МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ЖИГАРЕВИЧ Оксана Костянтинівна

УДК 004.056:004.057.3 (043.3)

СИСТЕМА КОРЕЛЮВАННЯ ПОДІЙ ТА УПРАВЛІННЯ ІТ-ІНЦИДЕНТАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.06 – «Інформаційні технології»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2026

Дисертацією є рукопис.

Робота виконана на кафедрі комп'ютерних інформаційних технологій Державного університету «Київський авіаційний інститут» Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент
Сидоренко Вікторія Миколаївна,
Державний університет «Київський авіаційний інститут», доцент кафедри комп'ютерних інформаційних технологій.

Офіційні опоненти: доктор технічних наук, професор
Цюцюра Микола Ігорович,
Державний торговельно-економічний університет, професор кафедри інженерії програмного забезпечення та кібербезпеки;

кандидат технічних наук, доцент
Складанний Павло Миколайович,
Київський столичний університет
імені Бориса Грінченка,
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.

Захист відбудеться «28» травня 2026 р. о 15^{00} на засіданні спеціалізованої вченої ради Д 26.062.01 при Державному університеті «Київський авіаційний інститут» за адресою: 03058, м. Київ, пр. Любомира Гузара, 1, корпус 1, ауд. 1.127.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Державного університету «Київський авіаційний інститут» за адресою: 03058, м. Київ, пр. Любомира Гузара, 1.

Автореферат розісланий «28» квітня 2026 р.

Вчений секретар
спеціалізованої вченої ради
к.т.н., доц. Анна ІЛЬЄНКО

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Сучасна інформаційна інфраструктура складається з великої кількості систем та компонентів, що потребують постійного моніторингу та контролю. В таких умовах провідними державами світу приділяється значна увага питанням забезпечення безпеки та сталого функціонування життєво важливих об’єктів, до яких належать великі гідротехнічні споруди, мережі електростанцій, шкідливі хімічні виробництва, транспортні вузли, аеродроми тощо. Виведення таких об'єктів інфраструктури з ладу може призвести до швидких негативних, а іноді і катастрофічних наслідків відповідної інформаційно-комунікаційної системи (ІКС). Для забезпечення необхідного рівня протидії загрозам в автоматизованих системах та ІКС, а також для зниження ризику виникнення аналогічних інцидентів у майбутньому в Україні функціонує Урядова команда реагування на комп’ютерні надзвичайні події (CERT або CSIRT). Особливої уваги потребує процес управління та прийняття рішень щодо виявлення та усунення можливих загроз об’єктам критичної інфраструктури (ОКІ). Серед існуючої множини інструментів для ефективного реагування на інциденти CSIRT на ОКІ є використання SIEM-систем, функціонування яких полягає в оперативному збиранні, збереженні та аналітичній обробці даних про події безпеки, що першочергово формуються та фіксуються в системних журналах різних апаратних і програмних елементів, а також формують інформаційні інфраструктури: сервери, робочі станції, маршрутизатори, мережеві екрани, системи управління базами даних, системи виявлення атак, антивірусні засоби тощо. Основною метою таких систем є підвищення рівня цифрової стійкості інформаційно-комунікаційних систем за рахунок забезпечення можливості в режимі, близькому до реального часу, обробляти інформацію про безпеку та здійснювати корелювання подій і управління інформаційно-технологічними (ІТ) інцидентами. У межах даного дослідження ІТ-інцидент розглядається як подія або набір подій в ІКС, що відображають відхилення від її нормального функціонування, зумовлені порушенням роботи сервісів, ресурсів чи ІТ процесів, і вимагають прийняття управлінських рішень.

Питаннями корелювання подій та управління ІТ-інцидентами у т.ч. на ОКІ займаються такі вітчизняні та закордонні вчені: Богачук І., Бурячок В., Складаний П., Соколов В., Aslan O., Berdibayev R., Karlzen H., Lee J., Pernul G., Vielberth M та інші. Проведений аналіз дозволив систематизувати існуючі SIEM-системи за їх функціональністю, основними принципами роботи, відповідністю до вимог міжнародних специфікацій і стандартів та інших запропонованих критеріїв. Було виділено перелік систем, які відповідають значній кількості критеріїв, проте відрізняються вартістю. Також визначено, що сьогодні доцільно використовувати open source системи з погляду витрат та можливості доповнення функціоналу під потреби конкретного підприємства (ОКІ). З точки зору безпеки, найбільш придатним варіантом є розробка власної системи, яка матиме широкий функціонал з ІБ, буде гнучкою та масштабованою, а також захищеною від можливих уразливостей та бекдорів. Незважаючи на велику кількість інструментальних рішень, жодне з них не вирішує всі наявні проблеми щодо управління ІТ-інцидентами. Для успішної реалізації заходів захисту ОКІ необхідне вирішення низки завдань, основне з яких пов'язане зі створенням єдиної системи моніторингу загроз безпеці, головною метою якої буде зниження до мінімального рівня ризику впливу на ОКІ і мінімізація збитків, що можуть виникнути внаслідок реалізації загроз.

З огляду на зазначене, розроблення системи корелювання подій та управління ІТ-інцидентами на ОКІ є *актуальною науково-технічною задачею*, що має теоретичне і практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота безпосередньо пов'язана з пріоритетними тематичними напрямами наукових досліджень і науково-технічних розробок, визначеними постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476, та відповідає напряму розвитку інформаційно-комунікаційних технологій, зокрема, інтелектуальні інформаційно-аналітичні системи, інтегровані системи баз даних і знань, національні інформаційні ресурси. Тематика дослідження також узгоджується зі Стратегією цифрового розвитку інновацій до 2030 року, зокрема в частині розвитку технологій штучного інтелекту, інтелектуального аналізу й оброблення даних. Теоретичні і практичні положення дисертаційної роботи було використано під час виконання науково-дослідної роботи у Державному університеті «Київський авіаційний інститут», а саме НДР «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (д.р. № 0125U000624, 2025-2026 рр.).

Мета і задачі дослідження. Метою дисертаційної роботи є забезпечення можливості управління IT-інцидентами на ОКІ на основі розроблення та удосконалення моделей і синтезу системи управління інцидентами.

Для досягнення поставленої мети необхідно розв'язати такі **основні задачі:**

1) провести аналіз сучасних підходів до управління IT-інцидентами на ОКІ для виявлення їх переваг та недоліків;

2) удосконалити структурно-аналітичну модель оброблення даних для інтелектуалізованого виявлення аномалій у хмарних системах ІКС;

3) розробити модель онтологіко-реляційного сховища даних для зберігання та оброблення великих масивів інформації;

4) удосконалити модель інтеграційної шини даних для розподілу навантаження та захищеного обміну даними;

5) на основі запропонованих моделей розробити систему корелювання подій та управління IT-інцидентами на ОКІ;

6) створити спеціалізоване програмне забезпечення та провести верифікацію розроблених у роботі моделей та системи.

Об'єктом дослідження є процеси управління IT-інцидентами на ОКІ.

Предметом дослідження є моделі, системи і засоби управління IT-інцидентами на ОКІ.

Методи дослідження. Проведені дослідження базуються на сучасних методах: математичної логіки, на основі якої розроблено модель онтологіко-реляційного сховища даних; теорії множин, для формалізації сукупності різноманітних баз даних та чинникових ознак, у вигляді основних критеріїв відбору; теорії штучного інтелекту, на основі якої, відбувалось навчання нейронної мережі для виявлення аномалій дата сету NSL-KDD; теорії комп'ютерних мереж, для розробки моделі інтеграційної шини даних; теорії системного та структурного аналізу, для представлення моделі оброблення даних. та обробки результатів експериментів і верифікації ефективності розроблених моделей та системи.

Наукова новизна одержаних результатів полягає у такому:

– *удосконалено* структурно-аналітичну модель оброблення даних, яка завдяки формулюванню команд для передачі керування програмному клієнту ІКТ, додатковій обробці метаданих у хмарній системі та інтелектуалізованому виявленню сигнатур, дозволяє підвищити ефективність виявлення аномалій в хмарних ІКС;

– *вперше розроблено* модель онтологіко-реляційного сховища даних, яка за рахунок попередньої індексації та синтезу двох різних баз даних (Elasticsearch та MongoDB) з відповідними характеристиками, дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації;

– *удосконалено* модель інтеграційної шини даних, яка за рахунок декомпозиції функціональності сервісів (кожен з яких відповідає за окреме завдання і може працювати ізольовано від інших) та визначення критичності сервісів, дозволяє розподілити навантаження на послуги та гарантує безперервність обміну даними для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами;

– *отримала подальший розвиток* система корелювання подій та управління ІТ-інцидентами, яка за рахунок використання розроблених моделей обробки даних, онтологіко-реляційного сховища даних та інтеграційної шини даних, дає змогу формалізувати інформаційну технологію, що реалізує процеси управління ІТ-інцидентами на ОКІ згідно вимог міжнародних стандартів та найкращих світових практик щодо створення систем управління ІТ-інцидентами.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані в галузі інформаційних технологій для забезпечення стійкого функціонування хмарної інформаційної інфраструктури (у т.ч. критичної) в умовах деструктивних інформаційно-технічних впливів.

Практична цінність роботи полягає у такому:

– на основі дата сету NSL-KDD навчено нейронну мережу з точки зору виявлення аномалій типу DoS, U2R, R2L та Probe.

– створено методику зберігання та класифікації даних, яка дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних, проводити масштабування, агрегацію, аналіз, збір закономірностей та забезпечувати високу швидкість пошуку.

– сформовано специфікацію реалізації SIEM-систем на ОКІ, у вигляді основних та додаткових вимог.

– розроблено спеціальний програмний застосунок, який можна використовувати для управління ІТ-інцидентами, які виникають в КІ і мають вплив на критично важливі ресурси (КВР).

– результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft» (акт про впровадження від 11.03.2026), НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 12.02.2024), а також у навчальному процесі кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки для підвищення ефективності підготовки фахівців з ІТ (акт про впровадження від 21.12.2023).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [14, 16, 18-19] – розроблення структурно-аналітичної моделі оброблення даних в хмарних ІКС; [1, 3, 10, 22] – теоретичне обґрунтування моделі онтологіко-реляційного сховища даних; [1-2, 21] – розроблення моделі інтеграційної шини даних; [1, 9-13, 17, 20] – представлення системи корелювання подій та управління ІТ-інцидентами; [1-3, 5-8, 10-11, 13, 16] – експериментальне дослідження та програмна реалізація запропонованої системи для управління ІТ-інцидентами; [1-2, 4-5, 9-16] – аналіз підходів до управління подіями та ІТ-інцидентами на ОКІ.

З робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються виключно результати, отримані особисто здобувачем.

Апробація результатів дисертації. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: «Cybersecurity Providing in Information and Telecommunication Systems» (CPITS) (Kyiv, 2023-2024); «International Conference on Dependable Systems, Services and Technologies» DESSERT-2024 (Athens, Greece 2023); «International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» IDAACS-2023 (Dortmund, Germany, 2023);

«International Conference on Conflict Management in Global Information Networks» CMiGiN (Kyiv, 2022, 2025); «Information Technology and Implementation» IT&I (Kyiv, 2022); «Системи та засоби штучного інтелекту» (Київ, 2021); «ABIA-2023» (Київ, 2023); «Кіберзахист особи, суспільства і держави» (с. Велятино, 2024) та ін.

Публікації. Основні положення дисертації опубліковано у 22 наукових працях, у тому числі: 19 наукових статтях, серед них 11 – у закордонних рецензованих виданнях, які входять до наукометричної бази даних Scopus, 8 – у вітчизняних фахових наукових журналах, а також у 3 матеріалах і тезах доповідей на конференціях.

Структура роботи та її обсяг. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, додатків, списку використаних джерел і має 153 сторінки основного тексту, 90 рисунків, 9 таблиць, 42 сторінки додатків. Список використаних джерел містить 101 найменування і займає 12 сторінок. Загальний обсяг роботи 196 сторінок.

ОСНОВНА ЧАСТИНА

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і задачі досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведено аналіз наукової літератури за темою дисертаційної роботи.

За результатами аналізу підходів до виявлення аномалій у хмарному середовищі встановлено, що найбільш поширеними та універсальними є підходи, засновані на аналізі поведінки, застосуванні ігрових моделей та використанні інтелектуальних методів оброблення даних. Загальною метою таких підходів є підвищення швидкості виявлення аномальних станів при одночасному зниженні рівня помилкової класифікації. Проведений аналіз показав, що, незважаючи на ефективність окремих методів для певних класів даних, жоден із них не забезпечує повного виявлення всіх можливих аномалій у хмарних ІКС.

Аналіз сучасних типів баз даних, що використовуються в SIEM-системах, показав, що кожен з видів баз даних залишається актуальним у власній сфері, де взаємозв'язки між даними обумовлені конкретною структурою системи управління базами даних (СУБД). Крім того, слід розглядати можливість використання гібридних баз даних, які поєднують у собі різні типи, такі як SQL та NoSQL. Для вирішення цього завдання доцільно розробити нову модель гібридного сховища даних, що базується на спільній роботі двох різних баз даних з відповідними характеристиками.

Крім того, проаналізовано існуючі на ринку рішення інтеграційних шин даних та встановлено, що кожне з них має власні функціональні особливості та суттєві відмінності, які визначають сферу їх застосування. Показано, що open-source рішення (наприклад, Fuse) є доцільними для використання в умовах обмежених ресурсів, однак потребують додаткових налаштувань на початкових етапах впровадження, тоді як комерційні платформи (Talend, Mule, WSO2) забезпечують розширену функціональність і спрощені механізми інтеграції, але відрізняються за вартістю та ліцензійною політикою.

Також у першому розділі систематизовано та проведено детальний аналіз 16 SIEM-систем за 18 запропонованими критеріями. Зокрема розглянуто їх функціональні можливості, принципи роботи, а також виконано порівняльний аналіз переваг і недоліків використання та відповідності міжнародним стандартам і специфікаціям. Результати дослідження показали, що системи IBM QRadar, LogRhythm, Splunk, McAfee (ESM), AlienVault USM, FortiSIEM, SolarWinds та ManageEngine відповідають більшості визначених критеріїв, однак відрізняються за вартістю, рівнем підтримки хмарних середовищ та можливостями подальшої інтеграції. На основі проведеного аналізу показано доцільність розроблення універсальної системи корелювання подій та управління ІТ-

інцидентами, у якій поєднуються основні функціональні переваги існуючих SIEM-рішень. Таким чином, у першому розділі, на основі проведеного аналізу, визначено і обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення поставленої мети.

Другий розділ присвячений розробленню моделей для управління IT-інцидентами на ОКІ, а саме розроблення структурно-аналітичної моделі оброблення даних та моделі онтологіко-реляційного сховища даних.

Структурно-аналітична модель оброблення даних.

Етап 1. Представлення основних часових характеристик метаданих для незалежних випадкових величин.

Представимо математичну формалізацію моделі та визначимо основні часові характеристики процесу оброблення метаданих. Час оброблення метаданих в аналізаторі хмарних систем виявлення аномалій (програмним сервером) подамо у вигляді суми незалежних випадкових величин $\xi_1,\xi_2,...,\xi_N$, які мають однаковий розподіл F з виробляючою функцією моментів $M(s)$.

Етап 2. Знаходження розподілу виробляючої функції моментів $\chi(s)$.

Нехай N – цілочисленна випадкова величина з виробляючою функцією $A(s)=\sum P_i s^i$ яка є незалежною від усіх ξ_j. Тоді випадкова сума $S=\xi_1+...+\xi_N$ має розподіл, що описується виробляючою функцією моментів:

$$\chi(s)=W(M(s)), \tag{1}$$

де $W(s)$ – виробляюча функція, що описує випадкове число запитуваних програмним клієнтом елементів метаданих, $M(s)$ – виробляюча функція моментів, що характеризує випадковий час оброблення одного елемента метаданих.

Етап 3. Знаходження виробляючої функції моментів $M(s)$.

Кількість елементів метаданих, запитуваних програмним клієнтом, опишемо рівномірним дискретним розподілом із цілими значеннями в межах від h до ℓ. За умови рівноймовірності подій з імовірністю $\overline{p}$, виробляюча функція моментів має вигляд:

$$M(s)=\overline{p}(e^{hs}+e^{(h+1)s}+...+e^{(l-1)s}+e^{ls})=\frac{(\overline{p}(e^{hs}-e^{(l+1)s}))}{(1-e^{s})}.$$

Етап 4. Знаходження виробляючої функції, запитуваних елементів метаданих $W(s)$.

Виробляюча функція цього розподілу $W(s)=\dfrac{(\overline{p}(s^h-s^{(\ell+1)}))}{(1-s)}$. Для оцінювання випадкового часу обробки одного елемента метаданих використовуємо рівномірний неперервний розподіл з параметрами a і b. Тоді відповідно до (1) виробляюча функція моментів сумарного часу оброблення визначається як:

$$\chi(s)=\overline{p}\left(\frac{\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^h-\left(\frac{e^{as}-e^{bs}}{(a-b)s}\right)^{\ell+1}}{1-\frac{e^{as}-e^{bs}}{(a-b)s}}\right). \tag{2}$$

Етап 5. Визначення першого μ_1 і другого μ_2 моменту часу виконання керуючої команди.

Диференціюючи $\chi(s)$ по змінній s і прирівнюючи в отриманих виразах величину s нулю, отримуємо перший μ_1 і другий μ_2 моменти щодо початку координат і, відповідно, середнє значення t_s та дисперсію D часу обробки одного елемента метаданих, переданих на запит програмного клієнта.

$$\mu_1 = t_{cp}^{(o)} = \frac{\partial(\chi(s))}{\partial s}\bigg|_{s=0} = \frac{(h+\ell)(a+b)}{4}, \tag{3}$$

$$J^{(o)} = \mu_2 - \mu_1^2 = \frac{\partial(\chi(s))}{\partial s^2}\bigg|_{s=0} - \left(\frac{\partial(\chi(s))}{\partial s}\bigg|_{s=0}\right)^2 = \frac{(h+\ell)(b-a)^2}{24}. \tag{4}$$

У випадку, коли аналізатор метаданих виконує обробку файлів різних незалежних інформаційних потоків, кількість вимог програмного клієнта на формування, аналіз та оброблення керуючих команд, доцільно описати розподілом Пуассона. В такому випадку виробляюча функція розподілу має вигляд $W(s) = e^{\lambda s - \lambda}$. Відповідно, виконуюча функція моментів часу формування та виконання команд визначається як:

$$\chi(s) = e^{\left(-\lambda + \lambda \frac{e^{as} - e^{bs}}{(a-b)s}\right)}. \tag{5}$$

Етап 6. Розрахунок середнього часу виконання керуючої команди t_s та її дисперсії D для обробки одного елемента метаданих, переданих на запит програмного клієнта.

З виразу (5) знаходимо середній час виконання завдання формування керуючої команди та його дисперсію:

$$t_{cp}^{(\phi)} = \frac{\lambda(a+b)}{2}, \tag{6}$$

$$J^{(\phi)} = \frac{\lambda(a^2+ab+b^2)}{3}. \tag{7}$$

Проведені дослідження процесу збирання, зберігання та обробки метаданих у хмарних системах виявлення аномалій показали, що загальну структуру моделі обробки даних можна представити у вигляді схеми рис. 1.

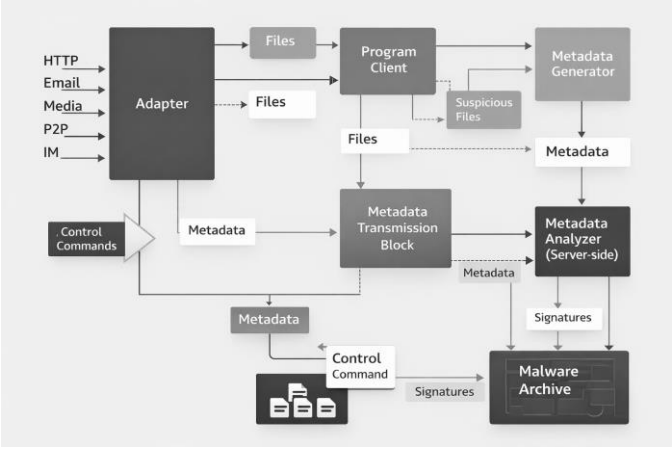


Рисунок 1 – Структурна схема обробки даних у хмарних системах виявлення аномалій

Таким чином, розроблено структурно-аналітичну модель обробки даних, що дозволяє оцінити часові характеристики обробки одного елемента метаданих та вироблення керуючої команди.

Крім того, у другому розділі було розроблено *модель онтологіко-реляційного сховища даних.* Для обґрунтування вибору найбільш ефективних СУБД, які використовуються в сучасних SIEM-системах, запропоновано процедуру, що включає наступні етапи:

Етап 1. Введення множини баз даних.

Введемо множину баз даних **DB** у наступному вигляді:

$$\mathbf{DB} = \{\bigcup_{i=1}^{n} DB_i\} = \{DB_1, DB_2, \ldots, DB_n\}, \tag{8}$$

де $DB_i \subseteq \mathbf{DB}\ (i = \overline{1,n})$ – різновиди СУБД, які використовуються в певних SIEM-системах, n – загальна кількість баз даних.

Етап 2. Введення множини чинникових ознак (критеріїв).

Для оцінювання ефективності баз даних **DB** визначимо множину чинникових ознак (критеріїв). Запропоновані критерії представимо у наступному вигляді:

$$\mathbf{EC} = \{\bigcup_{j=1}^{q} EC_j\} = \{EC_1, EC_2, \ldots, EC_q\}, \tag{9}$$

де $EC_j \subseteq \mathbf{EC}\ (j = \overline{1,q})$ – категорія критеріїв для оцінювання найефективніших СУБД, q – загальна кількість критеріїв.

Етап 3. Процедура ранжування баз даних.

Крок 3.1. Побудова матриць попарних порівнянь.

Крок 3.2. Побудова загального вектору критеріїв та оцінка ваги векторів відносно важливості кожного критерію.

Крок 3.3. Аналіз узгодженості матриці попарних порівнянь.

Крок 3.4. Побудова матриць вектору критеріїв та оцінка ваги векторів для кожного елемента множини баз даних DB та множини елементів критеріїв EC.

Крок 3.5. Визначення рангу найбільш ефективних баз даних DB.

Після того як для кожного елемента баз даних DB були побудовані матриці векторів критеріїв та оцінено ваги цих векторів необхідно обчислити ранг найбільш ефективних баз даних DB.

$$RN_{DB} = \sum_{j=1}^{q} EC_j \cdot W_{EC}. \tag{10}$$

В процесі дослідження було визначено, що до переліку найбільш ефективних за рангом БД доцільно відносити значення, що відповідають: $RN_{DB} \geq 0,75$.

Етап 4. Введення множини облікових задач.

У зв'язку з тим, що кожен елемент з наведеної множини баз даних DB має виконувати необхідні облікові задачі, введемо множину необхідних облікових задач у наступному вигляді:

$$\mathbf{TS} = \{\bigcup_{k=1}^{p} TS_k\} = \{TS_1, TS_2, \ldots, TS_p\}, \tag{11}$$

де $TS_k \subseteq \mathbf{TS}\ (k = \overline{1,p})$ – перелік облікових задач необхідних для ефективної роботи кожної СУБД, p – загальна кількість облікових задач.

Етап 5. Результат вибору найбільш ефективних баз даних.

Результати вибору найбільш ефективних БД представлені у вигляді кортежу:

$$MEF_{DB} = \langle RN_{DB}, EC_j, TS_k \rangle, \quad (12)$$

який характеризує БД з найвищим значенням рангового показника RN_{DB}, що відповідають визначеним критеріям ефективності EC_j, та здатні забезпечити виконання множини необхідних облікових задач TS_k.

Більш детальний опис етапів та кроків реалізації моделі онтологіко-реляційного сховища даних, представлено на рис. 2.

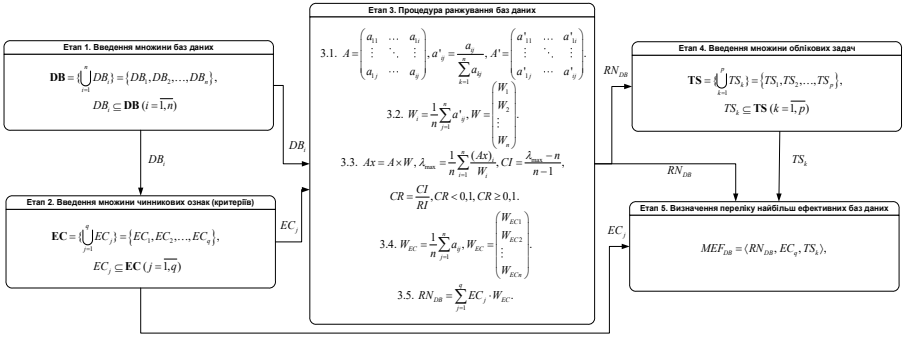


Рисунок 2 – Схема реалізації етапів моделі онтологіко-реляційного сховища даних

Таким чином, було розроблено модель онтологіко-реляційного сховища даних, яка дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації.

У **третьому розділі** наведено розроблення моделі інтеграційної шини даних та системи корелювання подій та управління ІТ-інцидентами.

Запропонована *модель інтеграційної шини даних (ІШД)* реалізується на основі сервіс-орієнтованої архітектури (SOA) та забезпечує інтеграцію програмних компонентів через стандартизовані сервісні інтерфейси. ІШД виступає шаблоном та центральним елементом ІКС, який забезпечує обмін даними між сервісами SIEM-системи та зовнішніми компонентами через сервісні інтерфейси і шлюзи доступу (рис. 3).

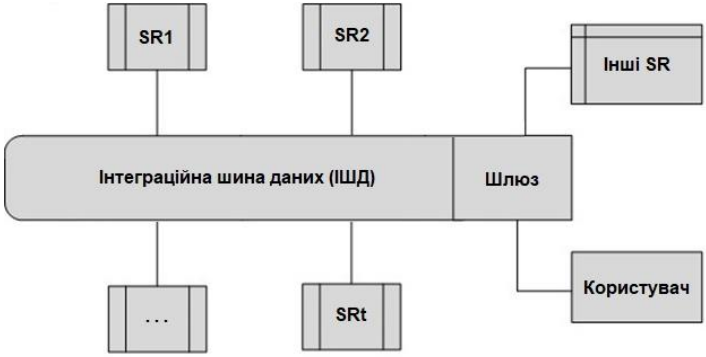


Рисунок 3 – Схема побудови ІШД

Встановлено, що для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами на ОКІ необхідно забезпечити безперервне надання сервісів SIEM-систем. Під сервісами у роботі розуміються послуги, що надаються SIEM-системами. Основним завданням ІШД є визначення режимів функціонування сервісів і формування оптимального порядку їх оброблення з урахуванням рівня критичності, що дає змогу мінімізувати втрати часу на очікування обслуговування та простої каналів. Для цього черга обслуговування сервісів визначається за рівнем їх критичності з використанням підходу FMECA.

Етап 1. Введення множини сервісів системи.

Введемо множину сервісів системи **SR** у наступному вигляді:

$$\mathbf{SR} = \{\bigcup_{s=1}^{t} SR_s\} = \{SR_1, SR_2, \ldots, SR_t\}, \tag{13}$$

де $SR_s \subseteq \mathbf{SR}$ $(s = \overline{1,t})$ – різновиди сервісів системи, які надають послуги SIEM-системам, t – загальна кількість сервісів.

Етап 2. Визначення критичності сервісів.

Для оцінювання критичності сервісів введемо множину значень рангу критичності **RN**:

$$\mathbf{RN} = \{\bigcup_{r=1}^{w} RN_r\} = \{RN_1, RN_2, \ldots, RN_w\}, \tag{14}$$

де $RN_r \subseteq \mathbf{RN}$ $(r = \overline{1,w})$ – ранги критичності сервісів SR, де w – загальна кількість показників рангів критичності.

Ранг критичності сервісів SR визначається інтегральною оцінкою:

$$RN_r = IN_{1a} \cdot IN_{2a} \cdot IN_{3a} \tag{15}$$

де IN_{1a} – оцінка ймовірності настання переривання роботи сервісу SR_s, IN_{2a} – оцінка ймовірності попереднього виявлення переривання сервісу та IN_{3a} – оцінка тяжкості настання переривання роботи сервісу.

Крок 2.1 – 2.3. Для визначення показників вводяться відповідні множини $\mathbf{IN}_1 = \{\bigcup_{a=1}^{z} IN_{1a}\} = \{IN_{11}, IN_{12}, \ldots, IN_{1z}\}$, $\mathbf{IN}_2 = \{\bigcup_{a=1}^{x} IN_{2a}\} = \{IN_{21}, IN_{22}, \ldots, IN_{2x}\}$, $\mathbf{IN}_3 = \{\bigcup_{a=1}^{c} IN_{3a}\} = \{IN_{31}, IN_{32}, \ldots, IN_{3c}\}$, а значення z, x, c знаходяться за таблицями, сформованими у залежності від типу SIEM-систем.

Крок 2.4. Розрахунок рангу критичності RN_r для кожного з перерахованих видів сервісів SIEM-систем згідно з (15).

Етап 3. Виділення переліку критичних сервісів SIEM-систем.

Введемо правила для визначення критичності сервісу $crt(SR_s) \in \{H, M, L\}$:

$$crt(SR_s) = \begin{cases} H, & RN_r > RN_k; \\ M, & RN_0 < RN_r \le RN_k; \\ L, & RN_r \le RN_0, \end{cases} \tag{16}$$

де RN_0, RN_k – порогові значення рангу критичності. У випадку, якщо $crt(SR_s) = H$ робота сервісу визнається критичним, при $crt(SR_s) = M$ необхідне застосування заходів щодо

зменшення критичності, при $crt(SR_s) = L$ переривання роботи сервісу вважається незначним і не потребує впровадження додаткових заходів.

Етап 4. Ранжування переліку критичних сервісів SIEM-систем за допомогою діаграми Парето.

Для ранжування переліку найбільш значущих (критичних) сервісів використовується діаграма Парето, яка будується окремо для кожної SIEM-системи. Ранжування сервісів SR_s здійснюється за значенням рангу критичності RN_r. Для наочності результати ранжування подаються у вигляді діаграми Парето з візуальним виділенням сервісів за рівнями критичності: H – червоним кольором, M – жовтим кольором, L – зеленим кольором.

Отже, зазначена модель інтеграційної шини даних, дозволяє розподілити навантаження на послуги та гарантує безперервність обміну даними для ефективного функціонування системи корелювання подій та управління IT-інцидентами.

Також у третьому розділі була розроблена *система корелювання подій та управління IT-інцидентами на ОКІ*. Рис. 4 відображає архітектуру запропонованої системи, яка орієнтована на використання в різних секторах КІ з підтримкою хмарних технологій. До основних структурних компонентів системи належать: горизонтальні бази даних (Horizontal Databases); блок аналітики (Analytics); блок моніторингу (Monitoring); хмарне сховище (Cloud Storage); шифратор даних (Encryptor); брокер повідомлень (Message Broker); джерела (System 1 – System *N*). Крім того, важливу роль у цій системі відіграє шифратор даних (Encryptor), який фактично є єдиним блоком з хмарним сховищем (Cloud Storage), забезпечуючи таким чином конфіденційність необроблених записів після збору агентами syslog, NetFlow і т.д. Крім цього, віртуальна машина (VirtualBox) відправляє зібрані дані у зашифрованому вигляді через брокер повідомлень (Message Broker) у горизонтальні бази даних (Horizontal Databases). У разі відсутності зв'язку з брокером повідомлень забезпечується тимчасове зберігання даних у хмарному сховищі, як уже зазначалося.

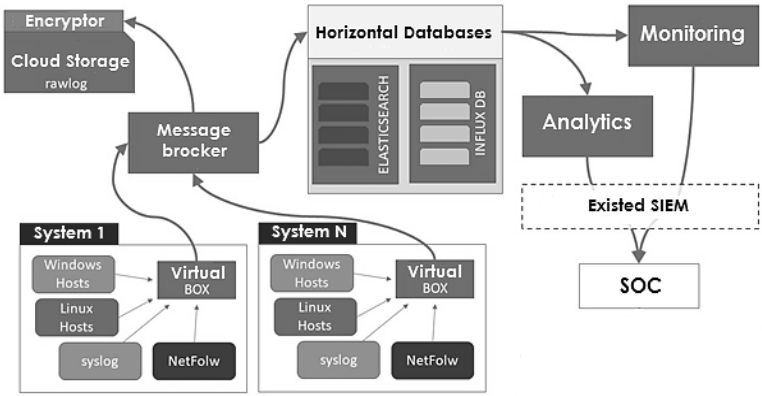


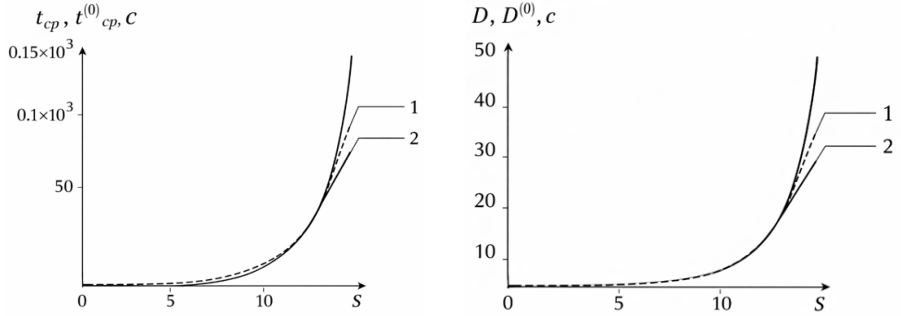
Рисунок 4 – Архітектура системи корелювання подій та управління IT-інцидентами на ОКІ

Далі, зазначена система була реалізована програмно та експериментально досліджена (у контексті відповідності визначеним критеріям і забезпечення ефективного корелювання подій та управління IT-інцидентами, які виникають на ОКІ і мають вплив на КВР).

Встановлено, що запропонована система корелювання подій, дає змогу забезпечити управління IT-інцидентами на ОКІ згідно вимог міжнародних стандартів та найкращих світових практик щодо створення систем управління IT-інцидентами.

Четвертий розділ присвячений практичним реалізаціям та експериментальним дослідженням розроблених моделей та системи.

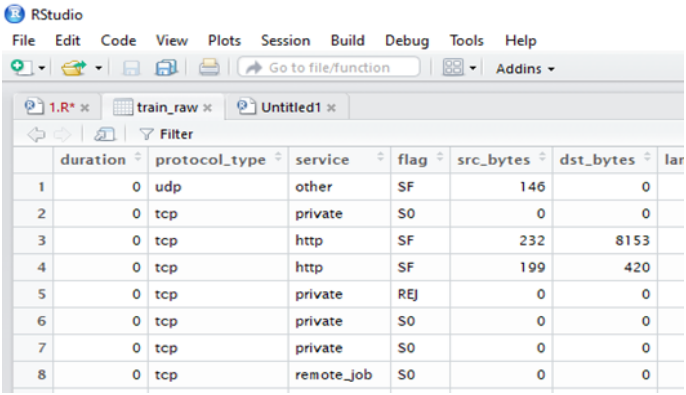
Було проведено експериментальне дослідження структурно-аналітичної моделі оброблення даних з метою оцінювання взаємозв'язку часових характеристик обробки метаданих і формування керуючих команд. На основі співвідношень (2), (4), (6), (7) досліджено залежності середнього часу обробки метаданих $t_{cp}(s)$, часу обробки одного елемента $t_{cp}^{(o)}(s)$ (рис. 5 а), а також відповідних дисперсій $D(s)$ та $D^{(o)}(s)$ (рис. 5 б). Графічні результати наведено на рис. 5 для параметрів $a=0,4;\ b=0,7;\ h=0,3;$ $\ell=1;\ p=0,3;\ \lambda=1200$. Отримані результати показали, що врахування процесу формування керуючих сигналів дозволяє підвищити точність оцінювання часових характеристик у 1,7 разів, а оцінювання характеристик спотворення (затримок) – у 4,5 разів.



а) *б)*

Рисунок 5 – Графіки залежностей $t_{cp}(s)$ та $t_{cp}^{(o)}(s)$, $D(s)$ та $D^{(o)}(s)$

Подальше експериментальне дослідження проведено в середовищі розробки з відкритим вихідним кодом RStudio. В якості вхідних даних використано підмножину (20 %) датасету NSL-KDD. На рис. 6 наведено фрагмент завантажених вхідних даних, а на рис. 7 – результати візуалізації розподілу ідентифікованих загроз і атак.



	duration	protocol_type	service	flag	src_bytes	dst_bytes	lar
1	0	udp	other	SF	146	0	
2	0	tcp	private	S0	0	0	
3	0	tcp	http	SF	232	8153	
4	0	tcp	http	SF	199	420	
5	0	tcp	private	REJ	0	0	
6	0	tcp	private	S0	0	0	
7	0	tcp	private	S0	0	0	
8	0	tcp	remote_job	S0	0	0	

Рисунок 6 – Завантаження навчальних даних NSL-KDD

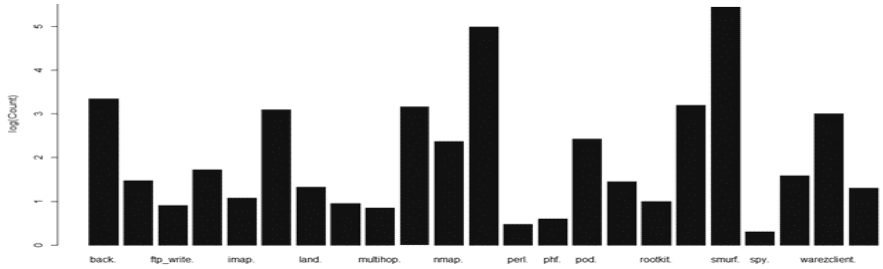


Рисунок 7 – Розподіл виявлених загроз та атак

На рис. 8 представлено порівняльний аналіз відсоткового розподілу виявлених загроз залежно від їх типу. Встановлено, що найбільшу частку становлять атаки типу DoS, при цьому запропонована модель демонструє кращі показники виявлення аномалій порівняно з існуючими підходами.

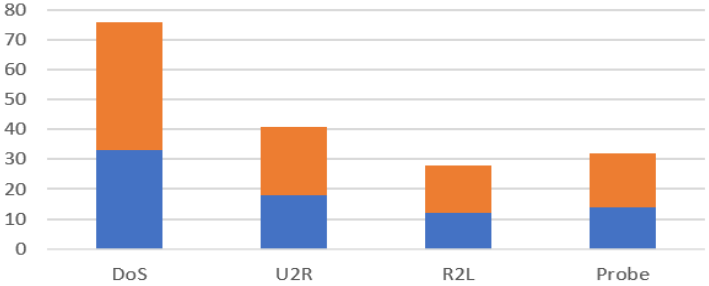


Рисунок 8 – Відсотковий розподіл виявлених загроз залежно від їх типу

Таким чином, результати експериментальних досліджень підтверджують адекватність структурно-аналітичної моделі оброблення даних та її ефективність для оцінювання часових характеристик обробки метаданих і формування керуючих команд у хмарних ІКС.

Крім того, було експериментально досліджено *модель онтологіко-реляційного сховища даних*, яка за допомогою розробленої процедури дозволила здійснити оцінювання множини сучасних баз даних **DB** на відповідність множині критеріїв EC_j, та здатність вирішувати множину облікових задач TS_k. За результатами аналізу $n=34$ систем, при $n=34$ з урахуванням (8), було визначено множину баз даних **DB**. При $q=7$ з урахуванням (9), визначено множину критеріїв: серед яких EC_1 – високоорганізована структура, EC_2 – гнучкість, EC_3 – швидкий доступ, EC_4 – підтримка різних типів даних, EC_5 – збереження даних конфігурацій, EC_6 – підтримка мови структурованих запитів, EC_7 – DBaaS (підтримка хмарних технологій). Відповідно, при $p=5$ з урахуванням (11), визначено множину облікових задач: TS_1 – швидке опрацювання журналів, TS_2 – легкість масштабування, TS_3 – надійність зберігання службової інформації, TS_4 – оперативний пошук та фільтрація даних, TS_5 – здійснення комплексної бізнес-аналітики даних.

У результаті експериментальних досліджень (див. рис. 9) були обґрунтовано виділені найбільш ефективні бази даних: DB_{23} – MongoDB та DB_{24} – Elasticsearch, що відповідають множині критеріїв та можуть вирішувати множину необхідних задач.

	EC_1	EC_2	EC_3	EC_4	EC_5	EC_6	EC_7	RN_{DB}
	0,098	0,098	0,184	0,115	0,184	0,184	0,135	
DB_1	0,54	0,2	0,3	0,12	0,5	0,6	0,37	0,39
DB_2	0,27	0,24	0,35	0,17	0,12	0,43	0,15	0,69
DB_4	0,49	0,37	0,2	0,54	0,34	0,32	0,14	0,68
DB_5	0,2	0,3	0,16	0,34	0,33	0,28	0,22	0,66
DB_6	0,5	0,21	0,39	0,37	0,44	0,46	0,12	0,65
DB_{23}	0,22	0,37	0,38	0,4	0,42	0,38	0,42	0,77
DB_{24}	0,31	0,23	0,2	0,23	0,32	0,31	0,48	0,78
DB_{31}	0,6	0,35	0,5	0,3	0,18	0,47	0,21	0,69

Рисунок 9 – Експериментальне дослідження ефективності баз даних за критеріями

Основним завданням онтологіко-реляційного сховища даних у системі корелювання подій та управління ІТ-інцидентами на ОКІ є забезпечення інтеграції двох типів баз даних із збереженням можливості їх кластеризації та узгодженої роботи.

У ході експериментальних досліджень обґрунтовано використання **Elasticsearch** для оперативного опрацювання журналів подій, що забезпечує індексацію, повнотекстовий пошук, фільтрацію та агрегацію даних. Для надійного зберігання службової інформації експериментально визначено застосування **MongoDB** як документоорієнтованої СУБД із гнучкою структурою даних та підтримкою масштабування.

На основі запропонованої моделі розроблено методику зберігання та класифікації даних, що забезпечує доступ сервісу індексації до розподілених сховищ, підтримку масштабування, аналітичну обробку подій та підвищення швидкодії пошуку.

Реалізовано та впроваджено *модель інтеграційної шини даних* для забезпечення ефективного функціонування SIEM-систем на ОКІ. Встановлено, що ІШД виступає централізованим компонентом (шаблоном), який забезпечує інтеграцію сервісів, маршрутизацію даних, їх перетворення та узгоджену взаємодію через сервісні інтерфейси.

У межах експериментального дослідження при $t = 8$ з урахуванням (13), визначимо множину сервісів, що включає SR_1 – збір та зберігання подій, які надходять до системи, SR_2 – виявлення та розбір інцидентів безпеки, SR_3 – виявлення атак та порушень політики безпеки, SR_4 – оцінка захищеності ресурсів системи, SR_5 – пошук та управління вразливостями, SR_6 – формування звітів, SR_7 – підтримка роботи з хмарними ІКС, SR_8 – розширені можливості пошуку. Крім того, відповідно до (15) обчислено ранги критичності сервісів. Значення рангу критичності для найбільш ефективних баз даних (MongoDB та Elasticsearch) наведено в табл. 1.

Таблиця 1

Значення рангу критичності сервісів SR для двох баз даних DB_{23} та DB_{24}

	SR_1	SR_2	SR_3	SR_4	SR_5	SR_6	SR_7	SR_8
RN Elasticsearch	125	95	85	70	57	120	145	125
RN MongoDB	95	90	75	58	75	127	140	126

Процес ранжування переліку критичних сервісів із використанням діаграми Парето представлено на рис. 10. Отримані результати дозволили визначити пріоритетну чергу обслуговування сервісів та забезпечити оптимальний розподіл навантаження в ІШД.

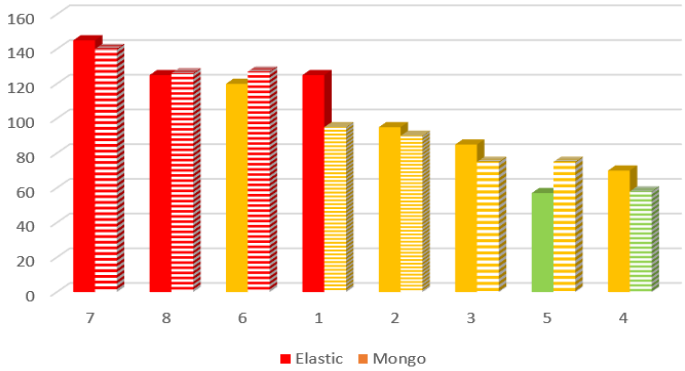


Рисунок 10 – Результати визначення пріоритетності сервісів

Крім того, було сформовано *специфікацію реалізації SIEM-систем на ОКІ* у вигляді основних та додаткових вимог (фрагмент якої представлено на рис. 11).

Технічна специфікація SIEM-систем на ОКІ

№	Назва	Опис
		Основні вимоги
1.	Системи спеціального призначення.	SIEM призначена для моніторингу та аналізу подій ІБ і повинна: ▪ здійснювати централізований збір, зберігання та обробку подій системних журналів (логів), а також мережевих потоків з різних систем інфраструктури Замовника; ▪ виділяти в загальному масиві даних важливі події та інциденти ІБ, що повинно дозволити фахівцям з ІБ Замовника, сконцентруватися на найбільш серйозних інцидентах і своєчасно реагувати на них; ▪ інформувати персонал Замовника про виявлені інциденти інформаційної безпеки шляхом надсилання повідомлень на електронну пошту.
2.	Системи з централізованим управлінням.	SIEM повинна забезпечувати централізоване управління всіма своїми компонентами і функціоналом через єдиний графічний веб-інтерфейс.
3.	Візуалізація даних (Dashboards).	SIEM: ▪ дозволяє створювати графічні панелі (дашборди) за будь-якими подіями, з автоматичним оновленням із заданим інтервалом; ▪ підтримує створення нових графічних панелей або модифікацію існуючих за допомогою "майстра", методом, що не вимагає використання мов програмування; ▪ дозволяє зберігати графічні панелі для колективного використання. Графічні панелі повинні підтримувати різні типи представлення даних: таблиці, кругові та лінійні діаграми тощо, вони повинні функціонувати автоматично, без необхідності регулярного обслуговування оператором; ▪ підтримка відображення графічних панелей через WEB інтерфейс.
4.	Підтримка API:	SIEM повинна мати відкритий програмний інтерфейс API для можливості інтеграції з іншими модулями.

Рисунок 11 – Специфікація SIEM-систем на ОКІ (фрагмент)

Архітектура розробленої *системи корелювання подій та управління IT-інцидентами на ОКІ* наведена на рис. 12. Система має високу гнучкість і горизонтальну масштабованість. Для зберігання подій використовується NoSQL СУБД Elasticsearch, для зберігання всієї інформації про конфігурацію та правила використовується NoSQL СУБД MongoDB.

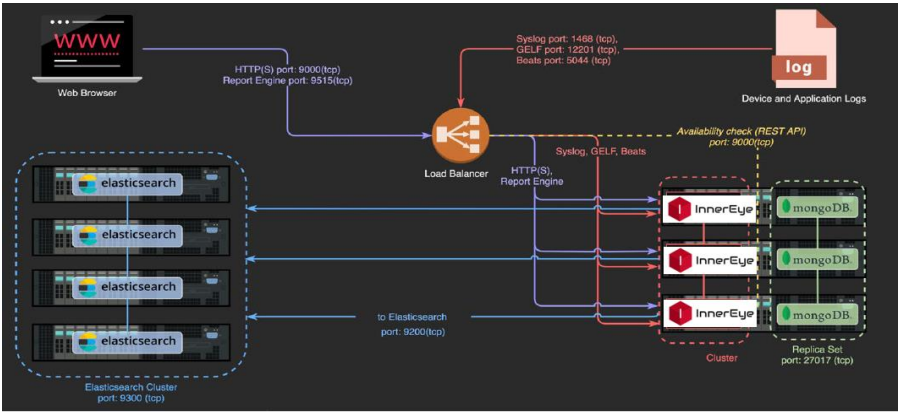


Рисунок 12 – Приклад архітектури системи корелювання подій та управління IT-інцидентами на ОКІ

Система, залежно від вимог до продуктивності та надійності, може бути розгорнута у різних варіантах. Використання кластерів у системі корелювання подій та управління ІТ-інцидентами на ОКІ забезпечує високу продуктивність та надійність системи в цілому та дозволяє гнучко адаптувати систему до конкретних умов.

Для формалізації процесів управління ІТ-інцидентами на ОКІ в роботі розроблено *інформаційну технологію управління ІТ-інцидентами* (рис. 13), що базується на використанні структурно-аналітичної моделі оброблення даних, онтологіко-реляційного сховища даних та інтеграційної шини даних.

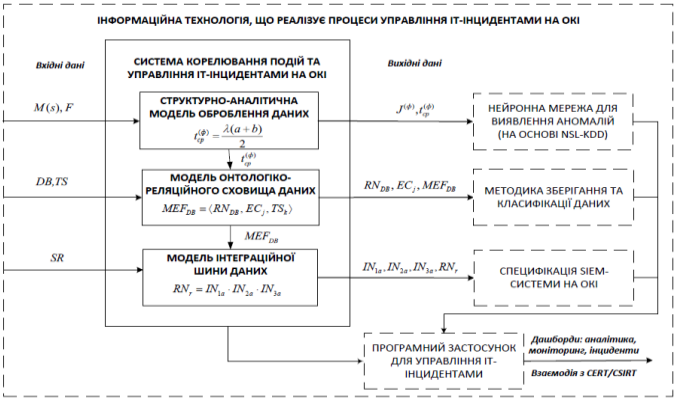


Рисунок 13 – Інформаційна технологія управління ІТ-інцидентами на ОКІ

Вхідними даними інформаційної технології є потоки подій безпеки (журнали, мережеві та системні повідомлення), параметри структурно-аналітичної моделі оброблення даних, множини баз даних і облікових задач (DB, TS), а також множина сервісів системи (SR). В процесі функціонування здійснюється збирання, індексація та зберігання подій, їх корелювання й аналітичне оброблення, розрахунок часових характеристик, визначення рангу критичності сервісів і формування керуючих впливів. Реалізація зазначених процесів забезпечується нейронною мережею для виявлення аномалій, методикою зберігання та класифікації даних, специфікацією побудови SIEM-системи та програмним застосунком управління ІТ-інцидентами. Результатом реалізації інформаційної технології є: виявлені ІТ-інциденти та аномалії, сформовані пріоритети їх оброблення, аналітичні звіти та візуалізовані результати моніторингу (дашборди), забезпечення взаємодії з CERT/CSIRT, практичні рекомендації щодо реагування та підвищення рівня захищеності ОКІ.

Експериментальне дослідження реалізації зазначеної інформаційної технології в складі системи корелювання подій та управління ІТ-інцидентами на ОКІ підтвердило її відповідність вимогам міжнародних стандартів і найкращих світових практик створення систем управління ІТ-інцидентами. Зокрема, забезпечено централізоване управління компонентами та функціональними можливостями системи, візуалізацію даних через відповідні інтерфейси, підтримку відкритого програмного інтерфейсу API, механізмів аутентифікації та авторизації, а також реалізовано властивості масштабованості, відмовостійкості, збору та фільтрації подій і управління обліковими записами. Розроблена система корелювання подій та управління ІТ-інцидентами на ОКІ може використовуватись для управління інцидентами, які виникають в КІ і мають вплив на КВР.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи і лістинги (фрагменти кодів) розробленого у роботі програмного застосунку.

ВИСНОВКИ

Результатом виконаної дисертаційної роботи є розв'язання актуальної науково-технічної задачі розроблення системи корелювання подій та управління ІТ-інцидентами на ОКІ.

У процесі виконання дисертаційної роботи отримані такі наукові та практичні результати:

1. Проведено аналіз сучасних підходів до управління ІТ-інцидентами на ОКІ для виявлення їх переваг та недоліків. За результатами проведеного аналізу підходів до виявлення аномалій в хмарному середовищі встановлено, що кожен метод виявлення має свої переваги та працює краще для певних наборів даних, але жоден не є універсальним і не може виявити всі сто відсотків шкідливих програм. Аналіз існуючих типів баз даних та інтеграційних шин даних, показав, що кожні з них мають свої особливості та суттєві відмінності, які визначають їх сферу використання, а також відрізняються функціоналом, додатковими налаштуваннями та вартістю ліцензії. Крім того, систематизовано та представлено детальний аналіз 16 SIEM-систем за 18 запропонованими критеріями. Зокрема відображено їх функціональність, основний принцип роботи, а також проведено порівняльний аналіз їх можливостей та відмінностей, переваг та недоліків використання, та відповідності до міжнародних специфікацій та стандартів. Проведений аналіз дозволив формалізувати завдання дисертаційного дослідження щодо розроблення моделей та системи корелювання подій та управління ІТ-інцидентами на ОКІ.

2. Удосконалено структурно-аналітичну модель оброблення даних, яка завдяки формулюванню команд для передачі керування програмному клієнту ІКТ, додатковій обробці метаданих у хмарній системі та інтелектуалізованому виявленню сигнатур, дозволяє підвищити ефективність виявлення аномалій в хмарних ІКС. Експериментальне дослідження моделі дозволило оцінити часові характеристики обробки одного елемента метаданих та розробити керуючі команди. Її відмінною особливістю є врахування необхідності формування команд передачі управління програмному клієнту ІКС, що загалом підвищило точність результатів оцінки часових характеристик до 1,7 разів, і характеристик спотворень (затримок) до 4,5 разів. Крім того, на основі дата сету NSL-KDD навчено нейронну мережу з точки зору виявлення аномалій типу DoS, U2R, R2L та Probe.

3. Розроблено модель онтологіко-реляційного сховища даних, яка за рахунок попередньої індексації та синтезу двох різних баз даних (Elasticsearch та MongoDB) з відповідними характеристиками, дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації. Крім того, створено методику, яка дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних, проводити масштабування, агрегацію, аналіз, збір закономірностей та забезпечувати високу швидкість пошуку.

4. Удосконалено модель інтеграційної шини даних, яка за рахунок декомпозиції функціональності сервісів (кожен з яких відповідає за окреме завдання і може працювати ізольовано від інших) та визначення критичності сервісів, дозволяє розподілити навантаження на послуги та гарантує безперервність обміну даними для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами. На основі розробленої моделі було сформовано відповідну специфікацію реалізації SIEM-систем на ОКІ, у вигляді основних та додаткових вимог.

5. Отримала подальший розвиток система корелювання подій та управління ІТ-інцидентами на ОКІ, яка за рахунок використання розроблених моделей обробки даних, онтологіко-реляційного сховища даних та інтеграційної шини даних, дає змогу формалізувати інформаційну технологію, що реалізує процеси управління ІТ-інцидентами на ОКІ згідно вимог міжнародних стандартів та найкращих світових практик щодо створення систем управління ІТ-інцидентами. Крім того, розроблено спеціальний

програмний застосунок, який можна використовувати для управління IT-інцидентами, які виникають в КІ і мають вплив на КВР.

6. На основі запропонованої інформаційної технології з використанням розробленого спеціалізованого програмного застосунку, проведено експериментальне дослідження і верифіковано отримані у роботі моделі та систему. Результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft» (акт про впровадження від 11.03.2026), НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 12.02.2024), а також у навчальному процесі кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки для підвищення ефективності підготовки фахівців з IT (акт про впровадження від 21.12.2023).

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., Смірнова Т.В. Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2023. Т. 3. № 19. С. 176-196.

2. Гнатюк С.О., Бердибаєв Р.Ш., Богун А.М., Сидоренко В.М., Положенцев А.А., Жигаревич О.К. Інтеграційна шина даних для ефективного функціонування системи управління подіями інформаційної безпеки. *Проблеми інформатизації та управління*. 2023. Т. 3. № 75. С. 29-40.

3. Жигаревич О.К., Бердибаєв Р.Ш., Сидоренко В.М., Положенцев А.А., Кримська А.О. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи. *Проблеми інформатизації та управління*. 2023. Т. 4. № 76. С. 17-27.

4. Дмитрук Я.В., Гришанович Т.О., Глинчук Л.Я., Жигаревич О.К. Кібервійна як різновид інформаційних війн. Захист кіберпростору України. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 4. №16. С. 28-36.

5. Жигаревич О.К., Медведєв М.В. Інформаційна ситема «Студент-ФКНІТ» засобами PHP. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2017. № 26. С. 88-92.

6. Жигаревич О.К., Котлярець В.В., Луць А.Р. Модель екосистеми навчального програмного забезпечення. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2017. № 26. С. 167-177.

7. Жигаревич О.К., Мельник В.М., Мельник К.В. Підтримка оголошеної/встановленої комунікації в мережі через стандартні сокети API. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2015. № 19. С. 23-27.

8. Мельник К.В., Мельник В.М., Багнюк Н.В., Жигаревич О.К., Климюк М. Система попереднього відбору кандидатів на основі нечіткої логіки. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2015. № 19. С. 114-120.

9. Pobochenko L., Prokopieva A., Zhyharevych O., Gavrylko O., Panikar G., Gavrilko T. Risks of investing in FinTech at the global and national levels. *CEUR Workshop Proceedings. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2025),* June 20 - 22, 2025, Kyiv, Ukraine, 2025. Vol. 4024. P. 468-478.

10. Sydorenko V., Zhyharevych O., Berdybaev R., Polozhentsev A., Fesenko A. Ontological-Relational Data Store Model for a Cloud-based SIEM System Development. *CEUR Workshop Proceedings. Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2024),* February 28, 2024, Kyiv, Ukraine, 2024. Vol. 3654. P. 343-354.

11. Gnatyuk S., Berdibayev R., Aleksander M., Sydorenko V., Zhyharevych O., Polozhentsev A. Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*. 2024. Vol. 213. P. 247-269. Springer, Cham.

12. Zdolbitska N., Ostapchuk O., Lavrenchuk S., Terletskyi T., Kaidyk O., Zhyharevych O. Business information system for forecasting raw material stocks for the production of flexible packaging. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Athens, Greece, 2024, P. 1-8.

13. Polozhentsev A., Gnatyuk S., Berdibayev R., Sydorenko V., Zhyharevych O. Novel Cyber Incident Management System for 5G-based Critical Infrastructures. *IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, P. 1037-1041.

14. Gnatyuk S., Satybaldiyeva F., Sydorenko V., Zhyharevych O., Polozhentsev A. Model of Information Technology for Efficient Data Processing in Cloud-based Malware Detection Systems of Critical Information Infrastructure. *CEUR Workshop Proceedings, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023)*, February 28, 2023, Kyiv, 2023, Vol. 3421, P. 206-213.

15. Gnatyuk S., Zhaksigulova D., Zhyharevych O., Ospanova D., Chuba I. Studies on WSN Models for IoT-based Monitoring Systems in the Critical Infrastructure of the State. *CEUR Workshop Proceedings, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023-II),* October 26, 2023, Kyiv, 2023, Vol. 3550, P. 167-180.

16. Smirnov O., Sydorenko V., Aleksander M., Zhyharevych O., Yenchev S. Simulation of the cloud IoT-based monitoring system for critical infrastructures. *CEUR Workshop Proceedings, Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022)*, November 30, 2022, Kyiv, 2023, Vol. 3530, P. 256-265.

17. Gnatyuk S., Sydorenko V., Yudin O., Zhyharevych O., Polozhentsev A. Method for Calculating the Criticality Level of Sectoral Information and Telecommunication Systems. *CEUR Workshop Proceedings*, Proceedings of the: Information Technology and Implementation (IT&I2022), November 30 - December 02, 2022, Kyiv, Ukraine, Vol. 3347, Paper 20, P.234-245.

18. Melnyk V., Bahnyuk N., Melnyk K., Zhyharevych O., Panasyuk N. Implementation of the simplified communication mechanism in the cloud of high performance computations. *East-European journal of Enterprise Technologies*. Kharkiv, 2017. No 2/2/86. P. 24-32.

19. Melnyk V., Pekh P., Melnyk K., Bahnyuk N., Zhyharevych O. Design and implementation of interdomain communication mechanism for high performance data processing, *East-European journal of Enterprise Technologies*. Kharkiv, 2016. No 1(9). P. 10-15.

20. Сидоренко В., Положенцев А., Юдін О., Жигаревич О. Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем. *ABIA-2023:* XVI міжнар. наук.-техніч. конф., 18-20 квітня 2023 р.: тези доп., Київ: НАУ, 2023. С. 16.14-16.17.

21. Здолбіцька Н.В., Ліщина Н.М., Лавренчук С.В., Давиденко Н.В., Жигаревич О.К. Інтелектуальна інформаційна система «робот-гід». Матеріали Міжнародної наукової молодіжної школи *«Системи та засоби штучного інтелекту»* 28.11.2021р. Київ, 2021. С. 19-21.

22. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи». *Кіберзахист особи, суспільства і держави*: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

АНОТАЦІЯ

Жигаревич О.К. Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». – Державний університет «Київський авіаційний інститут», Київ, 2026.

Дисертаційна робота присвячена розв'язанню актуальної науково-технічної задачі розроблення системи корелювання подій та управління ІТ-інцидентами на ОКІ. В роботі проведено аналіз сучасних підходів до управління ІТ-інцидентами на ОКІ для виявлення їх переваг та недоліків. Проведений аналіз дозволив формалізувати завдання дисертаційного дослідження щодо розробки і вдосконалення системи корелювання подій та управління ІТ-інцидентами на ОКІ. Удосконалено структурно-аналітичну модель оброблення даних, яка дозволяє підвищити ефективність виявлення аномалій в хмарних ІКС. Крім того, на основі дата сету NSL-KDD навчено нейронну мережу з точки зору виявлення аномалій типу DoS, U2R, R2L та Probe. Розроблено модель онтологіко-реляційного сховища даних, яка дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації. Крім того, створено методику, яка дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних, проводити масштабування, агрегацію, аналіз, збір закономірностей та забезпечувати високу швидкість пошуку. Удосконалено модель інтеграційної шини даних, яка дозволяє розподілити навантаження на послуги та гарантує безпеку обміну даними для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами. На основі розробленої моделі було сформовано відповідну специфікацію реалізації SIEM-систем на ОКІ, у вигляді основних та додаткових вимог. Отримала подальший розвиток система корелювання подій та управління ІТ-інцидентами на ОКІ, яка дала змогу формалізувати інформаційну технологію, що реалізує процеси управління ІТ-інцидентами на ОКІ згідно вимог міжнародних стандартів та найкращих світових практик щодо створення систем управління ІТ-інцидентами. Також, розроблено і впроваджено спеціальний програмний застосунок, який можна використовувати для управління інцидентами, які виникають в КІ і мають вплив на КВР. Результати дисертації впроваджені і використовуються у діяльності ТОВ «AxxonSoft», НДЛ протидії кіберзагрозам авіаційної галузі КАІ, а також у навчальному процесі кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки для підвищення ефективності підготовки фахівців з ІТ.

Ключові слова: ІТ-інцидент, критична інфраструктура, об'єкти критичної інфраструктури, інформаційний об'єкт, виявлення аномалій, виявлення вразливостей, види аномалій, хмарні системи, онтологія, підтримка рішень, SIEM, система корелювання подій та управління ІТ-інцидентами.

ABSTRACT

Zhyharevych O. System for events correlation and IT-incident management in critical infrastructure objects. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.06 «Information technologies». – State University «Kyiv Aviation Institute», Kyiv, 2026.

The dissertation is devoted to solving an actual scientific and technical problem of developing an event correlation and IT incident management system for critical infrastructure facilities. An analysis of modern approaches to IT incident management at critical infrastructure facilities (CIF) was carried out in order to identify their advantages and disadvantages. Based on the analysis of approaches to anomaly detection in cloud environments, it was established that the common goal of existing studies is the rapid identification of anomalies while reducing the level of misclassification. The analysis of modern database types used in SIEM systems showed that each type remains relevant within its specific application domain, where data relationships are determined by the particular DBMS structure, while the use of a single database for all such tasks does not meet

architectural and security requirements. In addition, existing data integration bus solutions available on the market were analyzed, and it was determined that each of them has specific features and significant differences that define their areas of application, functionality, configuration options, and licensing costs. Furthermore, a detailed analysis of 16 SIEM systems was systematized and presented based on 18 proposed criteria. The conducted analysis made it possible to formalize the objectives of the dissertation research aimed at the development and improvement of an event correlation and IT incident management system for CIF.

A structural and analytical data processing model was improved, which, due to the formulation of control commands for transmission to an ICT software client and additional processing of metadata in a cloud system, increases the efficiency of anomaly detection in cloud-based information and communication systems. Experimental studies of the model made it possible to evaluate the temporal characteristics of processing a single metadata element and to develop control commands. A distinctive feature of the model is the consideration of the need to generate control transmission commands to the ICS software client, which overall increased the accuracy of temporal characteristic estimation by up to 1.7 times and distortion (latency) characteristics by up to 4.5 times. In addition, a neural network was trained on the NSL-KDD dataset to detect anomalies of the DoS, U2R, R2L, and Probe types.

A model of an ontological-relational data storage was developed, which, through preliminary indexing and the synthesis of two different databases (Elasticsearch and MongoDB) with appropriate characteristics, improves data storage and classification convenience and ensures high-speed search and retrieval of large volumes of information. Moreover, a methodology was developed that enables the indexing service to access external data repositories, perform scaling, aggregation, analysis, pattern extraction, and ensure high search performance.

The data integration bus model was improved through the decomposition of service functionality, where each service is responsible for a specific task and can operate independently, as well as through the definition of service criticality levels. This approach allows load distribution among services and guarantees secure data exchange for the effective functioning of the event correlation and IT incident management system. Based on the developed model, a corresponding specification for the implementation of SIEM systems at CIF was formed in the form of basic and additional requirements.

The event correlation and IT incident management system has been further developed, which, through the use of developed data processing models, an ontological-relational data warehouse, and a data integration bus, allows for the formalization of information technology that implements IT incident management processes at CIF in accordance with the requirements of international standards and best global practices for creating IT incident management systems. In addition, a special software application has been developed that can be used to manage IT incidents that occur in the CI and have an impact on CIR (critically important resources).

Based on the proposed methodology and the developed specialized software application, experimental studies were conducted and the models and system obtained in the research were verified. The results of the dissertation have been implemented and are used in the activities of AxxonSoft LLC, of the Research Laboratory for Counteracting Cyber Threats in the Aviation Industry at KAI, as well as in the educational process of the Department of Computer Science and Cybersecurity at Lesya Ukrainka Volyn National University to improve the effectiveness of IT specialist training.

Keywords: IT incident, critical infrastructure, critical infrastructure objects, information object, anomaly detection, vulnerability detection, types of anomalies, cloud systems, ontology, decision support, SIEM, event correlation system and IT incident management.