Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0426U000095

Особливі позначки: відкрита

Дата реєстрації: 04-05-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Жигаревич Оксана Костянтинівна
2. Oksana Zhyharevych

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-7154-9733

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.06

Назва наукової спеціальності: Інформаційні технології

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 28-05-2026

Спеціальність за освітою: «Програмне забезпечення автоматизованих систем»

Місце роботи здобувача: Волинський національний університет імені Лесі Українки

Код за ЄДРПОУ: 02125102

Місцезнаходження: проспект Волі, Луцьк, Луцький р-н., 43025, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.062.01

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.39.17, 50.41.27

Тема дисертації:

1. Система корелювання подій та управління ІТ-інцидентами на об’єктах критичної інфраструктури

2. System for events correlation and IT-incident management in critical infrastructure objects

Реферат:

1. Сучасна інформаційна інфраструктура критичних об’єктів характеризується складністю, розподіленістю та потребує постійного моніторингу кіберзагроз і оперативного реагування на інциденти. Порушення функціонування об’єктів критичної інфраструктури може призводити до значних технічних, економічних і безпекових наслідків. Одним із перспективних засобів підвищення цифрової стійкості ІКС є використання SIEM-систем для збирання, аналізу та корелювання подій безпеки, однак існуючі рішення не повною мірою забезпечують ефективне управління ІТ-інцидентами на ОКІ та потребують подальшого розвитку моделей, методів і системних засобів. У зв’язку з цим розроблення системи корелювання подій та управління ІТ-інцидентами на об’єктах критичної інфраструктури є актуальною науково-технічною задачею. Метою дослідження є розроблення та удосконалення моделей і системи управління ІТ-інцидентами на об’єктах критичної інфраструктури. Об’єктом дослідження є процеси управління ІТ-інцидентами, предметом —

моделі, системи і засоби їх реалізації. У роботі проведено аналіз сучасних підходів до управління ІТ-інцидентами на об’єктах критичної інфраструктури, методів виявлення аномалій у хмарних середовищах, типів баз даних для SIEM-систем та рішень інтеграційних шин даних, що дозволило обґрунтувати вибір методів і сформулювати завдання дисертаційного дослідження. 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 полягає у можливості їх використання для забезпечення стійкого функціонування хмарної та критичної інформаційної інфраструктури в умовах деструктивних впливів. Практична цінність роботи полягає у навчанні нейронної мережі для виявлення аномалій, розробленні методики зберігання та класифікації даних, формуванні специфікації реалізації SIEM-систем на об’єктах критичної інфраструктури, а також створенні програмного застосунку для управління ІТ-інцидентами. Результати дослідження впроваджено 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.

2. Modern information infrastructure of critical facilities is characterized by complexity and distributed architecture and requires continuous monitoring of cyber threats and prompt incident response. Disruptions in the functioning of critical infrastructure facilities may lead to significant technical, economic, and security consequences. One of the promising means of improving the digital resilience of information and communication systems is the use of SIEM systems for collecting, analyzing, and correlating security events; however, existing solutions do not fully ensure effective IT incident management at critical infrastructure facilities and require further development of models, methods, and system tools. Therefore, the development of an event correlation and IT incident management system for critical infrastructure facilities is an urgent scientific and technical task. The purpose of the study is to develop and improve models and an IT incident management system for critical infrastructure facilities. The object of research is the processes of IT incident management at critical infrastructure facilities, while the subject of research includes models, systems, and means for their implementation. The study analyzes modern approaches to IT incident management at critical infrastructure facilities, anomaly detection methods in cloud environments, database types for SIEM systems, and data integration bus solutions, which made it possible to substantiate the choice of methods and formulate the objectives of the dissertation research. The scientific novelty of the obtained results lies in the following: – an improved structural-analytical data processing model has been developed that increases the efficiency of anomaly detection in cloud information and communication systems through control command generation, metadata processing, and intelligent signature detection; – for the first time, an ontology-relational data warehouse model

based on Elasticsearch and MongoDB has been developed to improve data storage, classification, and high-speed retrieval of large data volumes; – a data integration bus model has been improved through decomposition of service functionality and criticality assessment, ensuring load distribution and continuity of data exchange; – further development has been achieved for an event correlation and IT incident management system that formalizes an information technology for incident management in accordance with international standards and best global practices. The practical significance of the obtained results lies in the possibility of their application to ensure resilient functioning of cloud and critical information infrastructure under destructive information and technical impacts. The practical value of the work consists in training a neural network for anomaly detection, developing a methodology for data storage and classification, forming a specification for implementing SIEM systems at critical infrastructure facilities, and creating a software application for IT incident management. The research results have been implemented and are used in the activities of AxxonSoft LLC, the Research Laboratory for Countering Cyber Threats in Aviation of KAI, and in the educational process of the Department of Computer Science and Cybersecurity of Lesya Ukrainka Volyn National University. 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 and IT incident management system.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 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. DOI: https://doi.org/10.28925/2663-4023.2023.19.176196
- 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. DOI: https://doi.org/10.18372/2073-4751.75.18014
- 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. DOI: https://doi.org/10.18372/2073-4751.76.18236.
- 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. DOI: https://doi.org/10.28925/2663-4023.2022.16.2836.
- 5. Жигаревич О.К., Медведєв М.В. Інформаційна система «Студент-ФКНІТ» засобами PHP. Комп'терно-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'терно-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'терно-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'терно-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. URL: https://ceur-ws.org/Vol-4024/paper30.pdf. (Scopus) Q4, ISSN 1613-0073.
- 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. URL: https://ceur-ws.org/Vol-3654/paper29.pdf (Scopus) Q4, ISSN 1613-0073
- 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. DOI: https://doi.org/10.1007/978-3-031-62213-7_12. (Scopus) Q3, ISSN 2367-4512.
- 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. doi: 10.1109/DESSERT65323.2024.11122240. (Scopus), Q4.
- 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. DOI: 10.1109/IDAACS58523.2023.10348645. (Scopus), Q4, ISSN 2770-4262.
- 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. URL: https://ceur-ws.org/Vol-3421/short6.pdf (Scopus) Q4, ISSN 1613-0073.
- 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. URL: https://ceur-ws.org/Vol-3550/paper14.pdf (Scopus) Q4, ISSN 1613-0073.
- 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. URL: https://ceur-ws.org/Vol-3530/paper25.pdf (Scopus) Q4, ISSN 1613-0073.
- 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. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf (Scopus) Q4, ISSN 1613-0073.
- 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. DOI: 10.15587/1729-4061.2017.98896 (Scopus) Q3, ISSN 1729-3774.
- 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. DOI: 10.15587/1729-4061.2016.60629 (Scopus) Q3, ISSN 1729-

3774.

- 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.

Наукова (науково-технічна) продукція: розроблено: - структурно-аналітичну модель оброблення даних, - модель онтологіко-реляційного сховища даних, - модель інтеграційної шини даних, - систему корелювання подій та управління іт-інцидентами на окі.

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0125U000624

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Сидоренко Вікторія Миколаївна

2. Viktoriia Sydorenko

Кваліфікація: к. т. н., доцент, 21.05.01

Ідентифікатор ORCID ID: 0000-0002-5910-0837

Додаткова інформація:

Повне найменування юридичної особи: Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"

Код за ЄДРПОУ: 45853942

Місцезнаходження: просп. Гузара Любомира, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Цюцюра Микола Ігорович

2. Mykola I. Tsiutsiura

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0003-4713-7568

Додаткова інформація: ;https://scholar.google.com/citations?user=o-VsWrQAAAAJ&hl=uk

Повне найменування юридичної особи: Державний торговельно-економічний університет

Код за ЄДРПОУ: 44470624

Місцезнаходження: вул. Кіото, Київ, 02156, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович

2. Pavlo M. Skladannyi

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7775-6039

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 45307965

Місцезнаходження: вул. Бульварно-Кудрявська, Київ, 04053, Україна

Форма власності: Комунальна

Сфера управління: Держадміністрація

Ідентифікатор ROR:

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Гнатюк Сергій Олександрович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Гнатюк Сергій Олександрович
Відповідальний за підготовку облікових документів	Довженко Олена Андріївна
Реєстратор	Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна