ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента
завідувача кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка
Складанного Павла Миколайовича
на дисертаційну роботу Жигаревич Оксани Костянтинівни
на тему «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології»

1. Актуальність теми та мета дослідження

В умовах цифрової трансформації суспільства та широкого впровадження інформаційно-комунікаційних систем (ІКС) у різні сфери діяльності особливого значення набувають питання забезпечення їх безпеки та безперервності функціонування. Особливо це стосується об'єктів критичної інфраструктури (ОКІ), порушення роботи яких може призвести до значних соціально-економічних наслідків, дестабілізації функціонування держави та виникнення масштабних ІТ-інцидентів.

Одним із ключових засобів забезпечення інформаційної безпеки ІКС є використання SIEM-систем, що забезпечують збирання, зберігання, аналіз та корелювання подій безпеки, а також підтримують процеси управління ІТ-інцидентами. Водночас аналіз сучасних підходів показує, що існуючі рішення не завжди повною мірою забезпечують ефективне оброблення великих потоків подій, інтеграцію різнорідних джерел даних, масштабованість та своєчасне реагування на інциденти в умовах функціонування ОКІ.

У зв'язку з цим актуальним є розроблення нових моделей та системи корелювання подій і управління ІТ-інцидентами, що забезпечують ефективну інтеграцію даних, їх оброблення та підтримку прийняття рішень у процесі реагування на інциденти.

Саме вирішенню зазначених задач присвячена дисертаційна робота Жигаревич Оксани Костянтинівни «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», що визначає її актуальність і практичну значущість.

Метою дисертаційної роботи є забезпечення можливості ефективного управління ІТ-інцидентами на ОКІ на основі розроблення та удосконалення моделей і синтезу системи корелювання подій та управління інцидентами.

Для досягнення поставленої мети авторкою було вирішено такі основні задачі:

–проведено аналіз сучасних підходів до управління ІТ-інцидентами на ОКІ;

– удосконалено структурно-аналітичну модель оброблення даних для підвищення ефективності виявлення аномалій у хмарних ІКС;

– розроблено модель онтологіко-реляційного сховища даних для забезпечення ефективного зберігання та оброблення інформації;

– удосконалено модель інтеграційної шини даних для оптимального розподілу навантаження між сервісами;

– розроблено систему корелювання подій та управління ІТ-інцидентами на ОКІ;

– розроблено програмне забезпечення та проведено експериментальне дослідження запропонованих моделей і системи.

Таким чином, актуальність теми дисертаційної роботи не викликає сумнівів, оскільки вона зумовлена як теоретичною потребою розвитку інформаційних технологій управління ІТ-інцидентами, так і практичною необхідністю підвищення рівня захищеності ОКІ.

2. Ступінь обґрунтованості наукових положень, їх достовірність та новизна

У дисертаційній роботі Жигаревич Оксани Костянтинівни простежується цілісна концепція дослідження, що поєднує аналітичний огляд сучасних підходів, математичне моделювання процесів оброблення даних, розроблення програмних рішень та їх експериментальну перевірку. Це дозволило обґрунтувати низку наукових положень, які відзначаються новизною та підтвердженою достовірністю.

Наукова новизна дисертаційної роботи полягає у такому:

1. 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;

2. 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;

3. 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;

4. 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.

Обґрунтованість і достовірність результатів:

– розроблені моделі побудовані на основі сучасних методів математичного моделювання, системного аналізу та теорії множин, що забезпечує їх теоретичну коректність;

– результати дослідження отримано з використанням методів штучного інтелекту та аналізу даних, що дозволяє підвищити ефективність виявлення аномалій у хмарних ІКС;

– експериментальні дослідження проведено із застосуванням набору даних NSL-KDD та засобів імітаційного моделювання, що охоплюють різні сценарії функціонування системи;

– розроблені моделі та система реалізовані програмно і перевірені в експериментальному середовищі, що підтверджує їх працездатність та ефективність;

– результати дослідження апробовано у наукових публікаціях і впроваджено у практичну діяльність ТОВ «AxxonSoft», НДЛ протидії кіберзагрозам авіаційної галузі КАІ та у навчальний процес закладів вищої освіти, що підтверджено відповідними актами впровадження.

Сукупність отриманих наукових результатів свідчить про вагомий внесок здобувачки у розвиток інформаційних технологій, пов’язаних із корелюванням подій та управлінням ІТ-інцидентами в ІКС. Дисертаційна робота має як теоретичне, так і практичне значення, а її результати можуть бути використані при створенні та вдосконаленні SIEM-систем, а також для підвищення рівня захищеності ОКІ і підготовки фахівців у галузі інформаційних технологій.

3. Оцінка змісту дисертації, її завершеності, дотримання принципів академічної доброчесності

Зміст дисертаційної роботи Жигаревич Оксани Костянтинівни відзначається цілісністю, логічною послідовністю та науковою глибиною. Усі чотири основні розділи виконують чітко визначені функції, що в сукупності формують завершену концепцію дослідження.

У *першому розділі* проведено ґрунтовний аналіз сучасних підходів до управління IT-інцидентами, виявлення аномалій у хмарних середовищах, типів баз даних та інтеграційних шин даних. Особливу увагу приділено дослідженню існуючих SIEM-систем, їх функціональним можливостям, перевагам і недолікам, що дозволило обґрунтувати необхідність розроблення нових моделей та системи корелювання подій і управління IT-інцидентами.

У *другому розділі* розроблено та удосконалено математичні моделі, зокрема структурно-аналітичну модель оброблення даних та модель онтологіко-реляційного сховища даних. Запропоновано підхід до інтеграції реляційних і нереляційних баз даних, що забезпечує ефективне зберігання та оброблення інформації у SIEM-системах.

У *третьому розділі* удосконалено модель інтеграційної шини даних, яка забезпечує ефективний обмін даними між компонентами системи, а також розроблено систему корелювання подій та управління IT-інцидентами на ОКІ. Описано архітектуру системи та принципи її функціонування.

У *четвертому розділі* наведено результати експериментальних досліджень, що підтверджують ефективність запропонованих моделей та системи. Проведено оцінювання часових характеристик оброблення даних, а також досліджено ефективність виявлення аномалій і управління IT-інцидентами.

Завершеність дисертаційного дослідження підтверджується тим, що всі розділи логічно взаємопов’язані: від аналізу сучасних підходів і постановки задачі – через розроблення математичних моделей та системи – до їх програмної реалізації та експериментальної перевірки. Отримані результати узгоджуються з поставленими задачами, що свідчить про системний характер проведеного дослідження.

Щодо дотримання принципів академічної доброчесності, слід зазначити, що дисертаційна робота відповідає встановленим вимогам. Авторка коректно використовує наукові джерела, наводить необхідні посилання, чітко відокремлює власні результати від запозичених. Наявність наукових публікацій та актів

впровадження підтверджує самостійність, доброчесність і належний рівень виконаного дослідження.

4. Оприлюднення результатів дисертаційної роботи

Результати дисертаційного дослідження Жигаревич Оксани Костянтинівни отримали належне висвітлення у фаховій науковій літературі та пройшли апробацію у вітчизняному й міжнародному науковому середовищі.

Основні положення дисертаційної роботи опубліковані у наукових фахових виданнях України, що свідчить про їх відповідність встановленим вимогам. Крім того, результати дослідження оприлюднено у виданнях, що індексуються міжнародними наукометричними базами даних, зокрема Scopus, що підтверджує їх наукове визнання та актуальність у міжнародному науковому просторі.

Окремі результати дослідження апробовано на міжнародних та всеукраїнських науково-практичних конференціях, що дало можливість представити отримані наукові результати, обговорити їх із фахівцями та отримати відповідні наукові оцінки.

Публікації авторки відображають основні результати дисертаційної роботи та охоплюють різні етапи дослідження – від аналізу проблематики до розроблення моделей, системи та їх експериментальної перевірки, що свідчить про повноту оприлюднення результатів і високий рівень їх наукової апробації.

Загалом за темою дисертації опубліковано 22 наукові праці, серед яких:

– 8 статей у вітчизняних фахових наукових журналах;

– 11 статей у закордонних рецензованих виданнях, що індексуються у наукометричній базі даних Scopus;

– 3 публікації у матеріалах і тезах доповідей на конференціях.

Рівень оприлюднення наукових результатів повністю відповідає сучасним вимогам до дисертаційних робіт і підтверджує завершеність та системний характер проведеного дослідження.

5. Дискусійні питання та зауваження щодо змісту дисертаційної роботи і її окремих положень

Дисертаційна робота Жигаревич Оксани Костянтинівни справляє загалом позитивне враження завдяки чіткості структури, логічності викладення та високому рівню опрацювання матеріалу, проте окремі положення потребують уточнення та можуть бути предметом подальших досліджень.

1) У підрозділі 1.5, де наведено аналіз сучасних SIEM-систем, доцільно було б доповнити порівняльну оцінку з урахуванням практичних аспектів їх впровадження на ОКІ, зокрема показників продуктивності, вартості впровадження та складності інтеграції з існуючими ІКС.

2) У підрозділі 2.1, присвяченому структурно-аналітичній моделі оброблення даних, математичний опис моделі подано достатньо стисло, що ускладнює відтворення окремих етапів її реалізації. Доцільним було б більш детально представити послідовність виконання обчислювальних процедур та алгоритмічну реалізацію моделі.

3) У підрозділі 3.1, де розглядається модель інтеграційної шини даних, доцільно було б розширити опис оцінювання впливу рівня критичності сервісів на ефективність функціонування системи, зокрема з урахуванням змін навантаження та можливих відмов окремих компонентів.

4) У підрозділах 4.1-4.4, де наведено результати експериментальних досліджень, доцільно було б доповнити аналіз порівнянням отриманих результатів із існуючими підходами або аналогічними рішеннями, що дозволило б більш повно обґрунтувати переваги запропонованих моделей та системи.

5) У тексті дисертації зустрічаються окремі стилістичні та термінологічні неточності, зокрема у використанні англомовних термінів та їх транслітерації, а також окремі перевантажені синтаксичні конструкції, що не впливають на зміст роботи, проте потребують редакційного доопрацювання.

6. Висновки по дисертаційній роботі

Дисертаційна робота Жигаревич Оксани Костянтинівни на тему «Система корелювання подій та управління ІТ-інцидентами на об’єктах критичної інфраструктури» присвячена вирішенню актуальної науково-технічної задачі забезпечення ефективного управління ІТ-інцидентами в ІКС, зокрема на ОКІ.

У роботі вирішено важливе науково-практичне завдання, що полягає у розробленні та удосконаленні моделей оброблення даних, онтологіко-реляційного сховища даних та інтеграційної шини даних, а також у створенні системи корелювання подій та управління ІТ-інцидентами, яка забезпечує підвищення ефективності оброблення, аналізу та використання даних безпеки.

Достовірність отриманих результатів підтверджується використанням сучасного математичного апарату, проведенням експериментальних досліджень, а також впровадженням результатів у практичну діяльність.

За актуальністю теми, науковою новизною, обґрунтованістю та практичною значущістю отриманих результатів дисертаційна робота відповідає вимогам, що висуваються до кандидатських дисертацій за спеціальністю 05.13.06 «Інформаційні технології».

Дисертаційна робота Жигаревич О.К. за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів відповідає спеціальності 05.13.06 – «Інформаційні технології» та вимогам нормативних документів МОН України до кандидатських дисертацій (зокрема пп. 9, 11, 12, 13, 14 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 зі змінами і доповненнями).

Здобувачка Жигаревич Оксана Костянтинівна заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології».

Офіційний опонент:
кандидат технічних наук, доцент
завідувач кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київського столичного
університету імені Бориса Грінченка Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС П. Складанного ЗАСВІДЧУЮ
(ПІБ)
Провідний фахівець відділу
(посада)
Данилова О.