УДК 004.056:005.8:519.95 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.62

М. А. ФУКС
аспірант кафедри інфокомунікаційної інженерії
імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0009-0001-0248-2109

І. С. ДОБРИНІН
кандидат технічних наук, доцент,
доцент кафедри інфокомунікаційної інженерії
імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0000-0001-8910-2609

С. В. ПШЕНИЧНИХ
кандидат технічних наук, старший науковий співробітник,
доцент кафедри інфокомунікаційної інженерії
імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-0533-2306

А. В. СНІГУРОВ
кандидат технічних наук, доцент,
декан факультету інфокомунікацій
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-1355-7978

В. Х. ЧАКРЯН
кандидат технічних наук,
старший викладач кафедри інфокомунікаційної інженерії
імені В. В. Поповського
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-4827-9779

МЕТОДИКА ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ МЕТОДІВ АНАЛІЗУ ІЄРАРХІЙ, МЕРЕЖЕВОГО АНАЛІЗУ ТА ТЕОРІЇ ІГОР В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

В умовах цифровізації та швидкої еволюції кіберзагроз стає критично важливим побудова надійної системи управління інформаційною безпекою (СУІБ). Наявні міжнародні та національні стандарти побудови СУІБ не враховують специфіки розподілу ресурсів, а лише вказують на важливість забезпечення ресурсами для створення, реалізації, підтримки та безперервного розвитку СУІБ, тобто прослідковується певний брак механізмів прийняття управлінських рішень та оптимізації виділених ресурсів. Тому актуальною залишається проблема ідентифікації, розподілу та раціонального використання ресурсів для досягнення достатнього рівня ефективності СУІБ. Крім того, при імплементації СУІБ на базі будь-якої з методик, одним із найскладніших кроків є визначення та інтеграція дієвих заходів і інструментів інформаційного захисту. У цьому контексті відчувається нестача практичних та методичних інструментів для оптимізації, адже навіть за умов істотних вкладень і широкомасштабного впровадження засобів захисту інформації (ЗЗІ) виникає сумнів щодо доцільності та ефективності таких рішень. У роботі запропоновано методику побудови СУІБ, що поєднує метод аналізу ієрархій (МАІ), методи аналізу мереж (МАМ) та математичний апарат теорії ігор для вибору оптимальної базової методики і засобів захисту в умовах обмежених ресурсів та наявних загроз. Запропонований підхід також передбачає використання мережевого аналізу для моделювання проєкту з урахуванням строків, витрат, ресурсів та можливих сценаріїв реалізації. Методика включає побудову мережевої моделі проєкту, розрахунок критичного шляху, виявлення критичних та некритичних робіт, аналіз часових резервів, варіантів прискорення проєкту і визначення впливу прискорення на загальну вартість. Запропоновано спосіб порівняльної оцінки кількох сценаріїв реалізації проєкту: при звичайних строках, при прискоренні лише критичних робіт, а також при при-

скоренні всіх або лише некритичних робіт. У результаті отримано графіки розподілу ресурсів у часі, фінансових витрат та залученості людського ресурсу, що дозволяють приймати більш зважені управлінські рішення. Методика є практичним інструментом для Chief Information Security Officer (CISO) та керівників, що дозволяє визначити оптимальний обсяг інвестицій на кожному етапі проєкту СУІБ та обґрунтовано аргументувати потребу в ресурсах, забезпечуючи баланс між ефективністю та витратами.

Ключові слова: *система управління інформаційною безпекою, мережевий аналіз, критичний шлях, теорія ігор, оптимізація ресурсів, CISO, управлінські рішення.*

M. A. FUKS
Postgraduate Student at the V. V. Popovskyy Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0009-0001-0248-2109

I. S. DOBRYNIN
PhD, Associate Professor,
Associate Professor at the V. V. Popovsky Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0000-0001-8910-2609

S. V. PSHENYCHNYKH
PhD, Senior Researcher,
Associate Professor at the V. V. Popovsky Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0000-0003-0533-2306

A. V. SNIHUROV
PhD, Associate Professor,
Dean of the Faculty of Infocommunications
Kharkiv National University of Radio Electronics
ORCID: 0000-0003-1355-7978

V. H. CHAKRIAN
PhD, Senior Lecturer at the V. V. Popovskyy Department
of Infocommunication Engineering
Kharkiv National University of Radio Electronics
ORCID: 0000-0003-4827-9779

METHODOLOGY FOR DEVELOPING INFORMATION SECURITY MANAGEMENT SYSTEMS USING NETWORK ANALYSIS AND GAME THEORY

In the context of digitalization and the rapid evolution of cyber threats, building a reliable Information Security Management System (ISMS) becomes critically important. Existing international and national ISMS standards do not take into account the specifics of resource allocation; instead, they only emphasize the importance of providing resources for the creation, implementation, maintenance, and continuous improvement of ISMS. This indicates a certain lack of mechanisms for making management decisions and optimizing allocated resources. Therefore, the problem of identifying, distributing, and rationally using resources to achieve an adequate level of ISMS efficiency remains relevant. Moreover, during ISMS implementation based on any methodology, one of the most challenging steps is the identification and integration of effective information security measures and tools. In this context, there is a shortage of practical and methodological optimization tools, since even with substantial investments and large-scale deployment of information security measures (ISMs), doubts may arise regarding the expediency and efficiency of such solutions. This paper proposes a methodology for building ISMS that combines the Analytic Hierarchy Process (AHP), network analysis methods, and the mathematical apparatus of game theory to select the optimal baseline methodology and protection tools under conditions of limited resources and existing threats. The proposed approach also involves the use of network analysis to model the project, taking into account timelines, costs, resources, and possible implementation scenarios. The methodology includes the construction of a project network model, calculation of the critical path, identification of critical and non-critical activities, analysis of time reserves, acceleration options, and assessment of the impact of acceleration on total cost. A method for comparative evaluation of several implementation scenarios is proposed: with normal timelines, with acceleration of only critical activities, as well as with acceleration of all or only non-critical

activities. As a result, resource allocation over time, financial cost, and human resource engagement charts are obtained, enabling more informed management decisions. The methodology is a practical tool for the Chief Information Security Officer (CISO) and executives, allowing them to determine the optimal investment amount at each stage of the ISMS project and to substantiate resource requirements while ensuring a balance between efficiency and cost.

Key words: *information security management system, network analysis, critical path, game theory, resource optimization, CISO, managerial decisions.*

Постановка проблеми

Наразі існує низка визнаних підходів, які використовуються як базис для побудови СУІБ в організаціях, серед яких найпоширенішими є стандарт ISO/IEC 27001 [1], методологія IT-Grundschutz [2] та Постанова Національного банку України (НБУ) № 95 [3]. Аналіз [1]–[3] свідчить про те, що в усіх наявних підходах акцентується увага на необхідності залучення всіх типів ресурсів: людських, фінансових, технічних, організаційних та інфраструктурних – як ключової умови для ефективного формування СУІБ. При цьому склад і обсяг необхідних ресурсів мають варіюватися в залежності від масштабу організації, специфіки її діяльності і рівня ризиків, адже саме коректне визначення та раціональне використання ресурсів є запорукою стабільної роботи усіх бізнес-процесів.

Водночас аналіз наявних підходів свідчить, що, незважаючи на їхню кількість і здатність частково структурувати процес створення СУІБ, вони не надають вичерпаних відповідей на два критично важливих запитання:

– за якими критеріями слід обирати базову методику побудови СУІБ для конкретної організації;
– яким чином оптимізувати використання доступних ресурсів у межах СУІБ-проєкту.

Вочевидь, неефективне планування та використання ресурсів у рамках СУІБ може призвести до перевитрат бюджету, затримок у реалізації заходів інформаційної безпеки або недостатнього рівня захищеності, що в умовах зростання кіберзагроз є критичним фактором для організацій.

З огляду на вищезазначене, у цій роботі запропоновано інтегрований підхід, який ґрунтується на методі аналізу ієрархій, методі аналізу мереж, та теорії ігор для обґрунтованого вибору стратегії побудови СУІБ і ефективного управління ресурсами на всіх етапах проєкту.

Аналіз останніх досліджень і публікацій

Проблематика розробки підходів до побудови ефективних СУІБ є однією з пріоритетних у сучасній науково-практичній сфері інформаційної безпеки. Ця актуальність обумовлена як зростаючою кількістю та складністю кіберзагроз, так і стрімким розвитком цифрових технологій, що суттєво впливають на інформаційну інфраструктуру організацій.

Сучасні дослідження та практичні реалізації в цій області [4]–[9] переважно зосереджуються на двох напрямках. Перший – це оцінювання ефективності інвестицій у СУІБ, шо передбачає аналіз витрат та вигод, пов'язаних із впровадженням заходів інформаційної безпеки, а також формування моделей оптимального розподілу ресурсів. Другий напрямок спрямований на вибір та адаптацію конкретних методик і стандартів побудови СУІБ, що включає аналіз наявних методологій, визначення їх сильних і слабких сторін, а також розробку рекомендацій щодо їх застосування в залежності від специфіки організації.

Тематика оцінювання ефективності виконаних інвестицій в ІБ знайшла широке відображення в науковій літературі, численних публікаціях, дослідженнях та прикладних методиках.

Варто зазначити, що запобігання можливих втрат може розглядатися як економія різноманітних ресурсів усієї бізнес-системи. Часто наголошується, що жодна система управління не зможе працювати належним чином без належного рівня забезпечення ресурсів [4].

Економічна модель Гордона–Лоеба [5] на сьогодні вважається однією з ключових у визначенні оптимального обсягу інвестицій в ІБ. Її концептуальна суть полягає в оберненій залежності: зі зростанням вкладень у захист зменшується рівень вразливості системи. Під час аналізу класів функцій, автори дійшли висновку, що оптимальний обсяг інвестицій становить приблизно 37 % від очікуваних втрат, яких може зазнати організація під час реалізації загроз [5]. Таким чином, модель демонструє, що економічно доцільний рівень інвестування в ІБ є значно нижчим за самі можливі збитки. Однак ця модель є здебільшого формалізованою й аксіоматичною, що ускладнює врахування особливостей конкретної організації та середовища ведення діяльності.

Питання вибору оптимальної методики побудови СУІБ також досліджувалося в інших роботах. Так, у роботі [6], було застосовано методи Томаса Сааті для моделювання багатокритеріальної задачі оптимізації. У дослідженні [7] запропоновано підхід до оптимізації інвестицій в ІБ підприємства на основі формалізованої моделі, яка дозволяє визначити інтегральний показник ефективності інвестицій. Як оптимізаційні змінні в моделі розглядаються загальні витрати на ліквідацію наслідків реалізованих загроз та інших факторів, а також сукупні виплати джерелам фінансування. Водночас модель не враховує обмеження фінансування з боку самої компанії, що може лімітувати її практичне застосування. У роботі [8] в основу запропонованого методу проєктування кіберстійкої інфокомунікаційної мережі (ІКМ) покладено розв'язання оптимізаційної задачі, яка пов'язана з узгодженням різнотипних керуючих змінних, проте такий підхід зосереджується переважно на формальних аспектах оптимізації параметрів, не враховуючи практичних механізмів підтримки управлінських рішень з боку CISO. У роботі [9],

на основі критерія максимуму інтегрального показника ефективності, вирішується задача оптимального вибору засобів захисту інформації від загроз безпеки при впровадженні СУІБ.

Проте низка важливих питань залишається відкритою: який саме підхід використовувати до побудови СУІБ та як оцінювати ефективність інвестицій у захист інформації та побудову СУІБ з урахуванням сучасних вимог і середовища існування. Більшість підходів акцентують увагу саме на фінансовій складовій та ЗЗІ, тоді як час і людські ресурси, що також суттєво впливають на загальні витрати, часто залишають поза увагою. У цьому контексті доцільним є використання принципів методології управління проєктами. Через складність взаємозв'язків між цими елементами питання комплексної оптимізації інвестицій залишається актуальним і потребує подальшого дослідження.

Формулювання мети дослідження

Метою статті є розробка методики побудови СУІБ, що поєднує підходи методів аналізу ієрархій і мереж, теорію ігор та методів управління проєктами для забезпечення оптимального вибору стратегії захисту, раціонального розподілу ресурсів і прийняття обґрунтованих управлінських рішень.

Викладення основного матеріалу дослідження

Запропонована методика побудови суіб

У якості основи для формування запропонованої методики та визначення механізмів прийняття управлінських рішень, спрямованих на оптимізацію взаємопов'язаних людських, часових і фінансових ресурсів, запропоновано залучення методів мережевого аналізу, методу аналізу ієрархій, математичного апарату теорії ігор, а також інструментарію управління проєктами.

Запропонована методика складається з трьох ключових етапів.

1) Оцінювання початкового стану об'єкта та аналіз потенціалу впровадження методики в конкретній організації.

2) Основна частина методики, яка умовно поділена на дві підсистеми:

– перша спрямована на вибір методики, на основі якої розбудовувати СУІБ (через метод аналізу мереж (МАМ) або метод аналізу ієрархій (МАІ)) [10], [11], та визначення загальної стратегії інформаційного захисту (через математичний апарат теорії ігор) – для визначення оптимальної стратегії CISO і оптимізації фінансових вкладень у ЗЗІ;

– друга – для моделювання мережевої конфігурації проєкту з метою подальшого аналізу та оптимізації за допомогою методів мережевого аналізу і керування проєктами – щоб сформувати цілісне уявлення, яке слугуватиме підґрунтям для ухвалення управлінського рішення щодо обґрунтованості запиту та визначення необхідного обсягу інвестицій.

3) Етап впровадження, що включає процедури інтеграції розробленої методики в компанії.

На першому етапі визначається поточний рівень ІБ організації та проводиться оцінка можливостей впровадження СУІБ. Така оцінка може здійснюватися як силами внутрішніх фахівців самої компанії, так і шляхом залучення незалежних експертів консалтингових компаній. Однак якість цього етапу значною мірою залежить від компетентності та релевантності створеної експертної групи. У разі залучення недостатньо кваліфікованих спеціалістів або неправильної побудови процесу аудиту існує підвищений ризик отримання хибних результатів. Саме тому до формування експертних груп висуваються підвищені вимоги, спрямовані на забезпечення об'єктивності та достовірності оцінювання. Результатом розглянутого етапу є узагальнена експертна оцінка початкового стану об'єкта, що має ключове значення для подальшого проєктування СУІБ.

Розглянемо складові основної частини запропонованої методики. Перша підсистема основної частини методики передбачає вирішення багатокритеріальної задачі оптимізації, що виникає на початковому етапі впровадження СУІБ. Відповідальній особі необхідно обґрунтовано обрати оптимальну методику, яка стане основою для побудови СУІБ. Для цього можуть бути застосовані методи МАІ або МАМ [6].

Метод МАІ, розроблений Т. Сааті, засновується на декомпозиції проблеми вибору на більш прості складники і поступовому наданні пріоритетів компонентам використовуючи парні порівняння [6]. Такий підхід забезпечує прозорість і відносну простоту у прийнятті рішень. Водночас метод МАМ розширює можливості МАІ, оскільки враховує не лише ієрархічні залежності, а й складні взаємозв'язки між критеріями та альтернативами, що робить його більш придатним для комплексних багатокритеріальних задач, характерних для побудови СУІБ.

Структурування моделі багатокритеріальної задачі передбачає попереднє збирання та систематизацію інформації відповідальною особою або експертною групою. На цьому етапі можуть застосовуватися різні методи генерації ідей та колективного напрацювання рішень, а отримана й узгоджена інформація стає підґрунтям для побудови раціональної системи у вигляді ієрархії (мережі), що надалі аналізується за допомогою методів МАІ або МАМ. Важливим аспектом цього процесу є достатня компетентність експертів та глибоке розуміння проблематики, адже саме від цього залежить якість і коректність подальшого моделювання. Таким чином, обґрунтовується вибір оптимальної методики, яка визначає підґрунтя для подальшого проєктування СУІБ.

Наступним кроком у межах основної частини запропонованої методики є обґрунтований вибір ЗЗІ, які забезпечуватимуть належний рівень безпеки у межах побудови СУІБ, і вибір яких доцільно здійснювати із застосуванням теоретико-ігрового підходу. Такий підхід дозволяє моделювати протидію між потенційним зловмисником та CISO, забезпечуючи обґрунтоване прийняття рішень щодо вибору контрзаходів в умовах обмежених ресурсів.

У роботі [12] розглянуто задачу оптимізації стратегії захисту інформації шляхом моделювання біматричної гри між CISO та зловмисником. Модель базувалася на двох показниках: Return On Security Investment (ROSI) та Return On Attack (ROA). У роботі було висунуто припущення про повну невизначеність поведінки зловмисника. У цьому дослідженні робиться припущення, що CISO володіє ймовірнісною інформацією про можливі атаки на основі відкритих бібліотек вразливостей і атак, наприклад, CAPEC, OWASP Top Ten, CVE, CVSS, що дозволяє застосовувати модель з чистими стратегіями [13]–[16].

Нехай CISO має стратегії для вибору, що визначатимуться набором $S_a = \{b_1, b_2, \ldots, b_m\}$, де m відображає загальну кількість таких стратегій, тобто певний набір ЗЗІ.

Нехай утворена матриця виграшів CISO матиме вигляд, який надано на рис. 1 [12].

	b_1	b_2	b_3	…	b_m
a_1	$U_A(a_1,b_1)$	$U_A(a_1,b_2)$	$U_A(a_1,b_3)$	…	$U_A(a_1,b_m)$
a_2	$U_A(a_2,b_1)$	$U_A(a_2,b_2)$	$U_A(a_2,b_3)$	…	$U_A(a_2,b_m)$
a_3	$U_A(a_3,b_1)$	$U_A(a_3,b_2)$	$U_A(a_3,b_3)$	…	$U_A(a_3,b_m)$
…	…	…	…	…	…
a_n	$U_A(a_n,b_1)$	$U_A(a_n,b_2)$	$U_A(a_n,b_3)$	…	$U_A(a_n,b_m)$
a_1+a_2	$U_A(a_1+a_2,b_1)$	$U_A(a_1+a_2,b_2)$	$U_A(a_1+a_2,b_3)$	…	$U_A(a_1+a_2,b_m)$
…	…	…	…	…	…
$a_{n-1}+a_n$	$U_A(a_{n-1}+a_n,b_1)$	$U_A(a_{n-1}+a_n,b_2)$	$U_A(a_{n-1}+a_n,b_3)$	…	$U_A(a_{n-1}+a_n, b_m)$

Рис. 1. Матриця виграшів CISO

У якості функцій корисності братиметься запропонований показник повернення інвестицій у кібербезпеку ROSI [12]:

$$ROSI = \frac{AV \cdot EF_j \cdot ARO_j \cdot RM_{ij} - \cos t_i}{\cos t_i}, \tag{1}$$

де AV – вартість активу, EF_j – Exposure Factor, тобто втрачена частина активу від реалізації атаки, ARO_j – загальна кількість появи атаки на рік, RM_{ij} – ефективність відбиття атаки, $cost_i$ – витрати на підтримку ЗЗІ. Таким чином елементи матриці представляють кількісну характеристику вигоди впровадження певної стратегії захисту інформації проти можливих атак зловмисника.

Припустимо, що відомо ймовірнісний розподіл для стратегій зловмисника $p_i = \{p_i, p_2, \ldots, p_m\}$. Це дозволяє визначити виграші CISO, який обирає конкретні стратегії захисту, виходячи з того, що зловмисник діє за змішаною стратегією:

$$U_A(a_i) = \sum_{k=1}^{m} U_A(a_i, b_k) \cdot p_i, \quad k \in S_a, \forall i \in S_d. \tag{2}$$

Таким чином формується обґрунтована стратегія вибору засобів захисту інформації, яка забезпечує оптимальне використання ресурсів та мінімізацію потенційних збитків. Однак для реалізації такого вибору у межах конкретного проєкту необхідно врахувати ще й часові, фінансові та організаційні обмеження. Саме тому наступним кроком запропонованої методики є побудова мережевої моделі проєкту створення СУІБ, що становить другу підсистему основної частини методики та забезпечує аналіз і оптимізацію розподілу ресурсів у процесі впровадження. Необхідність мережевого представлення проєкту зумовлена тим, що воно забезпечує формалізацію всіх робіт і подій у струтуру, дозволяючи виявляти критичні шляхи, резерви часу, залежності між роботами та їхній вплив на ресурси. Таким чином створюється інструмент для комплексного аналізу та оптимізації проєкту побудови СУІБ.

Припустимо, що відповідальна особа прагне оцінити складність окремого етапу побудови СУІБ, спланувати його реалізацію як частину загального проєкту, визначити тривалість виконання, критичні роботи та забезпечити раціональний розподіл ресурсів із можливістю оптимізації строків.

Нехай уся мережа Grid представлятиметься у вигляді певного набору чисел:

$$Grid = (K, C), \tag{3}$$

де $K = (1, \ldots, n)$ – множина вершин мережі, n – загальна кількість таких вузлів, C – множина ребер робіт мережі, що зображуються роботи.

Нехай d_{ij} – тривалість певної роботи $(i, j) \in C, i \in K, j \in K$. $T_i(E)$ – найбільш ранній можливий час настання події (досягнення вершини i), де $i \in K$. $T_i(L)$ – найбільш пізній дозволений час настання події i, де $i \in K$. W_r – множина усіх шляхів від вершини 1 до вершини $i \in K$, r – кількість таких шляхів.

Кожен шлях містить у собі певну кількість робіт, сума тривалостей виконання яких і створює суму виконання цього шляху. Найбільша ж величина з декількох і буде значенням $T_i(E)$, тобто найбільш раннім можливим часом настання події $i \in K$. Обумовлені моменти представлені у формулі:

$$T_i(E) = \max\left(\sum_k \sum_q d_{kq}\right), \tag{4}$$

де $k, q \in W_r$, $i \in K$.

Необхідно зауважити, що найбільш ранній можливий час настання першої події 0.

Ключовим моментом у визначенні крайнього дозволеного терміну настання події є те, що подібне збільшення відстрочки не повинне змінювати загальну тривалість виконання робіт. Саме тому виконується умова, що найбільш пізній дозволений час настання події такий самий, як і найбільш ранній можливий час завершення проекту [17]:

$$T_n(L) = T_n(E). \tag{5}$$

Саме тому розрахунок $T_i(L)$ відбувається у зворотньому порядку (з кінця проекту до початку). Потрібно здійснити аналіз тривалості всіх робіт, що виходять із заданої події i, та визначити для неї мінімальну різницю між моментом настання наступної вершини j і тривалістю роботи, яка безпосередньо веде до цієї вершини:

$$T_i(L) = \min(T_j(L) - d_{ij}). \tag{6}$$

На рівні з вищезазначеними визначеннями $T_i(E)$ та $T_i(L)$ постають ще пара важливих компонент аналізу мереж: резерв часу та критичний шлях.

Резерв часу ΔT_i – це загальний час, на який може бути затримано настання певної події і за умовою, що загальний час проекту не збільшиться. Наступна формула відображає спосіб розрахунку резерву часу для певної події i:

$$\Delta T_i = T_i(L) - T_i(E). \tag{7}$$

Часовий резерв вершини визначається як різниця між максимально пізнім допустимим моментом настання події та мінімально можливим часом її виникнення. Інакше кажучи, це найбільший проміжок часу, на який може бути відтерміноване настання певної події i. Зауважимо, у разі наявності нульового значення резерву часу, затримка настання події не допускається, інакше відбудеться затримка виконання усього проекту. Такі нульові події утворюють ключову структуру: критичний шлях мережі, а роботи, які містяться на такому шляху – це критичні роботи.

Отже, вибудовується наступна послідовність розрахунків, яка наведена на рис. 2.

Критичний шлях задає мінімальну тривалість проєкту СУІБ, і затримка будь-якої роботи на ньому затягує реалізацію та потребує залучення додаткових ресурсів.

Некритичні роботи мають резерв часу, тому їх затримка не впливає на строк реалізації. Для скорочення тривалості проєкту доцільно прискорювати лише критичні роботи, оскільки оптимізація некритичних лише підвищує витрати без зміни загального часу.

Окрім найранішого та найпізнішого строків настання подій, важливими є й відповідні параметри для робіт, які визначають часові межі їх виконання без впливу на загальну тривалість проєкту.

Усі отримані результати фіксуються у зведеній таблиці, що допомагає відповідальній особі комплексно оцінювати характеристики кожної роботи: визначати її критичність, обсяг резервного часу, а також ступінь впливу на подальші етапи проєкту. Резерв часу відіграє ключову роль у керуванні ризиками, забезпечуючи гнучкість і стабільність проєкту у випадку непередбачуваних затримок або змін. Його наявність дозволяє перерозподіляти час, підтримувати графік і підвищувати впевненість у досягненні цілей.

У методах керування проєктами: методі критичного шляху (CPM) і методі оцінки та аналізу програми (PERT) основна увага приділяється часовим параметрам виконання робіт [18]. Однак для досягнення оптимізації ресурсів важливо враховувати фінансову складову, оскільки тривалість робіт може змінюватися залежно від обсягів виділених ресурсів. Скорочення часу критичних робіт дозволяє зменшити загальну тривалість проєкту, але потребує додаткових фінансових вкладень. Прискорення всіх робіт може бути нераціональним через значне зростання витрат без суттєвого ефекту. Отже, важливо зберігати баланс між часом і коштами для досягнення оптимального результату. Доцільно ввести додаткові поняття: запланована тривалість виконання роботи та прискорена. Припустимо, що ці параметри заздалегідь визначені та відображені в таблиці для відповідної мережі.

На основі введених даних пропонується здійснювати три варіанти аналізу.

1) Визначення критичного шляху та розрахунок витрат при запланованих строках виконання робіт.
2) Аналіз критичного шляху та витрат у разі повного прискорення всіх робіт.
3) Оцінка критичного шляху та витрат при прискоренні лише критичних робіт.

Ці сценарії дозволяють порівняти загальну тривалість реалізації проєкту та відповідні фінансові витрати. Отримані результати можуть бути використані для обґрунтованого прийняття управлінських рішень щодо оптимального розподілу ресурсів.

На основі трьох розрахованих сценаріїв визначаються характеристики робіт (найбільш ранній початок, найпізніше завершення, резерв часу тощо) та будується гістограма виконання робіт у часі з відповідними ресурсними потребами.

До кожної гістограми будуються графіки сумарних фінансових інвестицій і залучення людських ресурсів. Це дає можливість відповідальним особам регулювати споживання ресурсів відповідно до лімітів і резервів часу. Регулювання

Рис. 2. Послідовність розрахунків для визначення критичності подій

здійснюється шляхом маневрування робочою силою та зміщенням строків некритичних робіт у межах допустимих резервів, що дозволяє рівномірно розподілити навантаження без збільшення загальної тривалості проєкту.

Після виконання основної частини запропонованої методики постає завдання її інтеграції у процеси компанії, що становить завершальний етап, а саме етап впровадження. Реалізація етапу впровадження потребує поєднання технічних, організаційних і адміністративних заходів. До них належить підготовка персоналу, налаштування процесів моніторингу й контролю, інтеграція обраних ЗЗІ. Особливу роль відіграє підтримка з боку керівництва, адже саме від їх рішень залежить рівень ресурсного забезпечення та ефективність реалізації всієї СУІБ. Важливо підкреслити, що впровадження СУІБ здійснюється на основі тієї методики, яка була обґрунтовано обрана на попередньому етапі запропонованої методики. Це означає, що запропонований підхід не замінює існуючі стандарти й нормативні документи, а слугує надбудовою, яка дозволяє оптимізувати процес розподілу ресурсів, вибору засобів захисту та управлінських рішень у межах обраної методики. Таким чином, етап впровадження виступає завершальною та критично важливою фазою запропонованої методики, що забезпечує її практичну цінність і перетворює теоретичні результати на інструмент ухвалення управлінських рішень у сфері ІБ.

Результати дослідження

У дослідженні було розглянуто два підходи до розв'язання багатокритеріальної задачі вибору оптимальної методики побудови СУІБ: MAI та MAM. Основна відмінність між ними полягає в тому, що MAI враховує лише прямі ієрархічні залежності, тоді як MAM дозволяє моделювати взаємозв'язки будь-якого типу, включно з впливом альтернатив на критерії.

Нехай представлено наступні альтернативи для вибору методики побудови СУІБ організації. Лінійка ISO/IEC 2700x, що представлена сукупністю стандартів ISO/IEC 27001 (вимоги до СУІБ), ISO/IEC 27002 (заходи забезпечення ІБ), ISO/IEC 27003 (основна частина керівництва), тощо. Методологія IT-Grundschutz, що представлена сукупністю стандартів BSI-200-1 (вимоги), BSI-200-2 (сама методологія), тощо. А також Постанова НБУ № 95.

Для порівняння уведені такі критерії:

– простота використання;
– методологічне забезпечення;
– необхідний рівень компетентності осіб для розробки та впровадження;

– можливість використання математичних підходів аналізу;
– конкретність вимог до СУІБ;
– універсальність вимог;
– частота використання.

Для оцінки компонентів визначається спеціальна шкала від 1 до 9, де 1 – рівнозначні важливості (по діагоналі матриці), при помірній перевазі – 3, при значимій – 5, і так до 9. При заповненні матриці має місце зворотна симетрія. У результаті після отримання необхідних матриць виконується змістовний аналіз.

На основі експертної оцінки, проведеної за визначеними критеріями, обидва методи MAI та MAM продемонстрували схожі результати (див. рис. 3), що підтвердило доцільність вибору IT-Grundschutz як базової методики для побудови СУІБ.

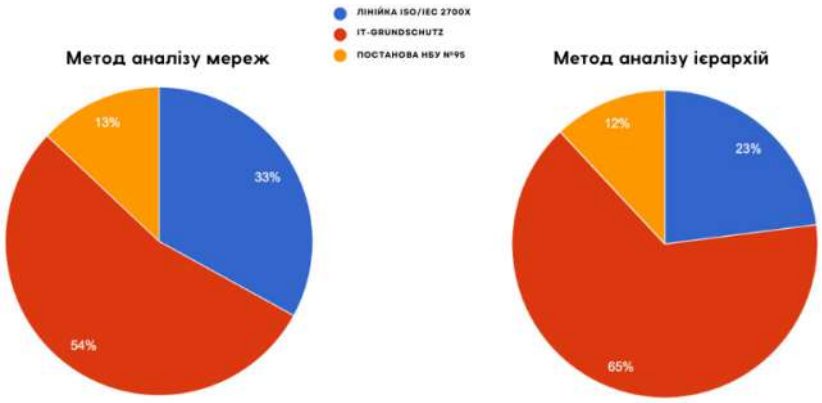

Рис. 3. Порівняльний аналіз результатів багатокритеріальної оптимізації

Водночас MAM, завдяки ширшому охопленню зв'язків, частково переорієнтував оцінки: сімейство ISO/IEC 2700x зайняло 10 %, а Постанова НБУ № 95 лише 1 %, що свідчить про більш глибокий аналіз. Обидва методи однозначно визнали найменш доцільною саме Постанову НБУ № 95, що є зрозумілим, зважаючи на її специфіку та вузькоспрямованість. Таким чином, метод MAM доцільно застосовувати у випадках, коли результати методу MAI потребують додаткової деталізації та врахування складніших взаємозв'язків між елементами задачі, що забезпечує більш глибоку та структуровану оцінку.

Завершивши вибір базової методики побудови СУІБ, методика пропонує перехід до наступного етапу: вибір оптимальної чистої стратегії CISO та забезпечення раціонального розподілу фінансових вкладень у ЗЗІ.

Розглянемо умовну організацію, у якій CISO прагне побудувати ефективну СУІБ із впровадженням лише тих засобів захисту, що є дійсно необхідними, враховуючи обмеженість затвердженого бюджету. Завдання зводиться до оптимізації вибору ЗЗІ.

У якості прикладу серед потенційних загроз інформаційній системі виділимо:
– шкідливе програмне забезпечення (ШПЗ);
– DDoS-атаки;
– фізичні впливи;
– фішингові атаки.
– Для протидії зазначеним загрозам розглядатимуться такі засоби захисту:
– антивірусне програмне забезпечення;
– криптографічні засоби (шифрувальне ПЗ);
– система захисту від DDoS-атак.

CISO має у своєму розпорядженні статистичні дані щодо реалізації загроз, отримані як із власного досвіду, так і на основі відомих джерел, зокрема CAPEC, CWE, OWASP, ENISA. Це дає змогу здійснити якісне моделювання ризиків і сценаріїв атак. Слід зазначити, що кількість загроз та засобів захисту у моделі не обмежується наведеними прикладами. Їх використано з метою спрощення розрахунків та наочної демонстрації можливостей запропонованої математичної моделі.

Перед пошуком розв'язків сформульованої гри необхідно визначити ключові показники для розрахунку функцій корисності та формування матриць учасників. Вихідні дані узгоджуються з аналітичними звітами організацій які піклуються питаннями інформаційної безреки, наприклад, ENISA, Gartner, BSI [19] – [21]. У таблиці 1 наведено значення показників Exposure Factor (EF) та Annual Rate of Occurrence (ARO), що використовуються для обчислення ROSI у матриці виграшів адміністратора безпеки. Додатково враховується показник Risk Mitigated (RM), який відображає ефективність засобів захисту та потребує експертної оцінки з боку CISO чи команди ІБ.

Таблиця 1

Початкові значення показників Exposure Factor, Annual Rate of Occurrence та Risk Mitigated

ЗЗІ	Показник	ШПЗ	Фізичний вплив	Фішингові атаки	DDoS атаки
–	EF	0,87	0,93	0,84	0,8
–	ARO	1	0,5	3	2
Антивірусне ПЗ	RM	0,85	0,05	0,2	0,05
Шифрувальне ПЗ		0,1	0,75	0,04	0,01
СЗ від DDoS атак		0	0	0	0,75
Антивірусне ПЗ + шифрувальне ПЗ		0,95	0,8	0,24	0,06
Шифрувальне ПЗ + СЗ від DDoS атак		0,1	0,75	0,04	0,76
Антивірусне ПЗ + СЗ від DDoS атак		0,85	0,05	0,2	0,8
Антивірусне ПЗ + шифрувальне ПЗ + СЗ від DDoS атак		0,95	0,8	0,24	0,81

На основі формули (1) було розраховано відповідні функції корисності CISO для кожної пари ЗЗІ-атака. Повна матриця для проведення аналізу показана на рис. 4.

p_i	27%	12%	41%	20%
	ШПЗ	Фізичний вплив	Фішингові атаки	DDoS атаки
Антивірусне ПЗ	23,65	-0,22	15,8	1,67
Шифрувальне ПЗ	0,45	4,81	0,68	-0,73
СЗ від DDoS атак	-1	-1	-1	16,14
Антивірусне ПЗ + шифрувальне ПЗ	8,18	3,13	5,72	0,07
Шифрувальне ПЗ + СЗ від DDoS атак	-0,33	1,68	-0,22	8,35
Антивірусне ПЗ + СЗ від DDoS атак	6,4	-0,77	4,04	11,8
Антивірусне ПЗ + шифрувальне ПЗ + СЗ від DDoS атак	4,17	1,33	2,78	7,1

Рис. 4. Матриця з функціями виграшів захисника та ймовірнісним розподілом стратегій зловмисника

Математичне очікування дискретної випадкової величини, тобто виграш, що отримує CISO, при можливому використанні кожної його стратегії розраховуємо за формулою (2). Результати розрахунку представлені на рис. 5.

Математичне очікування дискретної випадкової величини $U_A(a_i)$						
Антивірусне ПЗ	Шифрувальне ПЗ	СЗ від DDoS атак	Антивірусне ПЗ + шифрувальне ПЗ	Шифрувальне ПЗ + СЗ від DDoS атак	Антивірусне ПЗ + СЗ від DDoS атак	Антивірусне ПЗ + шифрувальне ПЗ + СЗ від DDoS атак
13,1711	**0,8315**	**2,428**	**4,9434**	**1,6923**	**5,652**	**3,8453**

Рис. 5. Розрахунок виграшів для кожної стратегії захисника

Також розв'язання сформульованої задачі здійснюється шляхом моделювання біматричної гри між CISO та зловмисником на основі підходу, описаного в роботі [12], що дозволяє забезпечити подальше коректне порівняння результатів. Для розгляду суперництва на основі біматричної гри необхідно створити матрицю й для зловмисника. У підготовчому етапі визначаються можливі витрати зловмисника на підготовку атаки та проведення, а також можливі втрати через впровадження певного механізму захисту адміністратором. Таким чином нехай адміністратором безпеки було визначено наступні значення показників cost та loss відповідно, що наведені у таблиці 2.

Таблиця 2

Значення показників cost та loss для розрахунку показників Return On Attack

	ШПЗ	Фізичний вплив	Фішингові атаки	DDoS атаки
cost	100000 (у.о.)	5000 (у.о.)	40000 (у.о.)	80000 (у.о.)
loss	60000 (у.о.)	10000 (у.о.)	50000 (у.о.)	30000 (у.о.)

Порівняння результатів двох досліджень, що враховують біматричну гру та статистику реалізації загроз зловмисником, наведено на рис. 6.

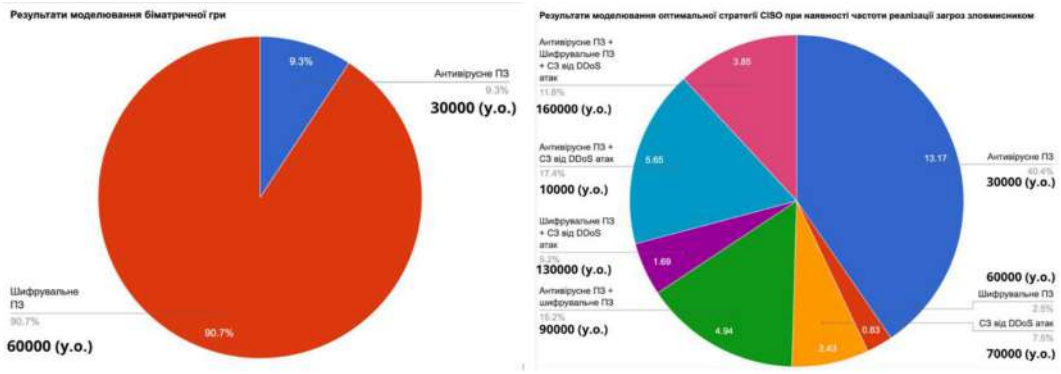

Рис. 6. Порівняння результатів двох досліджень за біматричною грою та частотами реалізації загроз зловмисником

Згідно з проведеним моделюванням на основі безкоаліційної гри двох гравців із ненульовою сумою, оптимальна стратегія супротивника визначала доцільність використання антивірусного ПЗ у 9 % випадків та шифрувального ПЗ у 91 %, із прогнозованою сумарною вартістю впровадження до 90 000 у.о. Таким чином, біматричне моделювання вказало на ефективність комбінованого залучення двох ЗЗІ (антивірусного та шифрувального ПЗ), тоді як моделювання у чистих стратегіях при відомому розподілі ймовірностей дозволило визначити оптимальний вибір CISO з погляду максимізації показника ROSI. Зокрема, використання лише антивірусного ПЗ із вартістю 30 000 у.о. забезпечує найвищий виграш, що свідчить про оптимальність цієї стратегії за заданих умов.

У межах другого етапу основної частини запропонованої методики здійснюється побудова мережевої моделі проєкту впровадження СУІБ, яка стала основою для подальшого аналізу та оптимізації за допомогою методів мережевого аналізу та керування проєктами.

Відповідно до формули (3), нехай розроблена мережа представляється у вигляді набору чисел (11, 12), де перше значення – множина вершин, а друге – множина робіт. CISO увідповіднив літерні позначення з найменуванням виконуваних робіт на основі власних експертних оцінок та аналізу специфіки проєкту. Було використано умовні числові значення, що співвідносяться з аналітичними звітами провідних міжнародних агентств (ENISA, Gartner, BSI) [19]–[21], а також із практичним досвідом і експертними оцінками. На основі проведеного аналізу та кореляції даних побудовано таблицю (див. рис. 7), яка містить заплановані та прискорені строки виконання робіт, відповідні фінансові та людські витрати. Таким чином, кожну роботу проєкту можна виконати у стандартний строк із типовими витратами або у скорочений строк із підвищеним ресурсним навантаженням.

Перше дослідження стосується аналізу критичного шляху за умов стандартних (запланованих) строків виконання робіт. Для його проведення всі параметри мережі, обчислені згідно з формулами (4)–(7), і узагальнено у зведеній таблиці, яка відображає критичний шлях розробленої моделі проєкту СУІБ.

Аналіз критичного шляху при запланованих строках показав загальну тривалість проєкту: 44 од. часу, із загальними витратами 344 000 у.о. На цьому етапі CISO, як керівник проєкту, зосереджується на критичних роботах, розуміючи, що саме вони визначають загальну тривалість. Доцільно перейти до аналізу ефективності проєкту за умов прискореного виконання всіх робіт.

Критичні роботи залишилися незмінними, однак тривалість проєкту скоротилася з 44 до 35,5 од. часу (приблизно на 20 %). Цього вдалося досягти шляхом суттєвого збільшення фінансових і людських ресурсів. Загальна вартість проєкту зросла з 344 000 до 453 000 у.о., на 32 %. Наслідком неправильного рішення щодо прискорення усіх робіт може стати нераціональне використання ресурсів. Третє дослідження зосереджується на аналізі критичного шляху за умови прискорення лише критичних робіт.

Аналіз даних показує, що прискорення лише критичних робіт не змінило б загальну тривалість проєкту порівняно з повним прискоренням, вона залишилася на рівні 35,5 од. часу. Однак вартість проєкту склала 433 000 у.о., що на 5 % менше, ніж у випадку прискорення всіх робіт, і свідчить про оптимальне використання ресурсів. У порівнянні зі звичайним графіком, витрати зросли на 25 %, але при цьому тривалість скоротилася на 8,5 од. часу (≈20 %), що підтверджує доцільність вибору цього сценарію.

З метою розширення аналізу було досліджено вплив прискорення лише некритичних робіт. Результати показали, що загальна тривалість проєкту залишилася на рівні 44 од. часу, однак вартість зросла до 364000 у.о., що на 6 % більше, ніж у базовому сценарії з аналогічною тривалістю. Таким чином, прискорення некритичних робіт не впливає на строк завершення проєкту, але призводить до неефективного використання ресурсів. Результати наведено на рис. 8.

	Робота	A	B	C	D	E	F	G	H	I	J	L	N
	Попередня вершина $i \in K$	1	2	3	3	4	5	6	6	7	8	9	10
	Наступна вершина $j \in K$	2	3	4	5	5	6	7	8	8	9	10	11
Заплановані строки	Тривалість dp_{ij}	4 од. часу	2 од. часу	2 од. часу	6 од. часу	6 од. часу	4 од. часу	3 од. часу	16 од. часу	6 од. часу	5 од. часу	3 од. часу	2 од. часу
	Витрати, $expp_{ij}$	25000 у.о.	7000 у.о.	7000 у.о.	25000 у.о.	30000 у.о.	25000 у.о.	20000 у.о.	100000 у.о.	10000 у.о.	60000 у.о.	20000 у.о.	15000 у.о.
	Необхідна кількість залучених осіб, $pplp_{ij}$	2	2	1	3	2	3	2	5	3	4	2	3
Прискорені строки	Тривалість, df_{ij}	3 од. часу	1,5 од. часу	1,5 од. часу	4,5 од. часу	5 од. часу	3 од. часу	2 од. часу	13 од. часу	5 од. часу	5 од. часу	2,5 од. часу	1 од. часу
	Витрати, $expf_{ij}$	30000 у.о.	10000 у.о.	9000 у.о.	35000 у.о.	40000 у.о.	35000 у.о.	25000 у.о.	140000 у.о.	15000 у.о.	60000 у.о.	24000 у.о.	30000 у.о.
	Необхідна кількість залучених осіб $pplf_{ij}$	2	3	1	4	3	3	2	7	3	4	2	3

Рис. 7. Зведення інформації щодо тривалості робіт та витрат ресурсів

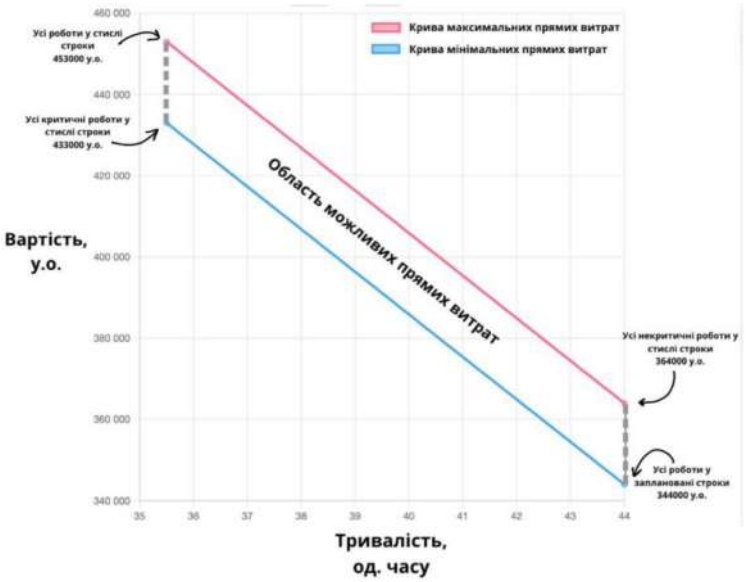

Рис. 8. Графік залежності між тривалістю проекту та прямими витратами

У результаті розрахунків побудовано графік, що наочно демонструє залежність між тривалістю проєкту та прямими витратами. Із графіка видно, що прискорення некритичних робіт не впливає на строки, але збільшує витрати на 6 % без жодної вигоди щодо часу. Прискорення всіх робіт дозволяє зменшити тривалість проєкту до 35,5 од. часу, однак вартість зростає на 32 %. Натомість, прискорення лише критичних робіт забезпечує аналогічне скорочення строків при меншому зростанні витрат лише на 26 %. Таким чином, CISO отримує інструмент для обґрунтованого прийняття управлінських рішень: визначати оптимальний баланс між строками реалізації проєкту та фінансовими ресурсами, виявляти критично важливі роботи та уникати нераціонального розподілу ресурсів.

Показники найбільш раннього можливого початку виконання роботи та найбільш пізнього часу для її завершення дозволяють побудувати гістограми, що відображають фактичне виконання робіт у часі, потребу у фінансових ресурсах та рівень залучення персоналу протягом усього проєкту. Такі візуалізації дають CISO змогу більш раціонально планувати проєкт, а залученим особам обрати найкращу конфігурацію реалізації з урахуванням доступних ресурсів.

Запропонована комплексна методика побудови СУІБ на основі багатокритеріального аналізу та мережевого моделювання дозволяє перейти від абстрактного уявлення до чітких кількісних оцінок, необхідних для ефективного планування, розподілу ресурсів та ухвалення обґрунтованих управлінських рішень. Такий підхід є особливо корисним як для фахівця з інформаційної безпеки, так і для керівництва організації, адже забезпечує прозорість, обґрунтованість і гнучкість на всіх етапах реалізації проєкту побудови СУІБ.

Висновки та перспективи подальших досліджень

Запропонована методика побудови СУІБ складається з трьох етапів (початковий, основний, впроваджувальний) і поєднує метод аналізу мереж, метод аналізу ієрархій та математичний апарат теорії ігор. На першому етапі основної частини методики вирішується багатокритеріальна задача вибору базової методики побудови СУІБ для конкретної організації. Порівняння результатів MAM і MAI на основі визначених критеріїв показало схожі висновки, найдоцільнішою є методика IT-Grundschutz (54 % та 33 % відповідно), причому MAM краще усереднює оцінки, виключаючи явно недоцільні варіанти.

Другий етап основної частини запропонованої методики присвячено визначенню оптимальних засобів захисту інформації з використанням теорії ігор. Запропоновано спрощену модель із чистими стратегіями для CISO, засновану на ймовірностях реалізації загроз зловмисником. Практичне моделювання показало, що найбільш доцільним варіантом є впровадження антивірусного ПЗ вартістю 30 000 у.о., що забезпечує максимальний виграш для CISO.

Третій етап базується на методі аналізу мереж для побудови моделі проєкту впровадження СУІБ, виявлення критичних і некритичних робіт, аналізу резервів часу та оптимізації використання ресурсів. Моделювання продемонструвало два варіанти ресурсних інвестицій: 44 од. часу та 344 000 у.о. при стандартних строках виконання усіх робіт проекту або 35,5 од. часу та 433 000 у.о. при прискоренні виконання усіх критичних робіт. Показано, що помилкові управлінські рішення можуть призвести до необґрунтованого зростання витрат без наявних переваг. Методика дозволяє уникнути цього завдяки попередньому моделюванню та візуалізації результатів у формі таблиць і графіків, що спрощує аргументацію перед керівництвом.

Подальші дослідження передбачають врахування невизначеності, ризиків та можливих змін у проєкті, проведення оцінювання ризиків, а також побудову графа атак для моделювання потенційних сценаріїв компрометації системи. Це дозволить поєднати управління проєктом із управлінням ризиками та забезпечити адаптивне планування СУІБ в умовах динамічного середовища.

Список використаної літератури

1. *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. (б. д.). iso.org. https://www.iso.org/standard/27001

2. *IT-Grundschutz*. (б. д.). Federal Office for Information Security. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

3. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, Постанова Національного банку України № 95 (2017) (Україна). https://zakon.rada.gov.ua/laws/show/v0095500-17#Text

4. Hoban, S. (2024, 19 листопада). *What is A resource in project management? 7 key types to know*. dpm. https://thedigitalprojectmanager.com/projects/managing-schedules/what-is-resource-project-management/

5. Gordon, L. A., & Loeb, M. P. (б. д.). The economics of information security investment. У *Economics of information security*. Kluwer Academic Publishers. https://doi.org/10.1007/1-4020-8090-5_9

6. Фукс, М. А. (2024). Моделювання багатокритеріальної задачі оптимізації вибору методики побудови СУІБ методами Томаса Сааті. У *Радіоелектроніка та молодь у XXI столітті* (с. 92–93). ХНУРЕ.

7. Жаринова, С., & Бабенко, А. (2014). Оптимізація інвестицій в інформаційну безпеку підприємства. *Науково-технічний журнал*, *3*(83), 115.

8. Lemeshko, O., Yeremenko, O., Kurenko, V., & Fuks, M. (2024). Method of designing a cyber-resilient information and communication network. *Problemi telekomunìkacìj*, (2(35)), 14–25. https://doi.org/10.30837/pt.2024.2.02

9. Пшеничних, С. В., Добринін, І. С., & Клочкова, Д. Ю. (2023). Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації. *Проблеми телекомунікацій*, *1*(32), 45–58. https://doi.org/10.30837/pt.2023.1.04

10. Saaty, T. L. (б. д.). The analytic network process. У *Decision making with the analytic network process* (с. 1–26). Springer US. https://doi.org/10.1007/0-387-33987-6_1

11. Saaty, T. L., & Vargas, L. G. (2012). *Models, methods, concepts & applications of the analytic hierarchy process*. Springer US. https://doi.org/10.1007/978-1-4614-3597-6

12. Фукс, М. А., & Добринін, І. С. (2023). Визначення стратегії захисту інформації на основі безкоаліційної гри двох гравців із ненульовою сумою. У *Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023)* (с. 185–188). ХНУРЕ. https://openarchive.nure.ua/handle/document/25471

13. *CAPEC – CAPEC list version 3.9*. (2019, 30 вересня). CAPEC – Common Attack Pattern Enumeration and Classification (CAPEC™). https://capec.mitre.org/data/index.html

14. *OWASP Top Ten | OWASP Foundation*. (б. д.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-project-top-ten/

15. *GitHub – CVEProject/cvelistV5: CVE cache of the official CVE List in CVE JSON 5 format*. (б. д.). GitHub. https://github.com/CVEProject/cvelistV5

16. *Common vulnerability scoring system CVSS SIG*. (б. д.). FIRST – Forum of Incident Response and Security Teams. https://www.first.org/cvss/

17. Phillips, D. T. (1981). *Fundamentals of network analysis*. Prentice-Hall.

18. Aston, B. (2025, 29 липня). *PERT vs CPM: 8 key differences for project managers to grasp*. dpm. https://thedigitalprojectmanager.com/project-management/pert-vs-cpm

19. *Publications | ENISA*. (б. д.). ENISA. https://www.enisa.europa.eu/publications#c3=2014&c3=2024&c3=false&c5=publicationDate&reversed=on&b_start=0

20. *Business and technology insights and trends*. (б. д.). GARTNER. https://www.gartner.com/en/insights

21. *Federal office for information security*. (б. д.). BSI. https://www.bsi.bund.de/EN/Home/home_node.html

References

1. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. (n.d.). iso.org. https://www.iso.org/standard/27001

2. *IT-Grundschutz*. (n.d.). Federal Office for Information Security. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

3. *On the approval of the Regulation on the organization of measures to ensure information security in the banking system of Ukraine*, Resolution of the National Bank of Ukraine No. 95 (2017) (Ukraine). https://zakon.rada.gov.ua/laws/show/v0095500-17#Text

4. Hoban, S. (2024, November 19). *What is a resource in project management? 7 key types to know*. dpm. https://thedigitalprojectmanager.com/projects/managing-schedules/what-is-resource-project-management/

5. Gordon, L. A., & Loeb, M. P. (n.d.). *The economics of information security investment*. In *Economics of information security*. Kluwer Academic Publishers. https://doi.org/10.1007/1-4020-8090-5_9

6. Fuks, M. A. (2024). Modeling a multi-criteria optimization problem for selecting a methodology for building an ISMS using Thomas Saaty's methods. In Radioelectronics and Youth in the XXI Century (pp. 92–93). Kharkiv National University of Radioelectronics (KhNURE).

7. Zharinova, S., & Babenko, A. (2014). *Optimization of investments in the information security of an enterprise*. Scientific and Technical Journal, 3(83), 115.

8. Lemeshko, O., Yeremenko, O., Kurenko, V., & Fuks, M. (2024). Method of designing a cyber-resilient information and communication network. *Problemi telekomunìkacìj*, (2(35)), 14–25. https://doi.org/10.30837/pt.2024.2.02

9. Pshenychnych, S., Dobrynin, I., & Klochkova, D. (2023). Mathematical model of optimal selection of information security measures in the design of an integrated security system at an informatization facility. *Problemi telekomunìkacìj*, (1(32)), 45–58. https://doi.org/10.30837/pt.2023.1.04

10. Saaty, T. L. (n.d.). *The analytic network process*. In *Decision making with the analytic network process* (pp. 1–26). Springer US. https://doi.org/10.1007/0-387-33987-6_1

11. Saaty, T. L., & Vargas, L. G. (2012). *Models, methods, concepts & applications of the analytic hierarchy process*. Springer US. https://doi.org/10.1007/978-1-4614-3597-6

12. Fuks, M. A., & Dobrynin, I. S. (2023). Determining the strategy of information protection based on a non-cooperative two-player game with a non-zero sum. In *Information and Communication Technologies and Cybersecurity (ICTC-2023)* (pp. 185–188). Kharkiv National University of Radio Electronics. https://openarchive.nure.ua/handle/document/25471

13. *CAPEC – CAPEC list version 3.9*. (2019, 30 вересня). CAPEC – Common Attack Pattern Enumeration and Classification (CAPEC™). https://capec.mitre.org/data/index.html

14. *OWASP Top Ten | OWASP Foundation*. (б. д.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-project-top-ten/

15. *GitHub – CVEProject/cvelistV5: CVE cache of the official CVE List in CVE JSON 5 format*. (б. д.). GitHub. https://github.com/CVEProject/cvelistV5

16. *Common vulnerability scoring system CVSS SIG*. (б. д.). FIRST – Forum of Incident Response and Security Teams. https://www.first.org/cvss/

17. Phillips, D. T. (1981). *Fundamentals of network analysis*. Prentice-Hall.

18. Aston, B. (2025, July 29). *PERT vs CPM: 8 key differences for project managers to grasp*. dpm. https://thedigitalprojectmanager.com/project-management/pert-vs-cpm

19. *Publications | ENISA*. (n.d.). ENISA. https://www.enisa.europa.eu/publications#c3=2014&c3=2024&c3=false&c5=publicationDate&reversed=on&b_start=0

20. *Business and technology insights and trends*. (n.d.). GARTNER. https://www.gartner.com/en/insights

21. *Federal Office for Information Security*. (n.d.). BSI. https://www.bsi.bund.de/EN/Home/home_node.html

Дата першого надходження рукопису до видання: 23.09.2025
Дата прийнятого до друку рукопису після рецензування: 20.10.2025
Дата публікації: 28.11.2025