УДК 681.5
DOI https://doi.org/10.32782/2663-5941/2025.6.2/32

Михалюк А.П.
Національний університет харчових технологій

Міркевич Р.М.
Національний університет харчових технологій

АВТОМАТИЗОВАНА МЕТОДОЛОГІЯ МОНІТОРИНГУ ТА КОНТРОЛЮ ЗМІН У СЕРЕДОВИЩАХ КІБЕРФІЗИЧНИХ СИСТЕМ ТА РОБОТИЗОВАНИХ КОМПЛЕКСІВ

У статті пропонується комп'ютеризований підхід до покращення відтворюваності подій та керованості змінами в роботизованих системах та кіберфізичних системах. Він спрямований на вирішення проблем моніторингу фрагментації практики, відсутності стандартизованих профілів автоматизації та низької застосовності традиційних рішень для середовища автоматизації на основі моделей. Рішення інтегрує багатоетапний конвеєр обробки подій із вибірковим збором, нормалізацією JSON, кореляцією на основі правил та автоматизованими перевірками цілісності об'єктів конфігурації, доповненими захистом конфіденційності конфіденційних параметрів. Для забезпечення семантичного аналізу подій використовується онтологія MITRE ATT&CK, яка забезпечує зіставлення адміністративних сценаріїв із задокументованими тактиками та методами атаки. Технологічний прогрес полягає у формалізації консенсусної моделі даних та профілів автоматизації, які поєднують мінімально інвазивні методи контролю з постійним тестуванням (політика як код). Прагматична корисність підтверджується статистичною перевіркою: досягнуто покращеної вибірковості сигналів, скорочення середнього часу виявлення (MTTD) та реагування (MTTR), зниження ризику хибнопозитивних результатів та втрат подій. Отримані результати забезпечують масштабованість та відтворюваність підходу в змішаних середовищах (контейнеризація та розгортання сервісів) без впливу на доступність виробничих процесів. Запропонований метод підтримує портативність у розгортаннях гетерогенних систем (systemd/containers) через єдині точки збору; інваріантність до драйверів журналів відповідає за його відтворюваність у гетерогенних системах. Потенціал майбутніх досліджень: адаптивна автоматизація порогових значень (контекстно-залежна), використання «цифрового двійника» для безпечного автоматизованого тестування.

Ключові слова: *роботизовані системи, гетерогенні системи, системи автоматизації, кіберфізичні системи, моніторинг, інформаційна безпека.*

Постановка проблеми. Швидка цифровізація виробництва призвела до масового впровадження Node-RED як інструменту потокової оркестрації в роботизованих та кіберфізичних системах. Зі збільшенням кількості вузлів, сервісів та інтеграцій, а також зі збільшенням частоти змін конфігурації виникає системна проблема підтримки відтворюваної спостережуваності та керованості змін без порушення технологічних процесів. Традиційні ручні методи моніторингу та аудиту не є масштабованими та не можуть забезпечити потреби в ефективності, доказовості та точності. Тому автоматизація є основою проблеми: автоматичні засоби для збору, нормалізації, кореляції та інтерпретації подій, а також автоматичне забезпечення цілісності об'єктів конфігурації (файлового представлення та системних параметрів), які зможуть працювати майже в режимі реального часу.

Нові правила безпеки вимагають не лише ведення журналу адміністративних дій (редагування потоку, розгортання, зміна прав доступу), але й можливості для забезпечення автоматизованих процедур перевірки їхньої правильності, відстежуваності та відповідності нормативним вимогам [2]. У зв'язку з цим, рішення SIEM (керування інформацією та подіями безпеки) повинні забезпечувати: (i) автоматичне вилучення значущих подій з потоків журналів великого обсягу зі зменшенням фонових подій (покращене співвідношення сигнал/шум) [1], (ii) автоматичне

об'єднання та збагачення інформації [3], (iii) автоматичне застосування правил кореляції [8] та (iv) автоматичне оповіщення та створення бази доказів для подальшого дослідження [13].

Додаткову складність додає необхідність зіставлення подій в оперативній реальності з онтологічною моделлю класифікації відомих тактик і методів противника. Для цієї мети використовується MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), яка є довідковою основою для автоматизованого віднесення подій до сценаріїв загроз та побудови спільних політик реагування [23]. Інтеграція операційних журналів з такою моделлю передбачає автоматизовану нормалізацію, маркування та зворотне відстеження змін у конфігураціях об'єктів конфігурації.

Практичність наукової теми випливає з формалізації та валідації ефективності методик, які:

– впровадити автоматизовану та толерантну до несправностей агрегацію подій у розподілених роботизованих комплексах та кіберфізичних системах [3];

– забезпечити автоматизоване керування об'єктами конфігурації Node-RED (потоки, облікові дані, параметри виконання) з можливістю відтворення причинно-наслідкових зв'язків [9];

– використовувати автоматизовану кореляцію подій на основі комбінованих правил та онтологічних моделей з метою посилення значущості сигналу [16];

– використання автоматизованих процедур конфігурації та перевірки правил без впливу на цілісність виробничих процесів [21].

З прагматичної точки зору, плоди таких досліджень потрібні для:

1. скорочення часу виявлення та вирішення інцидентів шляхом комплексної автоматизації операцій моніторингу та аналізу [19];

2. покращення доказовості та аудитності даних шляхом застосування автоматизованих механізмів відстеження змін [9].

3. забезпечення відповідності вимогам промислової кібербезпеки та якості операційної підтримки без шкоди для доступності критично важливих послуг [23].

Таким чином, проєкт характеризується як науково-практичний, що полягає у створенні автоматизованого методу відстеження та управління змінами в інфраструктурах Node-RED у робототехнічних комплексах та кіберфізичних системах з використанням інструментів та моделей класу SIEM, таких як MITRE ATT&CK (Массачусетський інститут технологічних досліджень та інженерії змагальних тактик, методів та загальних знань) [1, 3, 6], що гарантуватиме масштабованість, відтворюваність та керовану якість даних для прийняття майбутніх рішень.

Аналіз останніх досліджень і публікацій. Рецензовані журнали та огляди з промислової системної інженерії програмного забезпечення та кібербезпеки визнають зростаючу важливість автоматизації для забезпечення спостережуваності та управління змінами в середовищах оркестрації, наприклад, Node-RED у кіберфізичних системах та робототехніці [15]. Основна увага приділяється переходу від ручних процесів аудиту до автоматизованих конвеєрів збору, нормалізації, кореляції та інтерпретації подій, а також контролю цілісності конфігураційних об'єктів за допомогою автоматизації. Незважаючи на значний прогрес, огляд літератури виявляє різні відкриті питання, які перешкоджають масштабованому впровадженню автоматизованих підходів у виробничих сценаріях з високими вимогами до безперервності [10].

Системи SIEM (системи управління інформацією та подіями безпеки) традиційно позиціонуються як ядро автоматизованої кореляції та збору подій у розподілених системах [14]. Попередні дослідження демонструють розширений синтаксичний аналіз журналів ОС, підсистем додатків та мережевих датчиків, а також автоматичне застосування правил кореляції та сповіщень [8]. Тим часом більшість рішень стосуються подій системного рівня та не враховують семантику модельно-орієнтованого середовища автоматизації (наприклад, Node-RED): їх дії адміністрування, моделі оперативного розгортання та функції представлення конфігурації [20]. Це призводить до недостатньої автоматизованої вибірковості (недостатньо високого співвідношення сигнал/шум) та ручного збагачення подій змістовною інформацією [13].

Деякі проблеми ще не вирішені: відсутність стандартизованих автоматизованих шаблонів для вибору подій, нормалізації та семантичного збагачення в рамках Node-RED у промислових середовищах. Це пов'язано з орієнтацією на універсальність інструменту SIEM та недостатньою формалізацією моделі області подій для модельно-орієнтованих ланцюгів обробки даних [8].

Процедури безпеки Node-RED описують, як реєструються події адміністрування (редагування/запуск процесів, зміни палітри, доступ до API адміністратора) [4]. Однак більшість описів говорять про «можливість» ведення журналу, а не про

Таблиця 1

Порівняння основних напрямків роботи

Напрямок дослідження	Мета автоматизації	Ключові механізми автоматизації	Невирішені проблеми
SIEM у промисловому середовищі	Побудова автоматизованого конвеєра: збір → нормалізація → кореляція → сповіщення з покращеним співвідношенням сигнал/фон	Автоматизований розбір/уніфікація журналів, правила кореляції, збагачення контексту, тригери сповіщень	Недостатня семантика домену для Node-RED; немає типових автоматизованих профілів для середовища автоматизації на основі моделей
Аудит та журнали Node-RED	Автоматизоване вилучення та об'єднання адміністративних подій із гарантованою ідентифікацією джерела	Фільтрація за _SYSTEMD_ UNIT, автоматизована нормалізація JSON, узгоджена схема полів	Фрагментація практик (systemd/контейнери); відсутність відтворюваного автоматизованого збору профілів/генерації схем
FIM для сутностей конфігурації Node-RED	Автоматизований контроль цілісності конфігураційних сутностей з диференційованим відстеженням змін та захистом захищених змінних	report_changes, whodata, політика приховування (nodiff), механізми активації на основі подій	Змінність у зберіганні захищених змінних та шляхів; потрібен єдиний автоматизований профіль FIM для прямого розгортання обладнання та контейнерів
Семантична відповідність на MITER ATT&CK / ATT&CK для ICS	Автоматизація призначення подій онтології класифікації загроз	Правила кореляції, онтологічні відповідності	Відсутність публічних наборів даних Node-RED; необхідні автоматизовані правила перевірки якості
Безперервна перевірка (політика як код)	Автоматизована перевірка правил/декодерів без впливу на доступність (CI/CD для політик)	Офлайн-тести журналів, тестові вектори, регресійний контроль, метрики стабільності роботи	Розрив між SRE/DevOps та безпекою; відсутність стандартних профілів автоматизації процесу валідації
Операційні моделі (systemd проти контейнеризації)	Автоматизоване узгодження джерел подій та контурів керування в змішаних середовищах	Уніфіковані ланцюжки збору даних для сервісів та контейнерів, політики монтування /даних	Різнорідність форматів водіїв/журналів; необхідні стандартизовані шаблони автоматизованої інтеграції

автоматизовані процеси пересилання цих подій до SIEM із забезпеченою ідентифікацією джерела (сервісний блок), узгодженими ідентифікаторами вузлів та автоматичною нормалізацією JSON [7].

Відкритим питанням залишається уніфікований, відтворюваний та автоматизований процес обробки даних від журналів journald/service до уніфікованих подій SIEM з єдиною схемою полів. Це пов'язано з фрагментацією практик (пряме розгортання обладнання, systemd-сервіси, контейнеризація), різними рівнями формалізації подій та відсутністю єдиних профілів автоматизації для різних підходів до розгортання [6].

Використання з моніторингом цілісності файлів (FIM) демонструє перевірені методи виявлення модифікацій конфігураційних сутностей (потокових файлів, облікових даних, параметрів запуску). Перевагою таких програм є автоматичне створення розумних відмінностей (diff), призначення політик «хто/коли/що» та приховування для прихованих змінних. Але є деякі особливості Node-RED: розділення потокових даних та прихованих змінних на окремі файли, використання змінних середовища, контейнери з доступом до каталогу /data як до змонтованого тому. [9]

Проблема спільного автоматизованого профілю FIM для Node-RED, який забезпечує диференційоване відображення змін та безпеку захищених змінних у різних середовищах розгортання (systemd та контейнеризація), залишається невирішеною. Це пов'язано з відмінностями у представленні файлів, відмінностями в практиках зберігання захищених змінних та гібридним розгортанням, де важко класифікувати автоматизацію.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge – публічна база знань про тактики та методи зловмисників, розроблена Массачусетським технологічним інститутом) використовується переважно для опису поведінкових атрибутів. У літературі описано, як зіставити мережеву та системну активність з тактиками/методами, але майже немає

публікацій про те, як автоматизувати зіставлення подій адміністратора Node-RED з онтологією класифікації ATT&CK (включно з ATT&CK для ICS) з урахуванням змін конфігураційних сутностей та ліній промислового впровадження. [16, 23]

Проблема створення автоматизованого, заснованого на правилах або керованого даними процесу класифікації подій Node-RED з обов'язковим контролем якості (точність/повторність) та постійною перевіркою результатів залишається відкритою. Причиною є відсутність публічних наборів даних про події Node-RED для перевірки/навчання та відсутність чіткості щодо стандартизації семантики подій цієї платформи. [21, 22]

У кількох статтях обговорюється проблема тестування SIEM-декодерів та правил на штучні події, але автоматизовані методи тестування обговорюються епізодично. Узгодження скорочення часу простою з вимогою періодичного автоматизованого контролю коректності конфігурацій не враховується.

Рішення змішаної автоматизації безперервної валідації (політика як код) з вимірюваними сигналами якості та впливу на доступність є відкритою проблемою через невідповідність між практиками та засобами контролю безпеки SRE (Site Reliability Engineering) та DevOps (Development and Operations), а також відсутність еталонних профілів автоматизації для середовищ автоматизації, керованих моделями [19].

Поєднання виявлених прогалин свідчить про необхідність автоматизованого, малоінвазивного та відтворюваного рішення, яке:

1. створює наскрізний конвеєр подій Node-RED від журналів обслуговування до SIEM з автоматичною нормалізацією та підвищеною вибірковістю (покращене співвідношення сигнал/шум) [1, 3];

2. автоматизує профілювання FIM для сценаріїв systemd та контейнеризації (з диференційованим відображенням змін та захистом захищених змінних) [6, 9];

3. забезпечує автоматичну кореляцію даних з онтологією класифікації MITRE ATT&CK/ATT&CK для ICS [16, 23];

4. забезпечує автоматичну безперервну перевірку правила та декодера без шкоди для доступності виробничого сервісу [8, 21].

Постановка завдання. Метою дослідження є теоретичне обґрунтування та формалізація автоматизованого методу спостереження та управління змінами для середовищ Node-RED у рамках робототехнічних комплексів та кіберфізичних систем за допомогою інструментів SIEM (Security Information and Event Management). Підхід включає автоматизацію процесу «збір → нормалізація → кореляція → інтерпретація» інцидентів, автоматизований контроль цілісності об'єктів конфігурації (FIM) та автоматизовану кореляцію інцидентів з онтологією класифікації загроз MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Наукова інновація полягає у побудові узгодженої моделі даних та правил, яка забезпечить відтворюваність, масштабованість та покращене співвідношення сигнал/фон у виробничому середовищі без порушення технологічних процесів. Це дозволить впроваджувати в реальних умовах автоматизовані та неінвазивні практики моніторингу, аудиту та контролю цілісності в змішаних розгортаннях (systemd/контейнери), зменшити MTTD та MTTR, збагатити базу доказів для аналізу інцидентів, забезпечити дотримання нормативних положень та забезпечити стабільну роботу без додаткових простоїв.

Виклад основного матеріалу. Архітектурна модель автоматизованого спостереження. Запропоновано багаторівневий цикл управління подіями (рис. 1), де базові журнали виконання Node-RED автономно реплікуються через захищений сегмент мережі до ядра SIEM; процеси автоматизованої нормалізації, кореляції, семантичного зіставлення з онтологічною моделлю загроз та генерації інцидентів відбуваються на рівні SIEM. Багаторівневе розподілення є логічним та узгоджується з галузевими практиками (рівні L0–L4), що зменшує перешкоди у виробництві та відтворюваність дій під час експлуатації. Архітектура усуває фрагментацію практики та забезпечує єдиний автоматизований профіль обробки подій для різних стратегій розгортання (systemd/containers).

Для інсталяцій Node-RED як сервісу systemd використовується автоматичний збір подій безпосередньо з journald з фільтрацією за _SYSTEMD_UNIT=nodered.service [1]. Такий вибір значно зменшує обсяг фонових записів і пересилає лише важливі події з середовища Node-RED до SIEM, покращуючи вибірковість і стабільність джерела без ручного «відсіювання» шумових подій. Результатом є покращене співвідношення сигнал/фон і зменшена затримка доставки подій, що є вимогою для подальшої автоматизації кореляції. Події аудиту Node-RED генеруються у форматі JSON; їх розбір досягається вбудованим декодером Wazuh JSON з початковим видаленням префіксів сервісу (наприклад, [audit]) за допомогою попереднього зіставлення. В результаті всі важливі поля подій

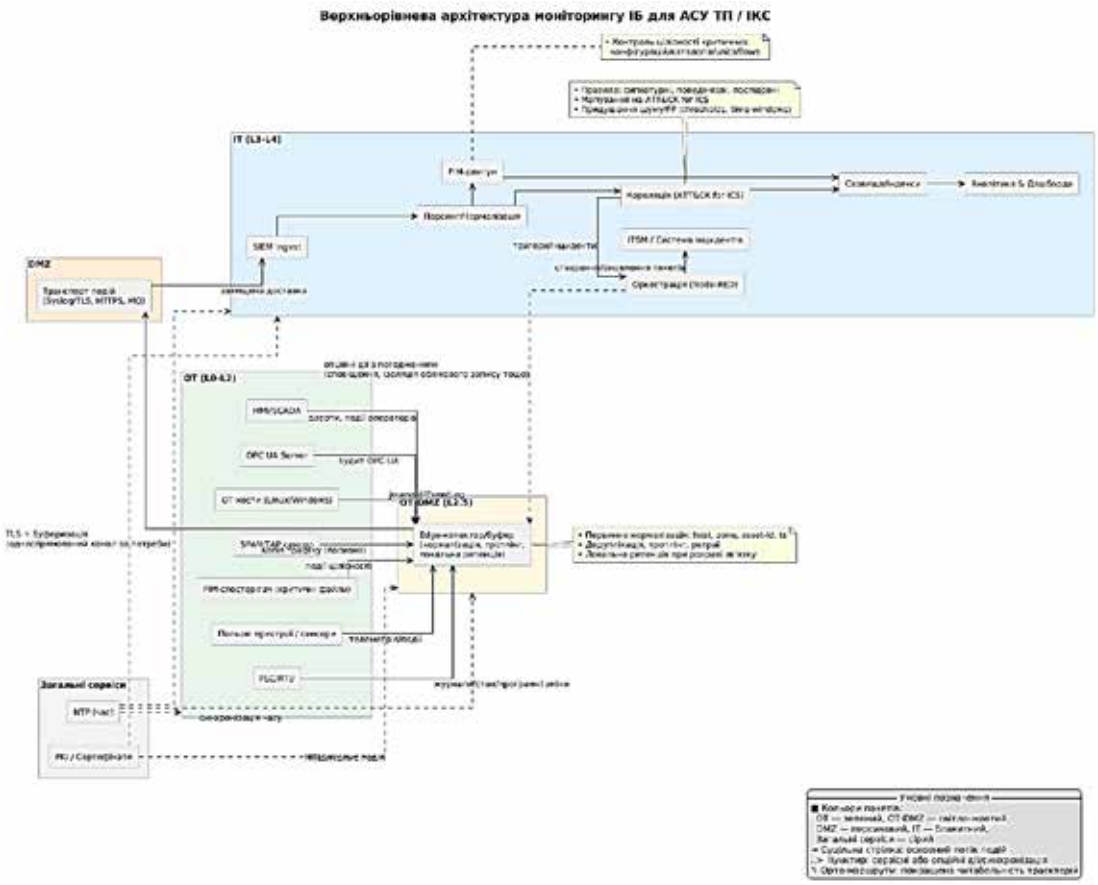

Рис. 1. Багатошарова схема керування подіями

однаково представлені механізмам кореляції в уніфікованому вигляді, що усуває відсутність спільної схеми полів і мінімізує ручні перетворення, що відкриває шлях для автоматичного семантичного аналізу [4, 7]. Локальні правила розроблені для ідентифікації подій розгортання потоку (flows.set), модифікації палітри (nodes.install/remove) та аномалій частоти (кілька розгортань з однієї IP-адреси протягом обмеженого періоду часу). Це дозволяє автоматично виявляти цікаві адміністративні сценарії без необхідності втручання оператора, що перетворює ручний аудит на автоматичний режим з керованими умовами запуску, роблячи сигнали більш релевантними, а їхню доказовість – кращою. Визначено набір цільових сутностей конфігурації для відтворюваності систем: топологія потоку (flows*.json) – відмінності вмісту (diff), захищені змінні (flows_cred.json) – заборона на розкриття (через nodiff), політика безпеки та ведення журналу (settings.js) та каталоги проектів, якщо в режимі Проекти (Git). Realtime, report_changes та whodata увімкнено для атрибуції змін за принципом «хто/ким/коли» для всіх цільових груп.

Для запобігання регресіям було використано wazuh-logtest, який дозволяє автоматично тестувати декодери та правила на зразках подій (CLI/dashboard/API) без перезапуску продуктивних сервісів, що формує безперервний цикл автоматизованої валідації, зменшуючи час ручних перевірок та ризик «тихого» блокування процесів.

Отримані наукові результати та описи наслідків

1. Покращена вибірковість сигналу. Застосування фільтрації _SYSTEMD_UNIT разом із нормалізацією JSON суворо видаляє неінформативні записи, що обґрунтовує покращення співвідношення сигнал/фон.

2. Повторюваність адміністративних сценаріїв. Локальні політики для flows.set та nodes.install/remove забезпечують структуровану інтерпретацію подій та ізоляцію тестового розгортання, що обґрунтовує підвищення точності виявлення змін стану системи.

3. Відстеження конфігураційних сутностей. report_changes/whodata/nodiff використовується для відстеження змін контенту та атрибуції змін без розкриття захищених змінних – опис впливу: розділення режимів представлення для публічних/захищених структур.

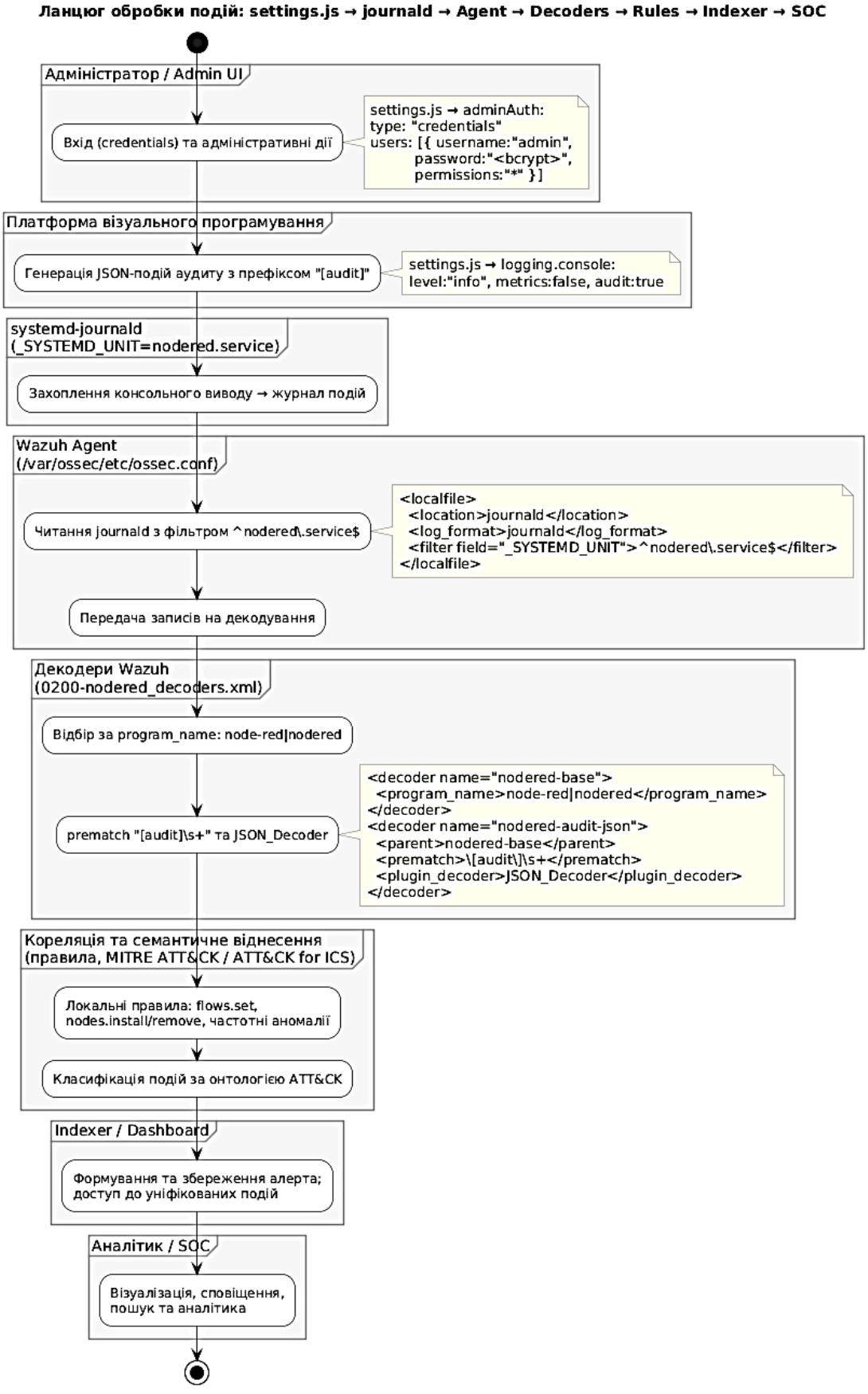

Рис. 2. Ланцюг обробки подій

Таблиця 2

Цільовий набір конфігурацій та потоків

Джерело події (OT/IT)	Приклад декодера/ нормалізатора	Правило/ кореляція (приклад)	Тактика → техніка (ATK&CK для ICS)	Дія оркестрування (приклад)
Linux journald (OT-хост)	Системний журнал/ журнал → поля: хост, пристрій, ідентифікатор користувача, зона	sudo без дозволу + зміна конфігурації служби протягом 5 хвилин	Ескалація привілеїв → T0811 (Зміна програми); Початковий доступ/ виконання, залежно від контексту	Автозавдання в ITSM, сповіщення SOC/OT, тимчасове вимкнення доступу користувачів
Журнал подій Windows (HMI/ інженерна станція)	WinEvent → поля: EventID, LogonType, користувач, хост	Аномальний тип входу в систему вночі + підозрілий запуск/ зупинка служби	Латеральний рух → T0866 (Дистанційні послуги); Початковий доступ → T0822	Створення інциденту, блокування сеансу через AD, повідомлення чергового
Сервер OPC UA (аудит)	Аудит OPC UA → дія, ідентифікатор вузла, користувач, статус	Зміна вузла конфігурації без оголошеного вікна обслуговування	Погіршити керування процесом → T0831; Пригнітити функцію реагування → T0814	Кнопка зупинки з м'якою дією: повідомити технолога, заморозити розгортання, вимагати схвалення
HMI/SCADA (сповіщення/ журнали)	Журнали → об'єднання: тег, тривога, підтвердження, оператор	Послідовність: відхилення параметра → вимкнення сигналізації → зміна заданого значення	Функція блокування відповіді → T0814; Зміна логіки керування → T0839	Збільшити пріоритет інциденту, вимагати другий підпис, зворотний запис у журналі
PLC/RTU (програмні події)	Журнали з програмної інженерії / Версіонування	Виявлено завантаження нової логіки без супровідного ідентифікатора зміни	Виконання → T0853 (Програмована логіка); Збереження → T0857	Створити запит на зміни, заблокувати подальші зміни до огляду, повідомити відповідальну особу
Промисловий шлюз/ маршрутизатор	Syslog/Netconf → нормалізація: ifName, src/dst, правило	Зміна ACL у міжзонному каналі + сплеск трафіку	Ухилення від захисту → T0809; Ексфільтрація → T0842	Автоматична генерація квитків, тимчасове відкатування попереднього ACL, сповіщення про мережеві команди
Мережевий трафік (SPAN/TAP)	DPI/метадані (IPFIX/ NetFlow)	Новий головний пристрій Modbus/TCP, що переглядає дані з нестандартного хоста	Діскавері → T0846; Бічний рух → T0865	Тригер NDR, сповіщення, розслідування з витягом PCAP
IDS/NDR (сегмент OT)	JSON сповіщення → поля: sig_id, dst, proto	Повторний підпис на міжзонному каналі + неочікуваної відповіді	Збір/ Командування та контроль (залежно від підпису)	Автоматичне визначення пріоритетів сповіщень, об'єднання подій SIEM, ескалація L2
FIM (вузли OT/IT)	Хеш/шлях/ процес → нормалізація: файл, хеш, актор	Зміна ключового блоку/ сценарію в сегменті OT поза робочим вікном	Вплив → T0805 (Маніпуляція контролем); Наполегливість	Блокування розгортання, заявка на аналіз розбіжностей, повідомлення чергового
Дії адміністратора (RBAC/ конфігурація)	Аудит подій SIEM/ системного адміністру-вання	Серія: створити обліковий запис → надати права → вимкнути журнал	Підвищення привілеїв → T0890; Ухилення від захисту → T0829	Негайне скасування прав, повідомлення CISO/ чергового офіцера, вимога щодо обґрунтування постфактум

4. Операційна гнучкість. Узгодження FIM з контейнером/даними позбавляє залежності від конкретного драйвера та формату журналу, сприяючи надійному автоматизованому моніторингу в гетерогенних інфраструктурах.

5. Зниження операційних ризиків. wazuh-logtest дозволяє проводити автоматизоване приймальне тестування без переривання обслуговування, зменшуючи MTTR завдяки швидкому виявленню помилок політики.

Обмеження дослідження (для практичного застосування та розширення)

• Залежність від якості джерела. Якщо journald або драйвер журналу контейнера використовує сувору ротацію, події можуть бути втрачені до часу збору.

• Версії та конфігурації Node-RED різноманітні. Зміни параметрів format/settings.js у файлі Event format вимагають автоматичних декодерів та оновлення правил.

• Секрети та конфіденційні дані. Nodiff зменшує витоки, але включає обачні винятки/маскування в похідних потоках (наприклад, під час експорту інцидентів).

• Синхронізація часу. Для забезпечення належної кореляції в розподілених конфігураціях необхідно підтримувати узгоджені часові бази (NTP).

• Обмежена доступність відкритих наборів даних. Недоступність отримання зразків подій Node-RED публічно обмежує кількісну перевірку автоматизованої кореляції MITRE ATT&CK.

Визначено недоліки та напрямки для покращення

• Одноразові витрати на параметризацію. Одноразове налаштування профілів (фільтри, схема полів, винятки FIM) вимагає спеціалізованих знань; у майбутньому – бібліотека спільних автоматизованих профілів Node-RED.

• Чутливість до організаційного контексту. Місцеве законодавство може призвести до хибнопозитивних результатів у періоди пікового випуску; необхідно застосовувати автоматичну адаптацію порогових значень (контекстні календарі/вікна змін).

• Онтологічне відображення. Відсутність стандартизованих контрольних показників для Node-RED ускладнює повну автоматизацію атрибуції подій до правил ATT&CK; розширення правил та накопичення правил перевірки знаходяться в розробці.

Емерджентний фреймворк забезпечує комплексну автоматизацію від вибіркового збору до об'єднаної нормалізації, кореляції на основі правил, та контрольованого FIM у гібридних розгортаннях з безперервною автоматичною валідацією. Запропоновані механізми усувають прогалини, встановлені в статті, водночас встановлюючи чіткі межі застосовності, а також можливі вдосконалення.

Висновки. Створено відтворюваний машинний ланцюг обробки подій Node-RED → SIEM (збір, JSON-нормалізація, кореляція, інтерпретація), який, на відміну від універсальних методів, враховує семантику модельно-керованого контексту автоматизації; ефект високої вибірковості сигналу протидіє фільтрації джерела (_SYSTEMD_UNIT) та однорідній схемі полів.

Розроблено рекомендації щодо автоматичних сповіщень про адміністративні умови (розгортання, зміна палітри, частота неочікуваних дій), які відрізняються від існуючих системних сповіщень тим, що вони враховують активність редактора; ручне скорочення аудиту виправдано формалізацією подій та параметризацією порогових значень. Побудовано профіль з підтримкою whodata для автоматизованого контролю цілісності об'єктів конфігурації (потоків/налаштувань/проектів та спеціального режиму для захищених змінних через nodiff), який відрізняється відповідністю традиціям Node-RED; відповідність «хто/що/коли» без порушення захищених змінних забезпечується диференційованим представленням змін. Детально описано автоматичне зіставлення подій з онтологією класифікації MITRE ATT&CK/ATT&CK для ICS порівняно з кореляцією на системному рівні щодо адміністративних дій; семантична уніфікація стосується покращення якості подальшої аналітики. Додано автоматизований цикл перевірки політик для прийняття (політика як код з офлайн-тестами журналів), що переводить політику безпеки в сферу практик SRE/DevOps; стабільність сигналу та мінімізований операційний ризик забезпечуються періодичним тестуванням без втрати сервісу.

Метод підтримує портативність у розгортаннях гетерогенних систем (systemd/containers) через єдині точки збору та FIM поверх змонтованого /data; інваріантність до драйверів журналів відповідає за його відтворюваність у гетерогенних системах.

Потенціал майбутніх досліджень: адаптивна автоматизація порогових значень (контекстнозалежна), використання «цифрового двійника» для безпечного автоматизованого тестування.

Список літератури:

1. Wazuh Documentation. Log data collection: Journald. URL: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/journald.html (дата звернення: 22.09.2025).

2. Node-RED. Securing Node-RED. URL: https://nodered.org/docs/user-guide/runtime/securing-node-red (дата звернення: 21.09.2025).

3. Wazuh Documentation. How log data collection works. URL: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/how-it-works.html (дата звернення: 20.09.2025).

4. Node-RED. Settings file. URL: https://nodered.org/docs/user-guide/runtime/settings-file (дата звернення: 19.09.2025).

5. Wazuh Documentation. Decoders Syntax. URL: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/decoders.html (дата звернення: 22.09.2025).

6. Node-RED. Getting started with Docker. URL: https://nodered.org/docs/getting-started/docker (дата звернення: 18.09.2025).
7. Wazuh Documentation. JSON Decoder. URL: https://documentation.wazuh.com/current/user-manual/ruleset/decoders/json-decoder.html (дата звернення: 22.09.2025).
8. Wazuh Documentation. Ruleset XML Syntax. URL: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html (дата звернення: 20.09.2025).
9. Wazuh Documentation. File Integrity Monitoring: Basic Settings. URL: https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/basic-settings.html (дата звернення: 22.09.2025).
10. Guan L., Tao K., Chen P. Research on Endogenous Security Defense for Cloud-Edge Collaborative Industrial Control Systems Based on Luenberger Observer. Mathematics. 2025. 13, 2703. DOI: https://doi.org/10.3390/math13172703.
11. Zhang L., Wang Y., Chang K., Shen H. Assessing Cross-Domain Threats in Cloud–Edge-Integrated Industrial Control Systems. Electronics. 2025. 14, 3242. DOI: https://doi.org/10.3390/electronics14163242.
12. Badawi M., Sherriff N.H., Abdel-Hamid A.A. Legacy ICS Cybersecurity Assessment Using Hybrid Threat Modeling – An Oil and Gas Sector Case Study. Applied Sciences. 2024. 14, 8398. DOI: https://doi.org/10.3390/app14188398.
13. Shiraz M., Durad M.H., Paracha M.A., Mohsin S.M., Kazmi S.N., Maple C. Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection. Sensors. 2024. 24, 4901. DOI: https://doi.org/10.3390/s24154901.
14. Manzur J., Walid A., Jamali A.F., Masud A. Cybersecurity on a budget: evaluating security and performance of open-source SIEM solutions for SMEs. PLoS ONE. 2024. 19(3): e0301183. DOI: https://doi.org/10.1371/journal.pone.0301183.
15. Nankya M., Chateau R., Akl R. Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. Sensors. 2023. 23, 8840. DOI: https://doi.org/10.3390/s23218840.
16. Afenu D.S., Asiri M., Saxena N. Industrial Control Systems Security Validation Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework. Electronics. 2024. 13(5), 917. DOI: https://doi.org/10.3390/electronics13050917.
17. Mantere M., Sailio M., Noponen S. Network Traffic Features for Anomaly Detection in Specific Industrial Control System Network. Future Internet. 2013. 5(4), 460–473. DOI: https://doi.org/10.3390/fi5040460.
18. Петрашко В., Улічев О. Дослідження існуючих підходів до створення безпечної мережі. Молодий вчений. 2023. № 12(124). С. 6–11. DOI: https://doi.org/10.32839/2304-5809/2023-12-124-3.
19. Ban T., Takahashi T., Ndichu S., Inoue D. Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response. Applied Sciences. 2023. 13(11), 6610. DOI: https://doi.org/10.3390/app13116610.
20. Omidi S.A., Baig M.J.A., Iqbal M.T. Design and Implementation of Node-Red Based Open-Source SCADA Architecture for a Hybrid Power System. Energies. 2023. 16(5), 2092. DOI: https://doi.org/10.3390/en16052092.
21. Ismail K., Widiyatama F., Wibawa I.M., Brata Z.A., Ukasha N., Nelistiani G.A., Kim H. Enhancing Security Operations Center: Wazuh Security Event Response with Retrieval-Augmented-Generation-Driven Copilot. Sensors. 2025. 25(3), 870. DOI: https://doi.org/10.3390/s25030870.
22. Chamkar S.A., Zaidi M., Maleh Y., Gherabi N. Improving Threat Detection in Wazuh Using Machine Learning Techniques. Journal of Cybersecurity and Privacy. 2025. 5(2), 34. DOI: https://doi.org/10.3390/jcp5020034.
23. Sindric I., Jurcevic M., Hadžina T. Mapping of Industrial IoT to IEC 62443 Standards. Sensors. 2025. 25(3), 728. DOI: https://doi.org/10.3390/s25030728.

Mykhalyuk A.P., Mirkevich R.M. AUTOMATED METHODOLOGY FOR MONITORING AND CONTROLLING CHANGES IN THE ENVIRONMENT OF CYBER-PHYSICAL SYSTEMS AND AUTOMATED COMPLEXES

This paper proposes a computer-based approach to improving event reproducibility and change management in robotic and cyber-physical systems. It addresses the challenges of monitoring practice fragmentation, lack of standardized automation profiles, and low applicability of traditional solutions to model-based automation environments. The solution integrates a multi-stage event processing pipeline with selective collection, JSON normalization, rule-based correlation, and automated integrity checks of configuration objects, complemented by privacy protection of sensitive parameters. The MITRE ATT&CK ontology is used to provide semantic analysis of events, which maps administrative scenarios to documented attack tactics and methods. The technological advancement lies in the formalization of a consensus data model and automation profiles that combine minimally invasive control methods with continuous testing (policy as code). The pragmatic utility is confirmed by statistical verification: improved signal selectivity, reduced mean time to detection (MTTD) and response (MTTR), reduced risk of false positives and event losses are achieved. The obtained results ensure scalability and reproducibility of the approach in mixed environments (containerization and service deployment) without affecting the availability of production processes. The proposed method supports portability in heterogeneous system deployments (systemd/containers) through single collection points; invariance to log drivers is responsible for its reproducibility in heterogeneous systems. Potential for future research: adaptive automation of thresholds (context-sensitive), use of a "digital twin" for secure automated testing.

Key words: *robotic systems, heterogeneous systems, automation systems, cyber-physical systems, monitoring, information security.*

Дата надходження статті: 22.10.2025
Дата прийняття статті: 13.11.2025
Опубліковано: 30.12.2025