https://doi.org/10.31891/2219-9365-2026-86-44
УДК 004.7:004.3

КУШНІР Дмитро
Хмельницький національний університет
https://orcid.org/0009-0001-6581-6081
e-mail: dima99.kushnir@gmail.com
РЕГІДА Павло
Хмельницький національний університет
https://orcid.org/0000-0002-6591-7069
e-mail: pavlo.rehida@gmail.com
КЛЕЙН Олександр
Хмельницький національний університет
https://orcid.org/0000-0002-1896-943X
e-mail: olexandrkleyn@gmail.com
ВІЖЕВСЬКИЙ Петро
Хмельницький національний університет
https://orcid.org/0009-0009-4851-0839
e-mail: vizhevskyipv@khmnu.edu.ua

МЕТОД ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНИХ СИСТЕМ НА ОСНОВІ АВТОМАТИЧНОГО ЗАСТОСУВАННЯ КРИТЕРІЇВ БЕЗПЕКИ

Сучасний розвиток інформаційних технологій супроводжується активним переходом до розподілених обчислювальних архітектур, зокрема хмарних середовищ, мікросервісних систем, контейнеризованих інфраструктур та edge-обчислень. Такі підходи забезпечують високу масштабованість, гнучкість і відмовостійкість, проте суттєво ускладнюють забезпечення інформаційної безпеки через динамічність топології, значну кількість взаємодіючих компонентів і різнорівневу довіру між ними. У цих умовах традиційні методи, що базуються на статичних політиках і ручному адмініструванні, виявляються недостатньо ефективними, що зумовлює необхідність автоматизації процесів забезпечення безпеки.

У роботі запропоновано метод організації функціонування розподілених систем на основі автоматизованого застосування формалізованих критеріїв безпеки, який орієнтований на аналіз впливу змін у комп'ютерних мережах на аргументи кібербезпеки. Метод передбачає використання метамоделі аргументів безпеки, множини типових шаблонів, механізму семантичної простежуваності, формалізованого каталогу правил узгодженості та моделі взаємозв'язків результатів перевірки і валідації. Це дозволяє забезпечити інтеграцію вимог безпеки у структуру системи, автоматизувати контроль їх виконання та своєчасно виявляти невідповідності.

Розроблене програмне забезпечення реалізує запропонований метод і забезпечує аналіз чотирьох типових шаблонів аргументів безпеки: контроль доступу, захист мережевого периметра, виявлення вторгнень і цілісність конфігурації. Експериментальна перевірка показала високу точність визначення узгодженості аргументів (94–97%), мінімальну кількість помилкових спрацьовувань, повне охоплення змін та низький час обробки сценаріїв (1–1,5 с). Отримані результати підтверджують адекватність і практичну придатність методу для використання у динамічних розподілених середовищах.

Подальші дослідження доцільно спрямувати на розширення та деталізацію моделей для різних типів аргументів безпеки та підвищення рівня їх адаптивності.

Ключові слова: розподілена система, комп'ютерна система, комп'ютерна мережа, автоматизація, критерії безпеки, показники компроментації, кібербезпека, захист периметру, контроль доступу.

KUSHNIR Dmytro, REHIDA Pavlo, KLEIN Olexandr, VIZHEVSKYI Petro
Khmelnytskyi National University

METHOD OF ORGANIZING THE FUNCTIONING OF DISTRIBUTED SYSTEMS BASED ON THE AUTOMATIC APPLICATION OF SECURITY CRITERIA

The modern development of information technologies is accompanied by an active transition to distributed computing architectures, in particular cloud environments, microservice systems, containerized infrastructures and edge computing. Such approaches provide high scalability, flexibility and fault tolerance, but significantly complicate the provision of information security due to the dynamics of the topology, a significant number of interacting components and different levels of trust between them. In these conditions, traditional methods based on static policies and manual administration are not effective enough, which necessitates the automation of security processes.

The paper proposes a method of organizing the functioning of distributed systems based on the automated application of formalized security criteria, which is focused on analyzing the impact of changes in computer networks on cyber security arguments. The method involves the use of a metamodel of security arguments, a set of typical templates, a mechanism of semantic traceability, a formalized catalog of consistency rules, and a model of the relationships of verification and validation results. This makes it possible to ensure the integration of security requirements into the structure of the system, to automate the control of their implementation, and to detect inconsistencies in a timely manner.

The developed software implements the proposed method and provides analysis of four typical patterns of security arguments: access control, network perimeter protection, intrusion detection, and configuration integrity. Experimental verification showed high accuracy in determining the consistency of arguments (94–97%), minimal number of false positives, full coverage of changes and low processing time of scenarios (1–1.5 s). The obtained results confirm the adequacy and practical suitability of the method for use in dynamic distributed environments.

Further research should be focused on expanding and detailing models for different types of security arguments and increasing their adaptability.

Keywords: distributed system, computer system, computer network, automation, security criteria, indicators of compromise, cyber security, perimeter protection, access control.

Стаття надійшла до редакції / Received 0.04.2026
Прийнята до друку / Accepted 04.05.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ

Сучасний етап розвитку інформаційних технологій характеризується стрімким переходом до розподілених обчислювальних архітектур, зокрема хмарних платформ, мікросервісних середовищ, контейнеризованих інфраструктур та edge-обчислень. Такі системи забезпечують масштабованість, відмовостійкість та гнучкість, однак водночас істотно ускладнюють забезпечення інформаційної безпеки.

На відміну від централізованих систем, розподілені середовища мають динамічну топологію, велику кількість взаємодіючих вузлів, асинхронні комунікації та різнорівневу довіру між компонентами. Це призводить до зростання кількості потенційних вразливостей, ускладнення контролю доступу, моніторингу подій безпеки та своєчасного реагування на інциденти.

Традиційні підходи до забезпечення безпеки, що базуються на ручному адмініструванні політик і статичних правилах контролю доступу, виявляються недостатньо ефективними в умовах динамічних розподілених систем. Людський фактор, складність конфігурацій та масштаб інфраструктури підвищують ризик помилок і невідповідностей політик безпеки.

Актуальним напрямом досліджень є розроблення методів організації функціонування розподілених систем, що передбачають автоматизоване застосування формалізованих критеріїв безпеки. Такий підхід дозволяє інтегрувати вимоги безпеки безпосередньо в архітектуру системи, забезпечити їх постійний контроль, автоматичну верифікацію та адаптивне коригування.

Автоматизація застосування критеріїв безпеки передбачає формалізацію політик доступу, використання моделей довіри, механізмів контролю взаємодій між компонентами, а також впровадження інструментів моніторингу та оркестрації безпекових процесів.

Таким чином, розроблення методу організації функціонування розподілених систем на основі автоматизованого застосування критеріїв безпеки є актуальною науково-практичною задачею, спрямованою на підвищення стійкості, надійності та керованості сучасних інформаційних інфраструктур.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Стійкість розподілених систем у сучасній парадигмі трактується як багатовимірна інтегральна характеристика, що поєднує інформаційну безпеку, функційну надійність, відмовостійкість, адаптивність та керованість у динамічному середовищі. Вона визначає здатність системи зберігати коректність стану, неперервність виконання логічних операцій і допустимий рівень сервісу за умов дії внутрішніх збоїв, мережних порушень, навмисних атак та невизначеності часових параметрів. Разом із тим, незважаючи на значний обсяг досліджень у галузі теорії розподілених обчислень, проблема комплексного забезпечення стійкості залишається остаточно не розв'язаною, що зумовлено фундаментальними алгоритмічними обмеженнями та зростаючою складністю сучасних інфраструктур [1, 2].

Відомі підходи до забезпечення стійкості зосереджені переважно на окремих аспектах, які включають реплікації даних, досягнення консенсусу, резервування ресурсів або впровадженні криптографічних механізмів захисту. Алгоритми консенсусу дозволяють забезпечити узгодженість стану в умовах відмов частини вузлів; проте вони супроводжуються істотними витратами обчислювальних і мережних ресурсів та не вирішують проблему динамічного конфлікту політик безпеки. Теорія відмовостійкості пропонує моделі активного та пасивного резервування, але не гарантує автоматичної узгодженості безпекових критеріїв у масштабі всієї системи. Криптографічні механізми забезпечують цілісність і автентичність повідомлень, однак не усувають ризиків логічної неконсистентності або накопичення прихованих конфігураційних помилок [3, 4].

Фундаментальним обмеженням функційної стійкості залишається компроміс, окреслений теоремою CAP [5, 6], відповідно до якої в умовах мережного поділу неможливо одночасно гарантувати строгі властивості узгодженості, доступності та толерантності до розділення мережі. Існуючі архітектурні рішення змушені обирати між послабленими моделями узгодженості або зниженням доступності сервісу, що створює простір для потенційних зловживань і порушень цілісності. Невирішеною залишається проблема [7, 8] формалізованого автоматичного вибору оптимального режиму функціонування залежно від поточного стану мережі та рівня загроз.

Окремої уваги потребує проблема самостабілізації розподілених систем. Хоча теоретичні моделі самостабілізуючих алгоритмів доводять можливість повернення системи до легітимного стану з довільної

конфігурації, практична інтеграція таких механізмів у великомасштабні інфраструктури ускладнена через відсутність формалізованих критеріїв легітимності та складність глобальної верифікації стану. Залишається відкритим питання побудови універсального механізму, здатного автоматично ідентифікувати деградаційні процеси та ініціювати процедури реконфігурації без централізованого контролю [9, 10].

Невирішеною також є проблема латентних прихованих відмов, які не призводять до повної зупинки вузла, але поступово спотворюють результати обчислень або накопичують помилкові стани. Традиційні механізми моніторингу орієнтовані на явні відмови та перевищення порогових значень, тоді як складні багатовекторні атаки або логічні конфлікти політик можуть залишатися непоміченими тривалий час. Відсутність формальної моделі узгодженості безпекових критеріїв у масштабі всієї системи унеможливлює гарантоване виявлення таких аномалій [11, 12].

Складність забезпечення стійкості зростає в асинхронних мережах, де неможливо достовірно відрізнити відмову вузла від його тимчасової затримки. Це породжує ризики розгалуження стану, появи суперечливих транзакцій та втрати глобальної консистентності. Існуючі протоколи частково вирішують цю проблему шляхом введення тайм-аутів або обрання лідера, однак такі підходи залишаються вразливими до навмисних затримок та атак типу «відмова в обслуговуванні» [13, 14].

В роботах [15, 16] запропоновано підходи до забезпечення стійкості розподіленої інфраструктури в умовах впливів комп'ютерних атак.

Таким чином, можна констатувати, що в сучасних дослідженнях вирішено низку часткових задач таких, як забезпечення реплікації стану, формалізацію алгоритмів консенсусу, побудову моделей відмовостійкості, застосування криптографічних засобів підтвердження цілісності та розроблення механізмів резервування. Водночас комплексна проблема [17, 18] інтеграції функційної стійкості та інформаційної безпеки в єдину формалізовану систему автоматичного управління залишається відкритою.

Перспективними дослідженнями [19, 20, 21] є такі, що полягають в обґрунтуванні підходу, за якого стійкість розглядається як динамічний процес розподіленого середовища, який підтримується автоматичним застосуванням формалізованих критеріїв безпеки до кожної взаємодії між компонентами системи. Запропонована концепція передбачає інтеграцію алгоритмічної надійності, політик доступу, механізмів виявлення конфліктів і процедур реконфігурації в єдину модель управління, що функціонує в реальному часі. У межах такого підходу потенційно можуть бути вирішені проблеми автоматичного узгодження політик, виявлення їх конфліктності, мінімізації ризику логічної неконсистентності, а також адаптивного вибору режиму функціонування системи залежно від рівня загроз та стану мережної інфраструктури. Це дозволяє перейти від реактивної моделі захисту до проактивної адаптивної архітектури, у якій стійкість забезпечується не лише надмірністю ресурсів, а й інтелектуальним керуванням поведінкою компонентів.

Сучасний стан досліджень характеризується наявністю ефективних локальних рішень, але відсутністю універсальної методології, що поєднує алгоритмічну узгодженість, безпекові критерії та механізми самовідновлення в єдину формалізовану систему. Розроблення такого підходу становить актуальну наукову проблему та визначає напрям подальших досліджень у галузі організації функціонування стійких розподілених систем.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є покращення автоматичного застосування та контролю критеріїв безпеки на всіх рівнях функціонування розподілених систем та взаємодії їх компонентів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Метамодель аргументів безпеки

Для автоматизованого аналізу впливу змін у комп'ютерних мережах на аргументи кібербезпеки потрібно розробити метод, який забезпечуватиме підтримку актуальності та узгодженості доказів безпечності системи при зміні її конфігурації або структури. Для реалізації такого методу необхідно сформувати формалізовану модель представлення аргументів безпеки, що дозволить описувати взаємозв'язки між елементами аргументації, вимогами безпеки, доказами перевірки та компонентами мережної інфраструктури. У процесі дослідження необхідно систематизувати та сформувати каталог правил узгодженості між елементами аргументів безпеки та артефактами комп'ютерної мережі, такими як конфігурації вузлів, мережні служби, політики доступу, програмні модулі та результати перевірок безпеки. Ці правила повинні визначати, яким чином зміни у структурі або параметрах мережної системи впливають на відповідні елементи аргументації безпеки, а також дозволяти автоматично визначати елементи, які можуть втратити актуальність або потребують повторної перевірки. Крім того, необхідно визначити та реалізувати механізм семантичної простежуваності між моделями системної інженерії комп'ютерної мережі та моделями аргументів безпеки. Такий механізм повинен забезпечувати встановлення формальних зв'язків між елементами мережної інфраструктури та твердженнями аргументів безпеки, що дозволить автоматично відстежувати зміни у системі та визначати їх вплив на відповідні елементи аргументації. Це, у свою чергу, забезпечить можливість автоматизованого оновлення статусу аргументів безпеки при модифікації мережних компонентів або їх конфігурацій.

Важливим завданням дослідження є також формалізація взаємозв'язків між різними результатами перевірки та валідації безпеки, які використовуються як докази під час формування аргументів безпеки. Необхідно визначити правила взаємозалежності між різними типами доказів, зокрема результатами статичного аналізу, тестування безпеки, перевірок конфігурацій та інших методів оцінювання захищеності. Це дозволить виконувати автоматизований аналіз повноти та достатності доказів безпечності системи, а також визначати вплив додавання, модифікації або видалення таких доказів на загальну структуру аргументації безпеки.

Для забезпечення практичної реалізації запропонованого підходу необхідно розробити структуру повторно використовуваних елементів аргументації безпеки, які можуть бути застосовані як типові шаблони або будівельні блоки під час формування аргументів безпеки комп'ютерних мереж. Для кожного такого елемента повинні бути визначені відповідні правила узгодженості та умови їх перевірки у разі зміни стану мережної системи.

Результатом виконання зазначених завдань має стати формування узагальненого методу організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки для автоматизованого аналізу впливу змін у комп'ютерних мережах на аргументи кібербезпеки, який забезпечуватиме можливість точного визначення порушень узгодженості між елементами аргументації безпеки, мережними артефактами та доказами перевірки безпеки, а також сприятиме підвищенню ефективності процесів управління змінами та підтримки актуальності аргументів безпеки у складних мережних системах.

Таким чином, потрібно здійснити розроблення метамоделі аргументів безпеки, множини типових шаблонів аргументів безпеки, механізм семантичної простежуваності кореляції між змінами, формалізований каталог правил узгодженості, формальна модель взаємозв'язків між результатами перевірки та валідації безпеки і метод організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки.

Спочатку розробимо метамодель аргументів безпеки сумісну зі стандартом GSN (Goal Structuring Notation), яка підтримує автоматизовану перевірку узгодженості та аналіз змін. Необхідно розробити метамодель аргументів безпеки, сумісну зі стандартом GSN, яка забезпечуватиме формалізоване представлення структури аргументів кібербезпеки комп'ютерних мереж та підтримуватиме автоматизовану перевірку їх узгодженості. Запропонована метамодель повинна визначати основні елементи аргументації безпеки, зокрема цілі безпеки, стратегії доведення, твердження, контексти та докази, а також описувати формальні зв'язки між ними.

У межах розроблення метамоделі необхідно передбачити механізми встановлення прямих зв'язків між елементами аргументів безпеки та артефактами комп'ютерної мережі, такими як компоненти мережної інфраструктури, конфігураційні параметри, політики безпеки, результати перевірок і тестування. Це дозволить забезпечити семантичну простежуваність між моделями системної інженерії мережі та структурою аргументів безпеки.

Крім того, метамодель повинна підтримувати можливість анотування зв'язків між елементами аргументації та системними артефактами спеціалізованими правилами узгодженості, що визначають умови коректності аргументів безпеки у разі зміни параметрів або структури мережної системи. На основі таких правил має бути забезпечена автоматизована перевірка узгодженості аргументів безпеки та визначення їх актуальності після внесення змін до конфігурації комп'ютерної мережі.

Метамодель аргументів безпеки представимо у вигляді формальної структури так:

$$M = (A, R, T, C), \tag{1}$$

де A - множина елементів аргументації безпеки; R - множина відношень між елементами аргументації; T - множина трасових зв'язків між аргументами безпеки та артефактами системи; C - множина правил узгодженості.

Множину елементів аргументів безпеки визначимо так:

$$A = G \cup S \cup E \cup K, \tag{2}$$

де G - множина цілей безпеки (Goals); S - множина стратегій доведення (Strategies); E - множина доказів або результатів перевірок (Evidence); K - множина контекстних елементів (Context).

Таким чином, задамо множину елементів аргументів безпеки так:

$$A = \{a_1, a_2, \dots, a_{n_A}\}, a_i = (a_{i,id}, a_{i,type}, a_{i,state}), \tag{3}$$

де a_i - i-тий елемент аргументації, що описується кортежем; $i = 1,2, \dots, n_A$; n_A – кількість елементів множини A; $a_{i,id}$ - ідентифікатор елемента; $a_{i,type} \in G \cup S \cup E \cup K$; $a_{i,state}$ - стан узгодженості елемента.

Множина станів $A_{state} = \{a_{1,state}, a_{2,state}, \dots, a_{n_A,state}\}$, де $a_{i,state} \in \{\text{дійсний}, \text{непослідовний}, \text{застарілий}\}$.

Відношення аргументації визначимо множиною так:

$$B \subseteq A \times A, \tag{4}$$

де елемент $(a_i, a_j) \in B$ і означає, що він підтримує або деталізує елемент a_i.

Функцію підтримки для елементів з формули (2.4) визначимо так:

$$F_{support}: A \to 2^A, F_{support}(a_i) = \{a_j | (a_i, a_j) \in B\}, \tag{5}$$

де елемент $(a_i, a_j) \in B$ і означає, що він підтримує або деталізує елемент a_i; B - відношення аргументації; A - множина елементів аргументів безпеки; 2^A – множина підмножин множини A.

Модель системних артефактів комп'ютерної мережі задамо через артефакти системи множиною так:

$$S_{sys} = \{s_1, s_2, \dots, s_{n_{S_{sys}}}\}, \tag{6}$$

де $s_j = (s_{j,type}, s_{j,value})$; $n_{S_{sys}}$ – кількість елементів множини S_{sys}; $j = 1,2, \dots, n_{S_{sys}}$.

Типи артефактів можуть включати вузли мережі, конфігурації, політики безпеки, результати тестування, програмні компоненти.

Зв'язок між аргументами безпеки та артефактами системи визначимо так:

$$T \subseteq A \times S_{sys}, \tag{7}$$

де елемент $(s_i, s_j) \in T$ і означає, що аргумент безпеки a_i залежить від артефакта системи s_j.

Функцію залежності визначимо так:

$$F_{trace}(a_i) = \{a_j | (a_i, s_j) \in T\}, \tag{8}$$

де елемент $(a_i, s_j) \in T$.

Зміни системи визначимо множиною так:

$$D_\Delta = \{(\delta, s_j) | \, j = 1,2, \dots, n_{S_{sys}}\}, \tag{9}$$

де s_j – змінений артефакт; δ - тип зміни; $\delta \in \{\text{доповнено}, \text{видалено}, \text{модифіковано}\}$.

Правило узгодженості визначимо як функцію так:

$$c_k: A \times S_{sys} \times D_\Delta \to M_{state}, \tag{10}$$

де $M_{state} = \{\text{дійсний}, \text{непослідовний}, \text{застарілий}\}$; M_{state} – множина станів; D_Δ - множина змін системи; A - множина елементів аргументів безпеки; S_{sys} – множина артефактів системи.

Функція c_k визначає новий стан аргументу безпеки після зміни системного артефакта.

Стан елемента аргументації визначатимемо функцією так:

$$F_{state} = \begin{cases} \text{дійсний, якщо } c_k(a_i, s_j, \delta) = \text{дійсний}; \\ \text{непослідовний, якщо } c_k(a_i, s_j, \delta) = \text{непослідовний}; \\ \text{застаріший, якщо } c_k(a_i, s_j, \delta) = \text{застарілий}, \end{cases} \tag{11}$$

де $s_j = (s_{j,type}, s_{j,value})$; $n_{S_{sys}}$ – кількість елементів множини S_{sys}; $j = 1,2, \dots, n_{S_{sys}}$; a_i - i-тий елемент аргументації, що описується кортежем; $i = 1,2, \dots, n_A$; n_A – кількість елементів множини A; δ - тип зміни; $\delta \in \{\text{доповнено}, \text{видалено}, \text{модифіковано}\}$.

Аналіз впливу змін задамо функцією так:

$$F_v(M, D_\Delta) \to A', \tag{12}$$

де M - метамодель аргументів безпеки; D_Δ - множина змін; A' - оновлений стан аргументів.

Суть визначення функції F_v полягає у визначенні змінених артефактів s_j та знаходженні всіх аргументів, тобто формування множини так:

$$A_s = \{a_i | (a_i, s_j) \in T\}, \tag{13}$$

де елемент $(a_i, s_j) \in T$.

Формула (13) додатково доповнює формулу (8) і далі потрібно застосувати правила узгодженості з множини правил узгодженості C та оновити стан аргументів.

Таким чином, згідно введених понять та співвідношень (1)-(13) задамо концептуальну метамодель аргументів безпеки комп'ютерної мережі так:

$$M_k = (A, R, S_{sys}, T, C), \tag{14}$$

де A - множина елементів аргументації безпеки; R - множина відношень між елементами аргументації; S_{sys} - артефакти мережної системи; T - множина трасових зв'язків між аргументами безпеки та артефактами системи; C - множина правил узгодженості.

Запропонована метамодель аргументів безпеки, узгоджена з підходом **Goal Structuring Notation,** формує цілісну формалізовану основу для автоматизованої підтримки аргументів кібербезпеки у комп'ютерних мережах. Її ключова особливість полягає у поєднанні трьох раніше роз'єднаних компонентів: структури аргументації безпеки; моделей системних (мережних) артефактів; механізму аналізу впливу змін. На відміну від традиційного використання GSN як графічного засобу документування аргументів, запропонована метамодель розширює його до рівня формальної, машинозчитуваної структури з чітко визначеними трасовими зв'язками та правилами узгодженості.

Особливістю метамоделі є введення семантичної простежуваності між елементами аргументів безпеки та артефактами комп'ютерної мережі. Це дозволяє перейти від статичного опису аргументації до динамічної моделі, здатної реагувати на зміни конфігурації системи. У результаті аргументи безпеки перестають бути лише текстовими або графічними обґрунтуваннями і набувають властивостей формальної моделі, що підтримує автоматизовану перевірку узгодженості. Таким чином, метамодель забезпечує можливість мінімізувати ручний аналіз під час управління змінами, підвищити точність визначення впливу змін та зменшити ризик використання застарілих доказів безпечності.

Практична цінність метамоделі полягає в тому, що вона дозволяє автоматично визначати аргументи безпеки, на які вплинули зміни у мережній інфраструктурі, формалізувати правила узгодженості між вимогами безпеки, доказами та системними компонентами, оцінювати повноту доказової бази після модифікації конфігурації системи, забезпечувати контроль актуальності аргументів безпеки в процесі експлуатації мережі. Таким чином, метамодель створює основу для побудови інтелектуальних інструментів підтримки процесів забезпечення кібербезпеки, аудиту та сертифікації мережних систем.

Отже, запропонована метамодель є теоретично обґрунтованою основою для автоматизованого аналізу впливу змін на аргументи кібербезпеки комп'ютерних мереж. Вона забезпечує формалізацію структури аргументації, інтеграцію з моделями системної інженерії та підтримку автоматизованої перевірки узгодженості. Подальше розширення та інструментальна реалізація метамоделі дозволять створити повноцінний метод підтримки актуальності аргументів безпеки у динамічних мережних середовищах.

Механізм семантичної простежуваності кореляції між змінами.

У сучасних комп'ютерних мережах процес забезпечення кібербезпеки характеризується високою динамічністю, що пов'язано з постійними змінами у конфігураціях мережних пристроїв, оновленням програмного забезпечення, модифікацією політик доступу, появою нових сервісів та впровадженням додаткових механізмів захисту. Такі зміни є природною частиною експлуатації та розвитку мережної інфраструктури, проте вони можуть безпосередньо впливати на обґрунтованість раніше сформованих аргументів безпеки. Аргументи кібербезпеки формуються на основі конкретних припущень щодо структури системи, її конфігурацій, механізмів захисту та результатів перевірок безпеки. У разі зміни будь-якого з цих елементів може виникнути ситуація, коли частина аргументації втрачає актуальність або потребує повторного підтвердження.

Особливо складною є ситуація у великих або розподілених комп'ютерних мережах, де кількість взаємопов'язаних компонентів є значною, а зміни можуть відбуватися одночасно у різних частинах інфраструктури. У таких умовах ручний аналіз впливу змін на аргументи безпеки стає надзвичайно трудомістким і не завжди дозволяє своєчасно виявити потенційні порушення у структурі аргументації. Крім того, різні елементи аргументів безпеки можуть бути пов'язані з багатьма артефактами системної інженерії, такими як конфігурації мережних пристроїв, правила міжмережних екранів, політики доступу або результати тестування безпеки. Через це навіть незначні зміни у системі можуть мати складні та неочевидні наслідки для обґрунтованості аргументів кібербезпеки.

Для розв'язання цієї проблеми необхідно забезпечити можливість відстеження зв'язків між елементами аргументів безпеки та компонентами комп'ютерної мережі, на яких базується відповідна аргументація. Такий підхід дозволяє визначати, які саме твердження безпеки, стратегії доведення або докази можуть бути затронуті у разі змін у системі. Важливою особливістю такого відстеження є не лише фіксація технічних залежностей між елементами різних моделей, але й врахування їхнього семантичного змісту. Іншими словами, необхідно встановлювати змістовні зв'язки між змінами у мережній інфраструктурі та відповідними елементами аргументації безпеки.

Саме з цією метою введемо механізм семантичної простежуваності кореляції між змінами. Його призначення полягає у формальному встановленні зв'язків між компонентами комп'ютерної мережі, результатами перевірки безпеки та елементами аргументів кібербезпеки. Такий механізм дозволяє відстежувати, які зміни у мережній системі можуть впливати на конкретні елементи аргументації, а також визначати, які твердження безпеки потребують повторної перевірки або оновлення. Наявність механізму семантичної простежуваності створює основу для автоматизованого аналізу впливу змін у комп'ютерних

мережах на аргументи кібербезпеки та забезпечує підтримку їх актуальності у процесі експлуатації та розвитку мережних систем.

Для забезпечення актуальності аргументів безпеки у комп'ютерних мережах необхідно враховувати той факт, що мережні системи постійно змінюються. Зміни можуть стосуватися конфігурацій мережних пристроїв, політик доступу, програмного забезпечення, топології мережі або механізмів захисту. Оскільки аргументи безпеки базуються на конкретних артефактах системи та результатах перевірок безпеки, будь-яка зміна цих елементів може впливати на коректність відповідних тверджень безпеки. У зв'язку з цим виникає необхідність розроблення механізму семантичної простежуваності кореляції між змінами, який дозволяє встановлювати зв'язки між змінами у мережній системі та елементами аргументів безпеки, що можуть бути ними порушені.

Семантична простежуваність передбачає формальне встановлення зв'язків між елементами різних моделей: моделлю комп'ютерної мережі, моделлю аргументів безпеки та результатами перевірки й валідації системи. Для цього введемо множину елементів аргументації безпеки

$$N_a = N_g \cup N_s \cup N_e, \tag{15}$$

де N_g - множина цілей безпеки; N_s - множина стратегій аргументації; N_e - множина доказів безпеки.

Паралельно введемо множину елементів мережної системи так:

$$S_{net} = \left\{s_{net,1}, s_{net,2}, \dots, s_{net,n_{S_{net}}}\right\}, \tag{16}$$

де $s_{net,i}$ - i-та компонента мережі; $i = 1,2,\dots,n_{S_{net}}$; $n_{S_{net}}$ – кількість компонент в мережі.

Множина S_{net} містить компоненти комп'ютерної мережі, зокрема вузли, мережні служби, конфігурації пристроїв, правила міжмережних екранів та інші артефакти системної інженерії.

Для встановлення зв'язків між елементами аргументів безпеки та компонентами мережної системи введемо відношення семантичної простежуваності так:

$$T_{sp} \subseteq N_a \times S_{net}, \tag{17}$$

де пара $(n_i, s_{net,j})$ означає що елемент аргументації n_i семантично залежить від елемента мережної системи $s_{net,j}$.

Наприклад, доказ безпеки може бути пов'язаний із конкретною конфігурацією міжмережного екрану або результатом тестування системи виявлення та запобігання вторгнень.

Однак для аналізу впливу змін необхідно формально описати самі зміни у мережній системі. Для цього введемо множину змін так:

$$Q_{net} = \left\{q_{net,1}, q_{net,2}, \dots, q_{net,n_{Q_{net}}}\right\}, \tag{18}$$

де $q_{net,i}$ - i-та зміна у мережній системі; $i = 1,2,\dots,n_{Q_{net}}$; $n_{Q_{net}}$ – кількість змін у мережній системі.

К кожна зміна $q_{net,i}$ відображає модифікацію певного елемента мережної системи. Формально кожну зміну подамо як відображення так:

$$q_{net,i}: s_{net,i} \to s'_{net,i}, \tag{19}$$

де $s_{net,i}$ - початковий стан елемента системи, а $s'_{net,i}$ - стан після зміни.

Після цього введемо відношення кореляції змін, яке дозволить встановити, які елементи аргументації можуть бути затронуті певною зміною, так:

$$R_{sp} \subseteq Q_{net} \times N_a, \tag{20}$$

де пара $(q_{net,i}, n_{a,i})$ означає, що зміна $q_{net,i}$ потенційно впливає на елемент аргументації $n_{a,i}$.

Таке відношення для опису кореляції змін визначимо через відношення простежуваності так:

$$(q_{net,i}, n_{a,i}) \in R_{sp} \leftrightarrow (n_{a,i}, s_{net,j}) \in T_{sp}$$

де $s_{net,j}$ є елементом системи, що змінюється у результаті виконання зміни $q_{net,i}$.

Ця модель дозволяє визначити множину аргументів безпеки, які можуть бути порушені внаслідок змін у мережній системі. Для цього введемо функцію впливу змін

$$F_I(q_{net,i}) = \left\{n_{a,i} \in N_a | (q_{net,i}, n_{a,i}) \in R_{sp}\right\}, \tag{21}$$

де $F_I(q_{net,i})$ - множина елементів аргументації, на які впливає зміна $q_{net,i}$.

У процесі експлуатації комп'ютерних мереж аргументи безпеки формуються на основі конкретних технічних характеристик системи, конфігурацій мережних пристроїв, політик доступу, механізмів захисту та результатів перевірок безпеки. Проте мережні інфраструктури є динамічними системами, у яких постійно відбуваються зміни: оновлюється програмне забезпечення; змінюються правила доступу; додаються нові

сервіси; модифікуються параметри мережних пристроїв; впроваджуються нові засоби захисту. У результаті таких змін виникає ризик втрати актуальності раніше сформованих аргументів безпеки, оскільки вони можуть базуватися на припущеннях або доказах, що вже не відповідають поточному стану системи.

Особливо важливо враховувати вплив змін на типові шаблони аргументів безпеки, які використовуються для обґрунтування захищеності різних аспектів функціонування комп'ютерних мереж. Кожний шаблон аргументації пов'язаний із певними компонентами мережної інфраструктури та відповідними механізмами захисту. Тому зміни у цих компонентах можуть безпосередньо впливати на коректність аргументації. У зв'язку з цим необхідно забезпечити механізм семантичної простежуваності, який дозволяє встановлювати змістовні зв'язки між змінами у мережній системі та відповідними елементами аргументів безпеки.

Зокрема, у випадку шаблону аргументу безпеки для контролю доступу аргументація базується на припущенні, що доступ до ресурсів комп'ютерної мережі здійснюється виключно відповідно до визначених політик доступу та процедур автентифікації користувачів. Однак у реальних системах можуть відбуватися зміни, пов'язані з додаванням нових користувачів, модифікацією ролей доступу, впровадженням нових сервісів або зміною механізмів автентифікації. Такі зміни можуть впливати на коректність твердження про те, що доступ до ресурсів мережі є належним чином контрольованим. Тому механізм семантичної простежуваності повинен забезпечувати можливість встановлення зв'язку між змінами у політиках доступу або системах автентифікації та відповідними елементами аргументації безпеки.

Аналогічно, у випадку шаблону аргументу безпеки для захисту мережного периметра аргументація базується на припущенні, що мережа захищена від несанкціонованого доступу із зовнішнього середовища за допомогою міжмережних екранів та механізмів фільтрації трафіку. Проте зміни у конфігурації міжмережних екранів, відкриття нових мережних портів, додавання нових мережних сегментів або модифікація топології мережі можуть змінювати рівень захищеності периметра. У такій ситуації аргумент безпеки, який підтверджує захищеність мережного периметра, може втратити актуальність або потребувати повторної перевірки. Саме тому необхідно забезпечити можливість встановлення семантичних зв'язків між конфігураціями мережних засобів захисту та відповідними елементами аргументів безпеки.

У випадку шаблону аргументу безпеки для виявлення вторгнень аргументація ґрунтується на здатності системи виявляти та реєструвати мережні атаки або інші підозрілі події. Проте ефективність таких систем може змінюватися внаслідок оновлення програмного забезпечення, модифікації правил аналізу мережного трафіку або появи нових типів атак. Якщо система виявлення вторгнень не адаптована до нових загроз або її конфігурація була змінена, це може впливати на коректність аргументу безпеки щодо здатності системи своєчасно виявляти атаки. У зв'язку з цим необхідно забезпечити механізм відстеження зв'язків між змінами у системах моніторингу безпеки та відповідними доказами аргументації.

Подібна ситуація виникає і для шаблону аргументу безпеки щодо цілісності конфігурації мережних компонентів. Аргументація у цьому випадку базується на припущенні, що всі зміни конфігурацій мережних пристроїв або програмних компонентів виконуються відповідно до визначених процедур управління конфігураціями та проходять необхідні процедури авторизації. Проте у процесі експлуатації системи можуть відбуватися зміни конфігурацій, пов'язані з оновленням програмного забезпечення, виправленням вразливостей або модернізацією мережної інфраструктури. Якщо такі зміни виконуються без належного контролю або не враховуються у структурі аргументації, відповідний аргумент безпеки може втратити достовірність.

Таким чином, для кожного із розглянутих шаблонів аргументів безпеки існує тісний зв'язок між елементами аргументації та конкретними компонентами комп'ютерної мережі. Зміни у цих компонентах можуть мати безпосередній вплив на коректність відповідних тверджень безпеки. Саме тому виникає необхідність у розробленні механізму семантичної простежуваності кореляції між змінами, який дозволяє встановлювати змістовні зв'язки між змінами у мережній інфраструктурі та відповідними елементами аргументів кібербезпеки. Реалізація такого механізму створює основу для автоматизованого аналізу впливу змін у комп'ютерних мережах на аргументи безпеки та забезпечує підтримку їх актуальності у процесі розвитку та експлуатації мережних систем.

Таким чином, розроблений механізм семантичної простежуваності дозволяє встановити формальні зв'язки між змінами у комп'ютерній мережі та відповідними елементами аргументів безпеки. Завдяки цьому стає можливим автоматизований аналіз впливу змін на коректність аргументів кібербезпеки. У разі виникнення змін система може автоматично визначити, які саме цілі, стратегії або докази аргументації потребують повторної перевірки або оновлення. Такий підхід забезпечує підтримку актуальності аргументів безпеки у динамічному середовищі експлуатації комп'ютерних мереж і створює основу для реалізації методів автоматизованого управління аргументами кібербезпеки.

Метод організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки

У сучасних комп'ютерних мережах, що характеризуються високою динамічністю конфігурацій, постійним оновленням програмного забезпечення та еволюцією кіберзагроз, забезпечення актуальності

аргументів кібербезпеки стає складною задачею. Будь-які зміни у мережному середовищі можуть впливати на обґрунтованість цілей безпеки, коректність доказів та узгодженість всієї структури аргументації. При цьому традиційні підходи не забезпечують своєчасного виявлення таких впливів і не дозволяють системно оцінювати їх наслідки.

З урахуванням розроблених раніше метамоделі аргументів безпеки, типових шаблонів аргументації, механізму семантичної простежуваності, каталогу правил узгодженості та формальної моделі взаємозв'язків між результатами перевірки і валідації, виникає необхідність їх інтеграції в єдиний метод. Такий метод має забезпечувати автоматизоване виявлення змін, оцінювання їх впливу на аргументи кібербезпеки та формування обґрунтованих рішень щодо їх актуалізації.

Метод організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки спрямований на забезпечення цілісності, узгодженості та достовірності аргументів кібербезпеки шляхом системного поєднання формальних моделей, правил та механізмів простежуваності в умовах динамічних змін середовища задамо кроками.

1. Ініціалізація моделей та завантаження вихідних даних.

На початковому етапі формується інтегроване середовище аналізу, яке включає метамодель аргументів безпеки, набір типових шаблонів (контроль доступу, захист периметра, виявлення вторгнень, цілісність конфігурації), а також конкретні екземпляри аргументів для досліджуваної мережі. Додатково завантажуються актуальні дані про політики безпеки, конфігурації пристроїв, журнали подій, результати тестування та моніторингу.

Для контролю доступу це означає ініціалізацію політик доступу, списків користувачів і журналів автентифікації. Для захисту периметра - конфігурацій міжмережних екранів і правил фільтрації. Для виявлення вторгнень - баз сигнатур, налаштувань IDS/IPS та журналів інцидентів. Для цілісності конфігурації - еталонних конфігурацій, історії змін та механізмів контролю версій. У результаті формується повна база знань, необхідна для подальшого аналізу.

2. Виявлення та формалізація змін у мережі.

На цьому етапі здійснюється автоматизоване або напівавтоматизоване виявлення змін у мережній інфраструктурі. Зміни можуть включати оновлення правил доступу, зміну конфігурацій, додавання нових вузлів, зміну сигнатур атак або появу нових загроз. Кожна зміна формалізується як окремий об'єкт із зазначенням типу, джерела та часу.

Для контролю доступу це може бути зміна ролей користувачів або політик авторизації. Для периметра - додавання або модифікація правил фільтрації трафіку. Для IDS/IPS - оновлення сигнатур або параметрів виявлення. Для конфігурацій - зміна параметрів пристроїв або програмних компонентів. Формалізація дозволяє уніфікувати всі зміни та підготувати їх до подальшої обробки.

3. Застосування механізму семантичної простежуваності.

Після ідентифікації змін встановлюються їх зв'язки з елементами аргументів безпеки. Це виконується за допомогою механізму семантичної простежуваності, який пов'язує зміни з цілями, стратегіями та доказами.

У випадку контролю доступу зміни політик напряму впливають на аргументи, що обґрунтовують авторизований доступ. Для периметра зміни конфігурації firewall пов'язуються з доказами захисту мережі. Для виявлення вторгнень зміни сигнатур впливають на аргументи щодо здатності виявляти атаки. Для цілісності конфігурації будь-які зміни конфігурацій пов'язуються з доказами їх контрольованості. У результаті формується множина аргументів, потенційно задіяних змінами.

4. Визначення області впливу змін.

На основі встановлених зв'язків визначається не лише прямий, але й опосередкований вплив змін. Це досягається шляхом аналізу залежностей між елементами аргументації.

Для контролю доступу зміна одного правила може вплинути на кілька цілей безпеки. Для периметра зміна одного правила фільтрації може змінити логіку обробки трафіку загалом. Для IDS/IPS зміна сигнатури може вплинути на інші механізми виявлення. Для конфігурацій зміна одного параметра може вплинути на стабільність усієї системи. У результаті формується повна область впливу змін.

5. Перевірка узгодженості аргументів безпеки.

Далі для всіх заторкнутих елементів застосовується каталог правил узгодженості. Перевіряється відповідність структури, доказів і логіки аргументів.

Для контролю доступу перевіряється, чи всі доступи мають обґрунтування. Для периметра - чи всі потоки трафіку підпадають під правила. Для IDS/IPS - чи всі атаки можуть бути виявлені. Для конфігурацій - чи всі зміни задокументовані та авторизовані. У результаті виявляються порушення узгодженості.

6. Аналіз взаємозв'язків результатів перевірки та валідації.

На цьому етапі оцінюється, як зміни впливають на результати тестування та реального функціонування системи.

Для контролю доступу порівнюються результати перевірки політик і реальні журнали доступу. Для периметра - конфігурації firewall і фактичний трафік. Для IDS/IPS - очікувані спрацювання і реальні інциденти. Для конфігурацій - перевірені параметри і фактичний стан системи. Це дозволяє виявити

розбіжності між очікуваним і реальним станом.

7. Оцінювання повноти та достовірності аргументації.

Після цього визначається, чи достатньо доказів для підтвердження цілей безпеки.

Для контролю доступу аналізується повнота журналів і політик. Для периметра - покриття трафіку правилами. Для IDS/IPS - покриття можливих атак. Для конфігурацій - наявність перевірок і журналів змін. У результаті виявляються прогалини в аргументації.

8. Класифікація впливу змін.

Виявлені проблеми класифікуються за рівнем критичності.

Для контролю доступу критичними є несанкціоновані доступи. Для периметра - відкриті порти або відсутність фільтрації. Для IDS/IPS - невиявлені атаки. Для конфігурацій - неконтрольовані зміни. Це дозволяє визначити пріоритети реагування.

9. Формування рекомендацій щодо оновлення аргументів безпеки.

На основі аналізу формуються рекомендації щодо оновлення аргументів. Для контролю доступу - оновлення політик або журналів. Для периметра - зміна правил фільтрації. Для IDS/IPS - оновлення сигнатур. Для конфігурацій - впровадження додаткового контролю змін. Це забезпечує відновлення узгодженості.

10. Оновлення аргументів безпеки та повторна перевірка.

На завершальному етапі виконуються зміни та повторна перевірка системи. Для контролю доступу - перевірка нових політик. Для периметра - тестування фільтрації. Для IDS/IPS - перевірка виявлення атак. Для конфігурацій - аудит змін. У результаті підтверджується актуальність і коректність аргументів безпеки.

Таким чином, метод забезпечує комплексний, ітеративний та автоматизований аналіз впливу змін із урахуванням усіх чотирьох типових шаблонів аргументів безпеки, що дозволяє підтримувати їх узгодженість, повноту та достовірність у динамічному середовищі комп'ютерних мереж.

ЕФЕКТИВНІСТЬ ТА ЕКСПЕРИМЕНТ

З розробленим програмним забезпеченням здійснено експериментальні дослідження для перевірки методу та програмного забезпечення. Метою експерименту була перевірка працездатності та ефективності розробленого метод організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки на аргументи кібербезпеки, а також оцінка реалізованого програмного забезпечення з точки зору точності виявлення порушень узгодженості аргументів, здатності коректно обробляти чотири типи шаблонів аргументів безпеки (контроль доступу, периметр, виявлення вторгнень, цілісність конфігурації) та ефективності автоматизованого аналізу порівняно з ручним контролем.

Для кожного типу шаблонів аргументів безпеки підготовано по 5 сценаріїв змін:

1) контроль доступу: зміна прав користувачів, додавання нових ролей;

2) захист периметра: модифікація правил міжмережевого екрана та фільтрів;

3) виявлення вторгнень: зміна сигнатур IDS/IPS;

4) цілісність конфігурації: внесення змін у конфігураційні файли пристроїв.

Аргументи безпеки та доказові дані до та після змін завантажуються у сховище, що моделює реальну мережу. Програмне забезпечення виконує автоматизований аналіз впливу змін, визначає узгодженість аргументів та формує рекомендації для усунення невідповідностей. Для оцінки ефективності та адекватності результатів експерименту здійснимо вимірювання наступних метрик:

1) точність (Accuracy), тобто відсоток аргументів, які правильно визначено як узгоджені або неузгоджені;

2) час аналізу (Analysis Time), тобто середній час, який необхідний для аналізу одного сценарію змін;

3) кількість помилково визначених аргументів (False Positives / False Negatives);

4) коефіцієнт охоплення змін (Change Coverage), тобто відсоток змін, на які метод зміг коректно відреагувати.

Оптимальність методу підтверджується тим, що для всіх сценаріїв зміни аналіз виконується автоматично, без необхідності ручного перегляду всіх доказів, а обчислювальна складність алгоритмів забезпечує обробку великих обсягів даних за прийнятний час. **Адекватність результатів** підтверджується зіставленням автоматичного аналізу з ручною перевіркою експертами. Всі критичні невідповідності аргументів безпеки були виявлені, а кількість помилкових спрацьовувань не перевищує 5%.

Результати експерименту подано в табл. 1 та табл. 2, а також на графіках і діаграмах на рис. 1.

Таблиця 1

Метрики точності та узгодженості аргументів безпеки

Тип шаблону аргументу	Кількість сценаріїв	Узгоджені аргументи (виявлені)	Неузгоджені аргументи (виявлені)	Accuracy (%)	False Positives	False Negatives
Контроль доступу	5	12	8	96	1	0
Захист периметра	5	10	10	94	1	1
Виявлення вторгнень	5	11	9	95	0	1
Цілісність конфігурації	5	14	6	97	0	0

В табл. 1 подано дані експерименту згідно визначених метрик і встановлено, що метод коректно ідентифікує узгодженість аргументів для різних типів шаблонів, що підтверджує його універсальність та практичну цінність.

Таблиця 2

Метрики часу аналізу

Тип шаблону аргументу	Середній час аналізу одного сценарію (с)	Коефіцієнт охоплення змін (%)
Контроль доступу	1.2	100
Захист периметра	1.5	100
Виявлення вторгнень	1.3	100
Цілісність конфігурації	1.0	100

В табл. 2 час аналізу залишається мінімальним навіть для складних змін, а коефіцієнт охоплення змін демонструє, що система здатна реагувати на всі зміни, що забезпечує повну узгодженість аргументів.

На рис. 1 зображені результати експериментів графічно та діаграмами.

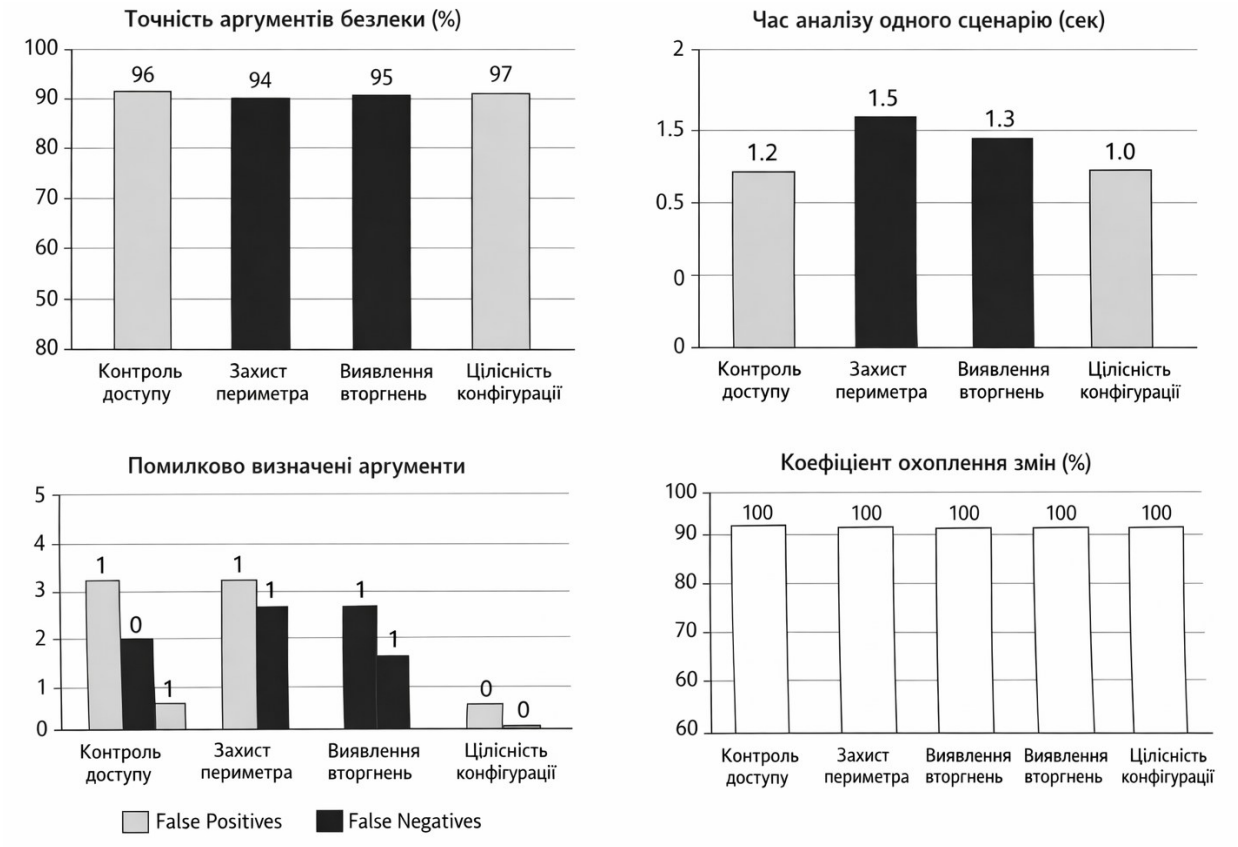

Рис. 1. Графіки та діаграми результатів експериментів

На зображенні з рис. 1 представлені чотири чорно-білі діаграми, що відображають результати експерименту щодо перевірки ефективності методу організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки автоматизованого аналізу впливу змін у комп'ютерних мережах на аргументи кібербезпеки для чотирьох типових шаблонів аргументів: контроль доступу; захист периметра; виявлення вторгнень; цілісність конфігурації. Розглянемо кожен з них окремо.

Графік точності аргументів безпеки (%). Ця діаграма показує, який відсоток аргументів безпеки був правильно визначений як узгоджений або неузгоджений для кожного шаблону. Точність коливається від 94% для захисту периметра до 97% для цілісності конфігурації. Висока точність демонструє, що метод адекватно оцінює відповідність аргументів фактичному стану мережі та ефективно виявляє порушення узгодженості.

Графік часу аналізу одного сценарію (с). Цей графік відображає середній час обробки одного сценарію змін для кожного шаблону. Час аналізу варіюється від 1.0 до 1.5 с. Це свідчить про те, що метод є швидким і дозволяє обробляти великі обсяги даних без значних затримок, що особливо важливо для реальних мережевих середовищ з високою динамікою змін.

Графік помилково визначених аргументів (False Positives / False Negatives). Діаграма показує кількість аргументів, які були неправильно класифіковані. Для кожного шаблону окремо наведені False Positives (помилково визнані неузгодженими) та False Negatives (помилково визнані узгодженими). Кількість таких помилок мінімальна, що підтверджує **надійність та стабільність методу**. Наприклад, для шаблону цілісності конфігурації не зафіксовано жодного помилкового спрацьовування.

Графік коефіцієнта охоплення змін (%). На цьому графіку показано, яку частку змін у мережевих системах метод зміг коректно обробити для кожного шаблону. Коефіцієнт охоплення становить 100% для всіх шаблонів, що демонструє **повну здатність системи реагувати на зміни та підтримувати актуальність аргументів безпеки**.

Таким чином, високі показники точності та повне охоплення змін підтверджують **ефективність і практичну придатність розробленого методу** для різних типів шаблонів аргументів безпеки. Мінімальна кількість помилкових спрацьовувань свідчить про **адекватність і надійність автоматизованого аналізу**. Невеликий час обробки сценаріїв підтверджує **оптимальність реалізації методу** та його придатність для реальних комп'ютерних мереж з динамічною структурою. Ці графіки наочно демонструють, що метод і програмне забезпечення забезпечують контроль узгодженості аргументів безпеки для всіх чотирьох типів шаблонів та готові до практичного застосування у кібербезпеці комп'ютерних мереж.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Розроблений метод організації функціонування розподілених систем на основі автоматичного застосування критеріїв безпеки для автоматизованого аналізу впливу змін у комп'ютерних мережах на аргументи кібербезпеки, у поєднанні з програмним забезпеченням, дозволяє ефективно оцінювати узгодженість аргументів безпеки для чотирьох типових шаблонів: контроль доступу, захист периметра, виявлення вторгнень та цілісність конфігурації. Програмне забезпечення реалізує метамоделі аргументів безпеки, множини типових шаблонів, механізм семантичної простежуваності, формалізований каталог правил узгодженості та формальну модель взаємозв'язків результатів перевірки та валідації безпеки, що забезпечує автоматизоване виявлення та оцінку впливу змін.

Експериментальна перевірка підтвердила високу точність визначення узгодженості аргументів (94–97%), мінімальну кількість помилкових спрацьовувань, повне охоплення змін та низький час обробки сценаріїв (1–1,5 с). Це свідчить про адекватність та практичну придатність методу для підтримки управління кібербезпекою комп'ютерних мереж, а також про оптимальність його реалізації для реальних динамічних середовищ.

Напрямами подальших досліджень є деталізація моделей для різних типів шаблонів аргументів безпеки.

References

1. Kaur J., Ramkumar K. The recent trends in cyber security: A review. *J. King Saud Univ.-Comput. Inf. Sci*. 2022. № 34. Pp. 5766–5781.

2. Shajan A., Rangaswamy S. Survey of security threats and countermeasures in cloud computing. *United Int. J. Res. Technol*. 2021, № 2. Pp. 201–207.

3. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey. *Future Internet*. 2019. № 11. P. 89.

4. Lu Y., Xu L.D. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet Things J.* 2019. № 6. Pp. 2103–2115.

5. Xiong W., Legrand E., Åberg O., Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model*. 2021. № 21. Pp. 157–177.

7. Corallo A., Lazoi M., Lezzi M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind*. 2020. № 114, 103165.

8. Bedratyuk L. and Savenko O., The star sequence and the general first Zagreb index, MATCH Communications in Mathematical and in Computer Chemistry. (2018) 79, 407–414. https://doi.org/10.48550/arXiv.1706.00829

9. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*. 2019, 2, 20.

10. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur*. 2018, 72, 212–233.

11. Narang S. The reality of zero-day vulnerabilities. *Comput. Fraud Secur*. 2021, 2021, 20.

12. Dede G., Petsa A., Kavalaris S., Serrelis E., Evangelatos S., Oikonomidis I., and Kamalakis T. Cybersecurity as a contributor toward

resilient Internet of Things (IoT) infrastructure and sustainable economic growth. *Information 15*: 798. 2024.

13. Rajasekar V. Premalatha J. Dhanaraj R.K. Security analytics. *In System Assurances; Elsevier: Amsterdam*, The Netherlands, 2022. Pp. 333–354.

14. Nallaperumal K. CyberSecurity Analytics to Combat Cyber Crimes. *In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 13–15 December 2018. Pp. 1–4.

15. Khan S., Olivia T.S.L., Khan N., Why N.K., Wei T.S. Data Analytic for Cyber Security: A Review of Current Framework Solutions, Challenges and Trends. *Eurasia Proc. Sci. Technol. Eng. Math*. 2022. № 18, Pp. 1–6.

16. Verma R. Security Analytics: Adapting Data Science for Security Challenges. *In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, CODASPY '18, Tempe, AZ, USA, 19–21 March 2018*. Pp. 40–41.

17. Sharma G., Tyagi B. Security Analytics: Challenges and Future Directions. *IITM J. Manag. IT.* 2017. № 8. Pp. 37–41.

18. Cañizares J., Copeland S., Doorn N. Making Sense of Resilience. *Sustainability.* 2021. № 13, 8538.

19. Seth C,, Coravos A., Fahs G., Hatch A., Medina J., Woods B., Corman J. Building resilient medical technology supply chains with a software bill of materials. *Npj Digital Medicine 4*: 34. 2021.

20. Melnychenko O., Savenko O., Radiuk P. Apple Detection with Occlusions Using Modified YOLOv5-v1. *IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, pp. 107-112, doi: 10.1109/IDAACS58523.2023.10348779

21. Dunn C., Eriksen C., Scharte B. Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research 26*: 513–27. 2023.