КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1064
УДК 004.056:519.816:004.421.8

Хавер Анюта Вячеславівна
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна,
ORCID: 0009-0003-4731-914X
innakot123z@gmail.com

МЕТОД ОБЧИСЛЕННЯ ЗАГАЛЬНОГО РЕСУРСНОГО ШЛЯХУ ДЕСТРУКТИВНИХ КІБЕРАТАК НА ПРОМИСЛОВІ ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. З метою ефективної пріоритезації кіберзахисту в умовах обмежених людських, часових та фінансових ресурсів на промислових об'єктах критичної інфраструктури у роботі пропонується застосування симбіозу математичного апарату імітаційно-аналітичного структурного моделювання кольоровими сітками Петрі та оцінки ресурсовитрат суб'єктом кіберзагрози в умовах невизначеності на основі PERT-аналізу. Така комбінація забезпечує можливість формалізованого опису різних векторів та тактик кібератак, моделювання траєкторій поширення спеціалізованого технологічного троянського програмного забезпечення, а також кількісного обчислення ресурсної складової реалізації кожного сценарію впливу на технологічну систему. Запропонований метод може бути практично використаний у процесі моделювання кіберзагроз, оскільки дозволяє представити їхні ресурсні показники у зручному для аналітичного оцінювання вигляді. Це створює основу для ухвалення управлінських рішень щодо кіберзахисту як керівною, так і виконавчою ланкою підрозділів кібербезпеки. Підхід дає змогу обчислити необхідні ресурсовитрати як з боку суб'єкта кіберзагрози, так і з боку захисної сторони для організації ефективних заходів протидії, а також визначити найбільш вразливі ділянки технологічної системи, що потребують першочергової уваги. Для практичного застосування методу фахівцям підрозділів кіберзахисту необхідно здійснити оцінку всього спектра актуальних векторів та тактик кібератак, після чого обчислити їхній загальний ресурсний шлях. Отримані кількісні показники використовуються для подальшого ранжування кіберзагроз та віднесення їх до короткострокової, середньої або довгострокової пріоритетності у кіберзахисті. Це забезпечує раціональний розподіл доступних ресурсів, підвищує адаптивність системи кібербезпеки та сприяє своєчасному впровадженню заходів протидії найбільш ресурсооптимальним і потенційно небезпечним тактикам, які дозволяють реалізувати деструктивний кібервплив.

Ключові слова: кіберзахист, технологічна система, імітаційно-аналітичне моделювання, PERT-аналіз, кольорові сітки Петрі.

ВСТУП

У сучасних умовах триваючої збройної агресії та систематичного зростання кількості цілеспрямованих кібератак на промислові об'єкти критичної інфраструктури забезпечення їх кіберстійкості стає одним із ключових завдань держави та керівництва таких об'єктів.

Ефективний кіберзахист таких об'єктів, в свою чергу, вимагає раціонального розподілу наявного ресурсу – людського (персоналу), часового, фінансового (на закупівлю програмно-апаратних засобів кіберзахисту, заходів модернізації, вдосконалення мережевої архітектури і т.д.). Такі ресурси, враховуючи сукупність поточних воєнних та соціально-економічних факторів можуть бути обмеженими.

Постановка проблеми. Технологічні системи промислових об'єктів критичної інфраструктури та, зокрема, їхні інформаційні підсистеми BPCS та SIS на рівнях 2-0 моделі Purdue, характеризуються високою складністю, неоднорідністю вузлів та динамічністю процесів, що утруднює оцінку одного з найнебезпечніших ризиків для їх сталого функціонування – деструктивних кібервпливів.

У межах процесів оцінки кіберризиків та ідентифікації/пріоритезації кіберзагроз в технологічних системах промислових об'єктів критичної інфраструктури виникає потреба у кількісному вимірюванні потенціалу суб'єктів загроз, що реалізують різні вектори та тактики кібератак. Проте наявні нормативні, методичні та аналітичні підходи здебільшого зосереджені на оцінці технічних вразливостей, ймовірностей інцидентів та тяжкості їхніх наслідків, але майже не враховують ресурсну складову деструктивних кібератак: обсяг людських, часових та фінансових ресурсів, необхідних для вчинення суб'єктом кіберзагрози деструктивної кібератаки.

За умов обмеженості ресурсів підприємства (людських, часових, фінансових) це призводить до проблеми відсутності об'єктивної ієрархії загроз, оскільки неможливо коректно визначити, які тактики є найбільш реалістичними і ресурсно доступними для зловмисника, а які — малоймовірними через високу ресурсоємність. Відповідно, ускладнюється ухвалення рішень щодо пріоритетного розподілу ресурсів кіберзахисту та вибору першочергових напрямів підсилення кіберстійкості.

Таким чином, невирішеною залишається науково-практична проблема розроблення методу обчислення загального ресурсного шляху деструктивної кібератаки в межах процесів оцінки кіберзагроз і кіберризиків. Такий метод має забезпечувати імітаційно-аналітичне моделювання (зокрема з використанням кольорових сіток Петрі) для кількісного визначення сумарних ресурсів, які необхідні суб'єкту загрози для реалізації певної тактики проникнення та поширення шкідливого програмного забезпечення в технологічній системі. Це дозволить здійснювати обґрунтовану пріоритезацію загроз і забезпечити більш раціональний розподіл ресурсів кіберзахисту, особливо коли вони є кількісно обмеженими.

Аналіз останніх досліджень і публікацій. За результатами аналізу останніх публікацій на міжнародній наукометричній платформі наукових публікацій та цитувань "Web of Science" (Clarivate Analytics) переважна більшість робіт досліджуваної тематики сфокусована на висвітленні відмінностей між кібератаками на комунікаційні та технологічні системи промислових об'єктів критичної інфраструктури [1], аналізі тактик, технік та процедур, які використовуються суб'єктами кіберзагрози для кібератак на технологічні системи [5], дослідженні кіберзагроз та ризик-менеджменті для технологічних систем об'єктів критичної інфраструктури [9,10]. Проте, вищезазначені публікації не використовують описаних в даному дослідженні методів та підходів, які базуються на оцінці ресурсів.

Метою статті є опис методу обчислення загального ресурсного шляху деструктивних кібератак з використанням імітаційно-аналітичного структурного моделювання кольоровими сітками Петрі для виявлення найбільш загрозливих сценаріїв їх реалізації на технологічні системи промислових об'єктів критичної інфраструктури. Для досягнення поставленої мети автором вирішуються наступні завдання:

- розкрити операційні можливості кольорових сіток Петрі як математичного засобу для імітаційно-аналітичного структурного моделювання деструктивних кібератак;
- оцінити ресурсовитрати суб'єкта кіберзагрози на реалізацію деструктивної кібератаки в умовах невизначеності;

- обчислити загальний ресурсний шлях деструктивної кібератаки з використанням багатокритеріального нормування з ваговим лінійним агрегуванням.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ.

Серед проаналізованих автором аналітичних та імітаційних математичних засобів моделювання процесу проведення деструктивних кібератак на технологічні системи промислових об'єктів критичної інфраструктури найкращим засобом було обрано кольорові сітки Петрі. Такий вибір зумовлений комплексною оцінкою низки математичних і системних характеристик досліджуваного об'єкта — технологічної системи, зокрема: неоднорідністю топології, високою архітектурною складністю, динамічністю та подієорієнтованістю, детермінованим характером фізичних процесів, наявністю змішаних (гібридних) процесів [1]. У сукупності ці властивості формують гібридну кіберфізичну систему, яка потребує інструменту моделювання, здатного: представляти дискретні стани, переходи та умови їхнього спрацювання; працювати з кольоровими (параметризованими) маркерами, які дозволяють кодувати різні типи вузлів, шкідливого ПЗ, станів SIS/BPCS, результатів кібератак; відображати паралелізм, блокування, конкуренцію ресурсів і конфлікти подій; підтримувати стохастичність, часові затримки, черги та умови пріоритетності; дозволяти формальну перевірку властивостей моделі [2].

Кольорові сітки Петрі є формальною математичною моделлю (точним математичним описом системи, поведінки або процесу, що заданий через формальні структури (множини, функції, відношення), який виключає двозначність і дозволяє проводити математичний аналіз) дискретних систем (граф з динамікою), які працюють у режимі "подія:зміна стану". Головною особливістю даного підходу є можливість одночасно описувати: структуру системи (які є стани та події), динаміку (як змінюється стан при настанні події), паралелізм і конкуренцію (кілька подій можуть відбуватися незалежно) [3].

Основними елементами кольорової сітки Петрі є: місця (позначаються колами та описують: стани системи; ресурси; умови; технологічні об'єкти. Кожне місце має кольорову множину (тип даних), що визначає, які токени місце може містити); переходи (позначаються прямокутником та описують: події; дії; кроки алгоритму; технологічні чи логічні операції. Перехід може спрацювати лише у разі виконання умови та наявності відповідних токенів у вхідних місцях); дуги (позначаються стрілками між місцями та переходами. Кожна дуга описує, які токени зчитуються або створюються); токени (позначаються крапками всередині місця та відображають динамічний стан системи); кольорові множини (позначають типи даних токенів, напри: числовий (int), рядковий (record), становий (open, closed) та інш.); змінні (позначають деякий тип даних з певної кольорової множини (наприклад: сенсори, команди, стани)); охоронні умови (англ. мовою - "Guard Functions", що визначають умови за яких перехід може спрацювати та можуть відображати межі спрацювання, логіку PLC, дозволи/блокування); вирази дуг (описують які токени зчитуються з місця, генеруються переходом або модифікуються); початкове маркування (задає кількість і значення токенів на початку моделювання). Таким чином, повна модель кольорової сітки Петрі задається 9-ти кортежем:

$$CPN = (P, T, A, \sum, V, C, G, E, I) \quad (1)$$

де: P – множина місць, T – множина переходів, A – множина дуг, ∑ - кольорові множини (типи), V – змінні, C – функція типів місць, G – охоронні умови, E – вирази дуг, I – початкове маркування [4].

Спрощений графічний приклад кольорової сітки Петрі, яка відображає реагування SIS на фіксацію небезпечного стану сенсором наведено на Рис. 1.1

Для подальшого дослідження змоделюємо конкретну тактику, яку може використовувати суб'єкт кіберзагрози для проникнення до технологічної системи ПОКІ. Наприклад, тактику прямого підключення вузла технологічної системи до Інтернету [5].

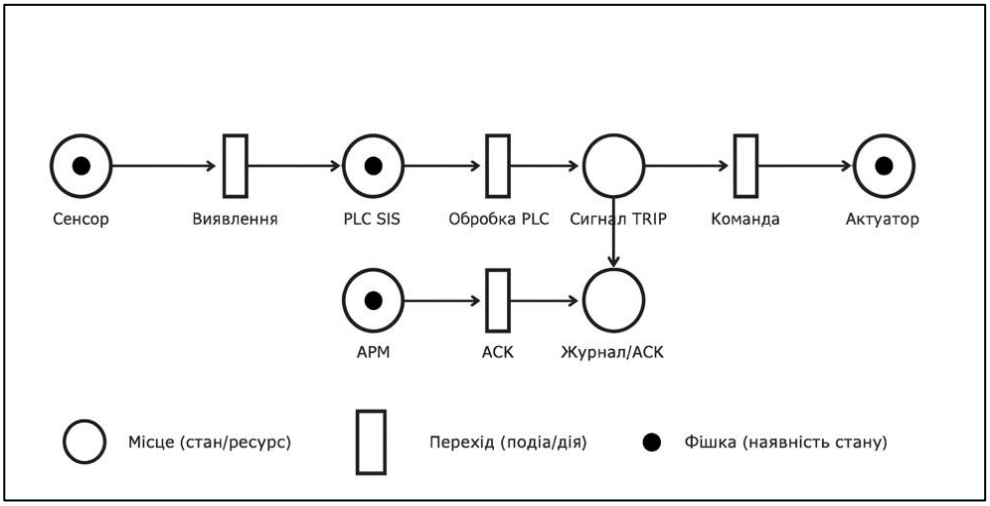

Рис.1.1 Спрощена графічна сітка Петрі для зображення принципу роботи SIS технологічної системи ПОКІ

Для зручності візуалізації такої кольорової сітки Петрі розділимо її позоново, послідовно, логічно в рамках процесу реалізації кібератаки: зовнішній периметр (за межами технологічної системи); внутрішній периметр (всередині технологічної системи, наприклад у межах BPCS або іншої інформаційної підсистеми); цільовий периметр (ділянка від інженерної робочої станції до цільового PLC критичної технологічної підсистеми ПОКІ) (Рис.1.2 — 1.4).

Опишемо параметри побудованої в рамках обраної тактики кольорової сітки Петрі відповідно до формули 1. Така кольорова сітка Петрі описує ланцюг взаємопов'язаних місць (які в даному контексті виступають основними вузлами (програмно-апаратними засобами) через які транзитно проходить спеціалізоване технологічне троянське програмне забезпечення (далі – СТТПЗ) до досягнення цільового периметру, цільового вузла, в рамках обраної тактики): суб'єкт кіберзагрози: проксі 1: проксі 2: роутер (прикордонний роутер технологічної системи): вузол BPCS: транзитний вузол (-ли) BPCS: інженерна робоча станція BPCS: критична технологічна підсистема технологічної системи ПОКІ: PLC BPCS: SIS (маються на увазі її виконавчі елементи — сенсори, актуатори).

До переходів зображеної кольорової сітки Петрі належать: до проксі 1: до проксі 2: до роутера: до вузла BPCS (не обов'язково: до роутера: до С2: до суб'єкта кіберзагрози): до транзитного вузла (-ів) BPCS (не обов'язково: до вузла BPCS: до роутера: до С2: до суб'єкта кіберзагрози): до інженерної робочої станції BPCS (не обов'язково: до транзитного вузла BPCS: до вузла BPCS: до роутера: до С2: до суб'єкта кіберзагрози): до критичної технологічної підсистеми технологічної системи ПОКІ: до PLC BPCS (не

обов'язково: до інженерної робочої станції BPCS: до транзитного вузла BPCS: до вузла BPCS: до роутера: до C2: до суб'єкта кіберзагрози): до SIS: до успіху деструктивної кібератаки (чи до не успіху).

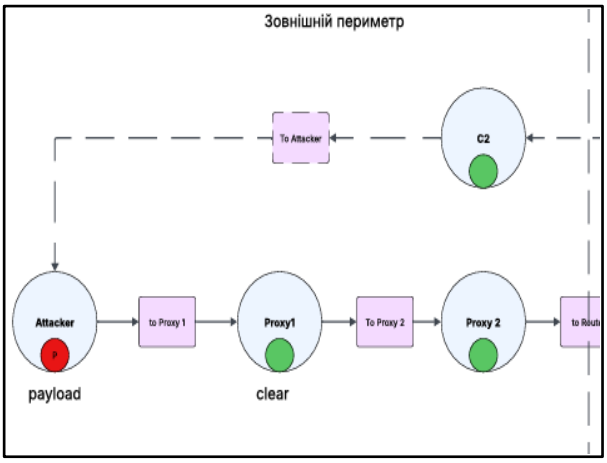

Рис.1.2 Кольорова сітка Петрі обраної тактики для зовнішнього периметру

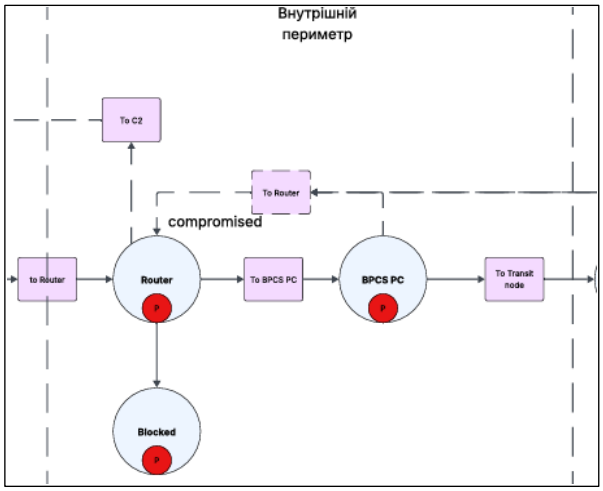

Рис. 1.3 Кольорова сітка Петрі обраної тактики для внутрішнього периметру

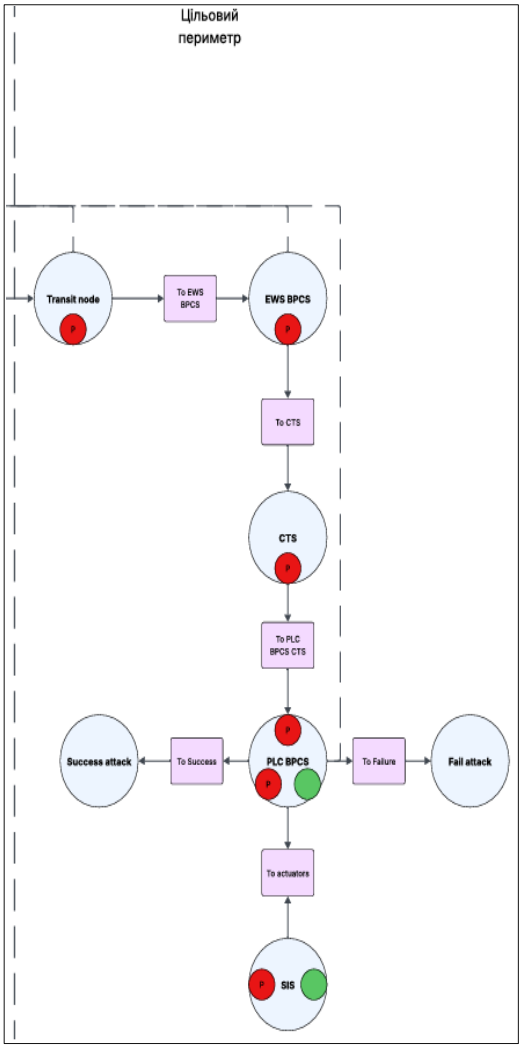

Рис.1.4 Кольорова сітка Петрі обраної тактики для цільового периметру

_ _ _ _ _ - позначає необов'язкові переходи (зв'язки) між основними вузлами обраної тактики

Зображена кольорова сітка Петрі передбачає, що суб'єкт кіберзагрози може використовувати С2, проте така можливість йому буде доступна лише за певних умов, тому це місце (С2) як і переходи до нього від інших місць не є обов'язковими.

До кольорових множин належать: стани вузла (clean, infected, vulnerable, compromised); стани SIS (ready, tripped, infected) тип шкідливого коду СТТПЗ (payload); результат кібератаки (success/fail). *Стани вузлів та SIS задаються саме англійською мовою та не допускають перекладу відповідно до міжнародного стандарту моделювання кольорових сіток Петрі.*

Початкове маркування для місць задамо в Таблиці 1:

Таблиця 1

Початкове маркування місць кольорової сітки Петрі для тактики прямого підключення вузла технологічної системи ПОКІ до Інтернету

№ з/п	Назва місця	Початкове маркування	Назва місця	Початкове
1.	Суб'єкт кіберзагрози	1’ (payload)	Інженерна робоча станція BPCS	1’ (clean)
2.	Проксі 1	1’ (clean)	Критична технологічна підсистема	1’ (clean)
3.	Проксі 2	1’ (clean)	PLC BPCS	1’ (clean)
4.	C2 (не обов'язковий елемент)	1’ (clean)	SIS	або 1’ ready; або 1’ infected; або 1’ tripped
5.	Роутер	1’ (clean)	Блокування	empty
6.	Вузол BPCS	1’ (clean)	Успіх	empty
7.	Транзитний вузол BPCS	1’ (clean)	Неуспіх	empty

До змінних, які буде використано в досліджуваній кольоровій сітці Петрі належать: ns (стан основного вузла); ml (malware); ss (стан SIS); rs (результат).

Охоронні умови (умови переходу) задамо в Таблиці 2:

Таблиця 2

Guard functions (охоронні умови) кольорової сітки Петрі для тактики прямого підключення вузла технологічної системи ПОКІ до Інтернету

№ з/п	Перехід	Умова спрацювання (guard Function)	Пояснення логіки
1.	До проксі 1	[ns <> blocked]	Перехід СТТПЗ дозволено, якщо проксі 1 не заблоковано
2.	До проксі 2	[ns <> blocked]	СТТПЗ просувається далі, якщо немає блокування.
3.	До роутера	[ns = vulnerable oreles ns = compromised]	СТТПЗ продовжує рух переходячи в зону внутрішнього периметру якщо роутер є вразливим чи скомпрометованим
4.	Router → Blocked	[ns = clean]	Роутер блокує payload СТТПЗ, якщо він чистий
5.	До вузла BPCS	[ns = vulnerable oreles ns = compromised]	Вузол BPCS пропускає СТТПЗ далі якщо його інфіковано

6.	До транзитного вузла BPCS	[ns = vulnerable oreles ns = compromised]	Транзитний вузол пропускає СТТПЗ далі якщо його інфіковано
7.	До інженерної робочої станції BPCS	[ns = vulnerable oreles ns = compromised]	Інженерна робоча станція пропустить СТТПЗ якщо вона вразлива або скомпрометована
8.	До критичної технологічної підсистеми	[ns = compromised]	СТТПЗ проникає гарантовано, якщо інженерну робочу станцію вже скомпрометовано (детермінований перехід)
9.	До PLC BPCS	[ns = compromised]	СТТПЗ отримує доступ до PLC однозначно, якщо скомпрометовано інженерну робочу станцію (детермінований перехід)
10.	SIS → Blocked	[ns <> compromised]	SIS переходить у стан безпечного блокування тільки якщо вона не заражена СТТПЗ

Вирази дуг для зазначеної кольорової сітки Петрі пропонується описати в Таблиці 3:

Таблиця 3

Вирази дуг кольорової сітки Петрі для тактики прямого підключення вузла технологічної системи ПОКІ до Інтернету

№ з/п	Назва переходу	Вхідна дуга (Arc In)	Вихідна дуга (ARC Out)
1.	До проксі 1	(ns, ml)	(clean, ml)
2.	До проксі 2	(ns, ml)	(clean, ml)
3.	До роутера	(ns, ml)	(compromised, ml)
4.	Роутер→ Blocked	(ns, ml)	(blocked, ml)
5.	До вузла BPCS	(ns, ml)	(compromised, ml)
6.	До транзитного вузла BPCS	(ns, ml)	(compromised, ml)
7.	До інженерної робочої станції BPCS	(ns, ml)	(compromised, ml)
8.	До критичної технологічної підсистеми	(ns, ml)	(compromised, ml)
9.	До PLC BPCS	(ns, ml)	(compromised, ml)
10.	SIS → Blocked	(ns, ml)	(compromised, ml)
11.	Success attack	(ns, ml)	success
12.	Fail attack	(ns, ml)	failure

Таким чином, завершено описову частину кольорової сітки Петрі для тактики прямого підключення вузла технологічної системи ПОКІ до Інтернету, яка включає всі важливі аспекти взаємодії СТТПЗ з місцями кольорової сітки Петрі, що в тому числі може бути використано для побудови працюючого програмного прототипу в середовищі ПЗ “CPN Tools”. Результати даного етапу імітаційно-аналітичного моделювання використаємо в подальших розрахунках загального ресурсного шляху для досліджуваної тактики.

МЕТОДИКА ДОСЛІДЖЕННЯ

З метою оцінки ресурсовитрат суб’єкта кіберзагрози на реалізацію деструктивної кібератаки в умовах невизначеності автор пропонує скористатися статистико-ймовірнісним підходом — PERT-аналізом (Program Evaluation and Review Technique), який традиційно використовується для планування та оцінювання складних проєктів. У межах запропонованого методу PERT-аналіз виконує роль доповнюючого інформаційного елементу до моделювання векторів і тактик за допомогою кольорових сіток Петрі.

Суть PERT-аналізу полягає у моделюванні трьох ймовірних сценаріїв розвитку складного процесу. В межах методу формалізуються “оптимістичний”, “реалістичний” (найбільш ймовірний) та “песимістичний” варіанти розвитку подій, що дозволяє врахувати невизначеність параметрів, притаманну реальним умовам.

Оцінювані ресурсовитрати суб’єкта кіберзагрози, на реалізацію конкретного вектора та тактики, пропонується розраховувати за класичною PERT формулою:

$$T_{PERT} = \frac{O+4P+П}{6} \quad (2)$$

де: О – кількісне значення оптимістичного коефіцієнта; Р – кількісне значення реалістичного коефіцієнта; П – кількісне значення песимістичного коефіцієнта [6].

Автором запропоновано використати метод експерних оцінок для оцінювання найбільш пріоритетних векторів, тактик та оцінювання ресурсовитрат суб'єктів кіберзагрози за трьома можливими сценаріями. До таких експертів пропонується віднести найбільш компетентних фахівців підрозділу Cyber Threat Intelligence або аналогічного йому за функціоналом технологічної системи ПОКІ (за таблицею “MITRE ATT&CK for ICS”, з урахуванням поточних тенденцій кібератак на ПОКІ, ОКІ та загальновідомих статистичних показників). Отримані експертні значення формують основу для розрахунку ресурсовитрат за кожним із трьох можливих сценаріїв для кожного вектора кібератаки та тактики відповідно.

Здійснимо PERT-оцінку досліджуваної тактики та оцінимо її ресурсовитрати за кожним етапом (місцем) згідно кольорової сітки Петрі (Таблиця 4).

Таблиця 4

PERT-оцінка кроків (місць) для реалізації успішної деструктивної кібератаки з використанням СТТПЗ згідно кольоровій сітці Петрі обраної тактики

№ з/п	Назва кроку (місця)	Назва ресурсу	Назва сценарію згідно PERT-аналізу			PERT-оцінка
			Оптимістичний	Реалістичний	Песимістичний	
1.	Проксі 1	Людський (в робочих одиницях)	1	1	2	2
		Часовий (в годинах в рамках 8-ми годинного робочого дня)	0,5	2	3	2
		Фінансовий (в доларах США)	100	200	300	200
2.	Проксі 2	Людський	1	1	2	2
		Часовий	0,5	2	3	2
		Фінансовий	100	200	300	200
3.	Роутер	Людський	1	1	1	1
		Часовий	1	40	480	107
		Фінансовий	0	0	1 000 000	150 000
4.	Вузол BPCS	Людський	1	2	3	2
		Часовий	1	5	24	7,5
		Фінансовий	0	0	0	0
5.	Інженерна робоча станція BPCS	Людський	2	3	5	3
		Часовий	24	40	120	51
		Фінансовий	0	0	1000 000	20000
6.	Критична технологічна підсистема	Людський	5	7	12	8
		Часовий	80	160	480	200
		Фінансовий	0	0	0	0
7.	PLC BPCS	Людський	2	3	4	3
		Часовий	24	80	160	84
		Фінансовий	0	0	0	0
8.	SIS	Людський	15	30	35	28
		Часовий	480	960	1920	1040
		Фінансовий	5000	7000	1000 000	172 167

Фінансовий ресурс за оцінками в Таблиці 4 зазначено без врахування оплати роботи працівників та з урахуванням, що пропрієтарні програмні засоби на основі технологій штучного інтелекту вже є в розпорядженні суб'єкта кіберзагрози перед початком кібератаки. Крім того, не враховується оплата роботи інсайдера [7]. Разом з тим, враховується, що середня (орієнтовна) ціна вразливості zero-day складає близько 100 тис.$;

часовий ресурс зазначено з урахуванням 8-ми годинного робочого дня та двох вихідних днів на тиждень;

людський ресурс зазначено з урахуванням, що певні етапи (місця) кібератаки може здійснювати одна особа, а решту – інші фахівці. Так, з 2 по 3 крок — здійснюють одні й ті ж фахівці; з 3 по 5 крок — фахівці іншого напрямку; 5-7 — може здійснити одна група людей; 8 — окрема, масштабна команда фахівців (найбільш ресурсовитратний етап в рамках деструктивної кібератаки на ПОКІ). В зазначених в Таблиці 4 показниках враховано діяльність інсайдера (на ділянці SIS). До людського ресурсу належать виключно особи задіяні до безпосереднього виконання (без управлінської/менеджерської ланок).

При розгляді оцінки фінансового ресурсу пункту 3 Таблиці 4 враховуємо, що зовнішній периметр технологічної системи (роутер) надійно захищений з точки зору конфігурації та оновлень (що, зокрема, залежить від його технічних характеристик (виробника)), вартість zero-day та ймовірність його використання суб'єктом кіберзагрози в конкретному випадку буде варіюватися (Таблиця 5). В контексті даного дослідження використаємо максимальну ймовірну вартість такого zero-day як песимістичний сценарій. Варто зазначити, що статистика використання zero-day суб'єктами кіберзагрози для отримання несанкціонованого доступу до технологічних систем для різних виробників прикордонного обладнання буде варіюватися (Таблиця 5). Для розрахунку середнього значення фінансового ресурсу в такому випадку скористаємося формулою 3 – очікуваної фінансової вартості для бінарного ризику з використанням статистичних даних Таблиці 5, з вибором режимної моделі для маршрутизатора “Cisco” [8]:

$$E[f_i] = p \cdot C_{max} + (1 - p) \cdot 0 \quad (3)$$

де: C_{max} = 100 000$ (вартість zero-day згідно песимістичного сценарію); 0 – типова вартість; p – ймовірність настання песимістичного сценарію для маршрутизатора “Cisco”= 0, 15.

Для розрахунку використання фінансового ресурсу для несанкціонованого доступу до інженерної робочої станції BPCS (пункт 5 Таблиці 4) скористаємося тим же підходом (формула 3). Разом з тим, ймовірність використання zero-day проти вищезазначеного вузла не більше 2%. Серед практичних прикладів використання zero-day для компрометації інженерної робочої станції BPCS можна назвати кібероперацію “Stuxnet”.

Таблиця 5

Порівняльна характеристика щодо статистики відсотка використання вразливості zero-day до обладнання різних виробників

№ з/п	Назва виробника	Оціночний діапазон використання zero-day серед APT	Коментар
1.	“Cisco”	10-15%	Найвища частота використання zero-day в реальних кібератаках
2.	“Fortinet”	5–12%	Вразливий VPN-шар
3.	“Juniper”	4–10%	ISP/державні мережі, висока цінність

4.	“Palo Alto Networks”	2–7%	Також ціль APT, але менш масове використання zero-day
5.	“MikroTik”	<1–3%	zero-day майже не продають і рідко застосовують
6.	SOHO бренди (“TP-Link”, “D-Link”)	≈0%	zero-day не купують, бо дешевше обійти іншим способом

Проведена оцінка ресурсовитрат з боку суб’єкта кіберзагрози на реалізацію деструктивної кібератаки з використанням обраної тактики забезпечує вихідними даними для обчислення загального ресурсного шляху через формулу багатокритеріального нормування з ваговим лінійним агрегуванням.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для отримання значення загального ресурсного шляху деструктивної кібератаки та змоги порівняти його з ресурсним шляхом інших тактик автор пропонує звести значення всіх ресурсів до єдиного числового значення. Такий метод називається багатокритеріальним нормуванням з ваговим лінійним агрегуванням. Класично такий підхід використовується для операційних досліджень в рамках яких розглядаються різні величини, які потребують зведення до єдиного індексу, а також в системному аналізі, управлінні проєктами, ризик-менеджменті та оцінці кіберризиків, моделях прийняття рішень та інш [9, 10].

З метою обчислення загального ресурсного шляху деструктивної кібератаки з використанням СТТПЗ для тактики прямого підключення вузла технологічної системи ПОКІ до Інтернету скористаємося формальним визначенням багатокритеріального нормування з ваговим лінійним агрегуванням (формула 4):

$$C(P) = at\frac{T\,(P)}{Tmax} + ah\frac{H\,(P)}{Hmax} + af\frac{F\,(P)}{Fmax} \quad (4)$$

де: C(P) – показник загального ресурсного шляху деструктивної кібератаки з використанням обраної тактики;

T (P) – загальний часовий ресурс на реалізацію деструктивної кібератаки з використанням обраної тактики; T_{max} – максимальний часовий ресурс етапу згідно PERT-оцінці;

H (P) – загальний людський ресурс на реалізацію деструктивної кібератаки з використанням обраної тактики; H_{max} – максимальний людський ресурс етапу згідно PERT-оцінці;

F (P) – загальний людський ресурс на реалізацію деструктивної кібератаки з використанням обраної тактики; F_{max} – максимальний фінансовий ресурс етапу згідно PERT-оцінці.

В подальших розрахунках згідно формули (4) враховуємо, що переважаючу вагу має часовий ресурс, далі людський, а потім фінансовий (така пріоритезація полягає у специфіці діяльності суб'єктів кіберзагрози, які спонсоруються державами та специфіці процесу виявлення деструктивної кібератаки, де більша тривалість деструктивної кібератаки дає більшу ймовірність на її виявлення підрозділом кіберзахисту ПОКІ до настання негативних наслідків), тому:

a_t = 0, 5 (так як час – 50% важливості); a_h = 0,3 (люди – 30% важливості); a_f = 0,2 (фінанси – 20% важливості).

Використовуючи числові показники з Таблиці 4 та переважаючі ваги зазначені вище здійснимо розрахунок згідно формули 4:

$$C\,(P) = (0{,}5 \cdot 1{,}44) + (0{,}3 \cdot 1{,}18) + (0{,}2 \cdot 1{,}99) = 1{,}47 \quad (5)$$

Таким чином, для обраної тактики загальний ресурсний шлях деструктивної кібератаки становить 1, 47.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, запропонований метод обчислення загального ресурсного шляху деструктивної кібератаки з використанням імітаційно-аналітичного структурного моделювання кольоровими сітками Петрі можна практично використовувати у ході прийняття рішень щодо пріоритезації кіберзахисту як технологічної системи ПОКІ в цілому так і її окремих критичних підсистем, зокрема, в умовах обмежених ресурсів. Для цього відповідними фахівцями кіберзахисту, згідно описаного методу, має бути оцінено весь спектр актуальних векторів та тактик, а також обчислено їх на загальний ресурсний шлях для подальшого ранжування та віднесення до короткострокової, середньої чи довгострокової пріоритетності у кіберзахисті.

Перспективи подальших досліджень полягають у:

- відпрацюванні практичної програмної реалізації досліджуваних векторів та тактик засобами універсального симулятора мереж Петрі – “GPenSIM” або “CPN Tools” для зображення процесу деструктивної кібератаки наочно з можливістю вносити точкові впливи (зміни) та відслідковувати зміни станів системи;
- удосконалення математичної моделі та її адаптації з урахуванням можливих додаткових параметрів впливу враховуючи актуальну інформацію про динамічний ландшафт кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Krotofil, M., Kursawe, K., & Gollmann, D. (2019). Securing industrial control systems. In *Security and privacy trends in the industrial Internet of Things* (pp. 3–27). Springer. https://doi.org/10.1007/978-3-030-12330-7_1
2. Dunn, D. G., & Cosman, E. (2024). Cybersecurity fundamentals are not just for industrial control systems: Guidance and direction are available. *IEEE*.
3. Davidrajuh, R. (2022). *Colored Petri nets for modeling of discrete systems*. Springer Nature.
4. Jensen, K., & Kristensen, L. M. (2009). *Coloured Petri nets: Modelling and validation of concurrent systems* (pp. 1–56). Springer.
5. Afenu, D. S., Asiri, M., & Saxena, N. (2024). Industrial control systems security validation based on the MITRE adversarial tactics, techniques, and common knowledge framework. *Electronics, 13*(5), Article 917. https://doi.org/10.3390/electronics13050917
6. Bergantiños, G., & Vidal-Puga, J. (2009). A value for PERT problems. *International Journal of Information Technology & Decision Making*. https://doi.org/10.1142/S0219198909002418
7. Savchenko, V. A., & Khaver, A. V. (2025). Assessing the impact of artificial intelligence–based software tools on resource efficiency in conducting destructive cyber operations against critical infrastructure facilities. *Modern Information Protection, 3*(63).
8. Mandiant. (2023, March 20). *Move, patch, get out the way: 2022 zero-day exploitation continues at an elevated pace*. https://cloud.google.com/blog/topics/threat-intelligence/zero-days-exploited-2022/
9. El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An integrated approach to cyber risk management with a cyber threat intelligence framework to secure critical infrastructure. *Journal of Cybersecurity and Privacy*, *4*(2), Article 18. https://doi.org/10.3390/jcp4020018

10. Paté-Cornell, M.-E. L., Kuypers, M., Smith, M., & Keller, P. (2020). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis, 38*(2). https://doi.org/10.1111/risa.12844

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

Khaver Anyuta
Postgraduate Student
State University of Information and Communication Technologies, Kyiv, Ukraine,
ORCID: 0009-0003-4731-914X
innakot123z@gmail.com

A METHOD FOR CALCULATING THE GENERAL RESOURCE PATH OF DESTRUCTIVE CYBERATTACKS ON INDUSTRIAL OBJECTS OF CRITICAL INFRASTRUCTURE

Abstract. For the purpose of effective cybersecurity prioritization under limited human, time, and financial resources at industrial critical infrastructure facilities, this study proposes the application of a symbiosis between the mathematical apparatus of simulation-analytical structural modeling using Colored Petri Nets and the assessment of adversary resource expenditures under uncertainty based on PERT analysis. This combination enables a formalized description of various cyberattack vectors and tactics, modeling the propagation trajectories of specialized technological Trojan malware, as well as quantitative calculation of the resource component required to implement each attack scenario against a technological system. The proposed method can be practically applied in the process of cyber-threat modeling, as it makes it possible to present their resource indicators in a format convenient for analytical evaluation. This creates a foundation for informed decision-making on cybersecurity measures by both managerial and operational levels of cybersecurity units. The approach allows calculating the necessary resource expenditures both from the adversary's perspective and that of the defensive side when planning effective countermeasures, as well as identifying the most vulnerable segments of the technological system that require priority attention. For practical implementation of the method, cybersecurity specialists must assess the full spectrum of relevant cyberattack vectors and tactics and subsequently compute their overall resource pathway. The resulting quantitative indicators are used for further ranking of cyber threats and assigning them to short-term, medium-term, or long-term cybersecurity priorities. This ensures a rational allocation of available resources, increases the adaptability of the cybersecurity system, and supports timely implementation of countermeasures against the most resource-efficient and potentially dangerous tactics capable of enabling destructive cyber-impact.

Keywords: cybersecurity, technological system, simulation-analytical modeling, PERT analysis, Colored Petri Nets.

REFERENCES

1. Krotofil, M., Kursawe, K., & Gollmann, D. (2019). Securing industrial control systems. In *Security and privacy trends in the industrial Internet of Things* (pp. 3–27). Springer. https://doi.org/10.1007/978-3-030-12330-7_1
2. Dunn, D. G., & Cosman, E. (2024). Cybersecurity fundamentals are not just for industrial control systems: Guidance and direction are available. *IEEE*.
3. Davidrajuh, R. (2022). *Colored Petri nets for modeling of discrete systems*. Springer Nature.
4. Jensen, K., & Kristensen, L. M. (2009). *Coloured Petri nets: Modelling and validation of concurrent systems* (pp. 1–56). Springer.
5. Afenu, D. S., Asiri, M., & Saxena, N. (2024). Industrial control systems security validation based on the MITRE adversarial tactics, techniques, and common knowledge framework. *Electronics, 13*(5), Article 917. https://doi.org/10.3390/electronics13050917
6. Bergantiños, G., & Vidal-Puga, J. (2009). A value for PERT problems. *International Journal of Information Technology & Decision Making*. https://doi.org/10.1142/S0219198909002418
7. Savchenko, V. A., & Khaver, A. V. (2025). Assessing the impact of artificial intelligence–based software tools on resource efficiency in conducting destructive cyber operations against critical infrastructure facilities. *Modern Information Protection, 3*(63).
8. Mandiant. (2023, March 20). *Move, patch, get out the way: 2022 zero-day exploitation continues at an elevated pace*. https://cloud.google.com/blog/topics/threat-intelligence/zero-days-exploited-2022/

9. El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An integrated approach to cyber risk management with a cyber threat intelligence framework to secure critical infrastructure. *Journal of Cybersecurity and Privacy*, *4*(2), Article 18. https://doi.org/10.3390/jcp4020018
10. Paté-Cornell, M.-E. L., Kuypers, M., Smith, M., & Keller, P. (2020). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2). https://doi.org/10.1111/risa.12844