КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1227
УДК 004.056.5

**Лахно Валерій Анатолійович**
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0001-9695-4543
*lva964@nubip.edu.ua*

# МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНОСТІ ПРОАКТИВНОГО ЗАХИСТУ ВІД HNDL АТАК

**Анотація.** Об'єкт дослідження – процес проактивної протидії кіберзагрозам типу «Harvest Now, Decrypt Later» (HNDL) в умовах квантового переходу. Мета роботи – розробка стохастичної теоретико-ігрової моделі конфлікту між Атакуючим та Захисником для оптимізації ресурсів проактивного пошуку загроз в умовах високої волатильності мережевого середовища об'єктів критичної інформаційної інфраструктури (КІІ). В статті використано апарат стохастичних диференціальних ігор (СДІ) з нульовою сумою. Модель побудована на системі стохастичних диференціальних рівнянь Іто, які описують зміну двох головних чинників – кумулятивного обсягу ексфільтрованих даних та «індексу прихованості» зловмисника. Для знаходження оптимальних стратегій управління використано рівняння Гамильтона-Якоби-Беллмана-Айзекса (HJBI). Чисельний розв'язок рівняння отримано методом апроксимації Марківськими ланцюгами (МСАМ). Отримані результати дозволили врахувати нелінійність витрат на захист КІІ та імовірнісну природу виявлення цифрових слідів у зашумленому трафіку КІІ. Проведено обчислювальний експеримент (ОЕ). У межах ОЕ порівняно два контрастні сценарії функціонування КІІ. Перший сценарій це базовий (стабільний трафік). Другий – високоволатильний сценарій з високим рівнем мережевого шуму. Встановлено, що в умовах значної волатильності зловмисник потенційно отримує перевагу через ефект маскування деструктивних дій під «білий шум». Доведено, що ігнорування стохастичної складової при моделюванні HNDL-атак потенційно призведе до статистично значущого заниження оцінки потенційного ущербу для КІІ в середньому на 19 %. Результати дослідження дозволяють Захиснику мінімізувати втрати при будь-яких варіаціях агресивності зловмисника. Новизна роботи полягає в інтеграції варіативного індексу прихованості у стохастичну модель диференціальної гри. Це дає змогу кількісно оцінити ризики відкладеного дешифрування даних в умовах неповного моніторингу мережі КІІ. Практична значущість результатів полягає у можливості впровадження моделі у систему СППР SOC-центрів для розподілу ресурсів у протидії складним стійким загрозам (APT).

**Ключові слова:** кібербезпека, квантовий перехід, HNDL-атаки, стохастичні диференціальні ігри, рівняння Іто, Threat Hunting, індекс прихованості, критична інфраструктура.

## ВСТУП

Розвиток квантових обчислень створив небезпеку для наявних стандартів асиметричного шифрування. Головний виклик полягає не лише у факті досягнення «квантової переваги», а у превентивній стратегії зловмисників, відомій як «Перехоплюй зараз, розшифровуй пізніше» (або Harvest Now, Decrypt Later – HNDL) [1]. В межах цієї стратегії APT-угруповання здійснюють латентне накопичення зашифрованого трафіку об'єктів критичної інформаційної інфраструктури (КІІ) з метою його ретроспективного дешифрування після появи промислових квантових комп'ютерів. Для держав, які перебувають у процесі розвитку цифрових систем, зокрема України, HNDL-атаки становлять стратегічну загрозу. В умовах активного впровадження технологій GovTech та FinTech компрометація даних КІІ потенційне призведе до втрати інформаційного суверенітету в довгостроковій перспективі. Зазначимо, що GovTech (Government Technology) – це сукупність цифрових технологій та платформ, що використовують державні органи для надання електронних публічних послуг, автоматизації державних процесів та забезпечення цифрового суверенітету. У розрізі КІІ – це насамперед національні е-громадські сервіси, реєстри, системи міжвідомчого обміну даними та платформи державних закупівель. Відповідно, FinTech (або Financial Technology) – це інноваційні технологічні рішення у сфері фінансових послуг, які

забезпечують швидкі, безпечні та масштабовані операції з грошима, цінними паперами та фінансовими даними, наприклад в Україні. У розрізі КІІ це включає банківські платформи, платіжні системи, системи дистанційного банківського обслуговування та інфраструктуру ринку капіталу. Чинні методи захисту є малоефективними проти HNDL, оскільки процес збору даних зловмисником зазвичай не порушує доступність сервісів КІІ. А також він часто є непомітним для стандартних систем виявлення вторгнень (IDS). Це зумовило необхідність переходу Захисту до концепції Proactive Threat Hunting, тобто ініціативного пошуку прихованих цифрових слідів (ЦС) присутності атакуючої сторони ще на етапі накопичення трафіку КІІ. Однак цей процес ускладнено імовірнісною природою мережевого середовища. Зокрема, флуктуації легітимного трафіку та мережевий шум перетворили задачу виявлення аномалій на ймовірнісну проблему [1-29]. Наукова новизна та внесок дослідження полягає у розробці стохастичної диференціальної гри, яка моделює конфлікт між APT-угрупованням та Захисником в умовах часткової спостережуваності. На відміну від наявних детермінованих моделей, запропонована модель: 1) інтегрувала «Індекс прихованості» атакуючого, описаний стохастичним рівнянням Ito; 2) врахувала нелінійні витрати Захисника на проактивний пошук загроз у зашумленому середовищі; 3) дозволила синтезувати оптимальні стратегії управління через розв'язання рівняння Гамильтона-Якобі-Беллмана-Айзекса (HJBI).

Зазначимо, що індекс прихованості $S(t)$ – стохастична величина, яка кількісно характеризує ступінь маскування дій атакуючого під легітимну мережеву активність. Тоді значення $S(t)=1$ відповідає ідеальній прихованій активності зловмисника в мережі КІІ. А зниження індексу віддзеркалить зростання ймовірності виявлення цифрових слідів (ЦС) засобами проактивного Threat Hunting. Також зазначимо, що зашумлений трафік КІІ – це сукупність випадкових флуктуацій, спричинених легітимними сплесками навантаження, варіаціями затримок пакетів та іншими стохастичними факторами мережевого середовища. Саме цей шум робить ЦС зловмисника статистично невідрізними від нормальної активності, що суттєво ускладнює їх виявлення стандартними засобами моніторингу безпеки КІІ.

Постановка проблеми. Ефективна протидія стратегіям HNDL ускладнена глибокою інформаційною асиметрією. Тобто Атакуючий діє латентно на етапі накопичення даних КІІ. Захисник змушений приймати рішення в умовах невизначеності що до дій зловмисника. Чинні теоретико-ігрові моделі захисту переважно спираються на детерміновані закони аналізу процесів накопичення даних КІІ. А це не дозволяє адекватно врахувати два важливі чинники. Перший – ймовірнісна природа ЦС. Виявлення артефактів APT-групи в трафіку не є гарантованим через вплив мережевого шуму, флуктуацій навантаження та ризику хибнопозитивних спрацьовувань. Другий – ресурсна витратність проактивного пошуку. Тобто реалізація стратегії Threat Hunting потребує значних обчислювальних та кадрових ресурсів КІІ. А це в умовах зашумленого середовища призведе до надмірних операційних витрат.

Отже, постає наукова проблема синтезу оптимальних стратегій управління в умовах антагоністичного конфлікту, в якому коливання прихованості зловмисника та обсяг ексфільтрованих даних є випадковими процесами. З математичної точки зору задача сформульована так – пошук сідлової точки у стохастичній диференціальній грі з нульовою сумою. Мета Захисника – мінімізація функціонала очікуваних втрат, відповідно вартість даних та витрати на пошук. Мета Атакуючого – максимізація через вибір темпу крадіжки, що балансує між швидкістю накопичення інформації та ризиком передчасного виявлення.

Аналіз останніх досліджень і публікацій. Проблема забезпечення кіберстійкості КІІ набула нового виміру в реаліях наближення квантового переходу. Як зазначено у стандартах NIST [22] та аналітичних оглядах [7, 12], поява промислових квантових обчислювачів здатна скомпрометувати чинні асиметричні алгоритми шифрування. Це зумовило актуалізацію специфічного класу відкладених загроз HNDL. Автори досліджень [1, 9, 10, 21] підкреслили, що головна небезпека HNDL-атак полягає в латентному перехопленні та накопиченні зашифрованого трафіку для його ретроспективного дешифрування в майбутньому.

Специфіка сучасних цільових атак (APT) детально розглянута в [8, 19, 20]. Автори звернули увагу на тенденцію переходу до «безмалварних» вторгнень [29], де активність зловмисника здійснюють через легітимні інструменти адміністрування. У подібних умовах наявні реактивні системи виявлення вторгнень стали малоефективними. Останнє пов’язано із тим, що збір даних Атакуючим не призводить до порушення доступності сервісів КІІ. Це вимагає зміни парадигми захисту КІІ в бік проактивного пошуку загроз або Threat Hunting, алгоритмічні та концептуальні засади якого висвітлено у [11, 17].

Для математичного моделювання протиборства між Захисником та Атакуючим зазвичай застосовують апарат теорії ігор [26, 27]. Зокрема, у [15] використано диференціальні ігри використано для оцінювання витрат фінансових ресурсів сторін під час реалізації APT-атаки. Проте більшість наявних рішень спиралася на детерміновані моделі. Або автори розглядали статичні сценарії HNDL-атак. А це

дозволяє адекватно врахувати ймовірнісну природу цифрових слідів у зашумленому мережевому середовищі КІІ.

Як доведено у [5, 16, 23, 25], перехід до стохастичних диференціальних ігор (СДІ) з нульовою та ненульовою сумою дозволить ефективніше описати зміни систем КІІ. Застосування математичного апарату неперервних процесів, зокрема стохастичних диференціальних рівнянь (СДР) Іто для моделювання систем під впливом «білого шуму», досліджено у [3, 4, 6].

Знаходження оптимальних стратегій в антагоністичних СДІ зводиться до розв'язання рівняння Гамильтона-Якоби-Беллмана-Айзекса (HJBI). Фундаментальні теоретичні аспекти динамічного програмування та крайові умови для таких рівнянь описані в роботах [2, 18]. Оскільки отримання аналітичного розв'язку для складних нелінійних моделей конфлікту є неможливим, автори запропонували застосовувати чисельні методи. Серед них виділимо метод апроксимації марковськими ланцюгами (МСАМ) [14], напівдискретні схеми високої роздільної здатності [13] та градієнтні алгоритми мінімаксного пошуку [28].

Незважаючи на ґрунтовну теоретичну базу щодо моделювання кіберфізичних систем, питання оцінки ризиків HNDL-атак залишилося недостатньо дослідженим. У розглянутих публікаціях відсутні моделі, які б інтегрували «індекс прихованості» Атакуючого у середовище диференціальної гри. Крім того, наявні методи та моделі не враховують нелінійність ресурсоємності процесу Threat Hunting при варіативній волатильності легітимного трафіку КІІ. Під волатильністю розуміємо значні стохастичні флуктуації параметрів трафіку, як-от обсяг пакетів, затримок, типових показників навантаження, характерних для систем GovTech та FinTech з піковими сплесками легітимного трафіку. Це підтвердило релевантність розробки математичної моделі, здатної кількісно оцінити ефективність проактивного захисту від латентного накопичення даних із урахуванням мережевого шуму в КІІ.

Мета та завдання дослідження. Мета роботи – обґрунтуванні теоретико-ігрової моделі проактивної протидії HNDL-атакам на КІІ та оцінці впливу волатильності мережевого середовища на ефективність стратегій захисту.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Сформулювати концептуальну модель конфлікту «Захисник – Атакуючий» у фазі латентного накопичення трафіку з урахуванням ймовірнісного характеру цифрових слідів.
2. Розробити математичний апарат на базі системи стохастичних диференціальних рівнянь Іто для опису коливань обсягу ексфільтрованих даних та індексу прихованості зловмисника.
3. Сформувати оптимальні стратегії проактивного пошуку загроз через розв'язання рівняння Гамильтона-Якоби-Беллмана-Айзекса.
4. Провести порівняльний аналіз двох сценаріїв функціонування КІІ (базового зі стабільним трафіком та високоволатильного) для кількісного оцінювання ризиків, що ігноруються детермінованими моделями.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В основі моделі лежить концепція безперервного протиборства двох агентів у стохастичному середовищі. Конфлікт розглянуто на горизонті планування $t \in [0, T]$ і описано вектором стану:

$$Y(t) = [X(t), S(t)]^T, \tag{1}$$

де $X(t)$ $u$ кумулятивний обсяг даних, ексфільтрованих зловмисником; $S(t)$ – індекс прихованості Атакуючого $S \in (0,1]$, де $S = 1$ відповідає ідеальному маскуванню.

Зміни станів описано системою нелінійних стохастичних диференціальних рівнянь Іто:

$$\begin{cases} dX(t) = \mu_x v(t) S(t) dt + \sigma_x v(t) S(t) dW_1(t); \\ dS(t) = -(\alpha v(t)^\theta + \beta u(t)) S(t) dt + \sigma_s S(t) dW_2(t), \end{cases} \tag{2}$$

де $u(t), v(t)$ – інтенсивність дій Захисника та Атакуючого (тобто агресивність перехоплення); $\mu_x, \sigma_x$ – параметри пропускної здатності та волатильності каналу; $\alpha, \theta$ – коефіцієнти, що визначають нелінійний «штраф» за агресивність атаки (демаскування); $dW_1, dW_2$ – вінерівські процеси, що моделюють мережевий шум.

Конфлікт моделюємо як антагоністичні гру з нульовою сумою. Захисник прагне мінімізувати, а Атакуючий максимізувати очікуваний ущерб $J(u,v)$:

$$J(u,v) = \mathrm{E}\left[\int_0^T (QX(t) + \frac{1}{2}R_v v^2 - \frac{1}{2}R_u u^2)dt + \Phi(X(T), S(T))\right], \quad (3)$$

де $Q$ – стратегічна цінність даних, а $R_u, R_v$ – вагові коефіцієнти витрат сторін. Термінальний член $\Phi$ враховує, що при виявленні зловмисника ($S(T) \to 0$) цінність вкрадених даних фактично нівельована.

Для знаходження оптимальних стратегій використано рівняння Гамильтона-Якоби-Беллмана-Айзекса (HJBI). Оскільки аналітичний розв'язок для такої нелінійної системи отримати неможливо, у роботі застосовано метод апроксимації марковськими ланцюгами (MCAM). Це дозволило перейти від неперервних процесів Ito до дискретної сітки станів і знайти сідлову точку гри чисельними методами. Управління Захисника $u(t)$ відповідає інтенсивності виділення ресурсів – кількість активних сесій Threat Hunting, потужності DPI-систем тощо. Управління Атакуючого $v(t)$ віддзеркалює агресивність HNDL-атаки. Тобто це частка цілеспрямовано перехоплених пакетів мережі КІІ. Зазначимо, що під агресивністю HNDL-атаки в межах запропонованої моделі розуміємо частку мережевих пакетів КІІ, які Атакуючий цілеспрямовано перехоплює в поточний момент часу. Цей параметр відобразить інтенсивність латентної ексфільтрації даних і безпосередньо вплине на швидкість накопичення вкраденої інформації. Наприклад у високоволатильному сценарії функціонування FinTech-платформи банку під час пікового навантаження, як от, у кінці місяця при масових виплатах зарплат, Атакуючий тимчасово підвищує агресивність атаки з 5 % до 35 % перехоплених пакетів. У стабільному трафіку така дія одразу спричинила б стрімке падіння індексу прихованості та ймовірне виявлення. Натомість у зашумленому середовищі сплеск легітимного трафіку маскує додаткові 30 % перехоплених пакетів під «білий шум». Відповідно це дозволить зловмиснику суттєво прискорити накопичення даних без пропорційного зростання ризику передчасного виявлення. Стохастичні члени $\sigma_x$ та $\sigma_s$ кількісно описують рівень фонового «шуму» мережі КІІ, що включає волатильність затримок, нетипові сплески легітимного трафіку та відсоток хибнопозитивних спрацювань систем моніторингу.

Метою експерименту є кількісна оцінка ефективності проактивної стратегії захисту в умовах різного рівня мережевої волатильності. Для моделювання обрано два сценарії:

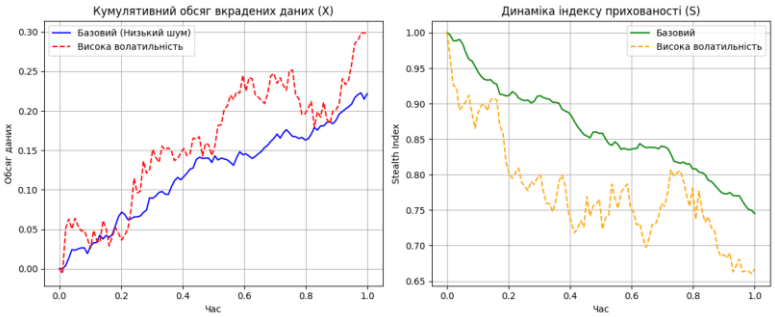
Базовий сценарій А – низький рівень мережевого шуму ($\sigma_x = 0,1, \sigma_s = 0,05$). Моделює стабільне корпоративне середовище з чітко визначеними профілями трафіку.

Сценарій Б, тобто висока волатильність трафіку – середовище зі значними флуктуаціями ($\sigma_x = 0,4, \sigma_s = 0,25$). Значення параметрів обрано з урахуванням специфіки національних сегментів КІІ, зокрема GovTech та FinTech платформ, де фіксують регулярні пікові навантаження та високу дисперсія легітимного трафіку. Це створює ідеальні умови для маскування APT-угруповань під «білий шум» систем КІІ. Під «білим шумом» мережі КІІ у межах запропонованої моделі розуміємо сукупність природних стохастичних флуктуацій мережевого середовища, які описуємо вінерівськими процесами в системі диференціальних рівнянь Ito. Цей шум охоплює волатильність затримок передачі пакетів, спонтанні сплески легітимного трафіку, а також хибнопозитивні спрацювання засобів моніторингу кібербезпеки КІІ. Параметри $\sigma_x, \sigma_s$ кількісно відображають рівень фонового шуму. А це робить виявлення цифрових слідів APT-угруповань імовірнісною задачею. У високоволатильному середовищі «білий шум» забезпечує маскування деструктивних дій зловмисника, перетворюючи їх на статистично невідрізнимі від нормальних коливань трафіку.

Для обох сценаріїв встановимо часовий горизонт $T = 100$ кроків. Початковий стан системи наступний: $X(0) = 0$ (дані не вкрадено), $S(0) = 1,0$ (повна прихованість атакуючого). Критерій ефективності – інтегральний показник очікуваного ущербу $J$.

Аналіз отриманих графічних залежностей, які наведено на рис. 1 а та б), дозволив зробити висновки про фундаментальну різницю у поведінці системи за різних рівнів мережевої волатильності. Порівняння траєкторій накопичення даних, див. рис. 1 б) $X(t)$ показало, що в Сценарії А (базовий) процес витоку інформації є майже лінійним. Тобто він є прогнозованим. Це свідчить про те, що в стабільному середовищі КІІ Захисник зможе ефективно оцінити швидкість HNDL-атаки. Отже захист здатен вчасно застосовувати контрзаходи для мінімізації наслідків HNDL-атаки.

Натомість у Сценарії Б (висока волатильність) спостерігаємо не лише зростання амплітуди коливань, а й зміщення середнього значення обсягу вкрадених даних у бік збільшення. Високий рівень стохастичного шуму ($\sigma_x = 0,4$) дозволить Атакуючому періодично нарощувати інтенсивність перехоплення трафіку без пропорційного зростання ризику виявлення.




а) Коливання кумулятивної ексфільтрації даних б) Коливання індексу прихованості

*Рис. 1. Результати обчислювального експерименту*

Результати моделювання підтвердили, що ігнорування стохастичної складової HNDL-атаки призведе до заниження потенційного ущербу в середньому на 18,7-19,2%. Для об'єктів КІІ така похибка є неприйнятною. Це пов'язано з тим, що така похибка створить ілюзію безпеки при фактичному перевищенні порогів допустимого ризику для КІІ.

Графік змін індексу прихованості $S(t)$ віддзеркалив латентність HNDL-атак. Так у базовому сценарії індекс прихованості знижувався під час емуляції доволі стабільно. Це означає, що заходи Threat Hunting дали накопичувальний ефект. Відповідно це дало змогу «витіснити» зловмисника з тіні. У волатильному сценарії крива $S(t)$ (показана помаранчевим кольором на рис. 1 б) має високу дисперсію. Маємо часові інтервали, коли індекс прихованості демонстрував локальне зростання, попри активні дії Захисника. Це пояснюється тим, що в умовах зміни параметрів мережі цифрові сліди (ЦС) зловмисника стають статистично невідмінними від легітимних аномалій трафіку.

Отримані результати довели наступне – для ефективного захисту систем КІІ недостатньо нарощувати потужність систем моніторингу. Необхідне впровадження варіативних стратегій управління захистом КІІ. Такі стратегії доцільно будувати на розв'язанні рівняння HJBI, оскільки вони дозволяють Захиснику варіативно коригувати інтенсивність проактивного пошуку. А також враховувати поточний рівень «зашумленості» каналів.

З практичної точки зору, виявлена похибка у 18,7-19,2% має пріоритетне значення для управління бюджетами КІІ на кібербезпеку. Вона математично доводить, що розрахунок ресурсів SOC-центрів виключно на основі детермінованих політик безпеки залишає КІІ вразливою до латентних HNDL-атак у зашумленому середовищі. Точка рівноваги, знайдена за допомогою СДІ та рівняння HJBI, дозволить адміністраторам мереж КІІ сформувати угоди про рівень послуг (SLA) таким чином, щоб додаткові інвестиції у проактивний Threat Hunting не перевищували межу економічної доцільності, але гарантовано перекривали ризики HNDL-атак.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведено дослідження проблеми протидії латентним загрозам типу Harvest Now, Decrypt Later (HNDL) в умовах квантового переходу. На основі отриманих результатів зроблено такі висновки:

Запропоновано теоретико-ігрову модель проактивного захисту об'єктів критичної інформаційної інфраструктури (КІІ), яка, на відміну від чинних детермінованих моделей, базується на математичному апараті стохастичних диференціальних ігор. Модель адекватно описує конфлікт між Атакуючим та Захисником через систему рівнянь Ітo, що враховують коливання «індексу прихованості» зловмисника та обсягу ексфільтрованих даних у зашумленому мережевому середовищі.

Отримано оптимальні стратегії управління ресурсами SOC-центрів шляхом чисельного розв'язання рівняння Гамильтона-Якоби-Беллмана-Айзекса (HJBI) із застосуванням методу апроксимації марковськими ланцюгами. Це дало змогу визначити точку рівноваги, яка мінімізує очікувані втрати Захисника при довільних змінах агресивності Атакуючого.

Проведено обчислювальні експерименти та виконано порівняльний аналіз двох сценаріїв функціонування КІІ. Обчислювальний експеримент підтвердив, що ігнорування стохастичної природи мережевого трафіку призведе до заниження оцінки потенційного ущербу в середньому на 19 %.

Продемонстровано, що практична значущість результатів полягає у можливості використання запропонованої моделі для наукового обґрунтування бюджетів на кібербезпеку та оптимізації інтенсивності процесів Threat Hunting. Використання моделі для корегування стратегій дозволить запобігти накопиченню неприпустимих обсягів зашифрованих даних зловмисниками ще до моменту появи промислових квантових обчислювачів.

Перспективи подальших досліджень пов'язані з розширенням моделі для випадку гри з багатьма учасниками, так звані коаліційні атаки APT-угруповань, а також інтеграцією методів глибокого навчання для оцінки параметрів волатильності мережі у синхронному режимі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Baseri, Y., & Waller, E. (2026). *Quantum attacks targeting nuclear power plants: Threat analysis, defense and mitigation strategies*. arXiv. https://doi.org/10.48550/arXiv.2602.21524
2. Bertsekas, D. P. (2022). *Abstract dynamic programming*. Athena Scientific.
3. Blanchet, J., & Zhang, F. (2020). Exact simulation for multivariate Itô diffusions. *Advances in Applied Probability*, *52*(4), 1003-1034. https://doi.org/10.1017/apr.2020.39
4. Bogoi, A., Dan, C. I., Strătilă, S., Cican, G., & Crunteanu, D. E. (2023). Assessment of stochastic numerical schemes for stochastic differential equations with white noise using Itô's integral. *Symmetry, 15*(11), 2038. https://doi.org/10.3390/sym15112038
5. Buckdahn, R., Cardaliaguet, P., & Rainer, C. (2004). Nash equilibrium payoffs for nonzero-sum stochastic differential games. *SIAM Journal on Control and Optimization, 43*(2), 624-642. https://doi.org/10.1137/S0363012902411556
6. Di Girolami, C., & Russo, F. (2014). Generalized covariation for Banach space valued processes, Itô formula and applications. *Probability Theory and Related Fields*.
7. Erol, V. (2025). *The strategic imperative of quantum readiness: A comprehensive review of post-quantum cryptography*. Preprints.org. https://doi.org/10.20944/preprints202509.1720.v1
8. Haddon, D. A. (2020). Attack vectors and the challenge of preventing data theft. In *Cyber security practitioner's guide* (pp. 1-50). https://doi.org/10.1142/9789811204463_0001
9. Jena, J. (2025). The quantum security deadline: Building crypto-agility against "Harvest Now, Decrypt Later" threats. *European Journal of Computer Science and Information Technology, 13*(52), 35-52. https://doi.org/10.37745/ejcsit.2013/vol13n523552
10. Kagai, F., Branch, P., But, J., & Allen, R. (2025). Harvest-now, decrypt-later: A temporal cybersecurity risk in the quantum transition. *Telecom, 6*(4), 100. https://doi.org/10.3390/telecom6040100
11. Kulkarni, M. S., Ashit, D. H., & Chetan, C. N. (2023). A proactive approach to advanced cyber threat hunting. In *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE. https://doi.org/10.1109/CSITSS60515.2023.10334219
12. Kulkarni, S. S., & Thakar, H. (2025). Quantum cryptanalysis: Analyzing Shor's algorithm and its impact on RSA. In *Proceedings of the 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*(Vol. 1181, p.347).Springer. https://doi.org/10.1007/978-981-97-8861-3_30
13. Kurganov, A., & Tadmor, E. (2000). New high-resolution semi-discrete central schemes for Hamilton–Jacobi equations. *Journal of Computational Physics, 160* (2), 720-742. https://doi.org/10.1006/jcph.2000.6485
14. Kushner, H. J. (1990). Numerical methods for stochastic control problems in continuous time. *SIAM Journal on Control and Optimization, 28*(5), 999-1048. https://doi.org/10.1137/032805
15. Lakhno, V., Malyukov, V., Makulov, K., Bebeshko, B., Chubaievskyi, V., Zvieriev, V., & Malyukova, I. (2024). Differential quality game for assessing the financial resources of parties during an APT attack. In *Computer Science On-line Conference* (pp. 404-415). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70285-3_30
16. Li, J., & Li, W. (2019). Nash equilibrium payoffs for non-zero-sum stochastic differential games without Isaacs condition. *Stochastics, 91*(1), 1-36. https://doi.org/10.1080/17442508.2018.1499104
17. Li, J., Zhang, R., Liu, J., & Liu, G. (2022). LogKernel: A threat hunting approach based on behaviour provenance graph and graph kernel clustering. *Security and Communication Networks, 2022*, 4577141. https://doi.org/10.1155/2022/4577141
18. Lions, P.-L. (1985). Neumann type boundary conditions for Hamilton–Jacobi equations. *Duke Mathematical Journal, 52*(4), 793-820. https://doi.org/10.1215/S0012-7094-85-05242-1

19. Makoshi, S. M. (2025). *The evolving cyber battlefield: A comprehensive analysis of state-sponsored APTs, TTPs, and strategic cyber defense mechanisms*. Authorea Preprints. https://doi.org/10.22541/au.175070902.28093557/v1
20. Małecka, A. (2024). Non-state actors in nation-state cyber operations. *Rocznik Bezpieczeństwa Międzynarodowego, 18*(1), 45-64. https://doi.org/10.34862/rbm.2024.1.4
21. Mascelli, J., & Rodden, M. (2025). "Harvest now decrypt later": Examining post-quantum cryptography and the data privacy risks for distributed ledger networks. *Journal of Data Privacy*. http://dx.doi.org/10.17016/FEDS.2025.093
22. National Institute of Standards and Technology. (2024). *FIPS 203, 204, and 205: Post-quantum cryptography standards*. U.S. Department of Commerce.
23. Park, S., Park, B., Lee, M., & Lee, C. (2023). Neural stochastic differential games for time-series analysis. *AI Research*.
24. Sasirekha, K. (2013). Users cell phone and short message service to prevent password stealing and password reuse attacks. In *International Conference on Engineering and Technology* (p. 102).
25. Ye, P., Tur, A., & Wu, Y. (2025). Non-renewable resource extraction model with uncertainties. *Games, 16*(5), 52. https://doi.org/10.3390/g16050052
26. Zhang, L. (2024). *Differential privacy and game theory in cybersecurity* [Doctoral dissertation, University of Technology Sydney].
27. Zhang, L., Zhu, T., Xiong, P., Zhou, W., & Yu, P. S. (2021). More than privacy: Adopting differential privacy in game-theoretic mechanism design. *ACM Computing Surveys, 54*(7), 1-37. https://doi.org/10.1145/3460771
28. Zheng, T., Zhu, L., So, A. M. C., Blanchet, J., & Li, J. (2023). Universal gradient descent ascent method for nonconvex-nonconcave minimax optimization. *Advances in Neural Information Processing Systems, 36*, 54075-54110.
29. Zimba, A. (2017). Malware-free intrusion: A novel approach to ransomware infection vectors. *International Journal of Computer Science and Information Security, 15*(2), 317.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

**Valerii Lakhno**
Doctor of Technical Sciences, Professor,
Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-9695-4543
*lva964@nubip.edu.ua*

## EFFICIENCY EVALUATION MODEL OF PROACTIVE DEFENSE AGAINST HNDL ATTACKS

**Abstract.** The object of the study is the process of proactive counteraction to cyber threats of the "Harvest Now, Decrypt Later" (HNDL) type in the context of the quantum transition. The aim of the paper is to develop and justify a stochastic game-theoretic model of the conflict between an Attacker and a Defender to optimize proactive threat hunting resources under conditions of high network volatility in critical information infrastructure (CII). The paper employs the framework of zero-sum stochastic differential games (SDG). In contrast to classical deterministic models, the proposed model is built upon a system of Itô stochastic differential equations describing the dynamics of two primary factors: the cumulative volume of exfiltrated data and the intruder's "Stealth Index." The Hamilton-Jacobi-Bellman-Isaacs (HJBI) equation is utilized to find optimal control strategies. The numerical solution of the equation is obtained using the Markov chain approximation method (MCAM). The findings allow for accounting for the non-linearity of CII protection costs and the probabilistic nature of detecting digital footprints within noisy CII traffic. A computational experiment (CE) was conducted, comparing two contrasting CII operation scenarios: a baseline scenario (stable traffic) and a high-volatility scenario with a high level of network noise. It is established that under significant volatility, the attacker gains a strategic advantage through the effect of masking destructive actions as "white noise." It is proven that ignoring the stochastic component when modeling HNDL attacks potentially leads to a statistically significant underestimation of potential CII damage by an average of 19%. Optimal proactive search intensity trajectories are synthesized. The research results enable the Defender to minimize losses regardless of the attacker's level of aggression. The scientific novelty lies in the integration of a variable stealth index into the stochastic differential game model, which allows for the quantitative assessment of delayed data decryption risks under conditions of incomplete CII network monitoring. The practical significance of the results consists in the possibility of implementing the model into the decision support systems of Ukrainian SOC centers for resource allocation in countering advanced persistent threats (APT).

**Keywords:** cybersecurity, quantum transition, HNDL attacks, stochastic differential games, Itô equations, threat hunting, stealth index, critical infrastructure.

### REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Baseri, Y., & Waller, E. (2026). *Quantum attacks targeting nuclear power plants: Threat analysis, defense and mitigation strategies*. arXiv. https://doi.org/10.48550/arXiv.2602.21524
2. Bertsekas, D. P. (2022). *Abstract dynamic programming*. Athena Scientific.
3. Blanchet, J., & Zhang, F. (2020). Exact simulation for multivariate Itô diffusions. *Advances in Applied Probability, 52*(4), 1003-1034. https://doi.org/10.1017/apr.2020.39
4. Bogoi, A., Dan, C. I., Strătilă, S., Cican, G., & Crunteanu, D. E. (2023). Assessment of stochastic numerical schemes for stochastic differential equations with white noise using Itô's integral. *Symmetry, 15*(11), 2038. https://doi.org/10.3390/sym15112038
5. Buckdahn, R., Cardaliaguet, P., & Rainer, C. (2004). Nash equilibrium payoffs for nonzero-sum stochastic differential games. *SIAM Journal on Control and Optimization, 43*(2), 624-642. https://doi.org/10.1137/S0363012902411556
6. Di Girolami, C., & Russo, F. (2014). Generalized covariation for Banach space valued processes, Itô formula and applications. *Probability Theory and Related Fields.*

7. Erol, V. (2025). *The strategic imperative of quantum readiness: A comprehensive review of post-quantum cryptography*. Preprints.org. https://doi.org/10.20944/preprints202509.1720.v1
8. Haddon, D. A. (2020). Attack vectors and the challenge of preventing data theft. In *Cyber security practitioner's guide* (pp. 1-50). https://doi.org/10.1142/9789811204463_0001
9. Jena, J. (2025). The quantum security deadline: Building crypto-agility against "Harvest Now, Decrypt Later" threats. *European Journal of Computer Science and Information Technology, 13*(52), 35-52. https://doi.org/10.37745/ejcsit.2013/vol13n523552
10. Kagai, F., Branch, P., But, J., & Allen, R. (2025). Harvest-now, decrypt-later: A temporal cybersecurity risk in the quantum transition. *Telecom, 6*(4), 100. https://doi.org/10.3390/telecom6040100
11. Kulkarni, M. S., Ashit, D. H., & Chetan, C. N. (2023). A proactive approach to advanced cyber threat hunting. In *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE. https://doi.org/10.1109/CSITSS60515.2023.10334219
12. Kulkarni, S. S., & Thakar, H. (2025). Quantum cryptanalysis: Analyzing Shor's algorithm and its impact on RSA. In *Proceedings of the 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*(Vol. 1181, p.347).Springer. https://doi.org/10.1007/978-981-97-8861-3_30
13. Kurganov, A., & Tadmor, E. (2000). New high-resolution semi-discrete central schemes for Hamilton–Jacobi equations. *Journal of Computational Physics, 160* (2), 720-742. https://doi.org/10.1006/jcph.2000.6485
14. Kushner, H. J. (1990). Numerical methods for stochastic control problems in continuous time. *SIAM Journal on Control and Optimization, 28*(5), 999-1048. https://doi.org/10.1137/032805
15. Lakhno, V., Malyukov, V., Makulov, K., Bebeshko, B., Chubaievskyi, V., Zvieriev, V., & Malyukova, I. (2024). Differential quality game for assessing the financial resources of parties during an APT attack. In *Computer Science On-line Conference* (pp. 404-415). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-70285-3_30
16. Li, J., & Li, W. (2019). Nash equilibrium payoffs for non-zero-sum stochastic differential games without Isaacs condition. *Stochastics, 91*(1), 1-36. https://doi.org/10.1080/17442508.2018.1499104
17. Li, J., Zhang, R., Liu, J., & Liu, G. (2022). LogKernel: A threat hunting approach based on behaviour provenance graph and graph kernel clustering. *Security and Communication Networks, 2022*, 4577141. https://doi.org/10.1155/2022/4577141
18. Lions, P.-L. (1985). Neumann type boundary conditions for Hamilton–Jacobi equations. *Duke Mathematical Journal, 52*(4), 793-820. https://doi.org/10.1215/S0012-7094-85-05242-1
19. Makoshi, S. M. (2025). *The evolving cyber battlefield: A comprehensive analysis of state-sponsored APTs, TTPs, and strategic cyber defense mechanisms*. Authorea Preprints. https://doi.org/10.22541/au.175070902.28093557/v1
20. Małecka, A. (2024). Non-state actors in nation-state cyber operations. *Rocznik Bezpieczeństwa Międzynarodowego, 18*(1), 45-64. https://doi.org/10.34862/rbm.2024.1.4
21. Mascelli, J., & Rodden, M. (2025). "Harvest now decrypt later": Examining post-quantum cryptography and the data privacy risks for distributed ledger networks. *Journal of Data Privacy*. http://dx.doi.org/10.17016/FEDS.2025.093
22. National Institute of Standards and Technology. (2024). *FIPS 203, 204, and 205: Post-quantum cryptography standards*. U.S. Department of Commerce.
23. Park, S., Park, B., Lee, M., & Lee, C. (2023). Neural stochastic differential games for time-series analysis. *AI Research*.
24. Sasirekha, K. (2013). Users cell phone and short message service to prevent password stealing and password reuse attacks. In *International Conference on Engineering and Technology* (p. 102).
25. Ye, P., Tur, A., & Wu, Y. (2025). Non-renewable resource extraction model with uncertainties. *Games, 16*(5), 52. https://doi.org/10.3390/g16050052

26. Zhang, L. (2024). *Differential privacy and game theory in cybersecurity* [Doctoral dissertation, University of Technology Sydney].
27. Zhang, L., Zhu, T., Xiong, P., Zhou, W., & Yu, P. S. (2021). More than privacy: Adopting differential privacy in game-theoretic mechanism design. *ACM Computing Surveys, 54*(7), 1-37. https://doi.org/10.1145/3460771
28. Zheng, T., Zhu, L., So, A. M. C., Blanchet, J., & Li, J. (2023). Universal gradient descent ascent method for nonconvex-nonconcave minimax optimization. *Advances in Neural Information Processing Systems, 36*, 54075-54110.
29. Zimba, A. (2017). Malware-free intrusion: A novel approach to ransomware infection vectors. *International Journal of Computer Science and Information Security, 15*(2), 317.

Отримано редакцією журналу / Received: 20.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26