КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.913
УДК 004.056:004.75

Яскевич Юрій Владиславович
аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID:0009-0005-6084-5229
y.yaskevych.asp@kubg.edu.ua

ІГРОВО-ОПТИМІЗАЦІЙНА МОДЕЛЬ ВИБОРУ ЗАСОБІВ ЗАХИСТУ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. У статті запропоновано ігрово-оптимізаційну модель вибору засобів захисту розподілених інформаційних систем (РІС) в умовах цілеспрямованої кібернетичної протидії. Актуальність дослідження зумовлена зростанням складності архітектури розподілених інформаційних систем, обмеженістю ресурсів сторони захисту на безпеку та наявністю раціонального або обмежено-раціонального противника, дії якого мають стратегічний характер. На відміну від наявних оптимізаційних методів та моделей і традиційних ігрових моделей, запропонована модель поєднала мережевий опис РІС, формалізацію вибору засобів захисту та баєсівську інтерпретацію поведінки нападника. В дослідженні РІС подано у вигляді орієнтованого графа з неоднорідною критичністю вузлів та врахуванням мережевих ефектів поширення атак. Засоби захисту моделюємо як дискретні альтернативи з обмеженим бюджетом захисника. Для оцінювання наслідків протидії введено функцію повної баєсівської очікувальної втрати. Ця функція агрегує локальні збитки з урахуванням апріорних імовірностей типів нападника та їхніх сценаріїв атак на РІС. Оптимальний вибір захисної стратегії подано як задачу мінімізації повних баєсівських очікуваних втрат, яка має ігрову інтерпретацію. Для апробації працездатності моделі проведено обчислювальні експерименти на алгоритмічні мові Python в IDE PyCharm. Отримані результати підтвердили нелінійний характер залежності рівня втрат від бюджету захисту та довели переваги стратегічно збалансованих рішень порівняно з локально оптимальними підходами. Отримані результати підтвердили доцільність застосування ігрово-оптимізаційного методу для підтримки прийняття рішень у сфері кібербезпеки розподілених інформаційних систем.

Ключові слова: розподілені інформаційні системи; кібербезпека; вибір засобів захисту; теорія ігор; баєсівські ігри; оптимізація; мережеві ефекти; очікувані втрати.

ВСТУП

З розвитком парадигми розподілених інформаційних систем (далі РІС) забезпечення їхньої безпеки ускладнено розподіленою архітектурою та наявністю цілеспрямованої протидії з боку потенційного порушника. У подібних умовах ефективність захисних рішень визначають не лише наявністю окремих технічних засобів захисту інформаційні (ЗЗІ), а й раціональністю їх вибору, розміщення та взаємодії в межах усієї системи за умов обмежених ресурсів. Як показано в [1] чинні методи та моделі, зокрема засновані на теорії ігор, дозволяють лише описати конфліктну взаємодію між захисником та зловмисником (хакером). Проте подібні дослідження, як-от [1] ґрунтувалися на абстрактних стратегіях. Отже, автори зазвичай не враховували архітектурну специфіку РІС, ресурсні обмеження та мережеві ефекти поширення атак. У свою чергу, класичні оптимізаційні моделі захисту, як правило, не відображають стратегічної природи кібернетичної протидії та припускають фіксовані або стохастичні загрози. Зважаючи на зазначене, виникла потреба у синтезі моделі, яка поєднає опис РІС,

оптимізаційні методи вибору ЗЗІ та формалізацію протидії з боку раціонального або обмежено-раціонального противника. Подібна модель має забезпечувати потенціал оцінювання ефективності захисних рішень з урахуванням топології РІС, важливості її компонентів, обмежених ресурсів та невизначеності щодо сценаріїв атак. Отже, головна мета поточного дослідження – опис моделі оптимального вибору засобів захисту РІС в умовах протидії. Запропонована далі математична модель створює підґрунтя для подальшого аналізу властивостей моделі, синтезу алгоритмічних методів розв'язання та практичної інтерпретації результатів у завданнях підтримки прийняття рішень у сфері кібербезпеки РІС.

Постановка проблеми. Розподілені інформаційні системи функціонують в умовах обмежених ресурсів та активної протидії з боку зловмисників, поведінка яких має стратегічний і варіативний характер. Наявні оптимізаційні моделі захисту, зазвичай, не враховують ігрову природу протидії. А наявні ігрові методи абстрагуються від архітектурних особливостей РІС і ресурсних обмежень. Це ускладнює формування обґрунтованих стратегій вибору засобів захисту та потребує синтезу інтегрованої моделі, яка поєднає оптимізацію, мережевий опис РІС і формалізацію дій противника.

Огляд попередніх досліджень. Проблеми моделювання захисту РІС активно розглядалися в останні роки [1 – 26]. Класичні роботи з теорії ігор у кібербезпеці [19–21] заклали підґрунтя для аналізу стратегічної взаємодії захисника і нападника. Проте зазвичай не враховують архітектурні та мережеві властивості РІС. Оптимізаційні та ризик-орієнтовані методи [6, 7, 11, 18] дозволяють оцінювати ефективність захисних заходів. Проте, автори [6, 7, 11, 18 – 21] здебільшого припускають фіксовані або стохастичні загрози без активної протидії. Також, низка робіт присвячена оцінюванню критичності вузлів та поширенню атак у мережах [2 – 4, 9], що довело релевантність мережевих ефектів у РІС. Вітчизняні дослідження [12, 24, 25] розглядають антагоністичні та оптимізаційні моделі вибору засобів захисту, проте, як правило, обмежуються статичними сценаріями або не інтегрують баєсівську невизначеність щодо типів нападника. Окремі сучасні моделі, як-от, [26] використовують еволюційні алгоритми, однак не надають ігрової інтерпретації отриманих рішень. Отже, релевантною є синтез моделі, яка поєднає ігрову теорію, оптимізацію та мережевий опис РІС, забезпечуючи комплексне оцінювання ефективності захисних стратегій в умовах реальної кібернетичної протидії.

Мета статті. Метою статті є розроблення та дослідження ігрово-оптимізаційної моделі оптимального вибору засобів захисту РІС, яка врахує обмеженість ресурсів, топологічну специфіку РІС, мережеві ефекти поширення атак та баєсівську невизначеність щодо типів і стратегій нападника.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Для математичного опису процесів вибору та застосування ЗЗІ насамперед задаємо структуру об'єкта, щодо якого приймаємо рішення. Оскільки РІС мають розподілену архітектуру та складаються з множини взаємопов'язаних компонентів, подальший аналіз проводимо з використанням мережевих моделей, див. рис. 1. Це дозволить враховувати не лише характеристики окремих вузлів, а також їхню взаємодію. Розглянемо РІС, яка функціонує в умовах цілеспрямованої протидії з боку зловмисника. Захисник має обмежені ресурси та здійснює вибір і розміщення ЗЗІ з метою мінімізації очікуваних втрат системи. Зловмисник, своєю чергою, обирає стратегію атаки, спрямовану на

максимізацію завданої шкоди. РІС моделюємо як мережа взаємопов'язаних компонентів, для яких враховуємо неоднорідність важливості, можливість поширення атак та взаємний вплив рішень щодо захисту. Подамо структуру РІС у вигляді орієнтованого графа, див. рис. 1:

$$G = (V, E), \tag{1}$$

де $V = \{v_1, v_2, \dots, v_N, \}$ – множина вузлів системи; $E \subseteq V \times V$ – множина зв'язків між вузлами; N – кількість вузлів системи.

Кожному вузлу системи ставимо у відповідність коефіцієнт критичності. Критичність вузла – це метрика важливості конкретного вузла РІС для функціонування. У літературі [2] її зазвичай визначають через структурну важливість у топології мережі, тобто через центральність у графі. Або використовують показники вразливостей чи ризиків, пов'язаних з цим вузлом [3]. Також є дослідження де коефіцієнт критичності визначають через навантаження вузлів [4]. На підставі [2 – 4] коефіцієнт критичності подамо так:

$$\omega_v \in \mathbb{R}_+, \ \forall v \in V, \tag{2}$$

де ω_v – показник важливості (критичності) вузла v.

Для опису варіативності зміни стану безпеки РІС доцільно перейти від локальних характеристик окремих вузлів до узагальненого вектора стану безпеки системи у момент часу t:

$$x(t) = \big(x_1(t), x_2(t), \dots, x_N(t)\big), \tag{3}$$

де $x_v(t)$ – стан безпеки вузла v у момент часу t.

Для критичних вузлів, зокрема головних сервісів РІС, див. рис. 1, зміна стану безпеки в часі має контрольований і відносно інерційний характер. Такі вузли функціонують у керованому середовищі. Тобто вони апріорі мають централізовані механізми моніторингу та захисту, а також пріоритет у розподілі ресурсів безпеки. Навіть за зростання інтенсивності загроз їхній стан безпеки зміниться поступово, оскільки негативний вплив компенсують гнучкими захисними заходами. Зокрема це реалізують посиленням політик доступу, резервуванням ресурсів та проактивним виявленням атак тощо. Натомість для вузлів із низьким рівнем критичності, таких як клієнтські пристрої, стан безпеки характеризують високою мінливістю. Його трансформації значною мірою визначають зовнішніми чинниками. Зокрема на його рівень впливають поведінка користувача, різноманітність програмного забезпечення (ПЗ), яке він використовує тощо. За відсутності оперативного управління захистом негативні впливи швидко призведуть до деградації стану безпеки пристрою. Також при цьому можливості компенсації загроз є обмеженими. Тобто варіативність стану безпеки критичних і некритичних вузлів РІС обґрунтовує потребу диференційованого підходу до управління захистом окремих компонентів.

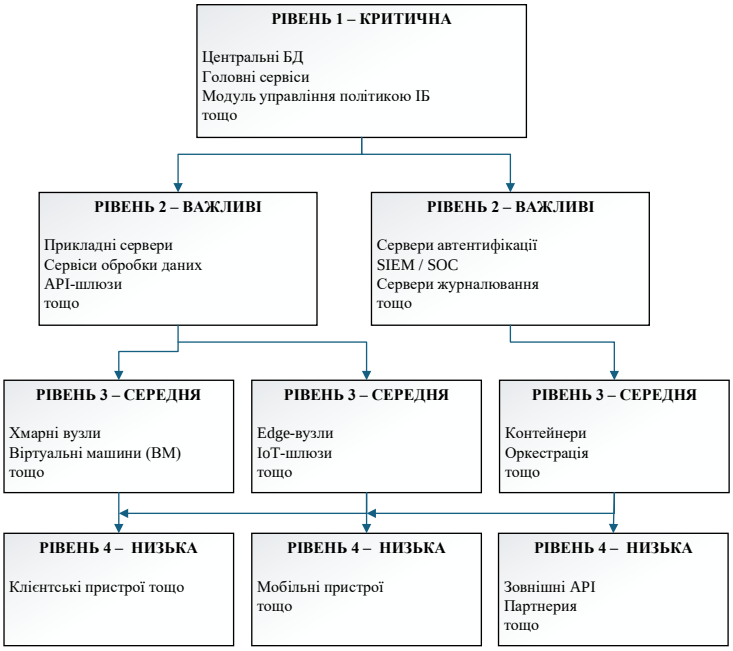

Рис. 1 – Концептуальна схема розподіленої інформаційної системи за рівнем критичності

Для опису стану безпеки окремого вузла РІС недостатньо розглянути його ізольовано. В РІС кожен вузол функціонує у взаємодії з іншими компонентами, див. рис. 1. Загрози, збої та захисні дії, що виникають у межах одного вузла, зазвичай поширюються через канали обміну даними та спільні ресурси. Відповідно це впливає на загальний стан безпеки пов'язаних елементів РІС. Тому введемо поняття сусідства вузла, яке віддзеркалить множину безпосередньо або функціонально пов'язаних вузлів РІС, взаємодія з якими матиме істотний вплив на загальний стан безпеки системи. Сусідство визначає локальне оточення вузла в архітектурі РІС та слугує механізмом передачі як негативних ефектів, зокрема розповсюдження атак або порушень доступності, так і позитивних впливів, пов'язаних із координацією захисних заходів з боку захисника.

Сусідство вузла визначаємо відповідно до [5]:

$$N(v) = \{u \in V | (v,u) \in E\}, \quad (4)$$

де $N(v)$ – множина вузлів, що мають прямий вплив на вузол v.

Задана мережева модель (1) – (4) системи визначає простір, у межах якого реалізуються як атаки, так і захисні дії. Проте для аналізу процесу захисту недостатньо лише описати топологію та критичність вузлів. В рамках синтезу ігрово-оптимізаційної моделі вибору засобів захисту РІС нам необхідно формалізувати інструментарій, яким володіє захисник, а також задати обмеження, які накладаються на його використання. Тому далі введемо як окремий компонент модель засобів захисту, яка дозволить описати можливість їх розміщення на окремих вузлах РІС та врахувати обмеженість доступних ресурсів.

Нехай множина доступних засобів захисту має вигляд:

$$K = \{1,2, \dots, K\}, \quad (5)$$

де K – кількість типів засобів захисту для РІС.

Введемо бінарні змінні вибору засобів захисту:

$$z_{v,k} \in \{0,1\}, \quad (6)$$

де $z_{v,k}$ – означає застосування засобу захисту типу k на вузлі v.

Залежність (6) відображає дискретний характер більшості заходів кіберзахисту, коли той чи інший ЗЗІ або впроваджують, або не використовують в межах заданого сценарію. Бінарна форма змінних спрощує нам інтерпретацію стратегій захисника, забезпечує однозначність вибору та дає можливість у підсумку упорядкувати процес прийняття рішень як вибір набору альтернатив із фіксованого переліку доступних ЗЗІ. Застосування бінарних змінних є методологічно узгодженим з ігровими моделями, які розглянуто в [1], у яких стратегії гравців автори трактували як кінцеві множини допустимих дій. Це створює передумову для синтезу функції виграшу, а також для інтеграції ігрової постановки задачі дослідження з методами комбінаторної та багатокритеріальної оптимізації ЗЗІ для РІС. Зазначимо, що далі ми розглядаємо обмеження на загальний бюджет захисника РІС. Мета – адекватного відобразити реальні ресурсні умови функціонування системи безпеки РІС. В реальному житті можливості захисника завжди є скінченними. А отже, вибір одного ЗЗІ неминуче зменшить доступні ресурси для застосування інших заходів. Тобто зведення ресурсних обмежень до узагальненого бюджетного обмеження дозволить нам абстрагувати компроміс між рівнем захищеності РІС та витратами. Також це обмеження забезпечить нам порівнюваність різних захисних стратегій у межах єдиного обмежувального контуру. У більш загальному трактуванні бюджетне обмеження розглядаємо далі не лише як фінансовий ліміт на ЗЗІ для РІС. В загальній постановці – це інтегральна характеристика сукупних витрат захисника, яка включає обчислювальні ресурси, часові витрати, експлуатаційну складність та організаційні обмеження. Вважаємо що подібне обмеження підвищить універсальність нашої моделі та потенційного дозволить налаштувати її до різних класів РІС.

Тоді вартість застосування ЗЗІ опишемо матрицею:

$$c_{v,k} \in \mathbb{R}_+, \quad (7)$$

де $c_{v,k}$ – вартість розгортання засобу k на вузлі v.

Отже, обмеження на загальний бюджет захисника матимуть вигляд [6, 7]:

$$\sum_{v \in V} \sum_{k \in K} c_{v,k} \cdot z_{v,k} \leq B, \quad (8)$$

де B – загальний бюджет, доступний для захисту РІС.

Опис засобів захисту та бюджетних обмежень задає нам множину допустимих рішень захисника. Однак ефективність будь-якого захисного рішення для РІС не можна оцінити ізольовано, без урахування дій протилежної сторони. Як показано в [1 – 5, 24, 25, 26] роботи будь-яка інформаційна система зазнає цілеспрямованих атак. Параметри атак змінюються залежно від обраної зловмисником або зловмисниками тактики нападу. Саме тому наступним кроком синтезу нашої моделі є абстрагування дій нападника (сторони яка реалізує атаку) та опис простору потенційних сценаріїв атак.

Тоді нехай множина дій зловмисника задана як:

$$A = \{a_1, a_2, \dots, a_M\}, \quad (9)$$

де M – кількість типів або сценаріїв атак.

Зазначимо, що у РІС мають багатовимірний характер і відрізняються як за цільовою спрямованістю, так і за механізмами реалізації. На відміну від централізованих систем, у РІС нападник зазвичай обирає не лише окремі вузли, а й канали взаємодії між ними, використовуючи під час атаки топологічні, функціональні та часові специфікації системи. Сценарії атак зазвичай спрямовані на порушення доступності сервісів, компрометацію конфіденційних даних, модифікацію інформаційних потоків або деградацію продуктивності системи. Нападники під час атаки реалізують як одноразові, так і багатоетапні стратегії. Отже, узагальнення подібних сценаріїв у скінченну множину дозволить нам обмежити простір стратегій зловмисника та забезпечити математичну постановку ігрової задачі.

Стратегію нападника задамо ймовірнісним розподілом:

$$\pi^{att} = \{\pi_1, \pi_2, \dots, \pi_M\}, \quad (10)$$

де $\pi_m = \mathbb{P}(a = a_m)$ – стратегія нападника; $\sum_{m=1}^{M} \pi_m = 1$.

Задання множини потенційних дій зловмисника створює нам основу для аналізу протидії. Однак для побудови цільової функції оптимізації потрібно встановити зв'язок між реалізованою атакою та її наслідками для РІС. Подібний зв'язок зазвичай описують через модель збитків, які виникають в результаті атаки з урахуванням застосованих засобів захисту [10, 11]. Оскільки система є розподіленою, шкода для окремого вузла РІС залежить не лише від його власного стану. Вона також визначає стани суміжних компонентів РІС. А це потребує врахування мережевих ефектів від атаки на окремий вузол РІС.

Тоді очікувану локальну шкоду для вузла v для фіксованих ЗЗІ та відповідної стратегії атаки визначимо так:

$$D_v = D_v\big(z_v, z_{N(v)}, a\big), \quad (11)$$

де D_v – шкода для вузла v; z_v – вектор захисту вузла v; $z_{N(v)}$ – захист сусідніх вузлів РІС; a – реалізація атаки.

Для врахування мережевого ефекту введемо коефіцієнти поширення:

$$a_{u,v} \in [0,1], \quad (12)$$

де $a_{u,v}$ – вплив компрометації вузла u на вузол v.

Тоді сумарну очікувану шкоду для вузла подамо так:

$$\widetilde{D_v} = D_v + \sum_{u \in N(v)} \alpha_{u,v} \cdot D_u, \quad (13)$$

е $\widetilde{D_v}$ – повна очікувана шкода вузла v.

Отримана модель шкоди (11) – (13) дозволить нам оцінити наслідки атак на рівні окремих вузлів РІС та їх оточення. Проте завдання захисника полягає у мінімізації втрат

усієї системи в цілому, а не окремих її вузлів. Для цього нам потрібно агрегувати локальні показники шкоди з урахуванням різної важливості вузлів РІС. Тому далі вводимо функцію втрат РВС, яку застосуємо далі як інтегральний критерій ефективності захисту РІС.

Відповідно загальні втрати РІС визначаємо як зважену сума локальних втрат:

$$L(z,a) = \sum_{v\in V} \omega_v \cdot \widetilde{D_v}\,, \tag{14}$$

де L – загальні втрати системи; z – матриця рішень захисту.

Тоді очікувані втрати за ймовірнісної стратегії нападника подамо так:

$$\mathbb{E}\,[L(z)] = \sum_{m=1}^{M} \pi_m L(z,a_m). \tag{15}$$

Відмітимо, що поки функція втрат (15), визначена для фіксованого сценарію атаки. Отже, вона дозволяє нам кількісно оцінити наслідки протидії за умови повної визначеності щодо дій зловмисника, який атакує РІС.

Відповідно, нехай множина типів нападника:

$$\Theta = \{\theta_1, \theta_2, \dots, \theta_T\}, \tag{16}$$

де θ_t – тип зловмисника.

Тоді апріорний розподіл типів нападників подамо так:

$$\mathbb{P}(\theta = \theta_t) = q_t, \tag{17}$$

де $\sum_{t=1}^{T} q_t = 1$.

З урахування цієї залежності дозволить нам адекватно оцінити наслідки атак і забезпечить коректний перехід до обчислення очікуваних втрат у межах баєсівської ігрової моделі. Тоді умовні втрати з урахуванням типу нападника подамо так:

$$L(z|\theta_t). \tag{18}$$

Але окремий розрахунок апріорних імовірностей типів та відповідних умовних втрат допускає лише проаналізувати специфіку окремих загроз. Однак не дає цілісної оцінки ризику для РІС. Для формування узагальненого критерію ефективності стратегій захисту потрібно інтегрувати ці компоненти в єдину метрику, яка врахує як невизначеність щодо типу нападника, так і масштаби можливих для РІС наслідків.

З цією метою в нашому методі використовуємо поняття повної баєсівської очікувальної втрати. Її інтерпретуємо як середній рівень шкоди, який ячу очікує захисник з урахуванням усіх можливих типів нападника та їхніх імовірностей. Подібна інтегральна метрика віддзеркалить зважений внесок кожного типу противника у загальні втрати системи, де ваги визначатиме апріорним розподілом, а величини втрат умовними наслідками відповідних сценаріїв атак.

Перехід до повної баєсівської очікувальної втрати має важливе методологічне значення. Це пов’язано з тим що повні баєсівські очікувальні втрати дозволять далі нам перейти від фрагментарного аналізу окремих сценаріїв атак на РІС до комплексного оцінювання ризиків. У подібній постановці стратегія захисника оцінюємо не за найгіршим або окремим випадком, а за її здатністю мінімізувати очікувану шкоду в

умовах неповної інформації про поведінку нападника. Отже, повна баєсівська очікувальна втрата виступить узагальненням умовних втрат і слугуватиме базисом оптимальності в ігрово-оптимізаційній моделі захисту РІС.

Повні байєсівські очікувані втрати РІС подамо так:

$$\mathbb{E}_\theta[L(z)] = \sum_{t=1}^{T} q_t \cdot L(z|\theta_t). \quad (19)$$

Урахування баєсівської невизначеності щодо типів зловмисника та відповідних умовних втрат дає нам змогу перейти від аналізу ізольованих сценаріїв атак до узагальненого оцінювання ризиків функціонування РІС. Замість розгляду окремих, наперед визначених варіантів поведінки противника, модель (16) – (19) оперує очікуваними втратами, які інтегрують усю множину можливих типів зловмисників з урахуванням їх імовірностей. Це на нашу думку забезпечить реалістичне відображення умов неповної інформації, характерних для задач кіберзахисту РІС.

Відповідно оптимальний вибір засобів захисту для РІС визначаємо як розв'язок наступної задачі:

$$z^* = arg \min_z \mathbb{E}_\theta[L(z)], \quad (20)$$

за умов

$$\sum_{v \in V} \sum_{k \in K} c_{v,k} \cdot z_{v,k} \leq B \quad (21)$$

$$z_{v,k} \in \{0,1\}. \quad (22)$$

Зазначимо, що сформульована оптимізаційна задача описує раціональний вибір захисника за заданої моделі загроз. Водночас сама структура задачі свідчить про наявність конфлікту інтересів між захисником та нападником. Саме тому для глибшого аналізу властивостей отриманих рішень інтерпретуємо цю задачу у термінах теорії ігор. На наш розсуд це дозволить дослідити, зокрема під час обчислювальних експериментів, рівноважні режими взаємодії сторін та паралельно встановити зв'язок між оптимальними рішеннями і мінімаксними принципами формуванні багатоконтурного захисту РІС.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для апробації працездатності ігрово-оптимізаційної моделі взаємодії суб'єктів конфлікту, а також методу оптимального вибору ЗЗІ для РІС в умовах цілеспрямованої протидії, проведені обчислювальні експерименти в IDE PyCharm, див. рис. 2. На рис. 2 наведено залежність повної баєсівської очікувальної втрати РІС від величини доступного бюджету захисника.

Отримані результати продемонстрували нелінійний характер зменшення втрат на ЗЗІ для РІС зі зростанням бюджету. На початковій ділянці збільшення ресурсів призвело до різкого зниження очікуваних втрат. Це випливає із можливості захисту найбільш важливих вузлів РІС.

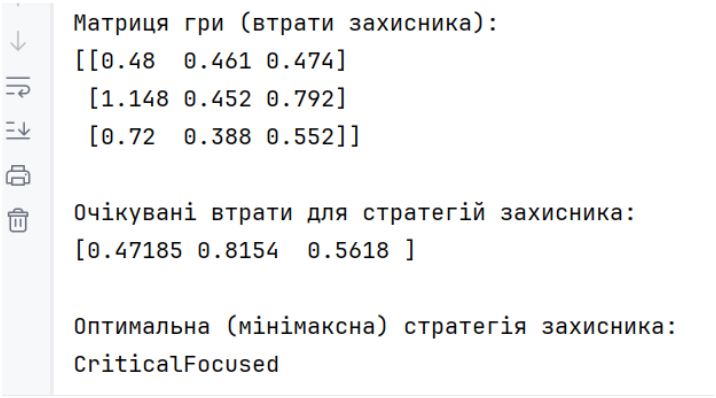

Рис. 2 – Вивід результатів обчислювального експерименту в консолі PyCharm

Подальше зростання бюджету характеризувалося ефектом насичення. Тобто додаткові витрати забезпечували лише маргінальне зменшення втрат на ІБ РІС. Отже, результат підтвердив, що оптимальний вибір ЗЗІ є важливішим за просте нарощування ресурсів. Це повністю узгоджено з логікою нашої ігрово-оптимізаційної моделі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Удосконалено ігрово-оптимізаційну модель взаємодії суб'єктів конфлікту, яка враховує, на відміну від відомих, не лише раціональність зловмисника, а й його обмежену раціональність, що дозволяє більш адекватно описати реальні сценарії атак на РІС за умов дефіциту бюджету на безпеку.

Доповнено баєсівську модель поведінки нападника, яка забезпечує можливість оцінювання повних очікуваних втрат системи. Показано, що використання апарату баєсівських ігор дозволило перейти від аналізу окремих інцидентів до формування стратегій захисту РІС, налаштованих на різні типи та мотивацію порушників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., & Smirnov, S. (2023, December). Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information. In International Symposium on Intelligent Informatics (pp. 377-389). Singapore: Springer Nature Singapore.
2. Faramondi, L., Oliva, G., & Setola, R. (2020). Multi-criteria node criticality assessment framework for critical infrastructure networks. International Journal of Critical Infrastructure Protection, 28, 100338.
3. Liu, L., Du, N., & Sheng, D. (2025). Security-centric node identification in complex networks. Scientific Reports, 15(1), 15568.
4. Liu, W., Gong, Q., Han, H., Wang, Z., & Wang, L. (2018). Reliability modeling and evaluation of active cyber physical distribution system. IEEE Transactions on Power Systems, 33(6), 7096-7108.
5. Yalagandula, P., & Dahlin, M. (2004). A scalable distributed information management system. ACM SIGCOMM Computer Communication Review, 34(4), 379-390.
6. Родін, Є. С., & Сініцин, І. П. Математичне моделювання бюджету витрат на інформаційну безпеку в багатофакторних розподіленних системах. секція 1 сучасні аспекти математичного та імітаційного моделювання систем в екології, 19, 422.
7. Шевченко, А. В. (2018). Управління функціональною стійкістю інформаційних систем на основі оптимізації видатків на захист. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 90-96.

8. Palko, D., Hnatiienko, H., Babenko, T., & Bigdan, A. (2021, September). Determining Key Risks for Modern Distributed Information Systems. In IntSol (pp. 81-100).
9. Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. Information Systems Research, 26(3), 565-584.
10. Рой, Я. В., Мазур, Н. П., & Складанний, П. М. (2018). Аудит інформаційної безпеки–основа ефективного захисту підприємства. Науково-технічний журнал" Кібербезпека: освіта, наука, техніка", (1), 86-93.
11. Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. J. Comput., 5(3), 352-359.
12. Глушак, О.М. Новіков, (2013). Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника. System research and information technologies, (2), 89-100.
13. Архіпов, О. Є., Скиба, А. В., & Хоріна, О. І. (2015). Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів зловмисника. Захист інформації, 1(17), 60-72.
14. Belej, O., Spas, N., & Artyshchuk, I. (2021, September). Development of an Algorithm for Detecting Cyberattacks in Distributed Information Systems. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 1, pp. 325-328). IEEE.
15. Gamundani, A. M., & Nekare, L. M. (2018, May). A review of new trends in cyber attacks: A zoom into distributed database systems. In 2018 IST-Africa Week Conference (IST-Africa) (pp. Page-1). IEEE.
16. Appiah-Kubi, J., & Liu, C. C. (2020). Decentralized intrusion prevention (DIP) against co-ordinated cyberattacks on distribution automation systems. IEEE Open Access Journal of Power and Energy, 7, 389-402.
17. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., ... & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. Applied Sciences, 13(4), 2393.
18. Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. IEEE Access, 6, 12175-12186.
19. Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.
20. Lye, K. W., & Wing, J. M. (2005). Game strategies in network security. International Journal of Information Security, 4(1), 71-86.
21. Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. Acm Computing Surveys (Csur), 45(3), 1-39.
22. Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.
23. Siegel, C. A., & Sweeney, M. (2020). Cyber strategy: risk-driven security and resiliency. Auerbach Publications.
24. Добринін, І. С., & Борова, М. П. (2018). Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі. Системи озброєння і військова техніка, (2), 89-93.
25. Пшеничних, С. В., Добринін, І. С., & Клочкова, Д. Ю. (2023). Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації. Проблеми телекомунікацій, (1 (32)), 45-58.
26. Лахно, В., Криворучко, О., & Каламан, Є. (2025). Програмна реалізація вирішення задачі оптимізації вибору засобів захисту інформації на основі еволюційного алгоритму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 257-268.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Yurii V. Yaskevych
PhD Student, Department of Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID:0009-0005-6084-5229
y.yaskevych.asp@kubg.edu.ua

GAME-THEORETIC OPTIMIZATION MODEL FOR SELECTING SECURITY CONTROLS IN DISTRIBUTED INFORMATION SYSTEMS

Abstract. The article proposes a game-theoretic optimization model for selecting security controls for distributed information systems (DIS) under conditions of targeted cyber opposition. The relevance of this study is driven by the increasing architectural complexity of distributed information systems, limited security resources on the defense side, and the presence of a rational or boundedly rational adversary acting strategically. In contrast to existing optimization methods and traditional game-theoretic models, the proposed model integrates a network-based description of the DIS, the formalization of security control selection, and a Bayesian interpretation of the attacker's behavior. In this study, the DIS is represented as a directed graph with heterogeneous node criticality, accounting for the network effects of attack propagation. Security controls are modeled as discrete alternatives subject to the defender's limited budget. To assess the consequences of the conflict, a total Bayesian expected loss function is introduced. This function aggregates local damages, taking into account the prior probabilities of attacker types and their attack scenarios against the DIS. The optimal selection of a defense strategy is formulated as a problem of minimizing total Bayesian expected losses, which possesses a game-theoretic interpretation. To validate the model's functionality, computational experiments were conducted using the Python programming language within the PyCharm IDE. The obtained results confirmed the non-linear nature of the dependency between loss levels and the security budget, demonstrating the advantages of strategically balanced solutions over locally optimal approaches. These findings confirm the expediency of applying the game-theoretic optimization method for decision support in the field of distributed information systems cybersecurity.

Keywords: distributed information systems; cybersecurity; selection of security controls; game theory; Bayesian games; optimization; network effects; expected losses.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., & Smirnov, S. (2023, December). Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information. In *International Symposium on Intelligent Informatics* (pp. 377-389). Singapore: Springer Nature Singapore.
2. Faramondi, L., Oliva, G., & Setola, R. (2020). Multi-criteria node criticality assessment framework for critical infrastructure networks. *International Journal of Critical Infrastructure Protection*, 28, 100338.
3. Liu, L., Du, N., & Sheng, D. (2025). Security-centric node identification in complex networks. *Scientific Reports*, 15(1), 15568.
4. Liu, W., Gong, Q., Han, H., Wang, Z., & Wang, L. (2018). Reliability modeling and evaluation of active cyber physical distribution system. *IEEE Transactions on Power Systems*, 33(6), 7096-7108.
5. Yalagandula, P., & Dahlin, M. (2004). A scalable distributed information management system. *ACM SIGCOMM Computer Communication Review*, 34(4), 379-390.
6. Rodin, Ye. S., & Sinitsyn, I. P. (2019). Mathematical modeling of the information security budget in multifactorial distributed systems. *Section 1: Modern aspects of mathematical and simulation modeling of systems in ecology*, 19, 422. (in Ukrainian)
7. Shevchenko, A. V. (2018). Management of functional stability of information systems based on optimization of security expenditures. *Collection of Scientific Works of the Center for Military-Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi*, 90-96. (in Ukrainian)
8. Palko, D., Hnatiienko, H., Babenko, T., & Bigdan, A. (2021, September). Determining Key Risks for

Modern Distributed Information Systems. In *IntSol* (pp. 81-100).
9. Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, 26(3), 565-584.
10. Roy, Ya. V., Mazur, N. P., & Skladannyi, P. M. (2018). Information security audit as a basis for effective enterprise protection. *Scientific and Technical Journal "Cybersecurity: Education, Science, Technique"*, (1), 86-93. (in Ukrainian)
11. Patel, S., & Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, 5(3), 352-359.
12. Glushak, O. M., & Novikov, O. M. (2013). Synthesis of the information protection system structure using a positional game of the defender and the attacker. *System Research and Information Technologies*, (2), 89-100. (in Ukrainian)
13. Arkhipov, O. Ye., Skyba, A. V., & Khorina, O. I. (2015). Expansion of economic-cost models of information risks through the use of socio-psychological types of the attacker. *Information Protection*, 1(17), 60-72. (in Ukrainian)
14. Belej, O., Spas, N., & Artyshchuk, I. (2021, September). Development of an Algorithm for Detecting Cyberattacks in Distributed Information Systems. In *2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT)* (Vol. 1, pp. 325-328). IEEE.
15. Gamundani, A. M., & Nekare, L. M. (2018, May). A review of new trends in cyber attacks: A zoom into distributed database systems. In *2018 IST-Africa Week Conference (IST-Africa)* (pp. Page-1). IEEE.
16. Appiah-Kubi, J., & Liu, C. C. (2020). Decentralized intrusion prevention (DIP) against co-ordinated cyberattacks on distribution automation systems. *IEEE Open Access Journal of Power and Energy*, 7, 389-402.
17. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., ... & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences*, 13(4), 2393.
18. Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. *IEEE Access*, 6, 12175-12186.
19. Alpcan, T., & Başar, T. (2010). *Network security: A decision and game-theoretic approach*. Cambridge University Press.
20. Lye, K. W., & Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security*, 4(1), 71-86.
21. Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., & Hubaux, J. P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3), 1-39.
22. Alpcan, T., & Başar, T. (2010). *Network security: A decision and game-theoretic approach*. Cambridge University Press.
23. Siegel, C. A., & Sweeney, M. (2020). *Cyber strategy: risk-driven security and resiliency*. Auerbach Publications.
24. Dobrynin, I. S., & Borova, M. P. (2018). Optimization of the choice of information protection system construction option against attacks in an antagonistic game. *Armament Systems and Military Equipment*, (2), 89-93. (in Ukrainian)
25. Pshenychnykh, S. V., Dobrynin, I. S., & Klochkova, D. Yu. (2023). Mathematical model of optimal selection of information protection means when designing a complex protection system at an informatization object. *Telecommunications Problems*, (1 (32)), 45-58. (in Ukrainian)
26. Lakhno, V., Kryvoruchko, O., & Kalaman, Ye. (2025). Software implementation of solving the problem of optimizing the choice of information protection means based on an evolutionary algorithm. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, 3(27), 257-268. (in Ukrainian)