DOI: https://doi.org/10.36910/6775-2524-0560-2026-63-20
УДК 004.056:519.83
Лахно Валерій Анатолійович[1], д.т.н., професор
https://orcid.org/0000-0001-9695-4543
Десятко Альона Миколаївна[2], PhD, доцент
https://orcid.org/0000-0002-2284-3418
Нікітенко Євгеній Васильович [1], к.ф.-м.н., доцент
https://orcid.org/0000-0002-9222-644X
Кайдик Олег Леонтійович [3], к.т.н, доцент
https://orcid.org/0000-0002-3620-270X
[1] Національний університет біоресурсів і природокористування України м. Київ, Україна
[2] Державний торговельно-економічний університет, м. Київ, Україна
[3] Луцький національний технічний університет, м. Луцьк, Україна

ПРЕДИКТИВНИЙ МАРКЕР ЦИФРОВИХ СЛІДІВ У СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ПРОТИДІЇ ПОСТКВАНТОВИМ КІБЕРАТАКАМ

Лахно В.А., Десятко А.М., Нікітенко Є. В., Кайдик О.Л. Предиктивний маркер цифрових слідів у системах підтримки прийняття рішень для протидії постквантовим кібератакам. У статті розв'язано актуальну науково-прикладну задачу розроблення інформаційної технології для систем підтримки прийняття рішень (СППР) із захисту гетерогенних мереж від атак на ланцюги постачання в умовах постквантової компрометації криптографічних протоколів. Обґрунтовано, що в умовах, коли квантові комп'ютери дозволяють здійснювати підробку цифрових підписів та TLS-сертифікатів, надійним джерелом даних для виявлення шкідливої активності стають поведінкові артефакти або цифрові сліди (ЦС). Математичним ядром запропонованої технології є антагоністична диференціальна гра, яка описує процеси поширення компрометації та накопичення ЦС із пороговим механізмом ізоляції вузлів. Науковою новизною роботи є виявлення та обґрунтування предиктивного маркера. Тобто тіньової ціни цифрових слідів $\lambda_F(t)$, зміна знаку якої сигналізує про перехід системи від фази спостереження до фази активної ізоляції. Застосування цього маркера в контурі СППР дозволить варіативно налаштовувати критичний поріг F_{crit}, мінімізуючи ризики лавиноподібної компрометації та надмірної кількості хибних спрацювань. Реалізація технології базується на модифікованому методі прямої та зворотної стрільби (FBSM) з релаксацією. Результати чисельного моделювання підтвердили, що використання предиктивного маркера для зниження порога ізоляції дозволить скоротити частку скомпрометованих вузлів майже вдвічі порівняно зі статичними політиками безпеки. Запропонована інформаційна технологія може бути інтегрована у діючи системи класу SIEM/IDS для автоматизованого керування політиками безпеки.
Ключові слова: інформаційна технологія, система підтримки прийняття рішень, постквантова криптографія, цифрові сліди, диференціальні ігри, тіньова ціна, критичний поріг

Lakhno V., Desiatko A., Nikitenko E., Kaidyk O. A predictive marker of digital traces in decision support systems for countering post-quantum cyberattacks. The article addresses the pressing scientific and applied problem of developing information technology for decision support systems (DSS) to protect heterogeneous networks against supply chain attacks under post-quantum compromise of cryptographic protocols. It is argued that in conditions where quantum computers enable the forgery of digital signatures and TLS certificates, behavioral artifacts or digital traces (DTs) become a reliable source of data for detecting malicious activity. The mathematical core of the proposed technology is an antagonistic differential game that describes the processes of compromise propagation and DS accumulation with a threshold mechanism for node isolation. The scientific novelty of this work lies in identifying and justifying a predictive marker: the shadow price of digital traces, λ_F(t), whose sign change signals the system's transition from the observation phase to the active isolation phase. The application of this marker in the DSS circuit will allow for the variable adjustment of the critical threshold F_crit, minimizing the risks of avalanche-like compromise and an excessive number of false positives. The implementation of the technology is based on a modified forward and backward shooting method (FBSM) with relaxation. Numerical simulation results confirmed that using a predictive marker to lower the isolation threshold reduces the proportion of compromised nodes by nearly half compared with static security policies. The proposed information technology can be integrated into existing SIEM/IDS systems for automated security policy management.
Keywords: information technology, decision support system, post-quantum cryptography, digital traces, differential games, shadow price, critical threshold

Постановка наукової проблеми.

Експоненційне зростання обчислювальних потужностей квантових комп'ютерів (КК) створило безпрецедентну загрозу для глобальної інфраструктури відкритих ключів (PKI) й протоколів захисту передавання даних TLS. Алгоритм Шора дав змогу за поліноміальний час факторизувати великі числа та обчислювати дискретні логарифмію Відповідно це математично компрометує криптосистеми RSA та алгоритми на еліптичних кривих. Саме ці алгоритми – це фундамент сучасної системи цифрового довіри. У постквантових реаліях зловмисник, отримавши

доступ до криптографічно релевантного квантового комп'ютера, зможе генерувати ідеальні підробки TLS-сертифікатів та цифрових підписів, не відмінні від легітимних [1, 2]. Це відкриє шлях до контрольованих атак на ланцюги постачання програмного забезпечення (ПЗ). Тобто в англомовній нотації supply chain attacks. Це сценарій коли шкідливий код упроваджують в ПЗ під виглядом валідних оновлень, а чинні засоби верифікації виявляються неефективними.

У подібній ситуації єдиним надійним бар'єром захисту стає не статична криптографічна перевірка, а неперервний моніторинг поведінки вузлів мережі. Будь-яка активність зловмисника, навіть ідеально замаскована під легітимний трафік, породжує атипові поведінкові артефакти або так звані цифрові сліди (далі ЦС), які фіксують зазвичай підсистемами IDS/IPS. Водночас накопичення таких ЦС не є самоціллю. Для ефективної ізоляції скомпрометованих вузлів потрібно визначити критичний поріг F_{crit} , після перевищення якого адміністратор або автоматизована система ухвалюють рішення про блокування хоста, незважаючи на формальну валідність його сертифіката. Вибір порога є головним архітектурним компромісом такої системи. Тобто занадто високий рівень призведе до запізнілої реакції й лавиноподібної компрометації. А занадто низький – до надмірної кількості хибних спрацювань (тобто Self-inflicted DoS).

Постає науково-прикладна задача – дослідити процес протиборства квантово-оснащеного атакуючого та захисника, який спирається виключно на аналіз поведінкових артефактів (ЦС). Далі на цій основі запропонувати інформаційну технологію підтримки прийняття рішень (СППР), здатну гнучко налаштовувати критичний поріг F_{crit} залежно від поточної стадії конфлікту. Проведені нами дослідження з використанням апарату антагоністичних диференціальних ігор дали змогу отримати оптимальні стратегії сторін й виявити важливий ефект, який полягає у наступному. Пов'язана з ЦС тіньова ціна $\lambda F(t)$, тобто спряжена змінна задачі оптимального керування змінює знак у процесі розвитку атаки – від від'ємного (це фаза «інвестування» ресурсів у збирання вулик) до додатного (фаза «окупності», коли накопичені свідчення дають змогу активувати ізоляцію). Момент переходу $\lambda F(t)$ через нуль виступає природним предиктивним маркером. Цей маркер сигналізує про наближення системи до критичного порога і необхідність знизити F_{crit} , переводячи захист зі спостережного режиму в активний.

В умовах дискредитації алгоритмів RSA, ECC квантовим комп'ютером єдиним джерелом даних для виявлення компрометації вузлів стають поведінкові артефакти (цифрові сліди – ЦС) атипової активності. Система захисту ухвалює рішення про ізоляцію хоста лише тоді, коли накопичений обсяг слідів $\mathrm{F}(t)$ перевищує критичний поріг F_{crit}. Фіксоване значення цього порога не дозволить гнучко реагувати на зміну тактики атаки. Зокрема, завищений поріг спричинить запізнілу ізоляцію та лавиноподібне поширення шкідливого коду. Навпаки, занижений створює надмірну кількість хибних блокувань й деградацію доступності легітимних сервісів. Отже, постає проблема синтезу інформаційної технології, яка здатна синхронно обчислювати об'єктивний предиктивний показник, який сигналізує про наближення до моменту, коли подальше зволікання з ізоляцією стає вкрай небезпечним. Таким показником в дослідженні виступає змінна $\lambda F(t)$ – тіньова ціна ЦС, зміна знаку якої (з від'ємного на додатний) позначає перехід від фази накопичення свідчень до фази, коли ці свідчення вже можуть бути використані для виправданої ізоляції. Наразі відсутня математично обґрунтована процедура інтеграції цього маркера в контур СППР для автоматичного синхронного налаштування порога F_{crit} під час постквантових атак на ланцюги постачання.

Метою даної статті є розроблення інформаційної технології для СППР із захисту гетерогенних мереж, яка використовує зміну знаку тіньової ціни цифрових слідів як предиктивний маркер для варіативного налаштування критичного порога ізоляції F_{crit}.

Для досягнення мети у роботі розв'язуються такі завдання:

- побудувати математичне ядро технології у вигляді диференціально-ігрової моделі, яка описує поширення компрометації та накопичення цифрових слідів із пороговим механізмом ізоляції;
- отримати аналітичні вирази для оптимальних стратегій захисника та показати, що інтенсивність поведінкового аналізу прямо пропорційна тіньовій ціні λF та поточній частці скомпрометованих вузлів;
- розробити алгоритм обчислення предиктивного маркера на основі модифікованого методу прямої та зворотної стрільби (FBSM) та інтегрувати його в архітектуру СППР;
- провести числове моделювання двох сценаріїв (високий та низький пороги F_{crit}) і кількісно оцінити виграш від застосування предиктивного керування.

Аналіз досліджень.

Перехід до постквантової епохи докорінно змінив ландшафт загроз. Саме тому, огляд попередніх досліджень структуровано за чотирма напрямами, що утворюють базис статті. Це відповідно: (1) квантова загроза для PKI і TLS; (2) еволюція атак на ланцюги постачання; (3) поведінковий аналіз як альтернатива криптографічному довірі; (4) диференціальні ігри в задачах кібербезпеки. Новизна дослідження полягає в інтеграції цих напрямів в єдину математичну модель.

Поява квантових комп'ютерів ставить під сумнів стійкість асиметричних криптосистем, що лежать в основі сучасної інфраструктури відкритих ключів. Алгоритм Шора [1] дав змогу за поліноміальний час факторизувати числа та обчислювати дискретні логарифми, компрометуючи RSA і ECC. Оцінка ресурсів, виконана в [3], показала, що 2048-бітний ключ RSA можна факторизувати за 8 годин на 20 млн. шумних кубітів, що робить загрозу кількісно вимірюваною. Концепція «harvest now, decrypt later» [4] додатково скоротила часовий горизонт для ухвалення рішень. Відповідно зловмисник може вже сьогодні накопичувати зашифрований трафік, очікуючи на появу квантового комп'ютера. Відповіддю стало прийняття NIST у 2024 р. постквантових стандартів FIPS 203, 204, 205 [5]. Однак міграція супроводжується значними витратами [6]. А також є проблеми сумісності [7]. Відкритим залишається питання, як діяти в перехідний період, коли формально валідні сертифікати можуть бути підроблені з використанням квантового ресурсу, що змушує перенести фокус із криптографічного захисту на поведінковий аналіз.

Зазначимо, що кількість атак на ланцюги постачання також стрімко зростає. Інциденти SolarWinds [8], компрометація XZ Utils [9, 10] та інші продемонстрували, що зловмисники навчилися впроваджувати шкідливий код на етапі збирання або постачання програмного забезпечення. Автори роботи [11] розробили таксономію, що охопила 107 векторів атак. А головним визнано підробку цифрових підписів. У постквантовому світі ця загроза набуває нового виміру. Отже ідеальна математична підробка знецінює механізми перевірки цілісності коду, а отже захист має переміститися на етап моніторингу поведінки вузлів після розгортання оновлень.

Коли чинна криптографічна верифікація поступово втрачає сенс, ефективним захистом стає неперервний моніторинг і виявлення атипової поведінки вузлів. В [12] авторами запропонували механізм виявлення аномалій (ABDM), інтегрований з архітектурою нульової довіри, яка аналізує трафік, не покладаючись на криптографічні атрибути. Дослідження на основі федеративного навчання також підтвердили, що поведінковий аналіз здатен виявляти скомпрометовані вузли без сигнатур зразків. Вразливість таких методів до змагальних атак обговорюється в [13]. В нашій моделі якість класифікації параметризовано коефіцієнтом κ, який визначає здатність системи подолати критичний поріг ізоляції.

Апарат диференціальних ігор [14, 15, 16, 17] дає змогу формально описувати конфлікти, що розвиваються в неперервному часі. Робота [14] автори одними з перших застосували його до задач мережевої безпеки. Сучасні роботи, наприклад [15], пропонують ігрові методи для оптимального розподілу захисних ресурсів у складних мережах. Спільною рисою цих праць є припущення про працездатність криптографічних механізмів [18]. Натомість у цій статті вперше формулюється диференціальна гра, в якій атакуючий оперує квантовим комп'ютером для ідеальної підробки підписів, а захисник покладається виключно на аналіз поведінкових артефактів. Саме таке поєднання квантової загрози та поведінкової відповіді становить наукову новизну дослідження.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.

Результати дослідження. Математичне ядро інформаційної технології.

Процес протиборства в умовах постквантових атак на ланцюги постачання – це система диференціальних рівнянь, які описують стан мережі.

Тоді, динаміка компрометації вузлів:

$$\frac{dC_t}{dt} = \alpha v_t \Psi(\tau)(1 - C_t) - \mu C_t \Theta(F_t - F_{crit}), \quad (1)$$

де C_t – частка скомпрометованих вузлів у мережі в момент часу t; v_t – інтенсивність атак зловмисника з використанням квантового ресурсу; α – коефіцієнт ефективності впровадження шкідливого коду; $\Psi(\tau)$ – функція потужності квантового ресурсу (здатність до підробки підписів); μ – інтенсивність відновлення або ізоляції вузлів; $\Theta(F_t - F_{crit})$ – згладжена функція Хевісайда, що активує ізоляцію лише при перевищенні накопиченими слідами порога F_{crit}.

Рівняння (1) показує, як поширюється зараження і як спрацьовує механізм ізоляції $\Theta(F_t - F_{crit})$.

Динаміка накопичення ЦС:

$$\frac{dF_t}{dt} = \beta v_t C_t + \kappa u_t C_t - \lambda F_t, \quad (2)$$

де F_t – обсяг накопичених цифрових слідів (поведінкових артефактів); u_t – інтенсивність захисних зусиль щодо збору та аналізу логів; β – коефіцієнт природного виникнення артефактів під час атаки; κ – ефективність виявлення слідів підсистемою моніторингу; λ – швидкість «застарівання» або забування цифрових слідів системою.

Рівняння (2) показує як генеруються артефакти ($\beta v_t C_t$), як їх виявляє захисник ($\kappa u_t C_t$) та як вони застарівають.

Для знаходження оптимальних стратегій сторін та аналізу динаміки предиктивного маркера скористаємося принципом максимуму Понтрягіна. Побудуємо функцію Гамільтоніана H для розглянутої антагоністичної диференціальної гри, яка поєднує миттєві втрати системи та динаміку фазових змінних через вектори спряжених змінних:

$$H(C, F, u, v, \lambda_C, \lambda_F) = W_C C^2 + W_F F^2 + \frac{1}{2} R_u u^2 - \frac{1}{2} R_v v^2 + \lambda_C \dot{C} + \lambda_F \dot{F}.$$

Підставляючи вирази для швидкостей зміни стану (1) та (2), отримаємо розгорнутий вигляд Гамільтоніана:

$$H = W_C C^2 + W_F F^2 + \frac{1}{2} R_u u^2 - \frac{1}{2} R_v v^2 + \lambda_C [\alpha v \Psi (1 - C) - \mu C \Theta (F - F_{crit})] + \lambda_F [\beta v C + \kappa u C - \lambda F],$$

де W_C, W_F – вагові коефіцієнти штрафів за рівень компрометації та накопичення неперевірених артефактів; R_u, R_v – вартісні коефіцієнти ресурсів захисника та атакуючого відповідно; λ_C, λ_F – спряжені змінні (тіньові ціни), що визначають граничну цінність зміни кожної з фазових координат для цільової функції гри.

Необхідні умови оптимуму першого порядку $\frac{\partial H}{\partial u} = 0$ та $\frac{\partial H}{\partial v} = 0$ дозволяють отримати аналітичні вирази для оптимальних керувань. Зокрема, для інтенсивності поведінкового аналізу u_t маємо оптимальну стратегію захисту (результат розв'язку гри):

$$u^*(t) = \max\left(0, \min\left(u_{max}, \frac{-\lambda_F \kappa C}{R_u}\right)\right), \quad (3)$$

де λ_F – спряжена змінна (тіньова ціна), що відповідає за внесок цифрових слідів у цільову функцію системи, а R_u – вартість ресурсів на проведення поведінкового аналізу.

Рівняння (3) доводить, що активність захисту повинна зростати пропорційно цінності накопичених ЦС. Це найголовніше рівняння для СППР, див. рис. 1. Воно доводить, що інтенсивність захисту прямо пропорційна тіньовій ціні накопичених артефактів (λ_F).

Запропонована інформаційна технологія реалізується через архітектуру СППР, див. рис. 1, де основним обчислювальним блоком є модуль предиктивного аналізу та також алгоритм FBSM, див. рис. 2 та 3.

Логіка роботи алгоритму наступна:

1. Фаза накопичення. На початковому етапі $\lambda_F < 0$. Це означає, що система «інвестує» ресурси в моніторинг, але доказів ще недостатньо для виправданої ізоляції.

2. Точка перелому тобто момент, коли $\lambda_F = 0$, цінність накопичених слідів стає суттєвою. Це і є предиктивним маркером.

3. Фаза активної дії. Коли $\lambda_F > 0$, СППР автоматично генерує рекомендацію знизити поріг F_{crit}, до прикладу, з 0,5 до 0,2, що відповідно ініціює агресивну ізоляцію підозрілих сегментів мережі.

Ядром запропонованої інформаційної технології є чисельне розв'язання сформульованої антагоністичної диференціальної гри з метою отримання оптимальних стратегій сторін $u^*(t)$, $\upsilon^*(t)$ та, головне, траєкторії тіньової ціни цифрових слідів $\lambda F(t)$. Для цієї мети реалізовано модифікований метод прямої та зворотної стрільби з релаксацією (FBSM), див. рис. 1 та рис. 2. Метода налаштовано до роботи в складі СППР. Алгоритм складається з трьох фаз. Перша – ітераційний пошук сідлової точки гри. Другий – виявлення предиктивного маркера. Третій – основний цикл періодичного перерахунку керувань із налаштуванням критичного порога F_{crit}.

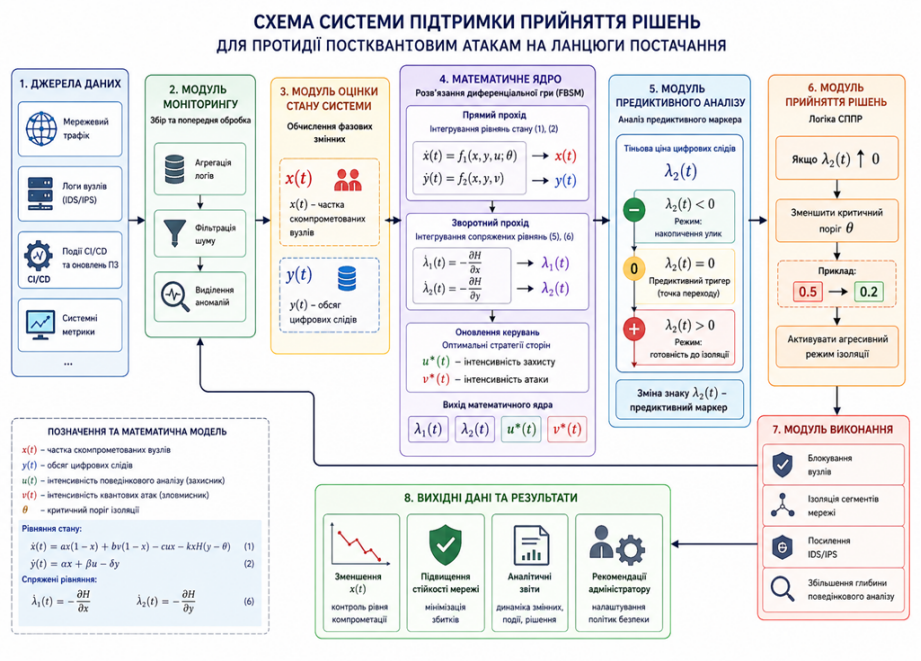

Рис. 1 Блок-схема СППР

Algorithm 1: Алгоритм роботи СППР: базова ітераційна процедура (Фаза 1) – розв'язання диференціальної гри

Вхідні дані : Параметри $\alpha, \mu, F_{\text{crit}}, k, \beta, \kappa, \lambda, W_C, W_F, R_u, R_v, v_{\max}, u_{\max}, \Psi, S_{\text{term}}$, горизонт T, крок Δt.

Вихідні дані : Оптимальні $u^*(t_i), v^*(t_i)$ та траєкторії C^*, F^*, λ_F^*.

Ініціалізація : Дискретизувати $[0,T]$: $t_i = i\Delta t$, $i = 0, \ldots, N-1$;

Початкові керування $u^{(0)}(t_i) = 0$, $v^{(0)}(t_i) = 0$;

Параметр релаксації $\rho \in (0,1]$ (рекомендовано $\rho = 0{,}3$);

Допустима похибка $\varepsilon = 10^{-6}$;

$k \leftarrow 0$;

repeat

  Прямий прохід (рівняння стану);

  Інтегрувати вперед від $t = 0$ до T:

$$\frac{dC}{dt} = \alpha v^{(k)} \Psi (1 - C) - \mu C \tilde{\Theta}(F - F_{\text{crit}}),$$
$$\frac{dF}{dt} = \beta v^{(k)} C + \kappa u^{(k)} C - \lambda F,$$

  з $C(0) = 0$, $F(0) = 0$. Зберегти $C^{(k)}(t_i), F^{(k)}(t_i)$;

  Зворотний прохід (спряжені рівняння);

  Інтегрувати назад від T до 0:

$$\frac{d\lambda_C}{dt} = -2W_C C^{(k)} + \lambda_C \left(\alpha v^{(k)} \Psi + \mu \tilde{\Theta}(F^{(k)} - F_{\text{crit}})\right) - \lambda_F \left(\beta v^{(k)} + \kappa u^{(k)}\right),$$
$$\frac{d\lambda_F}{dt} = 2W_F F^{(k)} + \lambda_C \mu C^{(k)} \tilde{\Theta}'(F^{(k)} - F_{\text{crit}}) + \lambda \lambda_F,$$

  з термінальними умовами $\lambda_C(T) = 2S_{\text{term}} C^{(k)}(T)$, $\lambda_F(T) = 0$;

  Зберегти $\lambda_C^{(k)}(t_i)$, $\lambda_F^{(k)}(t_i)$;

  Оновлення керувань;

  Для кожного t_i обчислити:

$$\tilde{u}(t_i) = -\frac{\lambda_F^{(k)}(t_i)\, \kappa\, C^{(k)}(t_i)}{R_u},$$
$$\tilde{v}(t_i) = \frac{\lambda_C^{(k)}(t_i)\, \alpha\, \Psi\, (1 - C^{(k)}(t_i)) + \lambda_F^{(k)}(t_i)\, \beta\, C^{(k)}(t_i)}{R_v}.$$

  Проекція:

$$u_{\text{new}}(t_i) = \max\left(0,\ \min(u_{\max},\ \tilde{u}(t_i))\right),$$
$$v_{\text{new}}(t_i) = \max\left(0,\ \min(v_{\max},\ \tilde{v}(t_i))\right).$$

  Релаксація;

$$u^{(k+1)}(t_i) = (1 - \rho) u^{(k)}(t_i) + \rho u_{\text{new}}(t_i),$$
$$v^{(k+1)}(t_i) = (1 - \rho) v^{(k)}(t_i) + \rho v_{\text{new}}(t_i).$$

  $k \leftarrow k + 1$;

until $\max_i \left(|u^{(k+1)}(t_i) - u^{(k)}(t_i)|,\ |v^{(k+1)}(t_i) - v^{(k)}(t_i)|\right) < \varepsilon$;

Рис. 2 Модифікований метод прямої та зворотної стрільби з релаксацією (FBSM) (Частина 1)

Algorithm 2: Алгоритм роботи СППР (продовження): виявлення предиктивного маркера та основний цикл (Фази 2–3)

Фаза 2: Маркер λ_F та корекція порога F_{crit}
begin
  Пошук моменту зміни знаку;
  Послідовно перевірити $\lambda_F^*(t_i)$ від $i = 0$ до $N-1$;
  Знайти перший t^*, де $\lambda_F^*(t_{i-1}) < 0$ і $\lambda_F^*(t_i) \geq 0$;
  if *такий t^* знайдено* **then**
    `// Система перейшла від «інвестування» до «окупності»`
    Розрахунок нового порога;
    $F_{\text{crit}}^{\text{new}} = \max\left(F_{\text{crit}}^{\min},\ F_{\text{crit}} - \Delta F\right)$, де ΔF – чутливість (наприклад, 0,2), $F_{\text{crit}}^{\min} = 0{,}1$;
    Рекомендація;
    Сповістити адміністратора (або автоматично встановити $F_{\text{crit}} \leftarrow F_{\text{crit}}^{\text{new}}$);
    `// Повідомлення: «Маркер` λ_F `змінив знак. Рекомендовано знизити поріг до` $F_{\text{crit}}^{\text{new}}$`»`
  else
    `// Маркер відсутній`
    ;
    Залишити поточний F_{crit} без змін;
  end
end
Фаза 3: Основний цикл функціонування СППР
begin
  Оновлення даних;
  Через інтервал ΔT (наприклад, 10 хв) отримати свіжі оцінки α, β, Ψ та частку підозрілих вузлів із SIEM;
  Виконання Фази 1 з актуальним F_{crit} (результат Фази 2 попереднього циклу);
  Виконання Фази 2 для виявлення маркера та корекції F_{crit};
  Застосування керувань;
  Реалізувати стратегію $u^*(t)$ через налаштування DPI та поведінкових сенсорів;
  return *Оновлені політики ізоляції на наступний інтервал* ΔT.
end

Рис. 3 Модифікований метод прямої та зворотної стрільби з релаксацією (FBSM) (Частина 2)

Рисунок 4 містить порівняльний аналіз двох сценаріїв перебігу антагоністичної гри, які відрізняються лише значенням критичного порога накопичення цифрових слідів F_{crit}. Перший сценарій (сині криві) відповідає високому порогу $F_{crit} = 0{,}5$. Сценарій моделює обережну стратегію захисника з високим рівнем довіри до формальної валідності сертифікатів. Другий сценарій (червоні криві) реалізує низький поріг $F_{crit} = 0{,}2$. Другий сценарій характерний для агресивної парадигми захисту. Відповідно, навіть невеликий обсяг атипової поведінки розглядаємо як достатню підставу для ізоляції вузла. Така постановка дає змогу кількісно оцінити виграш від зниження порога, ініційованого спрацюванням предиктивного маркера λF.

На панелі (а) представлено динаміку частки скомпрометованих вузлів $C(t)$ протягом усього горизонту планування $T = 10$. За високого порога система функціонує в пасивно-спостережному режимі. Тобто згладжена функція Хевісайда $\Theta\sim(F - F_{crit})$ залишається близькою до нуля. Відповідно, механізм ізоляції не активується. А крива $C(t)$ монотонно зростає, досягаючи фінального значення. Панель (б) деталізує процес накопичення цифрових слідів $F(t)$ для обох сценаріїв.

У високопороговому випадку (синя крива) $F(t)$ зростає вкрай повільно, не досягаючи $F_{crit} = 0{,}5$ упродовж усього періоду спостереження, що унеможливлює запуск ізоляції. У низькопороговому сценарії (червона крива) завдяки зменшеній швидкості забування слідів ($\lambda = 0{,}1$) та вищій інтенсивності захисного аналізу обсяг $F(t)$ накопичується значно швидше, долаючи поріг $F_{crit} = 0{,}5$ приблизно на 62 % часового горизонту. Момент перетину позначено чорним маркером зі стрілкою. Саме цей перетин є тригером для активації Θ-функції та переходу системи в активний режим протидії. Він же слугує візуальним підтвердженням коректності предиктивного маркера. Тобто починаючи з цієї точки, ізоляція стає економічно виправданою, оскільки накопичений обсяг доказів мінімізує ризик хибних спрацювань.

На панелі (в), зіставлено оптимальні стратегії атакуючого $\upsilon^*(t)$ та захисника $u^*(t)$ для двох порогів. У високопороговому сценарії інтенсивність захисту $u^*(t)$ залишається низькою впродовж усього горизонту (середнє значення $u^*(t)$≈0,051, оскільки система не отримує достатніх підстав для активних дій. Водночас атакуючий підтримує відносно стабільний рівень квантових атак $\upsilon^*(t)$≈0,053. У низькопороговому сценарії картина якісно змінюється. Отже, із наближенням $F(t)$ до F_{crit} захисник стрімко нарощує інтенсивність поведінкового аналізу. Тоді $u^*(t)$ зростає більш ніж удвічі, до середнього $u^*(t)$≈0,142, реалізуючи принцип масштабування. Атакуючий, навпаки, змушений знижувати інтенсивність квантових підробок ($\upsilon^*(t)$≈0,034), оскільки подальші атаки на ізольовані сегменти стають економічно невигідними через зменшення частки вразливих вузлів та зміну знака внеску. Це явище має чітку економічну інтерпретацію. Отже активна ізоляція позбавляє атакуючого плацдармів для поширення, примушуючи його згортати операцію.

Результати чисельного моделювання підтвердили центральну гіпотезу дослідження – у постквантовому середовищі, де криптографічна верифікація втрачає сенс, варіативне налаштування порога F_{crit} на основі предиктивного маркера λF є дієвим інструментом стримування атак на ланцюги постачання. Виявлений ефект – різке зростання захисної активності одразу після перетину порога дає змогу рекомендувати вбудовування модуля обчислення $\lambda F(t)$ у штатні засоби моніторингу безпеки (SIEM/IDS/IPS) для автоматизованого керування політиками ізоляції в реальному часі.

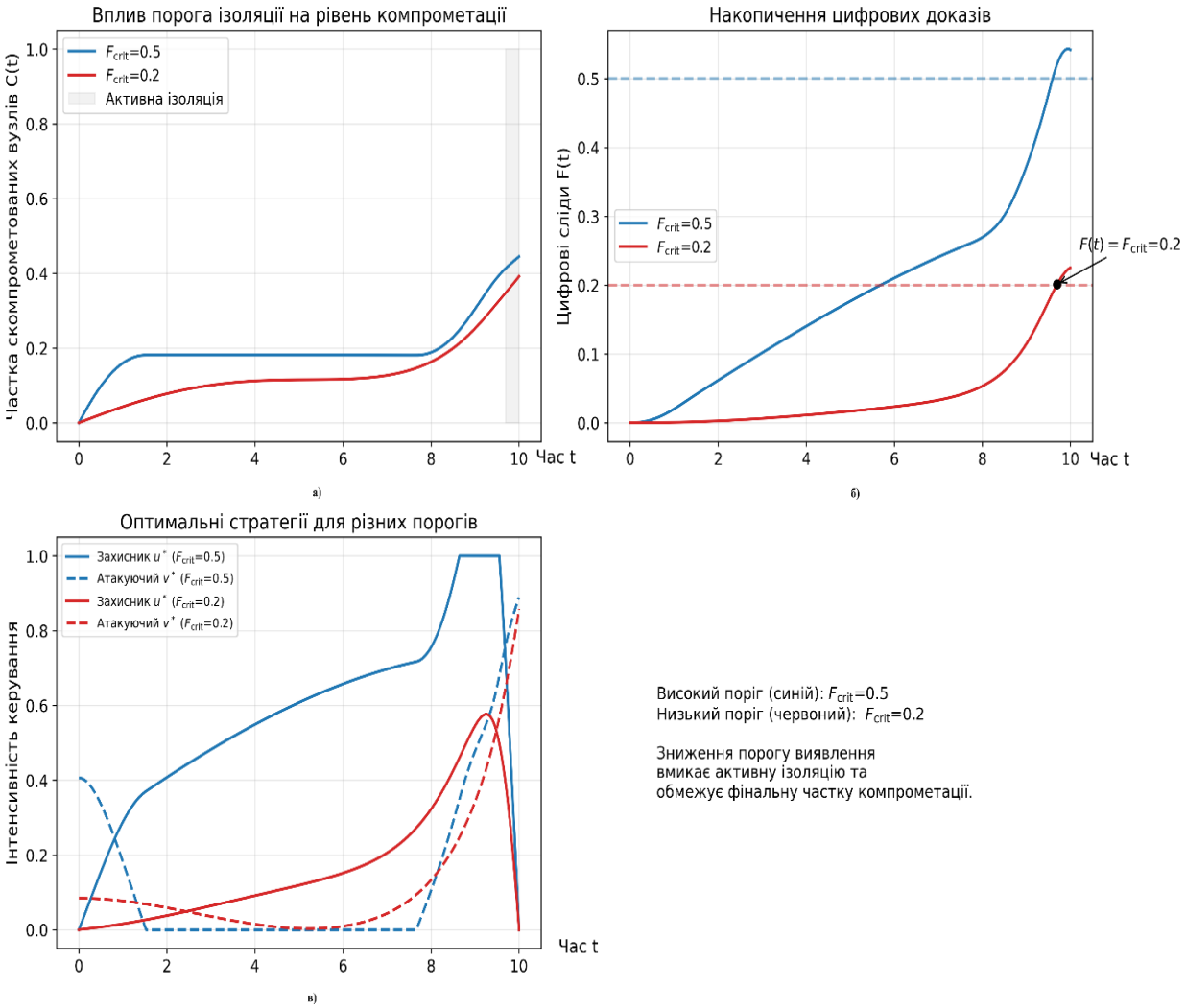

Рис. 4 – Результати обчислювального експерименту

Отже результати моделювання, див. рис. 4 повели переваги предиктивного керування. При високому статичному порозі $F_{crit} = 0{,}5$ (синя крива) система не встигає накопичити достатньо доказів, і частка компрометації $C(t)$ невпинно зростає.

Висновки та перспективи подальшого дослідження.

Розроблено інформаційну технологію СППР, яка базується на використанні тіньової ціни цифрових слідів (ЦС) як предиктивного маркера для гнучкого керування політиками кібербезпеки в постквантовий період. Доведено, що зміна знаку спряженої змінної λ_F є математично обґрунтованою умовою для зміни режиму захисту зі спостережного на активний, що дозволяє уникнути атак при низьких рівнях загрози. Чисельне моделювання підтвердило, що варіативне налаштування критичного порога ізоляції на основі запропонованого маркера забезпечить стійкість гетерогенних мереж навіть за умови ідеальної криптографічної підробки сертифікатів зловмисником.

Показано, що перспективою подальших досліджень є адаптація моделі до умов неповної інформації, коли параметри α та β оцінюються з використанням методів машинного навчання в реальному часі.

Список бібліографічного опису

1. P. W. Shor, "Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Review, Vol. 41, No. 2, 1999, pp. 303-332. doi:10.1137/S0036144598347011
2. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.
3. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.48550/arXiv.1905.09749
4. CISA. (2023). CISA, NSA and NIST Publish New Resource for Migrating to Post-Quantum Cryptography. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/36bf4b2
5. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
6. Joseph, D., Misoczki, R., Manzano, M. *et al.* Transitioning organizations to post-quantum cryptography. *Nature* **605**, 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2
7. Tan, T.G., Szalachowski, P. & Zhou, J. Challenges of post-quantum digital signing in real-world applications: a survey. *Int. J. Inf. Secur.* 21, 937–952 (2022). https://doi.org/10.1007/s10207-022-00587-6
8. The Hacker News. (2023). N. Korean Hackers Distribute Trojanized CyberLink Software in Supply Chain Attack. https://thehackernews.com/2023/11/north-korean-hackers-distribute.html
9. P. Przymus and T. Durieux, "Wolves in the Repository: A Software Engineering Analysis of the XZ Utils Supply Chain Attack," *2025 IEEE/ACM 22nd International Conference on Mining Software Repositories (MSR)*, Ottawa, ON, Canada, 2025, pp. 91-102, doi: 10.1109/MSR66628.2025.00026.
10. P. Ladisa, H. Plate, M. Martinez and O. Barais, "SoK: Taxonomy of Attacks on Open-Source Software Supply Chains," *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, pp. 1509-1526, doi: 10.1109/SP46215.2023.10179304.
11. Kim, HW., Song, EH. Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure. *Int. j. inf. tecnol.* **16**, 5091–5097 (2024). https://doi.org/10.1007/s41870-024-02110-7
12. Demontis, Ambra & Melis, Marco & Biggio, Battista & Maiorca, Davide & Arp, Daniel & Rieck, Konrad & Corona, Igino & Giacinto, Giorgio & Roli, Fabio. (2017). Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection. IEEE Transactions on Dependable and Secure Computing. PP. 10.1109/TDSC.2017.2700270.
13. Basar, T., & Olsder, G. J. (1999). Dynamic noncooperative game theory (2nd ed.). SIAM. https://doi.org/10.1137/1.9781611971132
14. Zhang, Hengwei & Mi, Yan & Fu, Yumeng & Liu, Xiaohu & Zhang, Yuchen & Wang, Jindong & Jinglei, Tan. (2023). Security Defense Decision Method Based on Potential Differential Game for Complex Networks. Computers & Security. 129. 103187. 10.1016/j.cose.2023.103187.
15. Бученко, І. (2025). ІНТЕЛЕКТУАЛЬНЕ УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ У ПЕРИФЕРІЙНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ НА ОСНОВІ ТЕОРІЇ ІГОР. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 180–192. https://doi.org/10.28925/2663-4023.2025.27.732
16. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). ТЕОРЕТИКО-ІГРОВИЙ ПІДХІД ДО МОДЕЛЮВАННЯ КОНФЛІКТІВ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *2*(22), 168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
17. Методика рішення задач із захисту інформації / В. В. Білозерський, О. Ю. Лебедєва, Н. П. Волкова, В. О. Назаров // Informatics and Mathematical Methods in Simulation. - 2023. - Vol.13, N 3-4. - P. 236-242.
18. Кудряшов, А. (2024). Штучний інтелект та безпека у мобільних технологіях 5G та 6G. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, (54), 236-242. https://doi.org/10.36910/6775-2524-0560-2024-54-29

References

1. P. W. Shor, "Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Review, Vol. 41, No. 2, 1999, pp. 303-332. doi:10.1137/S0036144598347011

2. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.
3. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433. https://doi.org/10.48550/arXiv.1905.09749
4. CISA. (2023). CISA, NSA and NIST Publish New Resource for Migrating to Post-Quantum Cryptography. https://content.govdelivery.com/accounts/USDHSCISA/bulletins/36bf4b2
5. National Institute of Standards and Technology. (2024). Module-lattice-based key-encapsulation mechanism standard (FIPS 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
6. Joseph, D., Misoczki, R., Manzano, M. *et al.* Transitioning organizations to post-quantum cryptography. *Nature* **605**, 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2
7. Tan, T.G., Szalachowski, P. & Zhou, J. Challenges of post-quantum digital signing in real-world applications: a survey. *Int. J. Inf. Secur.* 21, 937–952 (2022). https://doi.org/10.1007/s10207-022-00587-6
8. The Hacker News. (2023). N. Korean Hackers Distribute Trojanized CyberLink Software in Supply Chain Attack. https://thehackernews.com/2023/11/north-korean-hackers-distribute.html
9. P. Przymus and T. Durieux, "Wolves in the Repository: A Software Engineering Analysis of the XZ Utils Supply Chain Attack," *2025 IEEE/ACM 22nd International Conference on Mining Software Repositories (MSR)*, Ottawa, ON, Canada, 2025, pp. 91-102, doi: 10.1109/MSR66628.2025.00026.
10. P. Ladisa, H. Plate, M. Martinez and O. Barais, "SoK: Taxonomy of Attacks on Open-Source Software Supply Chains," *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, pp. 1509-1526, doi: 10.1109/SP46215.2023.10179304.
11. Kim, HW., Song, EH. Abnormal behavior detection mechanism using deep learning for zero-trust security infrastructure. *Int. j. inf. tecnol.* **16**, 5091–5097 (2024). https://doi.org/10.1007/s41870-024-02110-7
12. Demontis, Ambra & Melis, Marco & Biggio, Battista & Maiorca, Davide & Arp, Daniel & Rieck, Konrad & Corona, Igino & Giacinto, Giorgio & Roli, Fabio. (2017). Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection. IEEE Transactions on Dependable and Secure Computing. PP. 10.1109/TDSC.2017.2700270.
13. Basar, T., & Olsder, G. J. (1999). Dynamic noncooperative game theory (2nd ed.). SIAM. https://doi.org/10.1137/1.9781611971132
14. Zhang, Hengwei & Mi, Yan & Fu, Yumeng & Liu, Xiaohu & Zhang, Yuchen & Wang, Jindong & Jinglei, Tan. (2023). Security Defense Decision Method Based on Potential Differential Game for Complex Networks. Computers & Security. 129. 103187. 10.1016/j.cose.2023.103187.
15. Buchenko, I. (2025). INTELLIGENT ENERGY CONSUMPTION MANAGEMENT IN EDGE COMPUTING NETWORKS BASED ON GAME THEORY. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *3*(27), 180–192. https://doi.org/10.28925/2663-4023.2025.27.732
16. Shevchenko, S., Zhdanova Y., Skladannyi, P., & Boiko, S. (2023). GAME THEORETICAL APPROACH TO THE MODELING OF CONFLICTS IN INFORMATION SECURITY SYSTEMS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *2*(22), 168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
17. Bilozersky, V. V., Lebedeva, O. Yu., Volkova, N. P., & Nazarov, V. O. (2023). Methodology for solving information security problems. Informatics & Mathematical Methods in Simulation/Informatika ta Matematičnì Metodi v Modelûvannì, 13.
18. Kudryashov, A. (2024). Artificial Intelligence and Security in 5G and 6G Mobile Technologies. *Computer-integrated technologies: education, science, production*, (54), 236-242. https://doi.org/10.36910/6775-2524-0560-2024-54-29

Історія статті:
Отримано: 29.03.2026 Доопрацьовано: 09.04.2026 Прийнято до друку: 23.05.2026 Опубліковано: 29.05.2026