УДК 004.056.5:004.75 DOI: 10.31673/2412-4338.2026.019012

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

РОЗПОДІЛЕНІ ІНФОРМАЦІЙНІ СИСТЕМИ ЯК ОБ'ЄКТ КІБЕРЗАХИСТУ ТА ЗАГРОЗИ ЇХНЬОЇ БЕЗПЕКИ

Анотація. *У статті розглянуто розподілені інформаційні системи (далі РІС) як складні об'єкти кіберзахисту, які функціонують в умовах цілеспрямованої протидії з боку раціонального противника. Доведено, що характерними особливостями чинних РІС є гетерогенність вузлів, зміна станів, варіативна мережева топологія, відсутність єдиного периметра безпеки та можливість каскадного поширення кібернетичних інцидентів. Обґрунтовано, що зазначені властивості істотно ускладнили застосування класичних статичних методів в завданні оцінювання ризиків та вибору засобів захисту інформації для РІС. Виконано аналіз сучасних типів атак на РІС. Узагальнення статистичних даних за 2024–2025 роки засвідчило тренд до зростання інтенсивності та складності атак на хмарні, корпоративні та критично важливі РІС (або КВС). Показано, що більшість наявних методів вибору засобів захисту РІС не враховують стратегічну поведінку нападника та обмеженість ресурсів сторони захисту. На основі аналізу літературних джерел сформульовано наукову проблему оптимального вибору засобів захисту розподілених інформаційних систем як інтегровану ігрово-оптимізаційну задачу. Обґрунтовано доцільність використання апарату теорії ігор у поєднанні з методами багатокритеріальної оптимізації для моделювання взаємодії між стороною захисту та противником. Запропонований концептуальний підхід дозволить на нашу думку врахувати архітектурну специфіку РІС, трансформацію її станів та стратегічні аспекти кібернетичної протидії. Все перелічене у підсумку створить підґрунтя для підвищення ефективності прийняття рішень у системах кіберзахисту. Отримані результати поточного аналітичного дослідження підтвердили потребу синтезу гібридного методу оптимального вибору засобів захисту РІС. Такий метод має поєднувати апарат теорії ігор для моделювання протидії раціональному противнику та методи багатокритеріальної оптимізації для вибору конфігурації засобів захисту в умовах обмежених ресурсів.*

Ключові слова: *розподілені інформаційні системи; кіберзахист; засоби захисту інформації; аналіз попередніх досліджень; ігрові моделі; багатокритеріальна оптимізація; стратегічна протидія; кіберзагрози.*

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

DISTRIBUTED INFORMATION SYSTEMS AS CYBER DEFENSE OBJECTS AND THEIR SECURITY THREATS

Abstract. *The article examines distributed information systems (hereinafter referred to as DIS) as complex cyber-defense objects operating under conditions of targeted opposition from a rational adversary. It is proven that the characteristic features of modern DIS include node heterogeneity, state transitions, variable network topology, the absence of a single security perimeter, and the potential for cascading propagation of cyber incidents. It is substantiated that these properties significantly complicate the application of classical static methods in the tasks of risk assessment and the selection of information security tools for DIS. An analysis of modern types of attacks on DIS has been performed. The generalization of statistical data for 2024–2025 demonstrates a trend toward increasing intensity and complexity of attacks on cloud-based, corporate, and critical DIS (or CIS).*

It is shown that most existing methods for selecting DIS security tools fail to account for the attacker's strategic behavior and the defender's resource constraints. Based on the analysis of literature sources, the scientific problem of the optimal selection of security tools for distributed information systems is formulated as an integrated game-optimization task.

The expediency of using the game theory apparatus in combination with multi-criteria optimization methods for modeling the interaction between the defender and the adversary is substantiated. In our opinion, the proposed conceptual approach will allow for accounting for the architectural specifics of DIS, its state transformations, and the strategic aspects of cyber confrontation. Ultimately, all the aforementioned factors will create a foundation for increasing decision-

making efficiency in cyber defense systems. The results of the current analytical study confirmed the need to synthesize a hybrid method for the optimal selection of DIS security tools. Such a method should combine the game theory apparatus for modeling opposition to a rational adversary and multi-criteria optimization methods for choosing the configuration of security tools under limited resource conditions.

Keywords: *distributed information systems; cyber defense; information security tools; analysis of previous research; game models; multi-criteria optimization; strategic confrontation; cyber threats.*

1. Вступ.

Бурхливий розвиток інформаційно-комунікаційних технологій у 20 сторіччі зумовив перехід від централізованих інформаційних систем до розподілених інформаційних систем (далі РІС) [1]. В РІС опрацьовуванням, зберігання та передавання даних здійснюють між множиною просторово та логічно рознесених компонентів. До РІС, згідно [1 – 5] відносять корпоративні інформаційні системи (КІС) з багаторівневою архітектурою, хмарні та гібридні обчислювальні середовища, системи Інтернету речей (IoT), промислові системи керування (SCADA/ICS), фінансові та блокчейн-платформи, а також розподілені державні та КВС, див. таблицю 1.

На відміну від централізованих систем, РІС характеризують відсутністю єдиного обчислювального центру, див. таблицю 2. Також РІС притаманний високих ступень взаємозалежності компонентів та варіативна топологія. Кожен вузол РІС зазвичай виконує як локальні функції опрацювання даних, так і бере участь у колективних процесах при наданні сервісів. Унаслідок цього загальний рівень функціонування та безпеки РІС визначають не окремими компонентами, а сукупною поведінкою всієї мережі скоординованих вузлів.

Таблиця 1

Класи розподілених інформаційних систем та приклади їх застосування

Клас РІС	Приклади	Основні специфічні риси
Корпоративні РІС	ERP, CRM, DMS	Багаторівнева архітектура. Централізовані сервіси.
Хмарні та гібридні системи	IaaS, PaaS, SaaS	Гнучке масштабування. Віртуалізація
IoT-системи	Smart City, Smart Grid	Велика кількість слабко захищених вузлів.
SCADA/ICS	Промислові об’єкти	Віднесені до КВС. Жорсткі вимоги до доступності.
Децентралізовані платформи	Blockchain, DeFi	Відсутність єдиного центру довіри.

Таблиця 2

Порівняльна характеристика централізованих та розподілених інформаційних систем

Ознака	Централізовані ІС	Розподілені ІС
Архітектура	Один центр опрацювання.	Мережа вузлів
Вразливість	Єдина точка відмови.	Каскадні ефекти
Масштабованість	Обмежена.	Висока
Складність захисту	Відносно низька.	Висока
Характер загроз	Переважно локальний.	Стратегічний, мережевий

З погляду кіберзахисту РІС біль складніші об’єкти порівняно з централізованими ІС [6], див. таблицю 3. Так, неоднорідність вузлів РІС зумовлює різний рівень їх важливості для функціонування системи. Критичні серверні сервіси, вузли керування або бази даних (БД) апріорі мають істотно вищу вагу для цілісності та доступності РІС, ніж периферійні або клієнтські пристрої. Окрім цього, міжвузлові зв’язки створюють умови для каскадного поширення інцидентів інформаційної безпеки (ІБ). Це ситуація коли компрометація одного елемента призведе до деградації стану безпеки суміжних

компонентів РІС. Ще однією визначальною специфічною рисою РІС є варіативні стани. Тобто стані РІС змінюються, зокрема під впливом деструктивних дій зловмисників (зовнішні хакери, внутрішні порушники політики ІБ, інсайдери тощо).

Таблиця 3

Основні властивості РІС, значущі для задач кіберзахисту

Властивість	Опис	Вплив на захист
Неоднорідність вузлів	Різна важливість компонентів РІС.	Потреба диференційованого захисту.
Мережеві зв'язки	Взаємодія між вузлами.	Поширення атак
Варіативність станів	Зміна станів у часі.	Необхідність різнопланових моделей.
Обмежені ресурси	Бюджет, обчислення, час тощо.	Оптимізаційний вибір засобів захисту інформації (ЗЗІ).
Цілеспрямовані загрози	Кваліфікований противник	Ігрова постановка.

Склад вузлів РІС, канали взаємодії, інтенсивність інформаційних потоків і політики доступу змінюються з часом під впливом як внутрішніх факторів, як-от масштабування відповідно до специфіки бізнес-процесів, оновлення програмного забезпечення (ПЗ), зміни навантаження тощо, так і зовнішніх впливів, зокрема кібератак. Відповідне це унеможливлює використання статичних моделей безпеки. Отже, розв'язання задачі потребує формального опису еволюції станів РІС.

2. Постановка проблеми.

Збільшення складності РІС, їх гетерогенність, варіативна топологія та відсутність чітко визначеного периметра безпеки зумовлюють принципово нові вимоги до побудови систем кіберзахисту. У таких умовах чинні методи та моделі вибору засобів захисту інформації виявилися недостатньо ефективними. Додатковим фактором є цілеспрямований та стратегічний характер сучасних кіберзагроз, коли противник діє як раціональний або обмежено-раціональний агент, прилаштовуючи свої дії до конфігурації системи захисту та доступних ресурсів сторони захисту. Взаємодія між стороною захисту та нападником у РІС набуває ознак ігрового процесу з конфліктом інтересів, часовою еволюцією станів та наявністю обмежень на ресурси. За таких умов актуальною є науково-прикладна проблема розроблення моделей і методів оптимального вибору та структурного розміщення засобів захисту РІС, які б одночасно враховували архітектуру РІС, варіативність її станів, обмеженість ресурсів захисту та стратегічну поведінку противника. Розв'язання цієї проблеми потребує синтезу ігрових моделей протидії та методів багатокритеріальної оптимізації, що дозволить підвищити обґрунтованість управлінських рішень у сфері кіберзахисту розподілених інформаційних систем.

3. Огляд попередніх досліджень.

Наголосимо, що в завданнях забезпечення кіберзахисту РІС суттєвим є також те, що кібернетичні загрози мають цілеспрямований та варіативний характер. Нападник зазвичай не здійснює випадкові дії. Кваліфіковані хакери (далі зловмисники або нападники), обирають стратегії впливу з урахуванням архітектури системи, рівня захисту окремих вузлів, доступних ресурсів та очікуваного ефекту. При цьому зловмисник гнучко корегує дії в процесі атаки залежно від реакції системи захисту. Відповідно, РІС апріорі функціонує в умовах постійної стратегічної взаємодії між стороною захисту та потенційним противником.

Зазначені властивості зумовили потребу в процесі дослідження розглядати РІС не лише як сукупність технічних компонентів, а як складну соціотехнічну систему [7]. В подібних системах процеси захисту тісно пов'язані з обмеженістю ресурсів, організаційними чинниками та поведінкою раціонального або обмежено-раціонального противника. А отже, в таких умовах ефективність кіберзахисту визначають не тільки наявністю окремих засобів захисту інформації (ЗІ), а й обґрунтованістю їх вибору, розміщення та взаємодії в межах всієї РІС. Наголосимо, що РІС як об'єкт кіберзахисту характеризують сукупністю ознак, серед яких першочерговою є мережева структура,

неоднорідність вадливих вузлів, можливість поширення атак, варіативність станів та стратегічний характер кібернетичних загроз. Ця специфіка зумовила у підсумку потребу в синтезі нових моделей і методів, які дозволять враховувати як архітектуру РІС, так і поведінку противника при прийнятті рішень щодо захисту системи в умовах обмежених ресурсів сторони захисту.

В таблиці 4 наведена порівняльна характеристика систем за різними метриками кібербезпеки.

Таблиця 4

Порівняльна характеристика систем за різними метриками кібербезпеки

Критерій порівняння	Типи інформаційних систем		
	Локальні ІС (ЛІС)	Розподілені ІС (РІС)	Корпоративні розподілені ІС (КРІС)
Архітектура та топологія.	Орієнтована на централізацію в межах однієї локації (LAN).	Високий рівень децентралізації, географічна розсередженість.	Ієрархічна структура. Центральний офіс та віддалені філії та підрозділи.
Периметр захисту.	Чітко визначений фізичний та логічний периметр.	Розмитий або відсутній периметр. Велика кількість точок входу.	Комбінований - локальні периметри підрозділів та загальнокорпоративний контур.
Канали зв'язку.	Переважно контрольовані внутрішні лінії (Ethernet, Wi-Fi).	Недовірені публічні мережі (Internet), різнорідні протоколи.	Захищені тунелі (VPN) поверх публічних мереж, виділені канали.
Керування доступом.	Централізоване (як-от Active Directory в межах одного сегмента).	Гетерогенне, часто федеративне або децентралізоване.	Централізована політика з делегуванням повноважень на місцях.
Модель загроз.	Акцент на внутрішні порушення ІБ та фізичний доступ.	Акцент на MitM-атаки, DDoS, компрометацію вузлів зв’язку.	Складні таргетовані атаки (APT), загрози через ланцюжки поставок.
Управління засобами захисту.	Локальне, пряме адміністрування.	Складне узгодження конфігурацій між віддаленими вузлами.	Централізований моніторинг (SOC/SIEM) та оркестрація (SOAR).
Масштабованість.	Обмежена фізичною інфраструктурою будівлі/майданчика.	Легке підключення нових сегментів.	Масштабування згідно з бізнес-логікою корпорації.
Рівень гомогенності.	Зазвичай гомогенне середовище (однакові ОС, ПЗ).	Висока гетерогенність (різні платформи, пристрої IoT, хмари).	Помірна гетерогенність, прагнення до стандартизації.

Тенденції 2025 року показали суттєве ускладнення методів компрометації РІС, див. рис. 1 – 3. Для візуалізації поточної ситуації та виявлення найбільш ризикованих зон експлуатації РІС виконана систематизація емпіричних даних [18, 19], які наведено в відповідних звітах. Ці результати систематизації даних статистики слугують підґрунтям для подальшого аналізу ризиків для РІС. Перші місця за даними статистики посіли DDoS атаки, атаки на протоколи консенсусу та ланцюжки поставок.

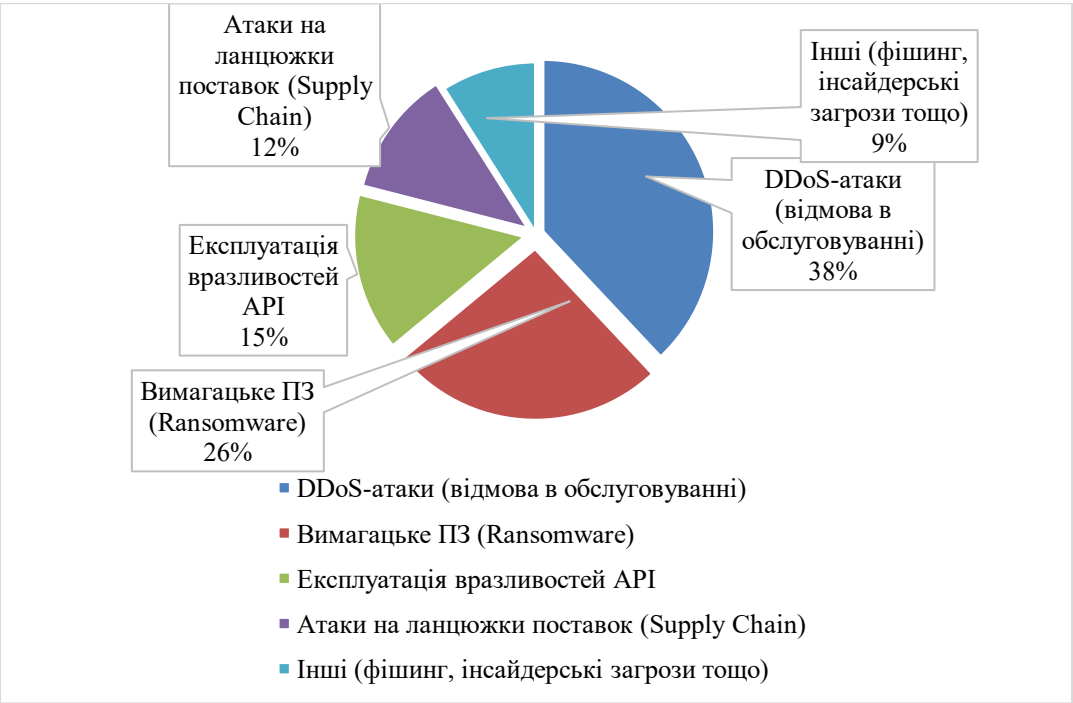

Рис. 1. Поширеність основних типів атак на розподілені системи у 2025 р.

Інші результати аналізу та систематизації наведено на рис. 2 та 3.

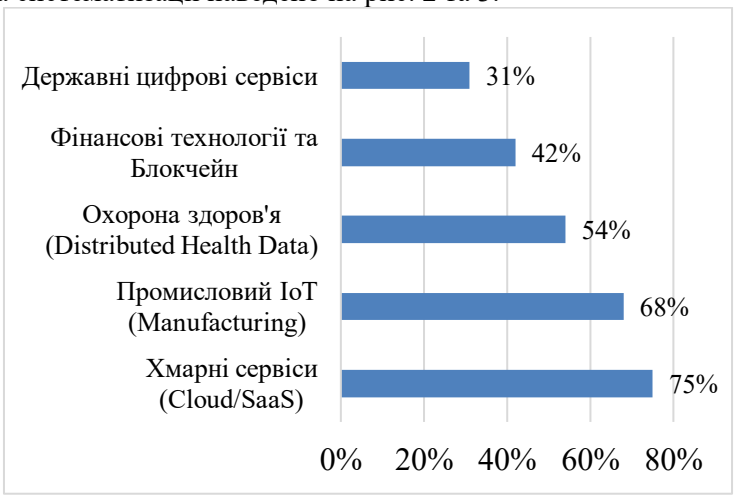

Рис. 2. Зростання інтенсивності атак на PIC за секторами у 2024 та 2025 роках

Рис. 3. Відсоток організацій, що постраждали у різних країнах в результаті атак на PIC у 2024 та 2025 роках

Таблиця 5

Класифікація типових атак на РІС

Тип атаки	Опис	Особливості в РІС	Приклади
Розподілена відмова в обслуговуванні (DDoS).	Перевантаження системи масовим трафіком з багатьох джерел (ботнетів), що робить ресурс недоступним для легітимних користувачів.	Найпоширеніша атака на РІС через розподілену архітектуру. Легко масштабувати за допомогою ботнетів. Включає перевантаження, протокол (SYN-flood) та прикладний рівень (HTTP-flood) варіанти.	Атаки на енергетичну інфраструктуру України (2015–2016 р.), GitHub (потужність 1,35 Tbps у 2018 р.), або атаки на хмарні сервіси. Потенційно може вивести з ладу весь кластер вузлів РІС.
Відмова в обслуговуванні (DoS).	Аналог DDoS, але з одного джерела. Перевантаження запитами чи пакетами.	Менш ефективна в РІС, але нападники використовують як частину гібридних атак для локального впливу на окремий вузол.	Локальне перевантаження сервера в розподіленій мережі (до прикладу, ping flood).
Man-in-the-Middle (MitM)	Перехоплення та можлива модифікація трафіку між вузлами.	Висока вразливість через відкриті канали зв'язку в РІС. Зловмисник зможе прослуховувати чи змінювати дані в транзиті.	Атаки типу MITB (Man-in-the-Browser) на розподілені системи, або перехоплення в незашифрованих мережах IoT.
Перехоплення даних (Eavesdropping).	Пасивне прослуховування трафіку для викрадення інформації.	Поширене в гетерогенних РІС з незахищеними з'єднаннями (наприклад, без TLS).	Викрадення конфіденційних даних у хмарних сховищах чи міжвузлових комунікаціях.
Ін'єкції (SQL, XSS, Command Injection).	Впровадження шкідливого коду в запити для доступу чи модифікації даних.	Експлуатує вразливості в веб-інтерфейсах чи API розподілених додатків.	SQL-ін'єкція в бази даних розподіленої системи для витоку даних.
Фішинг та соціальна інженерія.	Обман користувачів для отримання доступу (паролі, credentials).	Використовують для початкового проникнення в РІС, далі — латеральний рух між вузлами.	Фішингові листи для компрометації облікових записів у корпоративних мережах.
Шкідливе ПЗ (Malware, Ransomware, Worms).	Зараження вузлів вірусами, хробаками чи програмами-вимагачами.	Хробаки швидко поширюються в розподілених мережах (наприклад, через автодискавері). Ransomware блокує дані на багатьох вузлах.	Атаки на критичну інфраструктуру, як- от, NotPetya в Україні 2017 р. Або зараження IoT-пристроїв для ботнетів.
Підбір паролів (Brute-force, Dictionary attacks).	Автоматичний підбір та облікових даних.	Ефективно проти слабких політик аутентифікації в багатовікових РІС.	Атаки на SSH чи RDP в розподілених серверах.
Візантійські атаки (Byzantine faults).	Компрометація вузлів РІС для надсилання суперечливої інформації іншим вузлам.	Специфічні для консенсусних систем, як-от блокчейн, розподілені бази даних тощо. Порушує узгодженість даних.	Атаки на алгоритми консенсусу в блокчейні, зокрема, атака 51%.
Sybil-атаки.	Створення фальшивих ідентичностей для контролю частини мережі.	Поширене в P2P-мережах та блокчейні. Фальшиві вузли РІС впливають на голосування чи маршрутизацію.	Атаки на торренти чи децентралізовані мережі.

Як було показано в [3 – 19] РІС, такі як хмарні обчислення, IoT-мережі, блокчейн чи корпоративні мережі, є апріорі вразливими через свою децентралізовану природу. Дані та ресурси в РІС розподілені по багатьох вузлах. Відповідно це полегшує масштабні атаки. Зловмисники експлуатують вразливості в протоколах, комунікаціях та координації. Найпоширеніші атаки базуються на перевантаженні ресурсів, перехопленні даних чи компрометації вузлів (табл. 5).

Узагальнюючи, аналіз робіт [24 – 31] наголосимо, більшість із них не розглядали саме задачу оптимального структурного вибору засобів захисту розподілених інформаційних систем як інтегровану компоненту ігрово-оптимізаційної проблеми, що визначило методологічну доцільність запропонованого в [31] методу. На рис. 4 наведено узагальнену класифікацію моделей і методів, які використовують для розв'язання задачі оптимального вибору засобів захисту розподілених інформаційних систем.

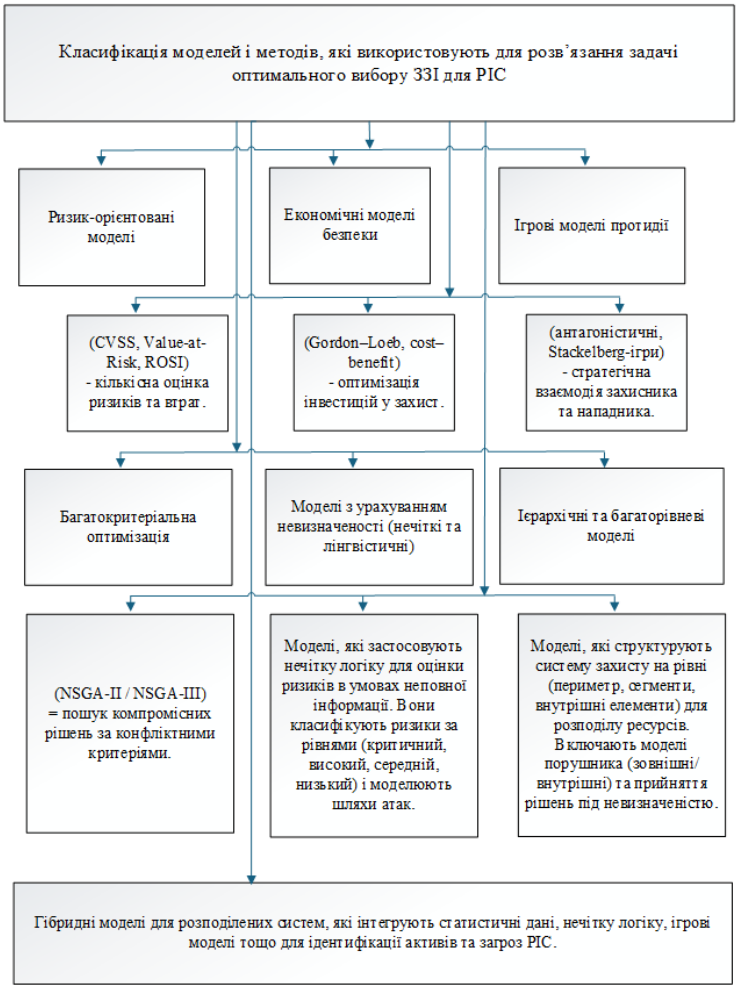

Рис. 4. Схема узагальненої класифікації моделей і методів, які використовують для розв'язання задачі оптимального вибору засобів захисту РІС

Подана на рис. 4 класифікація віддзеркалила еволюцію підходів від локальної оцінки ризиків інформаційної безпеки РІС та економічної доцільності до стратегічного та багатокритеріального прийняття рішень в умовах протидії нападнику.

4. Результати дослідження.

З урахуванням проведено аналізу літературних джерел та виявлених особливостей РІС й стратегічного характеру сучасних кібернетичних загроз, доцільним є формування цілісного методу оптимального вибору засобів захисту інформації, який поєднає моделі протидії раціональному противнику та процедури багатокритеріального прийняття рішень. Такий метод має забезпечувати формалізований опис взаємодії між стороною захисту та нападником, урахування архітектури РІС, варіативності її станів і бюджетних обмежень.

На рис. 5 наведено узагальнену схему методу оптимального вибору засобів захисту інформації для розподілених інформаційних систем, що відображає послідовність основних етапів формування захисної конфігурації в умовах кібернетичної протидії.

Поданий на рис. 5 метод ґрунтується на поетапному аналізі архітектури РІС, ідентифікації вадливих та можливих сценаріїв атак з боку противника. На початковому етапі формуємо модель РІС із урахуванням її топології, характеристик вузлів і каналів взаємодії, а також визначаються множини доступних засобів захисту та ресурсні обмеження сторони оборони.

На наступному етапі здійснюємо ігрове моделювання взаємодії між стороною захисту та нападником. Це дозволить формалізувати стратегічний характер кібернетичної протидії та оцінити наслідки застосування різних комбінацій атак і засобів захисту. Отримані результати використовуємо як вхідні дані для багатокритеріальної оптимізації, у межах якої виконуємо вибір раціональної конфігурації ЗЗІ з урахуванням показників ефективності, вартості та рівня зниження ризиків для вузлів РІС.

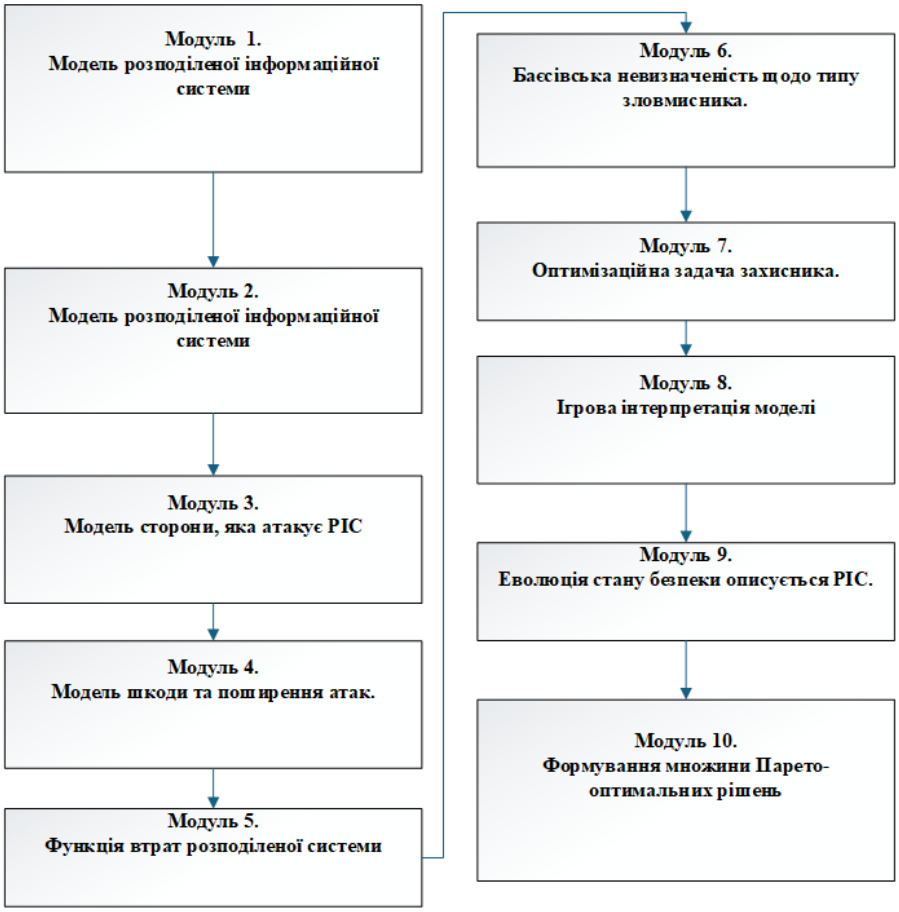

Рис. 5. Схема методу оптимального вибору ЗЗІ для РІС

Завершальним етапом методу є оцінювання отриманого рішення та, за потреби, його адаптація відповідно до зміни станів РІС або поведінки противника, що забезпечує гнучкість і придатність методу до використання в динамічних умовах функціонування розподілених інформаційних систем.

5. Висновки.

Доведено, що сучасна кіберзлочинність перейшла від випадкових атак до цілеспрямованої протидії, де сторона атаки (нападник) виступає як раціональний або обмежено-раціональний суб’єкт. Такий противник здатен передчасно оцінити ресурси захисту, обрати найбільш вразливі вузли розподіленої системи та оптимізувати власні витрати для досягнення максимальної шкоди. Це, відповідно, потребує перегляду наявних методів та моделей вибору ЗЗІ. Аналіз об'єкта захисту показав, що наявні РІС характеризують високим рівнем гетерогенності, великою кількістю точок входу та складністю ієрархічних зв'язків. Це створює надлишкову поверхню атаки, де наявні периметрові засоби захисту інформації стають малоефективними проти професійних APT-угруповань.

Огляд наявних методів вибору засобів захисту виявив суттєвий недолік. Доведено, що більшість із цих методів ґрунтується на статичному аналізі ризиків або експертних оцінках. Ці методи не враховують природний ігровий характер взаємодії із противником. Відсутні інтегровані методи, які дозволяли б одночасно враховувати технічні параметри засобів захисту, бюджетні обмеження, як-от ринкова вартість, а вона постійно стрімко зростає, та стратегічну поведінку сторони, яка атакує PIC. Отримані результати підтвердили потребу синтезу гібридного методу оптимального вибору засобів захисту. Такий метод має поєднувати апарат теорії ігор для моделювання протидії раціональному противнику та методи багатокритеріальної оптимізації для вибору конфігурації засобів захисту в умовах обмежених ресурсів.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Dodonov, O. H., Nykyforov, O. V., Putiatin, V. H., Dodonov, V. O., Kutsenko, S. A., & Hermaniuk, A. P. (2024). Territorial-distributed information computer systems in a unified information space: Basic concepts and definitions. *Data Registration, Storage and Processing, 26*(1), 89–112.
2. Barabash, O., Makarchuk, A., & Salanda, I. (2024). Study of the probabilistic indicator of functional stability of distributed information systems. *Measuring and Computing Devices in Technological Processes, 1*, 45–50.
3. Lienkov, S., Dzhulii, V., Muliar, I., Lienkov, Ye., & Koltsov, R. (2025). Evaluation of the effectiveness of confidential information protection systems in distributed information systems. *Cybersecurity: Education, Science, Technique, 1*(29), 628–644.
4. Heryak, Yu., & Berko, A. (2024). A system of criteria for assessing data quality in distributed information systems. *Information Systems and Networks, 16*, 191–202.
5. Bozhko, V. I., & Okhrimenko, O. H. (2006). Methodology for evaluating the functional stability of the structure of distributed information systems of critical application. *Radioelectronic and Computer Systems, 7*, 68–71.
6. Romaniv, R. S., & Bandurka, O. I. (2024). Methods for ensuring the functional stability of distributed information systems for monitoring vehicle movement using blockchain technology. *Information Technologies and Automation 2024*, 221.
7. Palko, D. V., & Myrutenko, L. V. (n.d.). Method for constructing a profile of key cybersecurity risk factors of modern distributed information systems. *Ukrainian Information Security Research Journal, 26*(2), 236–252.
8. Ziegler, K. (1979). A distributed information system study. *IBM Systems Journal, 18*(3), 374–401.
9. Björk, B. C. (2007). A model of scientific communication of a global distributed information system.
10. Pleskach, V., Pleskach, M., & Zelikovska, O. (2019). Information security management system in distributed information systems. In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 300–303). IEEE.
11. Kim, D., & Solomon, M. G. (2013). *Fundamentals of information systems security*. Jones & Bartlett.
12. Mitra, S., & Ransbotham, S. (2012). The effects of information disclosure policy on the diffusion of security attacks. In *Proceedings of the International Conference on Information Systems (ICIS 2012)*.
13. Riskhan, B., Safuan, H. A. J., Hussain, K., Elnour, A. A. H., Abdelmaboud, A., Khan, F., & Kundi, M. (2023). An adaptive distributed denial-of-service attack prevention technique in a distributed environment. *Sensors, 23*(14), 6574.
14. Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), & Multi-State Information Sharing and Analysis Center (MS-ISAC). (2024). *CISA, FBI, and MS-ISAC release update to joint guidance on distributed denial-of-service techniques*.

15. Abouzakhar, N. S., & Manson, G. A. (2002). An intelligent approach to prevent distributed systems attacks. *Information Management & Computer Security, 10*(5), 203–209.

16. Reddy, R. P. (2024). A survey of distributed denial-of-service (DDoS) attack mitigation techniques. *International Journal of Computer Trends and Technology, 72*(12), 69–77.

17. Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks, 13*(12), 1550147717741463.

18. Microsoft Corporation. (2025). *Microsoft digital defense report 2025: Understanding the threat landscape*.

19. Check Point Research. (2025). *The state of global cyber security 2025: Annual report*. Check Point Software Technologies Ltd.

20. Cloud Security Alliance. (2025). *Top threats to cloud computing: Deep dive 2025*.

21. Cloudflare. (2025). *DDoS threat report for 2025 Q1: Trends and insights*.

22. IBM Security. (2025). *Cost of a data breach report 2025*. IBM Corporation.

23. KELA Research. (2025). *Ransomware in critical infrastructure: 2025 global analysis*.

24. UK Department for Business, Innovation & Skills. (2012). *10 steps to cyber security: Executive companion*.

25. MWR InfoSecurity. (2013). *Mobile devices: Guide for implementers*.

26. European Union Agency for Cybersecurity (ENISA). (2012). *Consumerization of IT: Risk mitigation strategies*.

27. Osadchyi, V. V. (2018). Modern trends in informatics and cybernetics. In *Information technologies in education, science and technology: Proceedings of the IV International scientific and practical conference* (pp. 221–224).

28. Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open, 5*(2), 2158244015580372.

29. Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & Van Moorsel, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science, 64*, 1035–1042.

30. Diéguez, M., Cares, C., Cachero, C., & Hochstetter, J. (2023). MASISCo—Methodological approach for the selection of information security controls. *Applied Sciences, 13*(2), 1094.

31. Yaskevych, Yu. (2025). Game-theoretic optimization model for selecting protection means for distributed information systems. *Cybersecurity: Education, Science, Technique, 2*(30), 715–726. https://doi.org/10.28925/2663-4023.2025.30.913

Надійшла до редакції: 03.12.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26