступний вигляд (6):

$$REQ_{(0)} = \left\{\bigcup_{i=1}^{3} REQ_i\right\} = \{REQ_1, REQ_2, REQ_3\} = \{NIST, ISO, MITRE\}, \quad (6)$$

де $REQ_1 = NIST$ – це множина вимог кібербезпеки зі стандарту NIST 800-53, $REQ_2 = ISO$ – це множина вимог кібербезпеки зі стандарту ISO 22316 (в частині resilience-вимог, інтерпретованих для ПЗ / процесів), а $REQ_3 = MITRE$ – це множина вимог кібербезпеки з MITRE ATT&CK (threat-driven requirements).

Тоді початкова множина вимог в момент часу $t = 0$, з урахуванням описаного в [2] підходу матиме вигляд (7):

$$REQ_{(0)} = REQ_1 \cup REQ_2 \cup REQ_3 = NIST \cup ISO \cup MITRE, \quad (7)$$

Далі, введемо функцію нормалізації початкової множини вимог $REQ_{(0)}$, що задана виразом (8):

$$\varphi = REQ_1 \cup REQ_2 \cup REQ_3 \to U, \tag{8}$$

де U – це уніфікований простір опису вимог, що вводиться для синхронізації вимог кібербезпеки, які можуть бути представлені у різному вигляді в різних нормативних документах..

Тоді уніфіковане подання початкової множини вимог $REQ_{(0)}$ можна представити наступним чином (9):

$$\widetilde{REQ_{(0)}} = \{\varphi(REQ) | REQ \in REQ_{(0)}\}. \tag{9}$$

Далі, на наступному етапі, нам потрібно визначити тригери динамічного оновлення вимог кібербезпеки.

Етап 2. Визначення тригерів динамічного оновлення вимог кібербезпеки

Під «тригерами» у нашому випадку будемо розуміти певні типи подій (див. вираз (10)), які спричиняють оновлення / зміну вимог кібербезпеки при впровадженні ПЗ в бізнесі.

Нехай множина тригерів динамічного оновлення вимог кібербезпеки, що корелюється з множиною $SRC_{(t)}$ (5) джерел змін вимог (тобто $p = 4$), задана наступним виразом (10):

$$\begin{aligned} \Omega = \left\{\bigcup_{i=1}^{p} \Omega_i\right\} = \{\Omega_1, \Omega_2, \dots, \Omega_n\} = \left\{\bigcup_{i=1}^{4} \Omega_i\right\} = \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\} \\ = \{INCIDENT, AUDIT, ARCHITECTURE, LEGISLATION\}, \end{aligned} \tag{10}$$

де $\Omega_i \subseteq \Omega (i = \overline{1, p})$ – множина тригерів динамічного оновлення вимог кібербезпеки, а відповідно $\Omega_1 = INCIDENT$ – це множина інцидентів, які виникають і впливають на

зміну вимог кібербезпеки, $\Omega_2 = AUDIT$ – це множина аудитів, за результатами проведення яких необхідно змінювати вимоги кібербезпеки, $\Omega_3 = ARCHITECTURE$ – це множина змін архітектури системи, що має вплив на зміну вимог кібербезпеки, $\Omega_4 = LEGISLATION$ – це відповідні зміни законодавства, що впливають на зміну вимог кібербезпеки при впровадженні ПЗ в бізнесі.

Таким чином, певна подія в момент часу $t \subseteq \boldsymbol{T}$ є кортежем параметрів, визначених виразами (5) та (10), який можна представити у вигляді (11):

$$E_{(t)} = \langle \Omega, SRC, \Delta(t) \rangle, \tag{11}$$

де $\Delta(t)$ – це опис зміни вимог кібербезпеки.

Індикатор спрацювання тригера можна визначити таким чином:

$$\delta_{\Omega}(t) = \begin{cases} 1, \text{якщо } E_{(t)} \in \Omega \\ 0, \text{в іншому випадку} \end{cases}. \tag{12}$$

Динамічна зміна (оновлення) вимог кібербезпеки активується за умови (13):

$$\delta(t) = \bigvee_{\Omega_i \subseteq \Omega} \delta_{\Omega}(t) = 1. \tag{13}$$

Далі, на наступному етапі методу, формалізуємо процес моніторингу змін у середовищі впровадження ПЗ.

Етап 3. Моніторинг змін у середовищі впровадження ПЗ та актуальних загроз

Моніторинг здійснюється неперервно або з визначеною періодичністю та охоплює технічні, організаційні й безпекові (загрозові) аспекти функціонування системи. Стан середовища впровадження ПЗ у момент часу $t \subseteq \boldsymbol{T}$ можна представити у вигляді сукупності основних характеристик (14):

$$K_{(t)} = \langle SFT_{(t)}, ACT_{(t)}, THR_{(t)}, BUD_{(t)}, REG_{(t)} \rangle, \quad (14)$$

де параметри $SFT_{(t)}, ACT_{(t)}, THR_{(t)}$ визначаються відповідно до виразів (2), (3) та (4), а $BUD_{(t)}, REG_{(t)}$ – параметри, що означають бюджетні ресурси і регуляторні вимоги відповідно.

Таке представлення (14) дозволяє відобразити середовище не як окремі диференційовані компоненти (чинники), а як єдиний керований об'єкт.

Формалізацію ж змін середовища впровадження ПЗ у момент часу $t \subseteq \boldsymbol{T}$ можна представити у вигляді дельти стану:

$$\Delta K_{(t)} = K_{(t)} - K_{(t-1)}. \quad (15)$$

Враховуючи (14) – (15), зміни модулів ПЗ, активів, загроз, бюджетних ресурсів і регуляторних вимог представимо відповідно:

$$\begin{gathered} \Delta SFT_{(t)} = SFT_{(t)} - SFT_{(t-1)}; \\ \Delta ACT_{(t)} = ACT_{(t)} - ACT_{(t-1)}; \\ \Delta THR_{(t)} = THR_{(t)} - THR_{(t-1)}; \\ \Delta BUD_{(t)} = BUD_{(t)} - BUD_{(t-1)}; \\ \Delta REG_{(t)} = REG_{(t)} - REG_{(t-1)}. \end{gathered} \quad (16)$$

Для прикладу, при $\Delta SFT_{(t)} = \emptyset$ змінено модулі програмного забезпечення, при $\Delta ACT_{(t)} = \emptyset$ спостерігається зміна активів, $\Delta THR_{(t)} = \emptyset$ означає появу нових або модифікованих загроз, $\Delta BUD_{(t)} = \emptyset$ означає зміну доступних бюджетних ресурсів, а при $\Delta REG_{(t)} = \emptyset$ спостерігається зміна регуляторних вимог.

На наступному етапі, з урахуванням результатів перших трьох етапів методу, необхідно здійснити корелювання та оновлення оцінок (переоцінювання) вимог кібербезпеки з урахуванням змін.

Етап 4. Кореляція та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків

Метою цього етапу є встановлення та актуалізація взаємозв'язків між вимогами кібербезпеки, елементами ПЗ та актуальними загрозами з урахуванням виявлених змін у середовищі впровадження.

Для реалізації цього етапу використаємо теорію графів [11], Байєсові мережі [12] та теорію множин [13].

Крок 4.1. Визначимо орієнтований зважений граф:

$$G_{REQ_{(t)}} = (V_{REQ_{(t)}}, E_{REQ_{(t)}}, W_{REQ_{(t)}}), \tag{17}$$

де $V_{REQ_{(t)}} = REQ_{(t)}$ – вершини графа (вимоги), $E_{REQ_{(t)}} \subseteq V_{REQ_{(t)}} \times V_{REQ_{(t)}}$ – множина залежностей, $W_{REQ_{(t)}} = \left\{w_{ij_{(t)}}\right\}$ – ваги залежностей $w_{ij_{(t)}} \in [0; 1]$.

Якщо існує ребро $(REQ_i \rightarrow REQ_j)$, то виконання вимоги REQ_i впливає на виконання вимоги REQ_j.

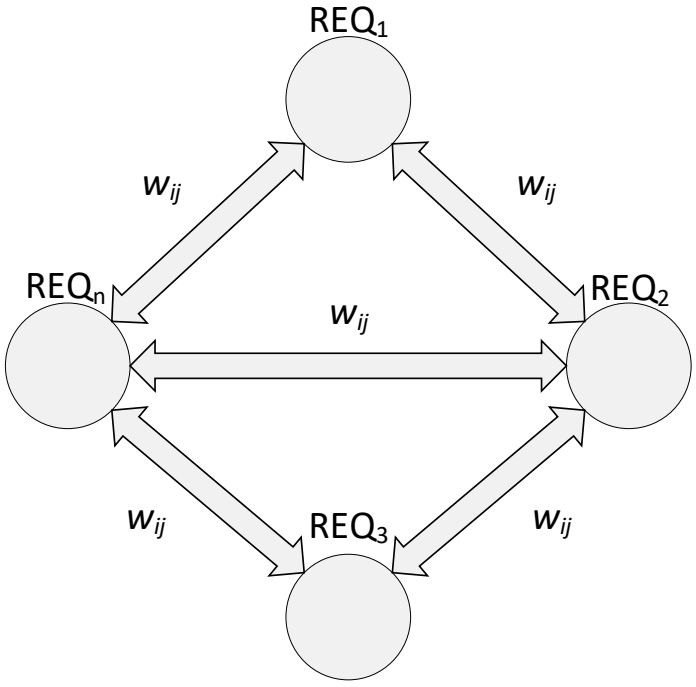


Рис. 1. Схематичне відображення графу $G_{REQ_{(t)}}$ (17)

Далі представимо граф $G_{REQ_{(t)}}$ у матричній формі, сформувавши матрицю суміжності зазначеного графа (17):

$$A_{(t)} = \left[a_{ij_{(t)}}\right], a_{ij_{(t)}} = \begin{cases} w_{ij_{(t)}}, (REQ_i, REQ_j) \in E_{REQ_{(t)}} \\ 0, \text{інакше.} \end{cases} \quad (18)$$

Крок 4.2. Корелювання з актуальними загрозами

Враховуючи (4), задано множину кіберзагроз $THR_{(t)}$, які мають вплив на зміну вимог кібербезпеки під час впровадження ПЗ. Введемо матрицю покриття $G_{RT_{(t)}} = \left[g_{ij_{(t)}}\right]$ $(i = \overline{1,n}), (j = \overline{1,q})$, яка фактично відображатиме зниження ризику від кіберзагроз за рахунок виконання відповідних вимог:

$$G_{RT_{(t)}} = \begin{vmatrix} g_{11_{(t)}} & g_{12_{(t)}} & \cdots & g_{1q_{(t)}} \\ g_{21_{(t)}} & g_{22_{(t)}} & \cdots & g_{2q_{(t)}} \\ \cdots & \cdots & \cdots & \cdots \\ g_{n1_{(t)}} & g_{n2_{(t)}} & \cdots & g_{nq_{(t)}} \end{vmatrix}, \quad (19)$$

де кожен елемент $g_{ij_{(t)}} = [0; 1]$ характеризує ступінь, з яким вимога REQ_i знижує ризик від кіберзагрози THR_i.

Таким чином, ймовірність реалізації кіберзагрози $THR_{(t)}$ за результатами моніторингу (14) – (16) у момент часу $t \subseteq \boldsymbol{T}$ можна представити наступним чином:

$$p_{k_{(t)}} = P\left(THR_{(t)} \middle| O_{(t)}\right), \quad (20)$$

де $O_{(t)}$ – це множина спостережуваних подій та параметрів середовища впровадження ПЗ, отриманих на етапі моніторингу (інциденти, результати аудиту, зміни архітектури, законодавчі зміни).

Враховуючи (10) у момент часу $t \subseteq \boldsymbol{T}$ ця множина може бути представлена таким чином: $O_{(t)} = \{INCIDENT_{(t)}, AUDIT_{(t)}, ARCHITECTURE_{(t)}, LEGISLATION_{(t)}\}$.

Крок 4.3. Оцінювання залишкового ризику

Позначимо ступінь реалізації (виконання) вимоги REQ_i у момент часу $t \subseteq \boldsymbol{T}$ як $x_{i_{(t)}} \in [0;1]$ (тобто при значенні «0» вимога не виконана, а при значенні «1» відповідно виконана) тоді залишковий ризик можна визначити за виразом (21) таким чином:

$$\rho_{i_{(t)}} = \left(\sum_{j=1}^{q} g_{ij_{(t)}} p_{k_{(t)}}\right) \cdot \left(1 - x_{i_{(t)}}\right). \tag{21}$$

Крок 4.4. Врахування важливості вимоги

На основі визначеного графа (17) та матриці (18) можна визначити зважений ступінь $d_{i_{(t)}} = \sum_{j=1}^{n} a_{ij_{(t)}}$ (сумарний вплив вимоги REQ_i на інші вимоги) та відповідно нормалізований вплив:

$$\hat{d}_{i_{(t)}} = \frac{d_{i_{(t)}}}{max_j d_{j_{(t)}}} \in [0;1], (i = \overline{1,n}), (j = \overline{1,q}). \tag{22}$$

Тобто, чим більше інших вимог залежать від вимоги REQ_i і чим більша вага цих залежностей, тим більшим є параметр $d_{i_{(t)}}$. Крім того, $max_j d_{j_{(t)}}$ – максимальний зважений ступінь серед усіх вимог, до того ж при $\hat{d}_{i_{(t)}} = 1$ вимога REQ_i є найбільш структурно значущою (важливою), а при $\hat{d}_{i_{(t)}} \approx 0$ вимога REQ_i майже не впливає на інші, тобто не є структурно значущою.

Цей показник враховує системну взаємозалежність вимог, каскадний ефект їх реалізації, архітектурну критичність. Тобто не оцінюється вимога ізольовано, а враховується її роль у структурі всієї системи.

Крок 4.5. Оновлення пріоритету вимоги

Пріоритет вимоги REQ_i у заданий момент часу $t \subseteq \boldsymbol{T}$ з урахуванням (21) – (22) можна представити таким чином:

$$\pi_{i_{(t)}} = \alpha\rho_{i_{(t)}} + \beta u_{i_{(t)}} + \gamma\hat{d}_{i_{(t)}}, \tag{23}$$

де $u_{i_{(t)}}$– це регуляторна важливість вимоги REQ_i, α, β, γ – це нормовані вагові коефіцієнти, що відображають відносну значущість структурного (залишкового) ризику, регуляторної важливості (критичності) та нормалізований вплив (каскадний ефект) відповідно. До того ж, обмеження $\alpha + \beta + \gamma = 1$ забезпечує інтерпретованість моделі та стабільність масштабування інтегрального показника пріоритету.

У результаті вектор пріоритетів виглядатиме наступним чином:

$$\Pi_{(t)} = \left\{\pi_{1_{(t)}}, \pi_{2_{(t)}}, \dots, \pi_{n_{(t)}}\right\}. \tag{24}$$

На наступному етапі, з урахуванням результатів попередніх чотирьох етапів методу, буде оптимізовано розподіл ресурсів між вимогами REQ_i з урахуванням оновлених пріоритетів $\pi_{i_{(t)}}$ та відповідних обмежень.

Етап 5. Оптимізація розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень

Цільова функція матиме вигляд (25), тобто фактично максимізується сумарна інтегральна корисність реалізованих вимог REQ_i:

$$max \sum_{i=1}^{n} \pi_{i_{(t)}} x_{i_{(t)}}, \tag{25}$$

де $\pi_{i_{(t)}}$ визначено в (23), а $x_{i_{(t)}} \in [0; 1]$ – це бінарний параметр, що відображає прийняття рішення щодо забезпечення вимоги REQ_i (див. крок 4.3).

При цьому обмеження ресурсів:

$$\sum_{i=1}^{n} c_{i_{(t)}} x_{i_{(t)}} \leq BUD_{(t)}, \tag{26}$$

де $c_{i_{(t)}} > 0$ – це ресурсна вартість забезпечення однієї вимоги REQ_i, а змінна $BUD_{(t)}$ визначена на 3 етапі методу і відображає сукупні бюджетні ресурси.

Якщо *i*-та вимога є залежною, тобто виконується тільки після виконання *j*-тої вимоги, то $x_{i_{(t)}} \leq x_{j_{(t)}}$ і відповідно для множини попередників, враховуючи (17):

$$PRE_{i_{(t)}} = \left\{ j \in V_{REQ_{(t)}} : (i,j) \in E_{REQ_{(t)}} \right\}. \quad (27)$$

Таким чином, отримуємо оптимальний вектор (28), який визначає множину вимог для реалізації у момент часу $t \subseteq \boldsymbol{T}$, отриманий з урахуванням пріоритетів, ресурсних обмежень та залежностей графа:

$$X^*_{(t)} = \left\{ x^*_{1_{(t)}}, x^*_{2_{(t)}}, \dots, x^*_{n_{(t)}} \right\}, \quad (28)$$

де $x^*_{i_{(t)}} \in [0;1]$ – це оптимальне значення параметру $x_{i_{(t)}}$, що отримане в результаті оптимізаційної задачі.

Останній етап цього методу описує формування зворотнього звязку та ініціацію наступного циклу управління вимогами кібербезпеки при впровадження ПЗ.

Етап 6. Формування зворотного зв'язку та ініціація наступного циклу управління вимогами

Для кожної вимоги REQ_i визначається її поточний стан виконання:

$$s_{i_{(t+1)}} = g(s_{i_{(t)}} + x^*_{i_{(t)}}), \quad (29)$$

$s_{i_{(t)}}$ – ступінь реалізації вимоги REQ_i.

Далі, на основі оновленого стану уточняється показник нормалізованого впливу $\hat{d}_{i_{(t+1)}} = h(s_{i_{(t+1)}})$ і за потреби актуалізуються структурні ($\rho_{i_{(t)}}$) та регуляторні ($u_{i_{(t)}}$) оцінки.

Таким чином, враховуючи вирази (23) та (24), новий вектор пріоритетів матиме вигляд:

$$\pi_{i_{(t+1)}} = \alpha\rho_{i_{(t+1)}} + \beta u_{i_{(t+1)}} + \gamma\hat{d}_{i_{(t+1)}}. \quad (30)$$

$$\Pi_{(t+1)} = \left\{\pi_{1_{(t+1)}}, \pi_{2_{(t+1)}}, \dots, \pi_{n_{(t+1)}}\right\}. \quad (31)$$

Наступний цикл управління ініціюється, якщо виконується хоча б одна з наступних умов:

1) зміна пріоритетів перевищує поріг ε;

2) з’явилися нові вимоги REQ_i або змінилися обмеження ресурсів $BUD_{(t)}$;

3) завершено поточний період планування.

Таким чином, метод набуває ітераційного характеру – результати оптимізації впливають на стан системи, що, у свою чергу, формує оновлені пріоритети та ініціює новий цикл управління вимогами. Це забезпечує адаптивність до змін середовища та ресурсних обмежень.

Структурна схема методу динамічного управління вимогами кібербезпеки відображена на рис. 2, а псевдокод його реалізації міститься на рис. 3 (повна версія псевдокоду міститься в Додатку А дисертаційної роботи).

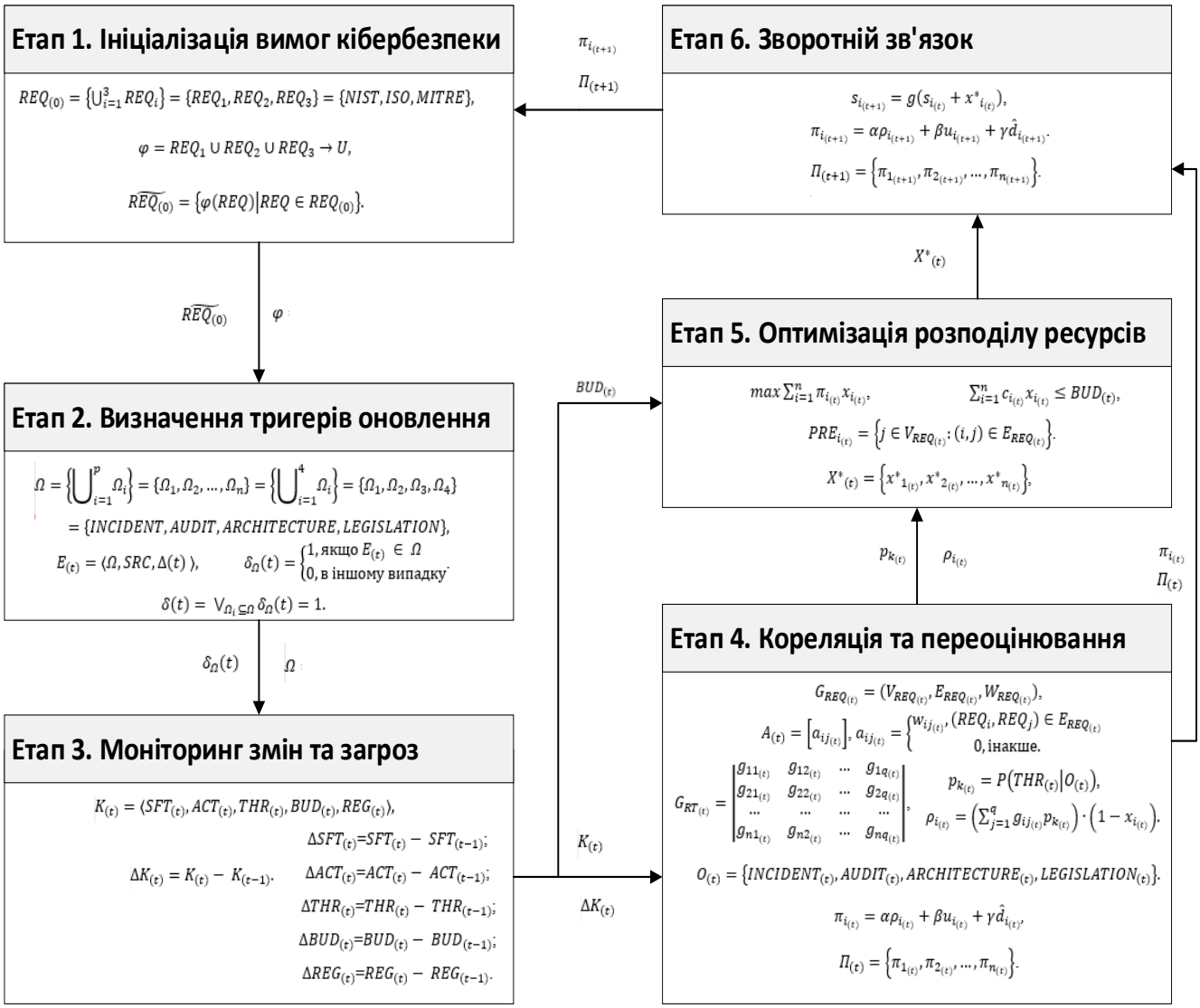


Рис. 2. Схема методу динамічного управління вимогами кібербезпеки

```
Initialize t ← 0
Compute structural importance ρ_i from graph G
Compute deviation ∂_i from state s_i
Compute priorities π_i(t) = α ρ_i + β u_i + γ ∂_i

repeat
    // Resource allocation
    Solve:
        maximize Σ π_i(t) x_i
        subject to:
            Σ c_i x_i ≤ B
            x_i ≤ x_j  for all dependencies j → i
            x_i ∈ {0,1}

    Obtain optimal plan X*(t)

    // Feedback update
    Update state s_i(t+1) based on X*(t)
    Recompute deviation ∂_i(t+1)
    Recompute priorities π_i(t+1)

    t ← t + 1
until  ||Π(t) - Π(t-1)|| ≤ ε
```

Рис. 3. Псевдокод практичної реалізації методу

3.3. Висновки до третього розділу дисертації

1) Проаналізовано основні підходи до управління вимогами кібербезпеки при впровадженні ПЗ. Зокрема, розглянуто галузево орієнтоване управління вимогами кібербезпеки, яке передбачає адаптацію методів пріоритезації, оцінювання ризиків і розподілу ресурсів відповідно до контексту застосування ПЗ. Крім того, різні типи середовищ потребують різних стратегій пріоритезації вимог, рівнів автоматизації та методів оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних і формалізованих моделей управління вимогами кібербезпеки, здатних динамічно враховувати зміну умов функціонування ПЗ. Отже, середовище орієнтоване управління вимогами кібербезпеки є актуальним підходом.

2) Розроблено метод динамічного управління вимогами кібербезпеки [17, 18], який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог

кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень, формування зворотного зв'язку та ініціації наступного циклу управління вимогами, дає змогу забезпечити інтегровану оцінку їх структурної, регуляторної та динамічної значущості з подальшою формалізацією управлінського рішення через оптимізаційну модель розподілу ресурсів та ітераційний механізм зворотного зв'язку, що дозволяє інтегрувати топологічні та станові характеристики системи, максимізувати ефект від використання бюджету, регулярно оновлювати пріоритети, врахувати нові вимоги кібребезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов.

3) Практична цінність методу полягає у створенні формалізованого адаптивного механізму управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості інформаційно-комунікаційних систем. Запропонований метод формалізований у вигляді псевдокоду та може бути реалізований у:

- системах підтримки прийняття рішень [14];
- програмних засобах управління кіберризиками [15];
- корпоративних GRC-платформах [16];
- автоматизованих системах планування тощо [17].

3.4. Список використаних джерел у третьому розділі

1. *National Institute of Standards and Technology Special Publication 800-53*, Rev. 5, 492 pages (September 2020), https://doi.org/10.6028/NIST.SP.800-53r5
2. *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements,* Ed. 3, 2022, 19 pages.
3. IT Governance Publishing; Stephen Hancock, *PCI DSS Version 4.0.1: A guide to the payment card industry data security standard,* Packt Publishing, 2025.

4. W. Wodo, D. Stygar, PSD2 Compliant Hardware Token for Digital Banking, *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),* Riga, Latvia, 2021, pp. 1-6.

5. W. -T. Tsai, J. -N. Luo and C. -L. Chou, Integrating Tree Structures with the MITRE ATT&CK Framework for APT Detection, *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, Okinawa, Japan, 2025, pp. 139-143, doi: 10.1109/CSP66295.2025.00031.

6. IT Governance Publishing; IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An implementation and compliance guide,* Packt Publishing, 2025.

7. Davis A., Overmyer S., Jordan K., Caruso J., Ashi F., Dinh A., Kincaid G., Ledeboer G., Reynolds P., Sitaram P. and others. Identifying and measuring quality in a software requirements specification. In: *Proceedings First International Software Metrics Symposium, IEEE,* 2019, pp. 141-152.

8. Гнатюк С., Сидоренко В., Скуратівський А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення, *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 2025, 4(28), с. 715-726. https://doi.org/10.28925/2663-4023.2025.28.841

9. Петренко М.А. Управління безпекою діяльності e-commerce підприємств, *кваліфікаційна робота другого (магістерського) рівня*, Харків, 2022, 91 с.

10. Alexander I. F., Stevens R. Writing better requirements. Pearson Education. Breach Level Index, 2019, 427 p.

11. H. A. Dawood, Graph Theory and Cyber Security, *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, Amman, Jordan, 2014, pp. 90-96, doi: 10.1109/ACSAT.2014.23.

12. Q. Yu and Z. Li, A Bayesian Model Averaging Method for Software Reliability Assessment, *2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM)*, Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/APARM49247.2020.9209504.

13. T. J. Mathew and E. Sherly, A Review on Soft Set-Based Theories Relevant to Decision Making in Computer Science, *2019 Third International Conference on Inventive*

Systems and Control (ICISC), Coimbatore, India, 2019, pp. 395-399, doi: 10.1109/ICISC44355.2019.9036419.

14. R. Kuceba and L. Kieltyka, Criteria classification Intelligent Decision Support Systems, *2009 ICCAS-SICE*, Fukuoka, Japan, 2009, pp. 5351-5355.

15. P. J. G. Guerra and D. A. Sepulveda Estay, An Impact-wave Analogy for Managing Cyber Risks in Supply Chains, *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Bangkok, Thailand, 2018, pp. 61-65, doi: 10.1109/IEEM.2018.8607563.

16. S. Stapleton, *Top 18 GRC (Governance, Risk & Compliance) Tools in 2025,* Published 24.10.2025, https://pathlock.com/blog/grc/list-of-top-grc-tools-and-softwares

17. Скуратівський А. Метод управління вимогами кібербезпеки при впровадженні програмного забезпечення у бізнесі, Безпека інформації, 2025, Том. 31, № 3, с. 135-142.

18. Gnatyuk S., Sydorenko V., Polozhentsev A., Skurativskyi A., Kluczewska-Chmielarz K., Shuitenov G. Modern approaches to cybersecurity requirements management for software implementation, CEUR Workshop Proceedings, 2025, Vol. 4024, pp. 186-200.

РОЗДІЛ 4. МЕТОД ІНТЕГРУВАННЯ ВИМОГ КІБЕРБЕЗПЕКИ В ЖИТТЄВИЙ ЦИКЛ РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1. Особливості інтегрування вимог кібербезпеки в життєвий цикл розроблення ПЗ

Життєвий цикл розроблення ПЗ (Software Development Life Cycle, SDLC) – це структурований процес створення, впровадження та супроводу ПЗ від моменту формування ідеї до завершення експлуатації [1]. Головною метою SDLC є забезпечення передбачуваності результатів, контролю якості, управління ризиками та оптимального використання ресурсів.

Класично SDLC включає такі фази (рис. 4.1) [2]:

1) збирання вимог та їх аналізування;
2) проєктування дизайну системи;
3) реалізація;
4) тестування;
5) впровадження (розгортання);
6) експлуатація та супровід.

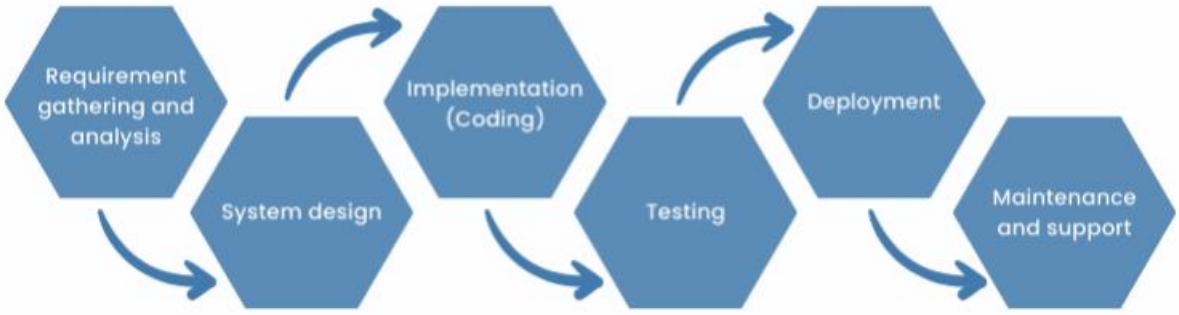


Рис. 4.1. Ключові фази SDLC [2]

У сучасних умовах до цих етапів дедалі частіше інтегруються практики DevOps [3], безперервної інтеграції та безперервної доставки (CI/CD), а також сучасної концепції DevSecOps [4], що передбачає вбудовування механізмів кібербезпеки на всіх фазах життєвого циклу.

У загальному вигляді життєвий цикл розроблення ПЗ можна відобразити за допомогою множини:

$$SDLC = \left\{ \bigcup_{i=1}^{n} SDLC_i \right\} = \{SDLC_1, SDLC_2, \dots, SDLC_n\}, \quad (4.1)$$

де $SDLC_i \subseteq SDLC (i = \overline{1,n})$ – фази життєвого циклу відповідно до певної моделі.

Для прикладу при *n*=6 (кейс відображено на рис. 4.1) уніфікована модель (4.1) матиме наступний вигляд:

$$\begin{aligned} SDLC_{classic} &= \left\{ \bigcup_{i=1}^{6} SDLC_i \right\} = \{SDLC_1, SDLC_2, \dots, SDLC_6\} \\ &= \{RGA, SYS, IMP, TES, DPL, MTN\}, \end{aligned} \quad (4.2)$$

де $SDLC_1 = RGA, SDLC_2 = SYS, SDLC_3 = IMP, SDLC_4 = TES, SDLC_5 = DPL, SDLC_6 = MTN$ – це відповідно фаза збирання вимог та їх аналізування; фаза проєктування дизайну системи; фаза реалізація; фаза тестування; фаза впровадження (розгортання); фаза експлуатації та супроводу.

Ключовою характеристикою SDLC є наявність формалізованих артефактів на кожному етапі: специфікацій вимог, моделей архітектури, технічної документації, тест-кейсів, звітів верифікації тощо. Від правильності формування вимог значною мірою залежить якість кінцевого продукту, оскільки помилки на ранніх етапах мають кумулятивний ефект і суттєво збільшують вартість їх виправлення на пізніх фазах. Саме тому сучасні підходи роблять акцент на ітеративності, прототипуванні та ранній валідації гіпотез. У випадку систем критичної інфраструктури або оборонного призначення життєвий цикл доповнюється процедурами сертифікації, управління конфігурацією, трасованості вимог та формальної перевірки відповідності стандартам (наприклад, розглянуті в попередніх розділах роботи стандарти: ISO/IEC [5], NIST [6], PCI DSS [7], PSD2 [8], GDPR [9], MITRE ATT&CK [10]).

Існує кілька базових моделей SDLC, які відрізняються ступенем формалізації, гнучкості та способами управління змінами. Розглянемо основні з них:

1) Класична каскадна (водоспадна) модель (Waterfall) (Рис. 4.2) [11] передбачає послідовне проходження етапів, де кожна наступна фаза починається лише після завершення попередньої. Вона добре підходить для проєктів зі стабільними вимогами та високими вимогами до документації, однак є не гнучкою (малогнучкою) у разі змін та впливів.

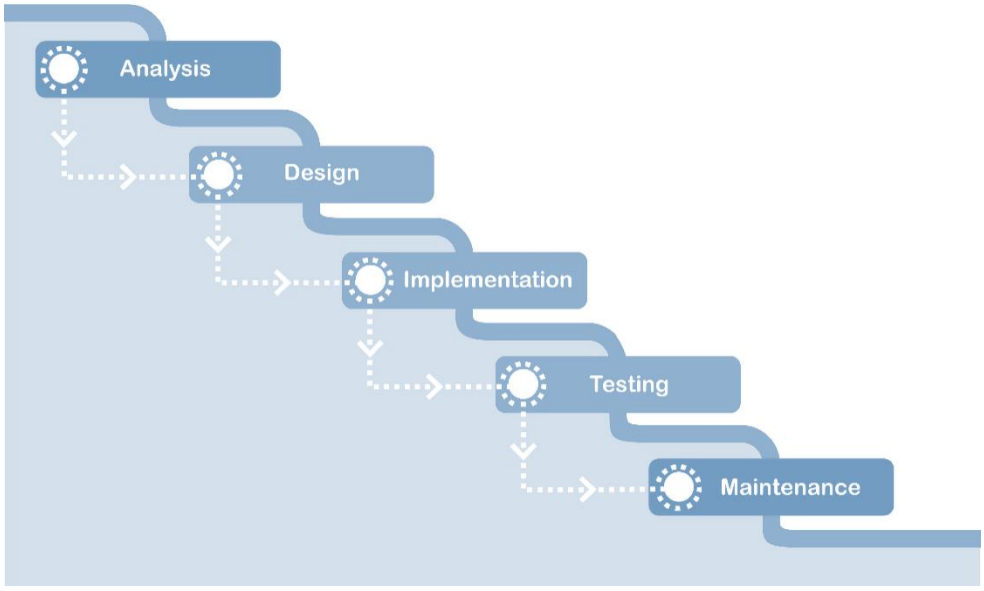


Рис. 4.2. Waterfall-модель [11]

Відповідно, для формалізації класичної каскадної моделі при *n*=6 (рис. 4.2) на основі (4.1) можна представити наступну множину:

$$SDLC_{waterfall} = \left\{ \bigcup_{i=1}^{5} SDLC_i \right\} = \{SDLC_1, SDLC_2, \dots, SDLC_6\} = \{RGA, SYS, IMP, TES, MTN\}, \quad (4.3)$$

де $SDLC_1 = RGA, SDLC_2 = SYS, SDLC_3 = IMP, SDLC_4 = TES, SDLC_5 = MTN$ – це відповідно фаза збирання вимог та їх аналізування; фаза проєктування дизайну системи; фаза реалізації; фаза тестування; фаза експлуатації та супроводу.

2) V-модель (рис. 4.3) [12] є розвитком каскадної, де кожному етапу розроблення відповідає відповідний рівень тестування, що забезпечує чітку кореляцію між верифікацією та валідацією.

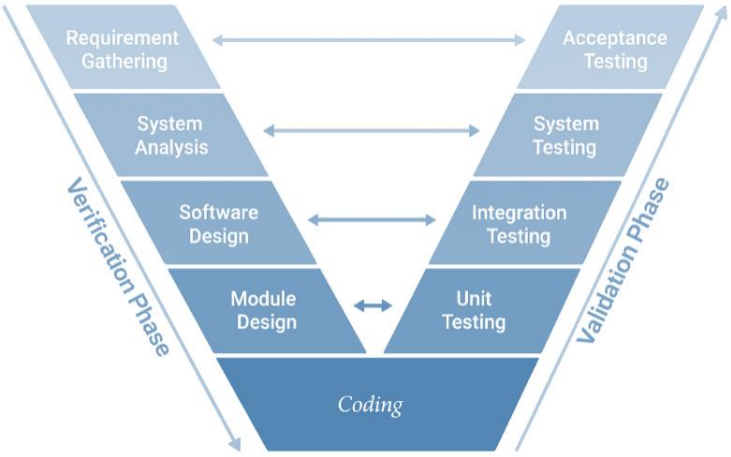


Рис. 4.3. V-модель [12]

Відповідно, для формалізації V-моделі при *n*=2 (рис. 4.3) на основі (4.1) можна представити наступну множину:

$$SDLC_V = \left\{ \bigcup_{i=1}^{2} SDLC_i \right\} = \{SDLC_1, SDLC_2\} = \{VER, VAL\}, \tag{4.3}$$

де $SDLC_1 = VER, SDLC_2 = VAL$ – це відповідно фази верифікації та валідації.

Далі, відповідно кожну з підмножин VER та VAL можна представити аналогічним чином.

Для VER при *n*=5 будемо мати:

$$\begin{aligned} VER = \left\{ \bigcup_{i=1}^{5} VER_i \right\} &= \{VER_1, VER_2, \dots, VER_5\} \\ &= \{RGA, SYS, SDS, MDS, IMP\}, \end{aligned} \tag{4.4}$$

де $VER_1 = RGA, VER_2 = SYS, VER_3 = SDS, VER_4 = MDS, VER_5 = IMP$ – це фаза збирання вимог та їх аналізування; фаза проєктування дизайну системи; фаза дизайну ПЗ; фаза дизайну модулів; фаза реалізація відповідно.

Для VER при *n*=5 будемо мати:

$$VAL = \left\{\bigcup_{i=1}^{5} VAL_i\right\} = \{VAL_1, VAL_2, \dots, VAL_5\} = \{IMP, UNT, INT, SYT, ACT\}, \quad (4.5)$$

де $VAL_1 = IMP, VAL_2 = UNT, VAL_3 = INT, VAL_4 = SYT, VAL_5 = ACT$ – це фаза реалізації, фаза тестування юнітів (компонентів), фаза інтегративного тестування, фаза системного тестування та фаза погодженого тестування відповідно.

З урахуванням (4.4) та (4.5) множину (4.3) і класичну каскадноу V-модель можна представити в узагальненому вигляді наступним чином:

$$SDLC_V = \{VER, VAL\} = \left\{\bigcup_{i=1}^{5} VER_i\right\} \cup \left\{\bigcup_{i=1}^{5} VAL_i\right\} = \{VER_1, VER_2, \dots, VER_5\} \cup \{VAL_1, VAL_2, \dots, VAL_5\} = \{RGA, SYS, SDS, MDS, IMP, UNT, INT, SYT, ACT\}, \quad (4.6)$$

3) Інкрементальна модель (рис. 4.4) [13] передбачає поетапне створення функціоналу з регулярним зворотним зв'язком. Відповідно до інкрементальної моделі ПЗ розробляється з лінійною послідовністю стадій, але в кілька інкрементів (версій). Таким чином, поліпшення продукту проходить заплановано весь час, поки життєвий цикл розробки ПЗ не завершиться.

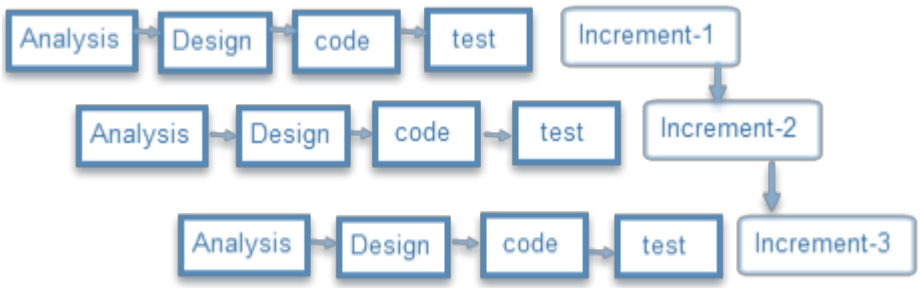


Рис. 4.4. Інкрементальна модель [13]

У випадку інкрементальної моделі вираз (4.1) матиме особливості – крім індексу $i = \overline{1,n}$ вводиться індекс $j = \overline{1,m}$ наступним чином:

$$SDLC_{increment} = \left\{ \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} SDLC_{ij} \right\} = \{SDLC_{11}, SDLC_{12}, \dots, SDLC_{nm}\}, (i = \overline{1,n}), (j = \overline{1,m}) \quad (4.7)$$

Тоді частковий випадок, відображений на рис. 4.4, з урахуванням (4.7) та n=4, m=3 можна представити таким чином:

$$SDLC_{increment} = \left\{ \bigcup_{i=1}^{4} \bigcup_{j=1}^{3} SDLC_{ij} \right\} = \{SDLC_{11}, SDLC_{12}, \dots, SDLC_{43}\} = \{RGA_1, SYS_1, IMP_1, TES_1\} \cup \{RGA_2, SYS_2, IMP_2, TES_2\} \cup \{RGA_3, SYS_3, IMP_3, TES_3\} \quad (4.8)$$

де відповідно за трьома інкрементами (версіями) RGA_1, RGA_2, RGA_3 – фази збирання вимог та їх аналізування, SYS_1, SYS_2, SYS_3 – фази проєктування дизайну системи, IMP_1, IMP_2, IMP_3 – фази реалізації, TES_1, TES_2, TES_3 – фази тестування.

4) Спіральна модель (Spiral Model) (рис. 4.5) [14] орієнтована на управління ризиками та передбачає циклічне проходження етапів із постійною оцінкою загроз і невизначеностей.

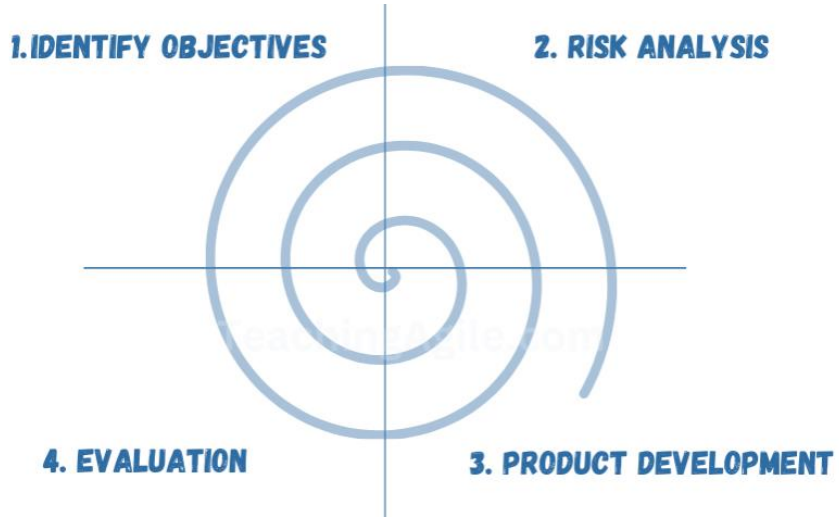


Рис. 4.5. Спіральна модель [14]

Відповідно, для формалізації спіральної моделі при *n*=4 (рис. 4.5) на основі (4.1) можна представити наступну множину:

$$SDLC_{spiral} = \left\{\bigcup_{i=1}^{4} SDLC_i\right\} = \{SDLC_1, SDLC_2, SDLC_3, SDLC_4 \dots\} \\ = \{IDN, RSK, PRD, EVL \dots\}, \tag{4.9}$$

де $SDLC_1 = IDN$ – фаза ідентифікації об'єктів, $SDLC_2 = RSK$ – фаза аналізування ризиків, $SDLC_3 = PRD$ – фаза розроблення продукту, $SDLC_4 = EVL$ – фаза оцінювання, які повторюються циклічно.

5) Гнучкі Agile-підходи (до таких підходів відносяться Scrum, Kanban, Extreme Programming) (рис. 4.6) [15] акцентують увагу на гнучкості, швидкій адаптації до змін вимог та активній взаємодії із замовником.

Для прикладу, Agile модель при *n*=5 (рис. 4.6) із врахуванням базового виразу (4.1), можна представити у вигляді такої множини:

$$SDLC_{agile} = \left\{\bigcup_{i=1}^{5} SDLC_i\right\} = \{SDLC_1, SDLC_2, SDLC_3, SDLC_4, SDLC_5\} \\ = \{SYS, DEV, TES, DPL, REV\}, \tag{4.10}$$

де $SDLC_1 = SYS$ – фаза проєктування дизайну системи, $SDLC_2 = DEV$ – фаза розроблення, $SDLC_3 = TES$ – фаза тестування, $SDLC_4 = DPL$ – фаза розгортання й експлуатації, $SDLC_5 = REV$ – фаза експертизи (зворотного зв'язку).

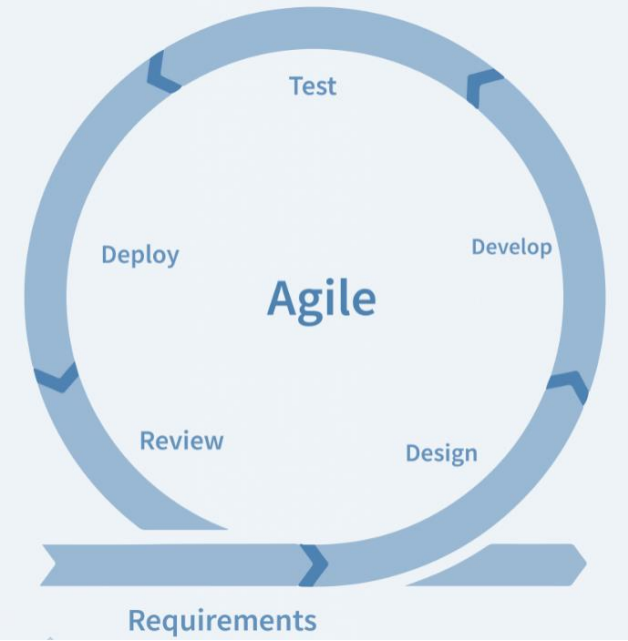


Рис. 4.6. Agile модель [15]

У рамках Agile розроблення здійснюється короткими ітераціями (sprints), а продукт формується інкрементально. Сучасним розвитком є DevOps-модель (рис. 4.7), яка інтегрує процеси розроблення та експлуатації, автоматизує тестування, розгортання та моніторинг, забезпечуючи безперервну доставку цінності користувачам.

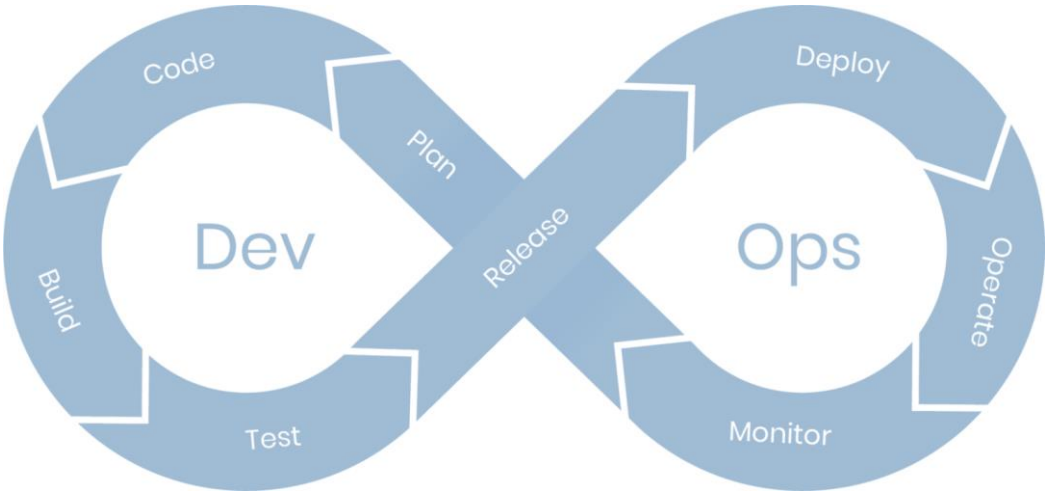


Рис. 4.7. DevOps модель [16]

Наприклад, при n=7 із врахуванням виразу (4.1), DevOps-модель можна представити таким чином:

$$SDLC_{DevOps} = \left\{\bigcup_{i=1}^{7} SDLC_i\right\} = \{SDLC_1, SDLC_2, \dots, SDLC_7\} = \{PLN, DEV, TES, INT, DPL, MTN, MON\}, \quad (4.11)$$

де $SDLC_1 = PLN$ – фаза планування, $SDLC_2 = DEV$ – фаза розроблення, $SDLC_3 = TES$ – фаза тестування, $SDLC_4 = INT$ – фаза інтегрування, $SDLC_5 = DPL$ – фаза розгортання, $SDLC_6 = MTN$ – фаза експлуатації, $SDLC_7 = MON$ – фаза моніторингу,

Враховуючи циклічність моделі (рис. 4.7), можна ввести множину відношень між фазами WFC і вираз (4.11) представити так:

$$DevOps = (SDLC_{DevOps}, WFC),$$
$$WFC = \begin{Bmatrix} (PLN, DEV), (DEV, TES), (TES, INT), (INT, DPL), \\ (DPL, MTN), (MTN, MON), (MON, PLN) \end{Bmatrix}. \quad (4.12)$$

Модель DevSecOps [4] є розвитком DevOps-моделі, що містить множину безпекових функцій, саме ця модель буде базовою для розроблення методу в наступному підрозділі дисертації.

Таким чином, вибір моделі SDLC залежить від характеру проєкту, рівня регуляторних вимог, масштабу системи, критичності застосування та динаміки змін у середовищі. Для високоризикових або регламентованих систем доцільні формалізовані моделі з жорсткою трасованістю вимог, тоді як інноваційні IT-продукти в умовах швидкої ринкової еволюції ефективніше реалізовувати через гнучкі або гібридні підходи. У будь-якому випадку сучасна практика свідчить про необхідність поєднання структурованості з адаптивністю та обов’язкової інтеграції механізмів забезпечення якості й кібербезпеки протягом усього SDLC.

4.2. Опис, формалізація та дослідження методу інтегрування вимог кібербезпеки в SDLC

Запропонований метод інтегрування вимог кібербезпеки в SDLC реалізується в 5 етапів, зокрема, етап формалізації DevSecOps, етап ідентифікації вимог кібербезпеки, етап трансформації вимог у контрольні механізми, етап інтегрування контрольних механізмів у SDLC, етап верифікування та моніторинг виконання вимог кібербезпеки**.**

Далі більш детально розглянемо кожен із етапів з наведенням прикладів практичної реалізації.

Етап 1. Формалізація моделі DevSecOps

Введемо множину безпекових функцій $SECF$:

$$SECF = \{SREQ, STES, SVER, SCMP, SIMN\}, \tag{4.13}$$

де $SREQ$ – множина безпекових вимог, $STES$ – множина етапів безпекового тестування, $SVER$ – множина заходів безпекового верифікування, $SCMP$ – множина заходів безпекового комплаєнсу, $SIMN$ – множина заходів моніторингу інцидентів безпеки.

Враховуючи (4.11) – (4.13) модель DevSecOps матиме такий вигляд:

$$\begin{gathered} DevSecOps = (SDLC_{DevSecOps} \cup SECF, WFC^{ext}), \\ WFC^{ext} = WFC \cup WFC_{SECF}, \\ WFC^{ext} = \begin{Bmatrix} (SREQ, DEV), (SREQ, TES), (STES, INT), (SVER, DPL), \\ (SCMP, MTN), (SIMN, MON) \end{Bmatrix}. \end{gathered} \tag{4.14}$$

На наступному етапі необхідно ідентифікувати вимоги кібербезпеки, що будуть інтегруватися в SDLC.

Етап 2. Ідентифікація вимог кібербезпеки

Введемо множину вимог відповідно до [17] згідно принципу, описаного в третьому розділі дисертації, і відповідно до (4.14):

$$SREQ = \left\{ \bigcup_{i=1}^{n} SREQ_i \right\} = \{SREQ_1, SREQ_2, \dots, SREQ_n\}, \quad (4.15)$$

де $SREQ_i \subseteq SREQ (i = \overline{1,n})$ – вимоги кібербезпеки, визначені певним нормативним документом.

Наприклад, в разі використання міжнародного стандарту NIST 800-53 [6] при n=5 (з огляду на кількість базових безпекових контролів, не враховуючи додаткові), вираз (4.15) матиме вигляд:

$$NIST = \left\{ \bigcup_{i=1}^{5} NIST_i \right\} = \{NIST_1, NIST_2, \dots, NIST_5\} = \{AC, SC, CM, AU, IR\}, \quad (4.16)$$

де $NIST_1 = AC$ – це підмножина вимог контролю доступу, $NIST_2 = SC$ – це підмножина вимог безпеки зв'язку, $NIST_3 = CM$ – це підмножина вимог конфігурування системи, $NIST_4 = AU$ – це підмножина вимог аудиту та підзвітності, а $NIST_5 = IR$ – це підмножина вимог реагування на інциденти.

Для більш детального представлення вимог, враховуючи елементи (контролі) в структурі базових підмножин стандарту NIST 800-53 [6], вираз (4.16) можна представити наступним чином:

$$NIST = \left\{ \bigcup_{i=1}^{5} NIST_i \right\} = \{NIST_1, NIST_2, \dots, NIST_5\} = \{AC, SC, CM, AU, IR\}$$
$$= \{AC_1, AC_2, AC_3\} \cup \{SC_1, SC_2\} \cup \{CM_1, CM_2\} \cup \{AU_1, AU_2\}$$
$$\cup \{IR_1, IR_2, IR_3\} =$$
$$= \{AUTHORIZATION, AUTHENTICATION, ACCOUNTING\}$$
$$\cup \{ENCRYPTION, CHANNEL\_SECURITY\} \quad (4.17)$$
$$\cup \{CHANGES\_MANAGMENT, BASE\_CONFIG\}$$
$$\cup \{LOGGING, MONITORING\}$$
$$\cup \{DETECTION, RESPONSE, RECOVERY\}$$

де $AC_1 = AUTHORIZATION$ – авторизація користувачів, $AC_2 = AUTHENTICATION$ – автентифікація користувачів, $AC_3 = ACCOUNTING$ – облікові записи, $SC_1 = ENCRYPTION$ – шифрування, $SC_2 = CHANNEL\_SECURITY$ – захист каналів передавання даних, $CM_1 = CHANGES\_MANAGMENT$ – управління змінами, $CM_2 = BASE\_CONFIG$ – базові конфігурування, $AU_1 = LOGGING$ – журналювання (логування), $AU_2 = MONITORING$ – моніторинг дій, $IR_1 = DETECTION$ – виявлення загроз, $IR_2 = RESPONSE$ – реагування, $IR_3 = RECOVERY$ – відновлення системи.

На наступному етапі необхідно трансформувати ідентифіковані вимоги кібербезпеки у контрольні механізми.

Етап 3. Трансформація вимог у контрольні механізми

Вимоги кібербезпеки визначені множиною (4.15), визначимо множину контрольних механізмів:

$$SMEC = \left\{ \bigcup_{j=1}^{m} SMEC_j \right\} = \{SMEC_1, SMEC_2, \dots, SMEC_m\}, \quad (4.18)$$

де $SMEC_j \subseteq SMEC (j = \overline{1, m})$ – контрольні механізми.

Тоді функцію трансформації вимог (4.15) у контрольні механізми (4.18) можна представити таким чином:

$$f_{transformation}: SREQ \rightarrow SMEC,$$
$$\forall\, SREQ_i \in SREQ\ \exists\, SMEC_j \in SMEC:\ SREQ_i \rightarrow SMEC_j \tag{4.19}$$

Тобто абсолютно кожна вимога $SREQ_i$ трансформується в контрольні механізми $SMEC_j$.

Наприклад, вимога $AC_1 = AUTHORIZATION$ трансформується в механізми забезпечення авторизації $AUTHORIZATION\_MECHANISM$, вимога $SC_2 = CHANNEL\_SECURITY$ трансформується в засоби забезпечення захисту каналів передавання даних $CHANNEL\_SECURITY\_MECHANISM$, вимога $IR_2 = INCIDENT\_RESPONSE$ трансформується в інструменти реагування на кіберзагрози $INCIDENT\_RESPONSE\_MECHANISM$ і т.д.

Етап 4. Інтегрування контрольних механізмів у SDLC

Виразом (4.14) визначено множину етапів SDLC для моделі DevSecOps, відповідно DevSecOps-модель можна представити аналогічно (4.11):

$$SDLC_{DevSecOps} = \{DEV, TES, INT, DPL, MTN, MON\}, \tag{4.20}$$

Визначимо множину процесів DevSecOps:

$$PIPELINE_{DevSecOps} = \left\{\bigcup_{i=1}^{k} PIPELINE_i\right\} \tag{4.21}$$
$$= \{PIPELINE_1, PIPELINE_2, \dots, PIPELINE_k\},$$

де $PIPELINE_i \subseteq PIPELINE\left(i = \overline{1,k}\right)$ – процеси DevSecOps моделі.

Функцію інтегрування контрольних механізмів у SDLC на основі (4.18) – (4.21) можна представити наступним чином:

$$f_{integration}: SMEC \rightarrow SDLC \times PIPELINE,$$
$$\forall SMEC_j \in SMEC \; \exists \; (SDLC_i, PIPELINE_i): SMEC_j \rightarrow (SDLC_i, PIPELINE_i) \tag{4.22}$$

Таким чином, контрольний механізм $SMEC_j$ інтегрується в певний процес $PIPELINE_i$ конкретного етапу (фази) життєвого циклу розроблення ПЗ $SDLC_i$.

Для прикладу, контрольний механізм забезпечення авторизації $AUTHORIZATION\_MECHANISM$ інтегрується в процес персоналізації системи $PERSONNEL$ фази розроблення DEV, засоби забезпечення захисту каналів передавання даних $CHANNEL\_SECURITY\_MECHANISM$ інтегруються в процес захисту системи $SYSTEM\_PROTECTION$ тієї ж фази розроблення DEV, а інструменти реагування на кіберзагрози $INCIDENT\_RESPONSE\_MECHANISM$ інтегруються в процес управління інцидентами безпеки $INCIDENT\_MANAGEMENT$ фази моніторингу MON.

На наступному етапі відбувається верифікування та моніторинг виконання інтегрованих вимог кібербезпеки в SDLC.

Етап 5. Верифікування та моніторингу виконання вимог кібербезпеки

Множину метрик кібербезпеки можна визначити наступним чином:

$$CSM = \left\{ \bigcup_{i=1}^{n} CSM_i \right\} = \{CSM_1, CSM_2, \dots, CSM_n\}, \tag{4.23}$$

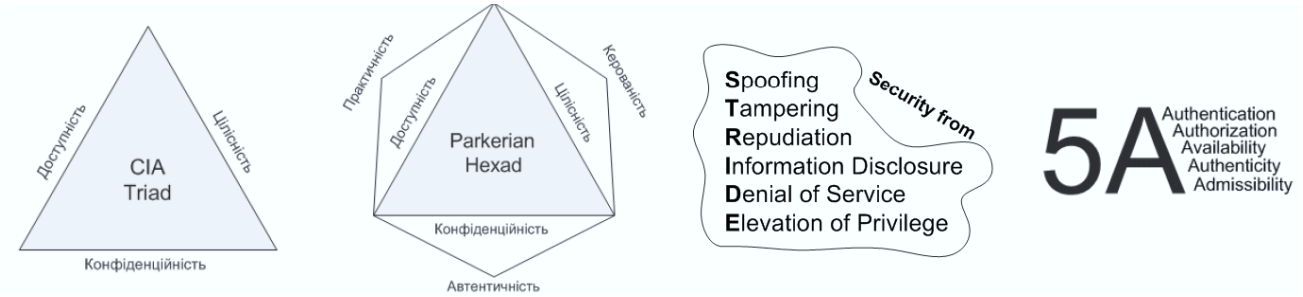
де $CSM_i \subseteq CSM (i = \overline{1,n})$ – метрики безпеки (кібербезпеки).

Наприклад, у відомій моделі кібербезпеки CIA [18] при n=3 вираз (4.23) матиме такий вигляд:

$$CSM_{CIA} = \left\{\bigcup_{i=1}^{3} CSM_i\right\} = \{CSM_1, CSM_2, CSM_3\} \quad (4.24)$$
$$= \{CONFIDENTIALITY, INTEGRITY, AVAILABILITY\},$$

де $CSM_1 = CONFIDENTIALITY$ – рівень (параметр) конфіденційності даних, $CSM_2 = INTEGRITY$ – рівень (параметр) цілісності даних, $CSM_3 = AVAILABILITY$ – рівень (параметр) доступності даних (інформаційних ресурсів).

Розширені моделі STRIDE, Parkerian Hexad та 5A, представлені на рис. 4.8, згідно (4.23) можна відповідно формалізувати таким чином:



а) б) в) г)

Рис. 4.8. Моделі кібербезпеки [19]: CIA (а), Parkerian Hexad (б), STRIDE (в) та 5A (г) [19]

1) при n=6 для моделі STRIDE вираз (4.23) матиме такий вигляд:

$$CSM_{STRIDE} = \left\{\bigcup_{i=1}^{6} CSM_i\right\} = \{CSM_1, CSM_2, \dots, CSM_6\} \quad (4.25)$$
$$= \{SPOOF, TAMP, REPUD, ID, DoS, EoP\},$$

де $CSM_1 = SPOOF$ – рівень захисту від підробки даних (Spoofing), $CSM_2 = TAMP$ – рівень захисту від несанкціонованого втручання в систему (Tampering), $CSM_3 = REPUD$ – рівень забезпечення неможливості відмови від авторства (Repudiation), $CSM_4 = ID$ – рівень захищеності від витоку й розголошення інформації з обмеженим доступом (Information disclosure), $CSM_5 = DoS$ – рівень захищеності від атак на

відмову в обслуговуванні (Denial of service), $CSM_6 = EoP$ – рівень захищеності від розширення зловмисником прав доступу в системі (Elevation of privilege).

2) при n=6 для моделі Parkerian Hexad, що є фактичним розширенням моделі CIA (4.24), вираз (4.23) матиме такий вигляд:

$$CSM_{PH} = \left\{\bigcup_{i=1}^{6} CSM_i\right\} = \{CSM_1, CSM_2, \dots, CSM_6\} \quad (4.26)$$
$$= \left\{\begin{matrix} CONFIDENTIALITY, INTEGRITY, AVAILABILITY, \\ POSSESSION, AUTHENTICITY, UTILITY \end{matrix}\right\},$$

де $CSM_1 = CONFIDENTIALITY$ – рівень (параметр) конфіденційності даних, $CSM_2 = INTEGRITY$ – рівень цілісності даних, $CSM_3 = AVAILABILITY$ – рівень доступності даних (інформаційних ресурсів), $CSM_4 = POSSESSION$ – рівень фізичного або логічного контролю даних, $CSM_5 = AUTHENTICITY$ – рівень аутентичності (підтвердження оригінальності авторства), $CSM_6 = UTILITY$ – рівень корисності та зручності використання даних.

3) при n=5 для моделі Б. Шнайєра 5A вираз (4.23) матиме такий вигляд:

$$CSM_{5A} = \left\{\bigcup_{i=1}^{5} CSM_i\right\} = \{CSM_1, CSM_2, \dots, CSM_5\} \quad (4.26)$$
$$= \left\{\begin{matrix} AUTHENTICATION, AUTHORIZATION, AVAILABILITY, \\ AUTHENTICITY, ADMISSIBILITY \end{matrix}\right\},$$

де $CSM_1 = AUTHENTICATION$ – рівень (параметр) забезпечення аутентифікації користувачів системи, $CSM_2 = AUTHORIZATION$ – рівень забезпечення авторизації користувачів системи, $CSM_3 = AVAILABILITY$ – рівень доступності даних (інформаційних ресурсів), $CSM_4 = AUTHENTICITY$ – рівень аутентичності (підтвердження оригінальності авторства), $CSM_5 = ADMISSIBILITY$ – рівень допустимості або прийнятності даних.

За результатами моніторингу, функцію оцінювання виконання вимог кібербезпеки (в продовження (4.19) та (4.22)), враховуючи (4.23), можна представити наступним чином:

$$f_{evaluation}: SMEC \to CSM \times VERIFICATION,$$
$$\forall SMEC_j \in SMEC \; \exists \; (CSM_i, VERIFICATION_i): SMEC_j \to (CSM_i, VERIFICATION_i), \tag{4.27}$$

де $VERIFICATION \subseteq [0,1]$ – параметр, що оцінює виконання контролів $SMEC_j$.

Ланцюг функціональних взаємодій методу можна представити у вигляді композиції відображень

$$SREQ \xrightarrow{f_{transformation}} SMEC \xrightarrow{f_{integration}} \langle SDLC \times PIPELINE \rangle \xrightarrow{f_{evaluation}} \langle CSM \times VERIFICATION \rangle . \tag{4.28}$$

Таким чином, відбувається перехід від вимог безпеки до верифікації метрик безпеки (через функції трансформації, інтегрування та оцінювання).

4.3. Висновки до четвертого розділу дисертації

1) Використовуючи теорію множин, було формалізовано у загальному вигляді відомі моделі життєвого циклу розроблення ПЗ (класична каскадна модель, V-модель, інкрементальна модель, спіральна модель, Agile, DevOps, DevSecOps), що дало можливість сформувати уніфіковану модель SDLC.

2) Використовуючи уніфіковану модель SDLC, розроблено метод інтегрування вимог кібербезпеки в SDLC [23], що за рахунок формалізації DevSecOps, ідентифікації вимог кібербезпеки, трансформації вимог у контрольні механізми, інтегрування контрольних механізмів у SDLC, верифікування та моніторингу виконання вимог кібербезпеки у вигляді системи множин та

відображень, дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень;

3) Практична цінність запропонованого методу полягає у можливості його використання для системного інтегрування вимог кібербезпеки в процеси розроблення ПЗ в організаціях, що створюють або експлуатують інформаційні системи критичної інфраструктури, хмарні сервіси та корпоративні інформаційно-комунікаційні системи.

4) Застосування розробленого методу дозволяє: забезпечити узгодженість вимог кібербезпеки на всіх етапах SDLC; підвищити рівень автоматизації контролю кібербезпеки у DevSecOps pipeline; зменшити ризик пропуску критичних вимог кібербезпеки під час швидких ітерацій розроблення; підвищити обґрунтованість вибору засобів захисту інформації; скоротити витрати на усунення вразливостей за рахунок їх виявлення на ранніх етапах SDLC [19,21]; забезпечити можливість кількісного оцінювання рівня реалізації вимог кібербезпеки за допомогою метрик кібербезпеки; створити інструментальні засоби підтримки прийняття рішень у процесах DevSecOps.

5) Запропонований метод може бути використаний при проєктуванні захищених інформаційно-комунікаційних систем [22]; аудиті процесів безпечної розробки ПЗ згідно стандартів ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних IT-системах тощо.

4.4. Список використаних джерел у четвертому розділі

1. M. Khari, Vaishali and P. Kumar, "Embedding security in Software Development Life Cycle (SDLC)," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2016, pp. 2182-2186.

2. Життєвий цикл розробки ПЗ (SDLC – Software Development Lifecycle) https://www.it-notes.wiki/other/software-development-lifecycle

3. V. B. Manjeti, S. Penumajji, S. R. Patlolla, Y. S. Srinath Abburi, J. Teppala and S. G. Krishna Patro, "Enhancing Security in SDLC with DevOps Tools and Practices," *2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET)*, Gunupur, India, 2025, pp. 1-5, doi: 10.1109/GIET65294.2025.11234805.

4. A. K. Bhardwaj, P. Anugula, S. Shilpi and P. Ranjan, "Zero Trust CI/CD Pipeline: A Blueprint for Secure Software Delivery in Modern DevSecOp," *2025 1st IEEE Uttar Pradesh Section Women in Engineering International Conference on Electrical Electronics and Computer Engineering (UPWIECON)*, Dehradun, India, 2025, pp. 233-237, doi: 10.1109/UPWIECON67212.2025.11390387.

5. *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements,* Ed. 3, 2022, 19 pages.

6. *National Institute of Standards and Technology Special Publication 800-53*, Rev. 5, 492 pages (September 2020), https://doi.org/10.6028/NIST.SP.800-53r5

7. IT Governance Publishing; Stephen Hancock, *PCI DSS Version 4.0.1: A guide to the payment card industry data security standard,* Packt Publishing, 2025.

8. W. Wodo, D. Stygar, PSD2 Compliant Hardware Token for Digital Banking, *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),* Riga, Latvia, 2021, pp. 1-6.

9. IT Governance Publishing; IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An implementation and compliance guide,* Packt Publishing, 2025.

10. W. -T. Tsai, J. -N. Luo and C. -L. Chou, Integrating Tree Structures with the MITRE ATT&CK Framework for APT Detection, *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, Okinawa, Japan, 2025, pp. 139-143, doi: 10.1109/CSP66295.2025.00031.

11. What Is Waterfall Project Management? https://technologyadvice.com/blog/project-management/what-is-waterfall-project-management

12. V-Model in Software Development: Complete Guide to Verification and Validation SDLC https://teachingagile.com/sdlc/models/v-model

13. Incremental Model in SDLC: Use, Advantage & Disadvantage: https://www.guru99.com/what-is-incremental-model-in-sdlc-advantages-disadvantages.html

14. Spiral Model: Definition, Phases, Advantages & Disadvantages: https://teachingagile.com/sdlc/models/spiral

15. Agile Model: https://www.interviewbit.com/blog/agile-model

16. What is DevOps? https://www.betsol.com/blog/what-is-devops

17. А. Скуратівський, Метод управління вимогами кібербезпеки при впровадженні програмного забезпечення у бізнесі, Безпека інформації, №3, 2025, с. 145-162.

18. J. Seol, J. Deuja, I. N. Park, C. Pu and N. Park, "A Quantitative Study across CIA (Confidentiality, Integrity, Availability) Triad and Performance in Blockchain-Based Crypto-Space," *2025 7th International Conference on Blockchain Computing and Applications (BCCA)*, Durbovnic, Croatia, 2025, pp. 161-168, doi: 10.1109/BCCA66705.2025.11229817.

19. В. Харченко, О. Корченко, С. Гнатюк, Мультирівнева модель даних для ідентифікації забезпеченості вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації, *Захист інформації,* Том 19, №1, 2017, с. 95-104, DOI: 10.18372/2410-7840.19.11499

20. G. Raj, D. Singh and A. Bansal, "Analysis for security implementation in SDLC," *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, Noida, India, 2014, pp. 221-226, doi: 10.1109/CONFLUENCE.2014.6949376.

21. Odarchenko R., Pinchuk A., Polihenko O., Skurativskyi A. A comparative analysis of cyber threat intelligence models, CEUR Workshop Proceedings, 2025, Vol. 3925, pp. 3-12.

22. Dorozhynskyi S., Zakutynskyi I., Ryabyy M., Skurativskyi A. Maximizing Security and Efficiency in 5G Networks by Means of Quantum Cryptography and Network Slicing Concepts, Proceedings of the IEEE International Conference on Intelligent Data

Acquisition and Advanced Computing Systems Technology and Applications, 2023, pp. 1031-1036, 10.1109/IDAACS58523.2023.10348871, ISSN 2770-4262

23. Гнатюк С., Побережна З., Скуратівський А. Метод інтегрування вимог кібербезпеки в життєвий цикл розроблення програмного забезпечення, Кібербезпека: освіта, наука, техніка, Т. 4, №32, с. 947-962. https://doi.org/10.28925/2663-4023.2026.32.1184

ВИСНОВКИ

У дисертаційній роботі проведені наукові дослідження, спрямовані на підвищення ефективності процесу впровадження ПЗ в бізнесі шляхом розроблення методів та інструментальних засобів управління вимогами кібербезпеки, які забезпечують їх формалізовану інтеграцію, трасованість, адаптацію до змін середовища загроз і ресурсних обмежень, а також узгодженість з функціональними та нефункціональними вимогами інформаційних систем.

Зокрема, було отримано такі вагомі наукові та практичні результати:

1. Проведено аналіз сучасних підходів до управління вимогами кібербезпеки при розробленні і впровадженні ПЗ, що дозволило виявити їх недоліки та вибрати найбільш ефективні математичні методи і підходи, а також формалізувати завдання дослідження. Аналіз сучасних наукових підходів до управління вимогами кібербезпеки показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на необхідності вдосконалення нормативно-правової бази, впровадження галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки. Основний недолік відомих підходів імплементації вимог в життєвий цикл розроблення ПЗ – це відсутність формалізованої, динамічної та трасованої інтеграції вимог кібербезпеки у всі етапи життєвого циклу розроблення ПЗ, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів та підвищення рівня ризику.

2. Розроблено математичну модель управління вимогами кібербезпеки при впровадженні ПЗ, що за рахунок створення графу залежностей вимог, використання методу AHP для пріоритезації вимог, застосування нечіткої логіки для оцінки рівня відповідності вимогам, моделювання ризиків за допомогою Байєсової мережі та оптимізації ресурсів за допомогою математичного програмування, дозволяє дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків, а також оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків, забезпечуючи комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків. На основі розробленої

моделі управління вимогами кібербезпеки при впровадженні ПЗ було проведено практичні симуляції з використанням фреймворків міжнародних стандартів і рекомендованих практик, зокрема досліджено:

- розроблену модель на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно з вимогами зазначеного стандарту;
- розроблену модель на основі стандарту ISO 22316, що забезпечило досягнення балансу між важливістю вимог, мінімізацією ризиків і наявними ресурсами, відповідно вимогам зазначеного стандарту для забезпечення стійкості організації;
- розроблену модель на основі стандарту MITRE ATT&CK, що забезпечило виконання критичних вимог зазначеного стандарту і мінімізацію загальних ризиків при дотриманні бюджету.

3. Розроблено метод динамічного управління вимогами кібербезпеки, який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень, формування зворотного зв’язку та ініціації наступного циклу управління вимогами, дає змогу регулярно оновлювати пріоритети, врахувати нові вимоги кібербезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов. Формалізовано адаптивний механізм управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості ІКС у вигляді псевдокоду, що та може бути реалізований у системах підтримки прийняття рішень; програмних засобах управління кіберризиками; корпоративних GRC-платформах; автоматизованих системах планування тощо.

4. Розроблено уніфіковану модель SDLC, яка за рахунок формалізованого відображення множин фаз життєвого циклу розроблення ПЗ, відношень між фазами

та функцій, дозволяє представити відомі моделі життєвого циклу розроблення ПЗ у зручній формі для інтегрування й імплементування вимог. На основі уніфікованої моделі SDLC було формалізовано відомі моделі життєвого циклу розроблення ПЗ, зокрема класичну каскадну модель, V-модель, інкрементальну модель, спіральну модель, Agile, DevOps та DevSecOps, що може бути використано при проєктуванні захищених ІКС; аудиті процесів безпечної розробки ПЗ згідно стандартів ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних IT-системах тощо.

5. Розроблено метод інтегрування вимог кібербезпеки в SDLC, що за рахунок формалізації моделі DevSecOps (на базі уніфікованої моделі SDLC), ідентифікації вимог кібербезпеки, трансформації вимог у контрольні механізми, інтегрування контрольних механізмів у SDLC, верифікування та моніторингу виконання вимог кібербезпеки у вигляді системи множин та відображень, дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень. Практична цінність цього методу полягає у можливості його використання для системного інтегрування вимог кібербезпеки в процеси розроблення ПЗ в організаціях, що створюють або експлуатують інформаційні системи критичної інфраструктури, хмарні сервіси та корпоративні ІКС. Застосування цього методу дозволяє: забезпечити узгодженість вимог кібербезпеки на всіх етапах SDLC; підвищити рівень автоматизації контролю кібербезпеки у DevSecOps pipeline; зменшити ризик пропуску критичних вимог кібербезпеки під час швидких ітерацій розроблення; підвищити обґрунтованість вибору засобів захисту інформації; скоротити витрати на усунення вразливостей за рахунок їх виявлення на ранніх етапах SDLC; забезпечити можливість кількісного оцінювання рівня реалізації вимог кібербезпеки за допомогою метрик кібербезпеки; створити інструментальні засоби підтримки прийняття рішень у процесах DevSecOps.

6. Результати роботи впроваджені у навчальний процес кафедри комп’ютерних інформаційних технологій Факультету комп’ютерних наук та технологій Державного університету «Київський авіаційний інститут» (акт від 18.02.2026) і діяльність Наукової асоціації кібербезпеки України (акт від 17.12.2025).