DOI: 10.58254/viti.9.2026.28.363

УДК 004.056:62-722:005.52

Хавер А. В. ORCID: 0009-0003-4731-914X (ДУІКТ)

МЕТОД ПРІОРИТЕЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ ТЕХНОЛОГІЧНИХ СИСТЕМ ПРОМИСЛОВИХ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЛЯ ПРОТИДІЇ ДЕСТРУКТИВНИМ КІБЕРАТАКАМ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

У статті вирішується завдання забезпечення функціонування технологічних систем промислових об’єктів критичної інфраструктури в умовах обмежених ресурсів та постійно зростаючих кіберзагроз.

Під впливом поточних воєнних і соціально-економічних факторів ресурсне забезпечення промислових об’єктів критичної інфраструктури має тенденцію до скорочення та обмеження, що зумовлює необхідність оптимізації розподілу наявних ресурсів для реалізації заходів кібербезпеки, особливо по відношенню до такого критично важливого компоненту, як технологічна система.

Дослідження спрямоване на визначення ролі і місця запропонованого методу, його поетапного опису з відображенням чіткого й злагодженого алгоритму пріоритезації заходів кібербезпеки технологічних систем промислових об’єктів критичної інфраструктури для протидії деструктивним кібератакам в умовах обмежених ресурсів.

Описані підходи спираються на основи теорії управління ресурсами й елементи операційних досліджень, зокрема задачі розподілу, пріоритезації та оптимізації обмежених ресурсів. Разом з тим, метод дозволяє приймати управлінські рішення щодо кібербезпеки технологічних систем в умовах невизначеності. В якості математичного апарату для виконання одного з ключових підетапів методу, який дозволяє здійснити моделювання потенційних деструктивних кібератак на активи технологічної системи, запропоновано використати імітаційно-аналітичне структурне моделювання із застосуванням кольорових сіток Петрі. Для вирішення завдань окремих підетапів методу, що зумовлюють прийняття рішень в умовах невизначеності, обрано PERT-підхід.

Практична цінність використання методу полягає у можливості його застосування для підтримки прийняття управлінських рішень під час формування Плану реалізації заходів кібербезпеки для протидії деструктивним кібератакам на технологічні системи промислових об’єктів критичної інфраструктури на рік.

Таким чином, метод враховує низку реальних практичних факторів, які є необхідними елементами для визначення найбільш ресурсооптимальних і ефективних заходів кібербезпеки для протидії деструктивним кібератакам на технологічну систему промислового об’єкта критичної інфраструктури в умовах обмежених ресурсів та враховує обґрунтування прийнятих рішень з їхнім відповідним документальним оформленням.

Ключові слова: *кібербезпека, метод пріоритезації заходів кібербезпеки, промислові об’єкти критичної інфраструктури, технологічна система, ресурсна обмеженість, управління ресурсами.*

A. Khaver. Method for prioritizing cybersecurity measures in technological systems of industrial critical infrastructure facilities to counter destructive cyberattacks under resource constraints

This paper addresses the problem of ensuring the reliable functioning of technological systems of industrial critical infrastructure facilities under conditions of limited resources and continuously increasing cyber threats. Under the influence of ongoing military and socio-economic factors, the resource provision of industrial critical infrastructure facilities tends to decrease, which necessitates the optimization of available resource allocation for the implementation of cybersecurity measures, particularly with respect to such a critically important component as the technological system.

The study is aimed at defining the role and place of the proposed method, as well as providing its step-by-step description through a coherent and structured algorithm for prioritizing cybersecurity measures in technological systems of industrial critical infrastructure facilities to counter destructive cyberattacks under resource constraints.

The proposed approaches are based on the principles of resource management theory and elements of operations research (in particular, problems of allocation, prioritization, and optimization of limited resources). In addition, the method enables informed managerial decision-making in the field of cybersecurity of technological systems under conditions of uncertainty. As a mathematical tool for one of the key sub-stages of the method, which allows modeling potential destructive cyberattacks on technological system assets, simulation-analytical structural modeling using Colored Petri Nets is employed. To address tasks of individual sub-stages associated with decision-making under uncertainty, the PERT approach is applied.

The practical value of the method lies in its applicability for supporting managerial decision-making during the development of cybersecurity implementation plans aimed at countering destructive cyberattacks on technological systems of industrial critical infrastructure facilities over a planning period.

Thus, the method takes into account a set of real-world practical factors that are essential for identifying the most resource-efficient and effective cybersecurity measures to counter destructive cyberattacks on technological systems of

industrial critical infrastructure under resource constraints, while also ensuring the justification and proper documentation of the decisions made.

Keywords: *cybersecurity, cybersecurity measures prioritization method, industrial critical infrastructure, technological system, resource constraints, resource management.*

Постановка завдання.

Ефективне та раціональне впровадження заходів кібербезпеки у технологічних системах промислових об’єктів критичної інфраструктури є ключовою передумовою забезпечення їхнього належного рівня кіберстійкості. Особливої актуальності це питання набуває в умовах обмеженості ресурсів, зокрема часових, людських та фінансових.

Стан ресурсної обмеженості стає характерною ознакою функціонування таких об’єктів в Україні, що зумовлено сукупністю факторів, серед яких: економічні обмеження, дефіцит кваліфікованого персоналу, постійне розширення та ускладнення ландшафту кіберзагроз, зростання кількості кібератак, а також необхідність оперативного реагування на кіберінциденти.

У зв’язку з цим виникає необхідність забезпечення оптимального використання наявних ресурсів із метою підтримання сталого функціонування технологічного процесу промислового об’єкта критичної інфраструктури та підвищення рівня кіберстійкості його активів. Це, у свою чергу, спрямовано на мінімізацію ризику реалізації деструктивних кібератак, здатних спричинити найбільш критичні наслідки. Для вирішення зазначеної проблеми автором пропонується відповідний метод пріоритезації заходів кібербезпеки.

Аналіз літератури.

Враховуючи аналіз актуальних публікацій на платформі “Web of Science” та “Google Scholar”, питаннями дослідження методів управління ресурсами та пріоритезації заходів здебільшого займаються іноземні науковці. Вони пропонують різні підходи та алгоритми, які не завжди безпосередньо мають відношення до галузі кібербезпеки або промислових об’єктів критичної інфраструктури, проте їхній досвід можна враховувати й у цьому контексті. Зокрема, алгоритм пріоритезації для розподілу керування в системах із пріоритетами задач, що базується на рекурсивному перетині допустимих областей, запропонували автори [1]. Крім того, альтернативні підходи наведено у дослідженні [2], де автори зосереджуються на пріоритезації та розподілі ресурсів у складних програмах із великою кількістю проєктів на основі портфельного об’єднання. Питання розподілу фінансового ресурсу на забезпечення різних сегментів кібербезпеки (комплаєнс, інструменти та технології, навчання та проактивний кіберзахист) банківських установ при обмеженому фінансуванні підіймається у дослідженні [3]. Автори джерела [3] притримуються ризик-орієнтованого принципу при розподілі коштів на відповідні сегменти кібербезпеки, спираючись на їхню критичність для загальної кіберстійкості системи. Зазначену класичну концепцію використано у дослідженні автора та доповнено у запропонованому методі. Проактивному прогнозуванню кібератак на об’єкти критичної інфраструктури присвячено дослідження [4], у якому мотиваційний фактор суб’єкта кіберзагрози розглядається як ключова детермінанта вибору типу атаки. Зазначене положення підтримується в контексті нижчезапропонованого методу, де мотиваційна складова інтегрується у процес оцінювання та аналізу потенційних сценаріїв кібератак, що крім того враховують їхню ресурсооптимальність і як ключові тези входять до одного з підетапів методу.

На відміну від джерела [5], де пріоритезація заходів кіберзахисту здійснюється на основі потенційних наслідків та якісної оцінки загроз і вразливостей, у запропонованому методі додатково враховується ступінь обмеженості ресурсів на промислових об’єктах критичної інфраструктури (ПОКІ), ресурсовитратність реалізації кібератак з боку суб’єкта кіберзагрози, ефективність та пріоритетність реалізації заходів, що дозволяє більш обґрунтовано визначати пріоритети кібербезпеки в умовах обмежених ресурсів.

Таким чином, жодна із опрацьованих публікацій не пропонувала комплексного підходу для вирішення поставленого завдання, який би включав запропонований автором комплекс взаємодоповнюючих підходів. Проте окремі концепції було використано автором з метою підтвердження своїх припущень або для якісного доповнення методу.

Мета дослідження. Формалізований опис призначення, цільового спрямування, ролі, місця та змісту запропонованого методу пріоритезації заходів кібербезпеки технологічних систем промислових об’єктів критичної інфраструктури для протидії деструктивним кібератакам в умовах обмежених ресурсів.

Основними завданнями дослідження є:

– визначення призначення, цільового спрямування та функціональної ролі запропонованого методу;

– з’ясування місця методу в ієрархічній системі управління кібербезпекою промислового об’єкта критичної інфраструктури;

– викладення змісту методу відповідно до етапності його практичного застосування.

Основна частина.

1. Запропонований автором метод призначений для пріоритезації заходів кібербезпеки технологічних систем промислових об’єктів критичної інфраструктури (ТС ПОКІ) з метою протидії деструктивним кібератакам в умовах обмежених ресурсів. Цільове спрямування методу полягає у забезпеченні досягнення необхідного рівня кіберстійкості ТС ПОКІ шляхом раціонального розподілу наявних ресурсів та визначення пріоритетності реалізації заходів кібербезпеки з урахуванням необхідних факторів, зокрема найбільш вагомого – реальних кіберзагроз.

Метод призначений для застосування щодо ТС ПОКІ, оскільки його цільовим спрямуванням є забезпечення кіберстійкості технологічного процесу. Водночас концептуально метод є придатним для застосування і до традиційних комунікаційних систем, що функціонують на об’єктах критичної інфраструктури, однак у такому випадку потребує адаптації з урахуванням специфіки їх функціонування та відсутності технологічних процесів, характерних для промислових систем.

Метод може бути застосований до промислових об’єктів критичної інфраструктури (ПОКІ) I–IV категорій критичності [6]. Для об’єктів I–II категорій, в окремих випадках, доцільною є автоматизація окремих підетапів методу (в частині підетапу 3.1).

Викладені в методі підходи придатні до застосування як в умовах достатнього рівня ресурсного забезпечення для реалізації заходів кібербезпеки ТС ПОКІ проти деструктивних кібератак – тоді він дозволяє визначити доцільність і пріоритетність реалізації таких заходів, так і в умовах обмеженості ресурсів – тоді він дозволяє визначити активи і заходи, які потребують першочергової уваги для збереження необхідного рівня кіберстійкості ТС ПОКІ.

Функціонально метод виконує роль інструменту підтримки прийняття управлінських рішень для уповноваженої особи з кібербезпеки (Chief Information Security Officer, CISO) у процесі формування Плану реалізації заходів кібербезпеки для протидії деструктивним кібератакам на ТС ПОКІ, враховуючи рівень ресурсного обмеження.

Можна сказати, що метод пріоритезації заходів кібербезпеки ТС ПОКІ – це сукупність взаємопов’язаних алгоритму, процедур та моделей, спрямованих на формалізоване визначення пріоритетності заходів кібербезпеки шляхом комплексного врахування рівня критичності активів ТС ПОКІ, цільових пріоритетів підвищення їхньої кіберстійкості, оцінки та прогнозування коливань ресурсного забезпечення впродовж планового періоду, визначення рівня обмеженості ресурсів, вибору відповідного управлінського режиму, а також аналізу потенційних деструктивних кібератак і обчислення їхнього загального ресурсного шляху з метою забезпечення необхідного рівня кіберстійкості технологічних систем в умовах обмеженості ресурсів.

2. Місце методу у ієрархічній системі управління кібербезпекою ПОКІ зображено на рисунку 1, що структурно являє собою п’ятирівневу пірамідальну модель, яка наочно зображує черговість застосування основних загальноприйнятих етапів для забезпечення кібербезпеки, кіберстійкості та адаптивності ТС ПОКІ, що і є кінцевою метою (рівень 5).

Проаналізуємо рівні, зображені на вищезазначеній моделі більш детально.

Рівень 1 є початковим етапом формування основ кібербезпеки сучасних українських ТС ПОКІ. На практиці його реалізація здійснюється через розробку та впровадження комплексу організаційно-нормативних документів, передбачених серією нормативних документів із технічного захисту інформації України (НД ТЗІ), а також через застосування профілів безпеки.

Рис. 1. Концептуальна пірамідальна модель ієрархічної системи управління кібербезпекою ПОКІ з урахуванням запропонованого методу

НД ТЗІ регламентують: формування концепції кіберзагроз, побудову моделі порушника, визначення потенційних каналів несанкціонованого доступу, а також встановлення вимог до організації заходів кібербезпеки, що в сукупності формує нормативну основу для створення комплексної системи захисту інформації в автоматизованих системах відповідного класу. Згідно з вимогами НД ТЗІ та з урахуванням класу критичності ПОКІ, автоматизовані системи управління технологічними процесами, такі як Basic Process Control System (BPCS) та Safety Instrumented System (SIS), за результатами обстеження та класифікації у більшості випадків відносяться до класу АС-2 (клас АС визначається залежно від потенційних наслідків втрати доступності, конфіденційності або цілісності даних, тому для конкретного об’єкта можуть застосовуватися інші класи). Це зумовлює необхідність впровадження комплексної системи захисту інформації відповідно до встановлених нормативних вимог.

З 2025 року в Україні набрав чинності Порядок розробки профілів безпеки, затверджений Кабінетом Міністрів України. Профілі безпеки дозволяють чітко визначити, які вимоги з кібербезпеки має бути реалізовано в системі, залежно від типу інформації, яку вона обробляє: відкрита, конфіденційна, службова тощо. Профілі безпеки поділяються на: базовий, галузевий, цільовий. На практиці профілі безпеки використовуються разом із НД ТЗІ, що дозволяє адаптувати правила та механізми технічного захисту інформації під конкретні типи систем та притаманні їм ризики.

Таким чином рівень 1 формує концептуально-нормативне підґрунтя всієї кібербезпеки ТС ПОКІ.

Рівень 2 є наступним етапом загальноприйнятої архітектури кібербезпеки ТС ПОКІ та відповідає міжнародним стандартам у галузі оцінювання та управління кіберризиками для ТС ПОКІ. До таких стандартів належать ISO 31000, ISO/IEC 31010 та ISO/IEC 27005,

які формують методологічну основу процесів ідентифікації, аналізу та оцінювання кіберризиків [7]. Зазначені стандарти дозволяють здійснювати систематизований аналіз сценаріїв кібервпливу та їхніх наслідків, однак не передбачають кількісного обґрунтування пріоритетності заходів кібербезпеки з урахуванням обмежених ресурсів і специфіки реалізації деструктивних кібератак у технологічних системах (що враховано в одному з етапів методу).

Отже, рівень 2 створює системну методологічну основу для управління кіберризиками ТС ПОКІ, однак не забезпечує формалізованого механізму оптимізації розподілу захисних ресурсів, що обумовлює необхідність розроблення та впровадження відповідного методу.

Рівень 3 передбачає застосування запропонованого автором методу пріоритезації заходів кібербезпеки для протидії деструктивним кібератакам в умовах обмежених ресурсів. Саме на цьому етапі, маючи вихідні дані, сформовані на першому та другому рівнях, але до початку технічної реалізації заходів кіберзахисту, доцільно застосовувати запропонований метод. Висновки, отримані в процесі його реалізації, дозволяють обґрунтовано прийняти найбільш ефективні управлінські рішення та визначити пріоритетність реалізації заходів кібербезпеки.

Отже, рівень 3 виступає інструментальним етапом моделі, який забезпечує формалізовану оптимізацію розподілу обмежених ресурсів кібербезпеки з урахуванням пріоритетності кіберзагроз.

Рівень 4 передбачає реалізацію практичних заходів кіберзахисту ТС ПОКІ через технічну складову з урахуванням результатів методу. На цьому рівні здійснюється впровадження технічних і організаційних заходів кібербезпеки для визначених підсистем [8]. Реалізація зазначених заходів здійснюється відповідно до положень галузевих стандартів кібербезпеки промислових систем, зокрема серії IEC 62443, а також із використанням рекомендаційних документів NIST, таких як NIST SP 800-82 та NIST SP 1800-10, які застосовуються як практичні керівництва з впровадження заходів кіберзахисту [9].

Таким чином, рівень 4 забезпечує практичну імплементацію управлінських рішень, сформованих на попередніх рівнях, та трансформує результати методу у конкретні технічні й організаційні механізми підвищення кіберстійкості ТС ПОКІ.

3. Метод логічно вписується в систему багаторівневого планування кібербезпеки на ПОКІ (рис. 2). На верхньому рівні ієрархії розташована Концепція кібербезпеки ПОКІ (далі – Концепція), яка визначає стратегічні цілі та орієнтири розвитку системи кібербезпеки на довгострокову перспективу. Заходи відповідно до Концепції конкретизуються у щорічному Плані реалізації заходів кібербезпеки для ПОКІ (в контексті цього дослідження План реалізації заходів кібербезпеки для протидії деструктивним кібератакам на ТС ПОКІ, далі – План), що є документом короткострокового планування (на 1 рік) і розглядається надалі як окремий документ. У свою чергу, План містить перелік заходів кібербезпеки за кожним активом ТС ПОКІ, розподілених за пріоритетністю їх реалізації (першочергові, планові та довгострокові), та призначений для практичного використання відповідними підрозділами кібербезпеки впродовж запланованого періоду.

Результати застосування методу оформлюються у вигляді інформаційних матеріалів, які додаються до Плану та використовуються для обґрунтування прийнятих управлінських рішень.

Для забезпечення адаптивності такого методу передбачено його (або окремих його етапів) повторне застосування впродовж року у разі: форс-мажорних обставин, які значно вплинули або можуть вплинути на систему кібербезпеки ТС ПОКІ, різкої зміни ландшафту кіберзагроз (виникнення нових небезпечних кіберзагроз), непередбачуваної зміни динаміки наявного ресурсного забезпечення на реалізацію заходів кібербезпеки ТС ПОКІ (збільшення або зменшення передбаченого людського, часового або фінансового ресурсу).

У процесі планування заходів щодо забезпечення кібербезпеки ТС ПОКІ на майбутній рік та при використанні методу важливо враховувати результати діяльності за поточний рік,

що дозволяють оцінити наявні ресурси та динаміку їхніх змін з урахуванням попереднього досвіду (накопиченої статистики).

Метод складається з чотирьох основних етапів: підготовчий, операційний, аналітичний та заключний. Виконання кожного з попередніх етапів забезпечує результат, необхідний для виконання наступного.

Рис. 2. Структурно-логічна схема багаторівневого планування кібербезпеки ПОКІ з урахуванням запропонованого методу

Розглянемо етапи методу більш детально.

1. Підготовчий етап методу складається з:

1.1. Оцінки критичності активів і поточного рівня кіберстійкості ТС ПОКІ (окремо за кожним активом ТС ПОКІ з 1-го по 3-й рівень моделі Purdue) [10].

Оцінка критичності активів ТС ПОКІ здійснюється з урахуванням методичних рекомендацій, наведених у додатках до методу, та базується на принципах ризик-орієнтованого управління, зокрема ідеях, закладених у IEC 62443, IEC 61511 та ISO 20815, де критичність визначається через наслідки відмови або компрометації системи. Рекомендації з оцінки рівня критичності активів методу ґрунтуються на багатокритеріальному аналізі з ваговими коефіцієнтами, що дозволяє кількісно оцінити рівень критичності активів за сукупністю факторів (безпека людей, каскадність, єдина точка відмови та інші релевантні фактори) та ранжувати їх для пріоритетного розподілу ресурсів кібербезпеки [11].

Оцінка поточного рівня кіберстійкості активів здійснюється з урахуванням методичних рекомендацій, наведених у додатках до методу, шляхом присвоєння їм кількісного значення за визначеними критеріями: кіберстійкість фізичної та логічної архітектури; повнота забезпечення та коректність конфігурації апаратного/програмного забезпечення та його кіберстійкість; повнота функціонування процесів моніторингу і логування; коректність політики розмежування доступу; ефективність політики усунення вразливостей; ризик перехоплення ланцюжка поставок; ступінь резервування та потенціал відновлення (як єдиний показник), кожен з яких оцінюється в інтервалі [0; 1].

Оцінка критичності та поточного рівня кіберстійкості активів ТС ПОКІ проводиться на підставі наказу (розпорядження) керівника ПОКІ щодо реалізації заходів кібербезпеки на майбутній рік. У зазначеному документі, зокрема, визначається склад експертної комісії та встановлюються строки проведення оцінювання. Склад експертної комісії попередньо визначається CISO та має становити не менше трьох профільних фахівців різного профілю функціональних обов'язків.

Якщо впродовж попереднього року не було функціональних змін у фізично-логічній архітектурі активів ТС ПОКІ, їхня критичність може визначатися на основі результатів оцінювання за попередній рік.

Визначені експерти надають CISO відомості щодо результатів оцінювання критичності активів та їхнього поточного стану кіберстійкості у вигляді Актів оцінки критичності та поточного стану кіберстійкості відповідно, в яких в обов'язковому порядку міститься перелік активів, які підлягали оцінці та їх складових підсистем із зазначенням ступеню їхньої критичності, перелік критеріїв, оцінка та її обґрунтування, а також як підсумок – узагальнені відомості щодо оцінювання кожного активу з використанням статистичної медіани або медіани Кеммелі (як робастної оцінки, що зменшує вплив крайніх значень експертних оцінок). Отримані вагові коефіцієнти підлягають нормалізації таким чином, щоб їх сума дорівнювала одиниці ($\sum wi = 1$), що забезпечує коректність застосування адитивної моделі згортки критеріїв та порівнюваність результатів оцінювання.

На підставі отриманих експертних оцінок щодо поточного стану кіберстійкості активів CISO за допомогою формули зваженої суми нормованих критеріїв розраховується поточний рівень кіберстійкості ТС ПОКІ (загальний для ТС ПОКІ і окремий за кожним активом/підсистемою активу), який відповідно до еталонної таблиці може класифікуватися як: низька кіберстійкість; середня кіберстійкість; задовільна кіберстійкість; висока кіберстійкість; дуже висока кіберстійкість, та оформлюється у вигляді документа "Відомість оцінки поточного рівня кіберстійкості ТС ПОКІ та її активів".

1.2. Формування цільових пріоритетів щодо підвищення рівня кіберстійкості за кожним з активів ТС ПОКІ на плановий період.

Цей підетап здійснюється за контролю CISO з урахуванням вихідних даних підетапу 1.1 (оцінки рівня критичності та поточного рівня кіберстійкості активів ТС ПОКІ), а також пропозицій керівників відповідних напрямків (підрозділів) кібербезпеки ТС ПОКІ. CISO розподіляє усі активи та їхні інформаційні підсистеми за рівнем критичності для функціонування технологічного процесу. Визначення цільових пріоритетів полягає у встановленні CISO, які активи та їхні підсистеми потребують підвищення рівня кіберстійкості впродовж планового періоду і в якому обсязі (наприклад, у одного з критичних активів ТС ПОКІ поточний рівень кіберстійкості "середній", а ціллю є досягнення рівня кіберстійкості не нижче "високого"). Визначені цільові пріоритети мають супроводжуватися оцінкою необхідних ресурсів для їх реалізації та не передбачати надлишкових заходів (лише оптимальні з точки зору ресурсовитрат варіанти заходів). Кінцевим результатом цього підетапу є формування документа – Матриці цільових пріоритетів щодо підвищення рівня кіберстійкості активів ТС ПОКІ.

У контексті протидії впливу деструктивних кібератак на кіберстійкість ТС ПОКІ до активів із підвищеним пріоритетом, як правило, належить інформаційна підсистема SIS. Ще одним важливим критерієм є пріоритетність у підвищенні рівня кіберстійкості активів 2-1 рівнів моделі Purdue, враховуючи, що ці рівні становлять ядро технологічного процесу. Разом із тим, цільові пріоритети мають формуватися так, щоб критичні активи та їхні підсистеми досягали рівня кіберстійкості не нижче "високого" в умовах обмеженості ресурсів. За умови достатності ресурсів цільовим є "дуже високий рівень кіберстійкості".

При формуванні цільових пріоритетів важливим для врахування з боку CISO залишається той факт, що впродовж року показники ресурсу все ще можуть коливатися.

Оскільки рівень коливання ресурсних показників перебуває в умовах невизначеності, доцільно застосувати PERT-підхід та розглянути три можливі сценарії коливання такого ресурсу (песимістичний, найбільш ймовірний та оптимістичний). Для подальшого планування цільових пріоритетів та розрахунку обмеженості ресурсу підетапу 1.3 за основу рекомендується обрати ресурсні показники песимістичного сценарію, оскільки він відповідає принципам консервативного планування.

1.3. Розрахунок можливих коливань ресурсного забезпечення впродовж планового періоду.

Зазначений підетап передбачає врахування можливих коливань наявного ресурсного забезпечення для забезпечення кібербезпеки ТС ПОКІ впродовж планового періоду завдяки використанню PERT-підходу із розглядом трьох сценаріїв: оптимістичного, найбільш ймовірного та песимістичного. Для кожного виду ресурсу (часового, людського, фінансового) визначаються відповідні значення ресурсного забезпечення за кожним зі сценаріїв.

З урахуванням необхідності забезпечення стійкості планування в умовах невизначеності та обмеженості ресурсів, для подальших розрахунків і формування цільових пріоритетів за основу приймаються показники песимістичного сценарію (показники двох інших сценаріїв враховуються як потенційний резерв ресурсного забезпечення).

Оцінка наявних ресурсів і динаміки їх змін з урахуванням попереднього періоду (накопиченої статистики), а також аналітичні прогнози на майбутній період дозволяють визначити раціональні межі варіації ресурсних показників між сценаріями.

Такий підхід дозволяє гарантувати реалізацію заходів кібербезпеки навіть у несприятливих умовах, а у разі покращення ресурсного забезпечення – забезпечує наявність резерву для додаткового підвищення рівня кіберстійкості пріоритетним активам. Таким чином, вибір базових значень ресурсного забезпечення для подальших розрахунків формалізується наступним співвідношенням, зазначеним у формулі (1):

$$R_i^{plan} = R_i^{pes}, \tag{1}$$

де R_i^{plan} – планове значення *i*-го ресурсу, що використовується для подальших розрахунків;
R_i^{pes} – значення *i*-го ресурсу за песимістичним сценарієм;
$i \in \{t, l, f\}$, де *t* – часовий ресурс; *l* – людський ресурс; *f* – фінансовий ресурс.

Результати цього підетапу використовуються як вхідні дані для подальших розрахунків обмеженості ресурсів на операційному етапі (підетап 2.1) й окремо не оформлюються у вигляді самостійного документа.

2. Операційний етап методу складається з:

2.1. Розрахунку обмеженості ресурсів для реалізації заходів кібербезпеки, визначених у межах цільових пріоритетів, для кожного активу ТС ПОКІ на плановий період.

Для розрахунку обмеженості ресурсів як планові значення наявних ресурсів використовуються кількісні показники часових, людських і фінансових ресурсів відповідно до песимістичного сценарію, а також кількісні показники необхідних ресурсів для реалізації цільових пріоритетів щодо підвищення рівня кіберстійкості за кожним з активів ТС ПОКІ на плановий період (результати підетапу 1.2).

Обмеженість ресурсу розраховується за кожним з його видів (часовим, людським і фінансовим, формули (2)–(10)), що в подальшому (з урахуванням низки нижчеописаних факторів), дозволить приймати зважені рішення щодо застосування кожного з них у процесі пріоритезації заходів кібербезпеки ТС ПОКІ. Загальний принцип розрахунку обмеженості ресурсів відповідає формулі (2):

$$K_R = \frac{R_{req}}{R_{avail}}\ , \tag{2}$$

де K_R – коефіцієнт обмеженості ресурсу;
R_{req} – необхідний ресурс;
R_{avail} – доступний ресурс.
При цьому:
$K_R < 1$ – ресурс достатній;
$K_R = 1$ – ресурс граничний;
$K_R > 1$ – дефіцит ресурсу.

Формула розрахунку часового ресурсу реалізації заходу залежить від характеру організації робіт. У разі послідовного виконання робіт часовий ресурс визначається як сума тривалостей усіх робіт, необхідних для виконання відповідного заходу, згідно з формулою (3). Якщо окремі роботи можуть виконуватися паралельно, часовий ресурс реалізації заходу визначається за тривалістю критичного шляху, тобто найдовшого ланцюга взаємозалежних робіт, згідно з формулами (3), (4).

$$T_i = \sum_{j=1}^{mi} t_{ij}, \tag{3}$$

де T_i – часовий ресурс реалізації i-го заходу;
t_{ij} – тривалість j-ї роботи в межах заходу;
m_i – кількість робіт.

$$T_i = max_{p \in P_i}\left(\sum_{j \in P} t_{ij}\right), \tag{4}$$

де T_i – часовий ресурс реалізації i-го заходу;
P_i – множина всіх можливих шляхів виконання робіт у межах i-го заходу;
p – окремий шлях із множини P_i;
t_{ij} – тривалість j-ї роботи, що входить до шляху p.

Рівень обмеженості часового ресурсу обчислюється за формулою (5):

$$K_T = \frac{T_{req}}{T_{avail}}, \tag{5}$$

де K_T – коефіцієнт обмеженості часового ресурсу;
T_{req} – необхідний часовий ресурс;
T_{avail} – доступний часовий ресурс.

Для розрахунку обмеженості людського ресурсу необхідно обчислити загальну витрату певної ролі для реалізації заходів цільового планування відповідно до формули (6):

$$L_r = \sum_{i=1}^{n} h_{ir}, \tag{6}$$

де L_r – загальна трудомісткість ролі;
h_{ir} – людино-години ролі r для заходу i.

Необхідна кількість фахівців конкретної ролі розраховується за формулою (7) (округлення результату здійснюється у більшу сторону):

$$N_r = \frac{L_r}{H_{year}}, \tag{7}$$

де N_r – необхідна кількість фахівців ролі r;
L_r – трудомісткість робіт для ролі r;
H_{year} – ефективний річний фонд робочого часу одного фахівця.

Обмеженість людського ресурсу розраховується згідно з формулою (8), при цьому передбачається, що кожен фахівець виконує роботи в межах однієї ролі без урахування багатофункціонального навантаження):

$$K_L = \frac{N_{req}}{N_{avail}}, \tag{8}$$

де K_L – коефіцієнт обмеженості людського ресурсу;
N_{reg} – необхідна кількість фахівців відповідної ролі, визначена за формулою (7);
N_{avail} – доступна кількість фахівців відповідної ролі, визначена з урахуванням песимістичного сценарію.

Необхідні фінансові ресурси рекомендується розраховувати за формулою (9):

$$F_{req} = F_{sal} + F_{autsors} + F_{soft} + F_{equip} + F_{educ}, \tag{9}$$

де F_{reg} – загальний обсяг необхідного фінансового ресурсу;
F_{sal} – витрати за оплату праці працівників;
$F_{autsors}$ – витрати на аутсорсингові послуги;
F_{soft} – витрати на придбання або оновлення необхідного програмного забезпечення;
F_{equip} – витрати на придбання або модернізацію обладнання;
F_{educ} – витрати на навчання та підвищення кваліфікації персоналу.

Обмеженість фінансового ресурсу розраховується за формулою (10):

$$K_F = \frac{F_{req}}{F_{avail}}, \tag{10}$$

де F_{reg} – загальний обсяг необхідного фінансового ресурсу;
F_{avail} – загальний обсяг доступного фінансового ресурсу.

Таким чином, результатом цього підетапу є визначення рівня обмеженості за кожним видом ресурсу, а також формування документа "Відомість оцінки обмеженості ресурсів для реалізації стратегічних цільових пріоритетів кібербезпеки активів ТС ПОКІ".

2.2. Вибору управлінського режиму щодо збереження або підвищення рівня кіберстійкості.

Вибір управлінського режиму здійснюється на основі значень коефіцієнтів обмеженості ресурсів K_T, K_L, K_F, отриманих на підетапі 2.1.

За результатами аналізу практичних кейсів, на підприємствах критичної інфраструктури дефіцит одного ресурсу (часового, людського або фінансового) до 30–40 % дозволяє підтримувати основні операційні процеси (узагальнення практики експлуатації ТС ПОКІ). Тому в подальшому дослідженні враховуємо, що критичним порогом обмеженості ресурсу вважається 40 % (якщо ресурсна обмеженість нижча 40 % хоча б за одним з видів ресурсу впродовж тривалого часу (до пів року) ТС ПОКІ з високою долею ймовірності вразлива до деструктивних кібератак).

Загалом можна сформулювати таке твердження, що на цьому етапі методу вважається, що при дефіциті одного з ресурсів, який не перевищує 40 %, можлива його часткова компенсація завдяки іншим видам ресурсів (часового, людського та фінансового) за умови адаптації управлінського режиму та корекції цільових пріоритетів. Такий підхід відповідає

нормативному (при незначних обмеженнях, до 20 %) та адаптивному (при обмеженнях понад 20 %) управлінським режимам. Вартий уваги і той факт, що у разі нормативного управлінського режиму серед цільових пріоритетів заходів із підвищення кіберстійкості залишаються всі активи 3-1 рівнів моделі Purdue (так як вони становлять основу технологічного процесу) [7]. У разі ж адаптивного управлінського режиму серед заходів із підвищення кіберстійкості залишаються всі активи 2-1 рівнів моделі Purdue та ключові активи 3-го рівня моделі Purdue (критичні міжрівневі вузли 3-го рівня, що мають найбільший вплив на безпеку та безперервність виробництва).

Якщо обмеженість виникає одразу за двома видами ресурсу та не перевищує 40 % за кожним з них, то можливо забезпечити підвищення рівня кіберстійкості лише для активів 2-1 рівня моделі Purdue (для 3-го рівня моделі Purdue – збереження поточного рівня кіберстійкості). Такий підхід відповідає селективному (якщо обмеження не значні < 20 %) та обмежувальному управлінським режимам (якщо обмеження значні > 20 %). Аналіз показує, що найбільш критичною комбінацією подвійної ресурсної обмеженості для ТС ПОКІ є одночасний дефіцит людського та часового ресурсів, оскільки така ситуація безпосередньо унеможливлює практичну реалізацію заходів кібербезпеки незалежно від рівня фінансового забезпечення. На відміну від фінансового дефіциту, який може бути компенсований управлінськими рішеннями, кадрово-часові обмеження мають високий рівень інерційності та істотно впливають на безперервність технологічного процесу.

Якщо існує обмеженість за трьома видами ресурсу, підвищення кіберстійкості значно ускладнюється і переходить в режим “збереження поточного рівня кіберстійкості”. Такий підхід відповідає обмежувальному (якщо обмеження не значні < 20 % за кожним видом ресурсу) та кризовому (якщо обмеження значні > 20 % за кожним видом ресурсу) управлінським режимам. Якщо зберігається обмежувальний підхід, то кіберстійкість підвищується лише для критичних активів 2-1 рівня моделі Purdue. У разі переходу на кризовий управлінський режим, головним завданням стає збереження поточного рівня кіберстійкості активів 2-1 рівня моделі Purdue [12].

Результатом етапу 2.2 є визначення вектору подальшого стратегічного руху та відбір активів ТС ПОКІ (залежно від управлінського режиму, який обрано), для яких в подальшому буде здійснюватися розрахунок загального ресурсного шляху деструктивної кібератаки в рамках аналітичного етапу методу.

Таким чином, вибір управлінського режиму безпосередньо впливає на подальшу пріоритезацію заходів кібербезпеки, оскільки визначає область аналізу та дозволяє сфокусуватися на активах відповідних рівнів моделі Purdue, для яких реалізація таких заходів є першочерговою за наявного обсягу ресурсів.

Кінцевим результатом цього підетапу є формування “Матриці вибору управлінського режиму та відбору активів ТС ПОКІ”, яка встановлює відповідність між рівнем ресурсної обмеженості, обраним управлінським режимом і переліком активів, що підлягають подальшому аналізу.

2.3. Визначення структури розподілу ресурсів між пріоритетними активами ТС ПОКІ.

Після вибору управлінського режиму здійснюється розподіл наявного обсягу ресурсів між його відповідними пріоритетними групами активів ТС ПОКІ. При цьому, незалежно від обраного управлінського режиму необхідно виділяти щонайменше мінімально необхідну кількість ресурсів на кібербезпеку активів вищих рівнів моделі Purdue (3-го рівня моделі), навіть в умовах дефіциту ресурсів (за виключенням кризового управлінського режиму). Вищезазначене обумовлено функціональними характеристиками 3-го рівня моделі, а саме – забезпеченням міжрівневої взаємодії, диспетчеризацією, збором технологічних даних та підтримкою безперервності виробництва. У зв’язку з цим, управлінський режим визначає не лише перелік активів, що підлягають подальшому ранжуванню за рівнем критичності, але й встановлює пропорції розподілу ресурсів між відповідними групами активів.

Для формалізації розподілу ресурсів виділяються три групи активів:

Група А: активи 1–2 рівнів моделі;

Група В: критичні активи 3 рівня моделі;

Група С: інші активи 3 рівня моделі (допоміжні системи управління та моніторингу).

Рекомендована автором відповідність між управлінським режимом і структурою розподілу ресурсів між групами активів наведена у таблиці 1. Нищенаведені значення отримані в межах запропонованого методу та відображають авторське бачення раціонального розподілу ресурсів залежно від управлінського режиму з урахуванням критичності активів, що належать до окремих груп.

Таблиця 1

Рекомендований відсотковий розподіл ресурсів між групами активів в межах обраного управлінського режиму

Назва управлінського режиму	**Рекомендований розподіл за кожним з видів ресурсів**		
	Група А	**Група В**	**Група С**
Нормативний	50 %–60 %	25 %–30 %	15 %–20 %
Адаптивний	60 %–70 %	20 %–25 %	10 %–15 %
Селективний	70 %–80 %	15 %–20 %	5 %–10 %
Обмежувальний	80 %–85 %	10 %–15 %	0 %–5 %
Кризовий	85 %–90 %	10 %–15 %	0 %

Розподіл ресурсів між групами активів здійснюється у вигляді визначення часток ресурсів для кожної групи активів у межах встановлених діапазонів залежно від обраного управлінського режиму. Зазначені у Таблиці 1 відсоткові частки мають інтервальний характер і визначають орієнтовну структуру спрямування ресурсів.

Враховуючи рекомендований ресурсний розподіл згідно з таблицею 1, за участі CISO формується попередній відсотковий розподіл ресурсів між активами ТС ПОКІ (таблиця 2):

Таблиця 2

Попередній відсотковий розподіл ресурсів між активами ТС ПОКІ

Назва управлінського режиму	**Група А (60 %)**						**Група В (25 %)**						**Група С (15 %)**					
Адаптивний	BPCS (поточний рівень кіберстійкості “високий”); SIS (поточний рівень кіберстійкості “високий”)						Manufacturing Execution System (поточний рівень кіберстійкості “середня кіберстійкість”); Historian (поточний рівень кіберстійкості “задовільна кіберстійкість”)						Система управління якістю (QMS) (поточний рівень кіберстійкості “задовільна кіберстійкість”); Система планування та диспетчеризації виробництва (APS / Scheduling) (поточний рівень кіберстійкості “середня кіберстійкість”)					
	T		L		F		T		L		F		T		L		F	
	30 %	30 %	35 %	25 %	25 %	35 %	10 %	15 %	5 %	20 %	10 %	15 %	10 %	5 %	10 %	5 %	11 %	4 %

Розподілені значення відповідно до таблиці 2 мають відносний характер і визначають структуру розподілу ресурсів у межах відповідної групи активів. Такий підхід забезпечує попереднє узгодження спрямування ресурсів перед етапом їх подальшого перерозподілу між заходами кібербезпеки в межах кожного активу. При цьому для розподілу ресурсів у межах окремого активу (підсистем активу) провідну роль відіграють його поточний та цільовий рівні кіберстійкості (визначається в рамках формування цільових пріоритетів, підпункт 1.2 Підготовчого етапу).

Конкретні значення часток часового, людського та фінансового ресурсів у межах зазначених діапазонів уточнюються CISO за результатами аналітичного етапу методу.

Кінцевим документом цього підетапу є відпрацювання Матриці попереднього розподілу ресурсів між активами ТС ПОКІ.

3. Аналітичний етап включає:

3.1. Обчислення загального ресурсного шляху потенційних деструктивних кібератак за кожним активом ТС ПОКІ.

З метою виявлення потенційно вразливих вузлів та/або ділянок (підсистем) технологічної системи, а також можливих способів реалізації деструктивного кібервпливу на технологічний процес з боку суб’єктів кіберзагрози, застосовується імітаційно-аналітичне структурне моделювання з використанням кольорових сіток Петрі [13; 14]. Зазначений підхід дозволяє здійснити формалізований опис можливих векторів і тактик реалізації кібератак та виконати обчислення загального ресурсного шляху потенційних деструктивних кібератак для кожного активу ТС ПОКІ.

Загальний ресурсний шлях деструктивної кібератаки — це інтегральний кількісний показник, який відображає сумарні витрати ресурсів (часових, людських і фінансових), необхідних суб’єкту кіберзагрози для повної реалізації обраного сценарію (тактики) кібератаки на технологічну систему, з урахуванням усіх етапів її виконання та невизначеності умов.

До виконання завдань з обчислення доцільно залучати фахівців напрямку Cyber Threat Intelligence або аналогічного за функціональним призначенням, із урахуванням повного вичерпного переліку актуальних векторів і тактик кіберзагроз.

За результатами моделювання визначаються та оцінюються потенційні вектори реалізації деструктивних кібератак для кожного активу з метою подальшого використання в процесі пріоритезації заходів кібербезпеки в умовах обмежених ресурсів.

Отримані результати використовуються для:

уточнення розподілу ресурсів між групами активів ТС ПОКІ;

обґрунтування порядку пріоритетності реалізації заходів кібербезпеки з урахуванням обраного управлінського режиму;

віднесення заходів кібербезпеки до відповідних класів пріоритетності: першочергової (оперативної) реалізації; планової реалізації; довгострокової реалізації [15].

Результати цього етапу оформлюються у вигляді Імітаційно-аналітичних моделей загального ресурсного шляху потенційних деструктивних кібератак на активи ТС ПОКІ. А результати таких моделей у вигляді ранжування тактик і технік потенційних деструктивних кібератак оформлюються у вигляді Відомості оцінювання загального ресурсного шляху деструктивних кібератак (за активами ТС ПОКІ).

3.2. Розрахунок відносного показника ефективності та пріоритетності заходів кібербезпеки.

У контексті цього дослідження захід кібербезпеки ми можемо вважати ефективним, якщо він суттєво підвищує рівень кіберстійкості активу/підсистеми активу і одночасно при цьому не вимагає надмірних ресурсовитрат. Захід вважається пріоритетнішим у тому випадку, якщо його реалізація забезпечує більший приріст рівня кіберстійкості активу/підсистеми активу на одиницю витраченого ресурсу порівняно з альтернативними заходами.

З метою обґрунтування пріоритетності заходів кібербезпеки в умовах обмежених ресурсів на цьому етапі методу здійснюється оцінювання відносної ефективності кожного заходу щодо окремого активу/підсистеми активу згідно з обраним управлінським режимом, а також формування інтегрального показника його пріоритетності.

Для кожного заходу кібербезпеки і відносний показник ефективності визначається за формулою (11):

$$E_i = \frac{\Delta S_i}{aT_i + bL_i + cF_i}, \tag{11}$$

де ΔS_i – очікуване нарощення рівня кіберстійкості активу, внаслідок впровадження заходу;
T_i – часові витрати;
L_i – людські ресурси;
F_i – фінансові ресурси;
a, b, c – вагові коефіцієнти ресурсів, причому $a + b + c = 1$.

Для подальших розрахунків і оцінки показника ефективності заходу кожен розглянемо з позиції безпекової потреби у захисті та ресурсно-управлінської доцільності.

Безпекова потреба у заході обчислюється за формулою (12):

$$N_i = a_1 K_i + a_2 (1 - S_i) + a_3 (1 - G_i), \tag{12}$$

де K_i – нормована критичність активу;
S_i – нормований поточний рівень кіберстійкості;
G_i – нормований показник загального ресурсного шляху кібератаки;
a_1, a_2, a_3 – вагові коефіцієнти ($a_1 + a_2 + a_3 = 1$).

Такий показник, як G_i пропонується унормувати до інтервалу [0;1] через максимальне значення за формулою (13):

$$G_i = \frac{G_i}{max j G_i}. \tag{13}$$

Оскільки абсолютне максимальне значення загального ресурсного шляху кібератаки апріорі невідоме, нормування показника G_i здійснюється відносно максимального значення, отриманого в межах активів, які розглядаються, або сценаріїв кібератак.

Ресурсно-управлінська доцільність обчислюється згідно з формулою (14):

$$D_i = b_1 (1 - O_i) + b_2 E_i, \tag{14}$$

де O_i – нормований показник обмеженості ресурсів;
E_i – нормований показник ефективності заходу;
b_1, b_2 – вагові коефіцієнти ($b_1 + b_2 = 1$).

При цьому показник обмеженості ресурсів визначається як зважена сума обмеженості часових, людських і фінансових ресурсів згідно з формулою (15):

$$O_i = w_t O_t + w_l O_l + w_f O_f. \tag{15}$$

Кінцевий інтегральний показник пріоритетності заходу обчислюється за формулою (16):

$$P_i = \lambda N_i + (1 - \lambda) D_i, \tag{16}$$

де P_i – інтегральний показник пріоритетності заходу;
$\lambda \in [0;1]$ – коефіцієнт балансу між безпековою потребою та ресурсною доцільністю.

Отримані значення P_i використовуються для ранжування заходів кібербезпеки та їх віднесення до класів пріоритетності в межах кожного активу/підсистеми активу управлінського режиму та відносяться до першочергової (оперативної), планової або довгострокової реалізації.

Наведемо приклад розрахунку відносного показника ефективності та пріоритетності заходів кібербезпеки активів інформаційної підсистеми BPCS на умовних числових значеннях. Для прикладу використаємо такий захід кібербезпеки як сегментація мережі BPCS.

Першочергово обчислимо відносний показник ефективності заходу кібербезпеки для BPCS. Експертно присвоємо значення для змінних $\Delta Si = 0{,}30$; $T_i, L_i, F_i \geq 0$. Врахуємо, що існує обмеженість фінансового ресурсу на реалізацію зазначеного заходу. Припустимо, що існує потреба у 120 тисячах гривень на реалізацію сегментації, а доступно 100 тисяч гривень. Тоді відносний показник обмеженості фінансового ресурсу обчислюватиметься за формулою (17):

$$F_i = \frac{120}{100} = 1{,}2. \tag{17}$$

Врахуємо, що відповідно до формули (11) $T_i = 0{,}40$; $L_i = 0{,}50$; $F_i = 1{,}2$; $\alpha = 0{,}4$; $b = 0{,}3$; $c = 0{,}3$. Таким чином, відносний показник ефективності згідно з формулою (18) дорівнює:

$$E_i = \frac{0{,}30}{0{,}67} = 0{,}448; E_i \approx 0{,}45. \tag{18}$$

Наступним кроком розрахуємо безпекову доцільність сегментування мережі згідно з формулою (12).

Задамо значення для $K_i = 0{,}80$; $S_i = 0{,}40$; а показник G_i розрахуємо через максимальне значення загального ресурсного шляху деструктивної кібератаки для конкретного активу/підсистеми активу згідно з формулою (13): $G_i = 0{,}70$. Значення вагових коефіцієнтів $a_1 = 0{,}4$; $a_2 = 0{,}3$; $a_3 = 0{,}3$. Таким чином, безпекова доцільність згідно з формулою (19) дорівнює:

$$N_i = 0{,}32 + 0{,}18 + 0{,}09 = 0{,}59. \tag{19}$$

Наступним кроком розрахуємо ресурсно-управлінську доцільність реалізації заходу кібербезпеки згідно з формулою (14). Для цього спочатку обчислимо значення показника O_i згідно з уточнюючою формулою (15). Показник обмеженості ресурсів визначається як зважена сума обмеженості часових, людських і фінансових ресурсів. Для прикладу: $O_i = 0{,}4 \times 0{,}40 + 0{,}3 \times 0{,}60 + 0{,}3 \times 0{,}50 = 0{,}49$.

За умови, що відносний показник ефективності заходу $E_i = 0{,}45$, при вагових коефіцієнтах $b_1 = 0{,}5$; $b_2 = 0{,}5$ ресурсно-управлінська доцільність заходу відповідно до формули (20) дорівнює:

$$D_i = 0{,}5(1 - 0{,}49) + 0{,}5 \times 0{,}76 = 0{,}635. \tag{20}$$

Отже, $D_i \approx 0{,}64$, що відповідно до рекомендованої шкали (таблиця 3) свідчить про доцільність реалізації сегментації мережі BPCS з точки зору співвідношення ресурсно-управлінської доцільності.

Таблиця 3

Шкала оцінювання ресурсно-управлінської доцільності заходів кібербезпеки

Кількісне значення показника D_i	**Інтерпретація**	**Рекомендоване рішення відповідно до ступеню пріоритезації заходу**
0,76–1	Висока доцільність реалізації заходу	Реалізувати першочергово
0,50–0,75	Помірна доцільність	Реалізувати планово
0,25–0,49	Низька пріоритетність	Віднести до довгострокової реалізації
0–0,24	Недоцільність реалізації у разі обмеженості ресурсів	Не реалізовувати у разі обмеженості ресурсів

Інтегральний показник пріоритетності заходу визначається як зважена комбінація безпекової потреби та ресурсно-управлінської доцільності. Для вищезазначеного прикладу розрахунків, за умови, що $N_i = 0{,}59$; $D_i = 0{,}64$, а коефіцієнт балансу $\lambda = 0{,}6$ (показує збільшений пріоритет безпекової складової) згідно з формулою (16) та відповідно до розрахунків формули (21) отримуємо:

$$P_i = 0{,}6 \times 0{,}59 + 0{,}4 \times 0{,}64 = 0{,}61. \qquad (21)$$

$\lambda \in [0;1]$, де при $\lambda \to 1$ пріоритезація заходів визначається переважно безпековою потребою, тоді як при $\lambda \to 0$ – ресурсною доцільністю. Це дозволяє використовувати метод як в умовах обмеженості ресурсів, так і в умовах планового управління.

Визначимо остаточну пріоритетність заходу кібербезпеки згідно зі шкалою оцінювання (таблиця 4).

Таблиця 4

Шкала оцінювання пріоритетності реалізації заходу кібербезпеки в умовах обмежених ресурсів

Кількісне значення показника P_i	**Значення пріоритету**
0,75–1	Високий (першочергова реалізація)
0,50–0,74	Середній (планова реалізація)
0,25–0,49	Низький (довгострокова реалізація)
< 0,25	Не пріоритетний

Таким чином, захід сегментації мережі для активу інформаційної підсистеми BPCS за отриманим значенням інтегрального показника пріоритетності $P_i = 0{,}61$ належить до категорії заходів планової реалізації. При цьому враховується наявність дефіциту фінансового ресурсу на рівні 20 %, що знижує його ресурсно-управлінську доцільність, однак не виключає доцільності впровадження цього заходу кібербезпеки.

Результати підетапу оформлюються у Матрицю інтегральних показників ефективності та пріоритетності заходів кібербезпеки для активів ТС ПОКІ.

3.3. Розподіл часток ресурсів у межах груп активів управлінського режиму.

За результатами аналітичного етапу методу, зокрема обчислення загального ресурсного шляху потенційних деструктивних кібератак та розрахунку відносних показників ефективності і пріоритетності заходів кібербезпеки, забезпечується можливість більш обґрунтованого розподілу обмежених ресурсів між групами активів технологічної системи (підпункт 2.3 в продовження таблиці 2). Результатом цього етапу є визначення розподілу всіх трьох видів ресурсів (часового, людського і фінансового) в рамках управлінського режиму між заходами кібербезпеки груп активів (та їх підсистем) та відпрацювання Матриці уточненого розподілу ресурсів між заходами кібербезпеки для активів ТС ПОКІ.

Заключний етап методу включає:

4.1. Ранжування заходів кібербезпеки за кожним активом ТС ПОКІ за черговістю їх реалізації відповідно до визначеної пріоритетності.

Цей підетап передбачає віднесення заходів кібербезпеки до пріоритетності їх реалізації: першочергової реалізації; планової реалізації; довгострокової реалізації та в рамках обраного управлінського режиму згідно з підходом, описаним у підпункті 3.2. Результатом виконання підетапу є складання Реєстру пріоритетності та черговості реалізації заходів кібербезпеки для активів ТС ПОКІ.

4.2. Формування Плану реалізації заходів кібербезпеки ТС ПОКІ.

Підетап є завершальною частиною методу та полягає у формуванні остаточної версії Плану реалізації заходів кібербезпеки ТС ПОКІ з урахуванням обмеженості ресурсів, який містить ранжований перелік заходів, розподіл ресурсів та відповідні додатки, що обґрунтовують прийняті управлінські рішення. Перелік рекомендованих додатків згідно з черговістю виконання етапів/підпунктів методу відображено у таблиці 5.

Таблиця 5

Перелік рекомендованих додатків згідно з черговістю виконання етапів/підетапів методу

Підпункт етапу методу	**Назва додатку до Плану**
1.1	Акти оцінки критичності та поточного стану кіберстійкості активів ТС ПОКІ
	Відомість оцінки поточного рівня кіберстійкості ТС ПОКІ та її активів
1.2	Матриця цільових пріоритетів щодо підвищення рівня кіберстійкості активів ТС ПОКІ
2.1	Відомість оцінки обмеженості ресурсів для реалізації цільових пріоритетів кібербезпеки активів ТС ПОКІ
2.2	Матриця вибору управлінського режиму та відбору активів ТС ПОКІ
2.3	Матриця попереднього розподілу ресурсів між активами ТС ПОКІ
3.1	Імітаційно-аналітичні моделі загального ресурсного шляху потенційних деструктивних кібератак на активи ТС ПОКІ
	Відомість оцінювання загального ресурсного шляху деструктивних кібератак
3.2	Матриця оцінки ефективності та пріоритетності заходів кібербезпеки для активів ТС ПОКІ
3.3	Матриця інтегрованого розподілу ресурсів між заходами кібербезпеки для активів ТС ПОКІ
4.1	Реєстр пріоритетності та черговості реалізації заходів кібербезпеки для активів ТС ПОКІ

Висновки. Таким чином, з аналізу змісту описаного методу встановлено, що пріоритезація заходів кібербезпеки для протидії деструктивним кібератакам в умовах обмежених ресурсів здійснюється з урахуванням таких головних критеріїв:

рівня критичності активів ТС ПОКІ;

рівня цільових пріоритетів щодо підвищення кіберстійкості активів ТС ПОКІ;

найбільш ймовірних коливань рівня ресурсного забезпечення впродовж планового періоду;

рівня обмеженості ресурсів;

загального ресурсного шляху потенційних деструктивних кібератак проти активів ТС ПОКІ.

Зазначені фактори інтегруються в узагальнений показник пріоритезації заходів кібербезпеки *I*, який можна описати формулою (22):

$$I = \sum_{i=1}^{5} w_i \times K_i. \quad (22)$$

На відміну від класичних підходів до управління ресурсами (cost-benefit аналіз, risk-based підходи, AHP, optimization-моделі), запропонований метод поєднує оцінку внутрішніх параметрів системи з урахуванням поведінки суб’єкта кіберзагрози, що реалізується через використання імітаційно-аналітичного моделювання з використанням кольорових сіток Петрі. Це забезпечує перехід від статичної до сценарно-орієнтованої та адаптивної пріоритезації заходів кібербезпеки.

Таким чином, запропонований метод підвищує ефективність управління кібербезпекою ТС ПОКІ та забезпечує можливість обґрунтованого розподілу обмежених ресурсів з урахуванням актуального ландшафту кіберзагроз.

Майбутні шляхи досліджень.

Перспективними напрямами подальших досліджень є розвиток запропонованого методу у частині підвищення рівня його автоматизації та експериментальної верифікації. Зокрема, доцільним є розроблення програмних засобів, спрямованих на автоматизацію окремих підетапів методу, передусім підетапу обчислення загального ресурсного шляху потенційних деструктивних кібератак на основі імітаційно-аналітичного моделювання з використанням кольорових сіток Петрі. Автоматизація цього процесу може бути реалізована із застосуванням спеціалізованих середовищ моделювання (зокрема, “CPN Tools”) у поєднанні з програмними засобами обробки даних (наприклад, з використанням мови програмування Python).

Окрім цього, перспективним є проведення експериментальної апробації методу на реальних або наближених до реальних ТС ПОКІ, зокрема об’єктах енергетичної галузі (наприклад, теплових електростанціях). Така апробація дозволить оцінити ефективність методу, його чутливість до змін ресурсного забезпечення та релевантність отриманих управлінських рішень порівняно з існуючими підходами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Novais I., Marinatto M., Lizarralde F., Peixoto A. J. Hard Prioritization Control Allocation: Dealing With the Priority Inversion Phenomenon. URL: https://ieeexplore.ieee.org/document/11038928.

2. Miller C., Sage A. P. Application of a methodology for evaluation prioritization and resource allocation to energy conservation program planning. URL: https://www.sciencedirect.com/science/article/abs/pii/0045790681900203?via%3Dihub.

3. Mohammad Amir Hossain, Md. Adil Raza, Taqi Yaseer Rahman. Resource allocation and budgetary constraints for cybersecurity projects in small to medium sized banks. URL: http://dx.doi.org/10.2139/ssrn.5207138.

4. Rodrigo Román-Castro, Adel Alqudhaibi, Majed Albarrak, Abdulmohsan Aloseel, Sandeep Jagtap, Konstantinos Salonitis. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. URL: https://doi.org/10.3390/s23094539.

5. SANDIA REPORT Methodology for Prioritizing Cyber vulnerable Critical Infrastructure Equipment and Mitigation Strategies. URL: https://doi.org/10.2172/1028958).

6. Про критичну інфраструктуру: Закон України від 18.11.2021 № 1909-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

7. Paté-Cornell M.-E. L., Kuypers M., Smith M., Keller P. Cyber risk management for critical infrastructure: A risk analysis model and three case studies // Risk Analysis. 2020. № 38 (2). URL: https://doi.org/10.1111/risa.12844.

8. Eric D. Knapp. Industrial Network Security Securing Critical Infrastructure Networks For Smart Grid Scada and other Industrial Control Systems 1st Edition. URL: https://www.slideshare.net/slideshow/industrial-network-security-securing-critical-infrastructure-networks-for-smart-grid-scada-and-other-industrial-control-systems-1st-edition-eric-d-knapp/279202298#3.

9. Ackerman Pascal. Industrial Cybersecurity Second Edition. 2021. 800 p.

10. What is the Purdue Model? URL: https://www.pera.net/Pera/Wha_PERA_Ref_Model.html?utm_source=chatgpt.com.

11. Хавер А. В. Метод ранжування критичності технологічних підсистем для визначення пріоритетності їх кіберзахисту на промислових об’єктах критичної інфраструктури // Всеукраїнська науково-практична конференція “Актуальні проблеми кібербезпеки”: тези доповідей, 2025 р. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf.

12. Савченко В. А., Хавер А. В. Метод розрахунку кіберстійкості 2-1 рівнів моделі Purdue проти спеціалізованого технологічного троянського програмного забезпечення // Системи і технології зв’язку, інформатизації та кібербезпеки. 2025. № 7. URL: https://doi.org/10.58254/viti.7.2025.14.147.

13. Harvey M. Wagner. Principles of Operations Research. URL: https://ia801701.us.archive.org/33/items/in.ernet.dli.2015.132568/2015.132568.Principles-Of-Operations Research-Second-Edition.pdf.

14. An Introduction to the Theoretical Aspects of Coloured Petri Nets. URL: https://tidsskrift.dk/daimipb/article/view/6949?utm_source=chatgpt.com.

15. Хавер А. В. Метод обчислення загального ресурсного шляху деструктивних кібератак на промислові об’єкти критичної інфраструктури //Кібербезпека: освіта, наука, техніка. 2025. Том 3, № 31. URL: https://doi.org/10.28925/2663-4023.2025.31.1064.

Надійшла до редколегії 06.04.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.