ВІДГУК

ОФІЦІЙНОГО ОПОНЕНТА

професора кафедри інженерії програмного забезпечення та кібербезпеки
Державного торговельно-економічного університету,
доктора технічних наук, професора ЦЮЦЮРИ Миколи Ігоровича
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»

Актуальність теми та мета дослідження

Сучасні інформаційно-комунікаційні системи характеризуються високим рівнем складності, динамічності та взаємозалежності їх компонентів, що особливо проявляється в умовах функціонування об'єктів критичної інфраструктури. У таких умовах навіть незначні порушення або інциденти інформаційної безпеки можуть призводити до суттєвих соціально-економічних наслідків.

Значна роль у забезпеченні безпеки та стабільності функціонування таких систем належить засобам централізованого моніторингу та аналізу подій, зокрема SIEM-системам. Однак існуючі рішення не завжди забезпечують ефективну обробку великих обсягів подій, інтеграцію різнорідних джерел даних та оперативне реагування на інциденти в умовах функціонування об'єктів критичної інфраструктури.

У зв'язку з цим актуальним є розвиток підходів до побудови систем корелювання подій та управління ІТ-інцидентами, які забезпечують підвищення ефективності аналізу подій безпеки, своєчасне виявлення інцидентів та підтримку процесів прийняття рішень.

Метою дисертаційної роботи є підвищення ефективності управління ІТ-інцидентами на об'єктах критичної інфраструктури шляхом розроблення та удосконалення моделей оброблення даних і створення системи корелювання подій.

Ступінь обґрунтованості наукових положень, їх достовірність та новизна

Наукові положення, висновки та рекомендації, сформульовані у дисертаційній роботі Жигаревич Оксани Костянтинівни, ґрунтуються на комплексному підході, що поєднує аналітичний огляд сучасних підходів до управління ІТ-інцидентами, побудову математичних моделей оброблення даних, розроблення архітектурних рішень та їх експериментальну перевірку. Така багаторівнева методологія забезпечує високий рівень обґрунтованості одержаних результатів.

Насамперед слід відзначити, що теоретичні положення роботи підтверджені використанням сучасного математичного апарату. У дисертації послідовно формалізовано процеси оброблення та корелювання подій безпеки в інформаційно-комунікаційних системах, з урахуванням особливостей їх функціонування в умовах критичної інфраструктури. Запропоновані моделі дозволяють оцінювати ефективність оброблення даних, виявлення аномалій та управління ІТ-інцидентами з урахуванням різних факторів, що впливають на роботу системи.

Достовірність результатів підтверджується проведенням експериментальних досліджень із використанням імітаційного моделювання та тестових наборів даних. У роботі наведено результати досліджень у різних сценаріях функціонування системи, що дозволяє оцінити її ефективність в умовах змінного навантаження та різних типів інцидентів. Отримані результати підтверджують підвищення ефективності оброблення подій безпеки та своєчасності реагування на ІТ-інциденти.

Важливим підтвердженням наукової достовірності є апробація результатів дослідження у реальних умовах, зокрема у навчальному процесі та у співпраці з підприємствами, що підтверджено відповідними актами впровадження. Це свідчить про можливість практичного застосування запропонованих моделей і системи.

Щодо наукової новизни, то вона проявляється на кількох рівнях:

– удосконалено структурно-аналітичну модель оброблення даних, що дозволяє підвищити ефективність виявлення аномалій у хмарних інформаційно-комунікаційних системах;

– розроблено модель онтологіко-реляційного сховища даних, яка забезпечує ефективне поєднання реляційних і нереляційних підходів до зберігання та оброблення інформації;

– удосконалено модель інтеграційної шини даних із урахуванням критичності сервісів та їх взаємодії;

– подальшого розвитку набула система корелювання подій та управління ІТ-інцидентами, що забезпечує підвищення ефективності аналізу та використання даних безпеки.

Таким чином, можна стверджувати, що наукові положення, викладені у дисертації, є логічно обґрунтованими, теоретично коректними та експериментально підтвердженими.

Достовірність результатів забезпечується поєднанням аналітичного, математичного та експериментального рівнів дослідження.

Новизна роботи не викликає сумнівів, оскільки запропоновані рішення розширюють існуючі підходи до побудови систем корелювання подій та управління ІТ-інцидентами і створюють основу для подальшого розвитку як теоретичних, так і прикладних досліджень у цій сфері.

Оцінка змісту дисертації, її завершеності, дотримання принципів академічної доброчесності

Дисертаційна робота Жигаревич Оксани Костянтинівни складається зі вступу, чотирьох основних розділів, висновків, списку використаних джерел та додатків.

Зміст дисертації свідчить про завершеність проведеного дослідження. У роботі визначено мету та завдання, сформовано методологічну основу,

розроблено математичні моделі, запропоновано архітектурні та програмні рішення, а також здійснено їх експериментальну перевірку. Кожний розділ логічно пов’язаний із попереднім та послідовно розкриває етапи дослідження:

– у першому розділі проведено аналіз сучасних підходів до управління IT-інцидентами, досліджено особливості SIEM-систем та обґрунтовано постановку задачі дослідження;

– у другому розділі розроблено та удосконалено математичні моделі оброблення даних і організації їх зберігання;

– у третьому розділі запропоновано модель інтеграційної шини даних та розроблено систему корелювання подій і управління IT-інцидентами;

– у четвертому розділі наведено результати експериментальних досліджень та оцінювання ефективності запропонованих рішень.

Таким чином, дисертаційна робота є логічно завершеним дослідженням, у якому послідовно розкрито шлях від аналізу предметної області до розроблення моделей, створення системи та підтвердження її ефективності.

Особливо слід відзначити поєднання у роботі теоретичного та прикладного аспектів. З одного боку, авторкою розроблено математичні моделі та обґрунтовано їх коректність, з іншого – результати дослідження реалізовано у вигляді програмної системи та перевірено в експериментальних і практичних умовах. Такий підхід свідчить про високий рівень наукової та практичної підготовки здобувачки.

Щодо дотримання принципів академічної доброчесності, слід зазначити, що дисертаційна робота відповідає встановленим вимогам: використані літературні джерела належним чином опрацьовані, у тексті наведено відповідні посилання, результати попередніх досліджень коректно відмежовані від авторських напрацювань. У роботі відсутні ознаки плагіату або некоректного використання чужих матеріалів, а здобувачка чітко формулює власний внесок у розвиток досліджуваного напряму.

Мова і стиль дисертації загалом відповідають академічним стандартам, текст викладено з використанням сучасної наукової термінології. Разом з тим, окремі фрагменти роботи містять складні конструкції та значну кількість технічних деталей, що дещо ускладнює сприйняття матеріалу, однак це не знижує загального рівня виконаної роботи.

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.

Апробацію результатів здійснено на міжнародних і всеукраїнських наукових конференціях, зокрема:

– «Cybersecurity Providing in Information and Telecommunication Systems» (CPITS) (Київ, 2023–2024),

– «International Conference on Dependable Systems, Services and Technologies» (DESSERT-2024) (Афіни, Греція, 2023),

– «International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS-2023) (Дортмунд, Німеччина, 2023),

– «International Conference on Conflict Management in Global Information Networks» (CMiGiN) (Київ, 2022, 2025),

– «Information Technology and Implementation» (IT&I) (Київ, 2022),

– а також на інших науково-практичних конференціях, присвячених питанням інформаційних технологій, оброблення даних та управління IT-інцидентами.

Основні положення дисертації оприлюднено у наукових публікаціях, серед яких значну частину становлять статті у закордонних рецензованих виданнях, що

індексуються у наукометричній базі даних Scopus, а також у вітчизняних фахових наукових журналах.

Загалом за темою дисертації опубліковано 22 наукові праці, у тому числі 19 наукових статей, серед яких 11 – у закордонних рецензованих виданнях, що входять до наукометричної бази даних Scopus, 8 – у вітчизняних фахових наукових журналах, а також 3 публікації у матеріалах і тезах доповідей на конференціях.

Рівень оприлюднення результатів дисертаційного дослідження відповідає вимогам до кандидатських дисертацій і підтверджує повноту їх висвітлення та завершеність проведеного дослідження.

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

Як і будь-яке складне наукове дослідження, дисертаційна робота Жигаревич Оксани Костянтинівни не позбавлена окремих дискусійних моментів, які не знижують її загальної наукової та практичної цінності, проте можуть бути предметом подальших досліджень і уточнень.

1. У підрозділі 1.5, присвяченому аналізу сучасних SIEM-систем, доцільним є більш детальне обґрунтування вибору та вагомості використаних критеріїв оцінювання, а також розгляд можливості їх адаптації до різних класів інформаційно-комунікаційних систем.

2. У розділі 2 при побудові моделей оброблення даних не в повній мірі розкрито питання масштабованості запропонованих рішень, що не дозволяє оцінити їх ефективність при обробленні великих обсягів даних.

3. У розділі 3, де розглядається модель інтеграційної шини даних та система корелювання подій, потребує додаткового висвітлення питання взаємодії запропонованої системи з існуючими IT-інфраструктурами та стандартами інтеграції, а також формалізація критеріїв визначення критичності сервісів.

4. У розділах, присвячених опису моделей та системи, доцільним є розширений розгляд питання узагальнення запропонованих рішень для різних класів інформаційно-комунікаційних систем, а також визначення меж їх застосування залежно від умов функціонування та характеристик середовища.

5. У розділі 4 не наведено результатів експериментальних досліджень із використанням альтернативних сучасних наборів даних, що обмежує узагальненість та універсальність отриманих результатів.

6. У роботі доцільним було б висвітлити кількісну оцінку відмовостійкості та надійності функціонування системи корелювання подій та управління ІТ-інцидентами в умовах збоїв або часткової недоступності окремих компонентів, що дозволило б більш повно оцінити її ефективність.

Наведені зауваження мають дискусійний характер і не впливають на загальну позитивну оцінку дисертаційної роботи, а лише окреслюють можливі напрями подальших досліджень.

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 інформаційно-комунікаційних системах, зокрема на об’єктах критичної інфраструктури.

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 коректним застосуванням сучасного математичного апарату, проведенням

експериментальних досліджень, а також апробацією результатів і їх впровадженням у практичну діяльність.

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:
доктор технічних наук, професор
професор кафедри інженерії
програмного забезпечення та кібербезпеки
Державного торговельно-
економічного університету Микола ЦЮЦЮРА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
44470624

Підпис Цюцюри засвідчую
Начальник відділу кадрів
Н. Шевченко