Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002965

Особливі позначки: відкрита

Дата реєстрації: 02-09-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Положенцев Артем Анатолійович

2. Artem Polozhentsev

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерні науки

Дата захисту: 30-08-2024

Спеціальність за освітою: 125 Кібербезпека

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Разова спеціалізована вчена рада №6598

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, 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: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, 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: 50.41.25

Тема дисертації:

1. Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури

2. Methods and means of IT Incident Management at CriticalInformation Infrastructure Facilities.

Реферат:

1. Захист критичної інфраструктури від ІТ-загроз є нагальною потребою в сучасному цифровому світі, оскільки від цього залежить стабільність держави та суспільства. Розробка нових методів управління ІТ-інцидентами дозволить ефективно реагувати на загрози та забезпечити безперебійну роботу критично важливих систем. Метою дисертаційної роботи є удосконалення системи управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту. Об’єктом дослідження є процеси управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури. Предметом дослідження є методи та засоби управління інцидентами на об'єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту. Наукова новизна одержаних результатів полягає у наступному: – вперше розроблено метод управління ІТ-загрозами, який за рахунок синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції перспективної цінності, дає змогу ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для

оптимального розподілу ресурсів захисту критичної інфраструктури держави. – удосконалено метод визначення пріоритетів ІТ-інцидентів, який за рахунок представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації, дозволяє кількісно оцінити пріоритети ІТ-інцидентів та управляти ними для забезпечення необхідного рівня захисту життєво важливих інтересів громадян, суспільства, держави та правопорядку; – отримав подальшого розвитку метод оцінювання рівня захищеності, який за рахунок використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації, а також розроблених рекомендацій для оптимізації захисту дає змогу визначити стан захищеності об'єктів критичної інфраструктури (сектору/підсектору чи держави в цілому), а також управляти захистом зазначених об'єктів в умовах виникнення ІТ-інцидентів

2. Protecting critical infrastructure from IT threats is an urgent need in the modern digital world, as the stability of the state and society depends on it. The development of new IT incident management methods will allow for effective response to threats and ensure the uninterrupted operation of critical systems. The aim of the dissertation is to improve the IT incident management system at critical information infrastructure facilities under threat realization and limited protection resources. The object of research is the processes of IT incident management at critical information infrastructure facilities. The subject of research is the methods and tools for managing incidents at critical information infrastructure facilities under threat realization and limited protection resources. The scientific novelty of the obtained results is as follows: – For the first time, a method for managing IT threats has been developed, which, due to the synthesis of methods of multi-criteria decision-making, threat modeling, and the prospective value function, allows identifying, assessing, and prioritizing IT threats for the optimal allocation of resources for the protection of the state's critical infrastructure. – The method for determining the priorities of IT incidents has been improved, which, due to the presentation of hierarchical structures of elements of potential threats and the calculation of the probability of their implementation, allows for quantitative assessment of IT incident priorities and management thereof to ensure the necessary level of protection of the vital interests of citizens, society, the state, and law and order. – The method of assessing the level of protection has been further developed, which, due to the use of new IT security indicators and the level of digital transformation, as well as the developed recommendations for optimizing protection, allows determining the state of protection of critical infrastructure facilities (sector/subsector or the state as a whole), as well as manage the protection of these facilities in the event of IT incidents.

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: Нове вирішення актуального наукового завдання

Публікації:

- 1. Polozhentsev A., Fesenko A., Gnatyuk V, (2017) Method for CSIRT performance evaluation, Project interdyscyplinarny projektem XXI wieku, Tom 2 (263-269).
- 2. Положенцев А. А., Сидоренко В. М. Метод управління ІТ-загрозами на об'єктах критичної інформаційної інфраструктури. Наукоємні технології. 2024. Т. 2, № 62. С. 121–133.
- 3. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об'єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління. 2024. Т. 2. N°78. С. 68-80.
- 4. Сидоренко В.М., Положенцев А.А., Гнатюк С.О. Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави. Вісник інженерної академії України. 2017. № 42. С. 81–89.
- 5. 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.
- 6. Жигаревич О.К., Бердибаєв Р.Ш., Сидоренко В.М., Положенцев А.А., Кримська А.О. Модель онтоголіко-реляційного сховища даних для функціонування хмарної SIEM-системи. Проблеми інформатизації та управління. 2023. Т. 4. № 76. С. 17-27.
- 7. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N., Zhilkishbayeva, G. Method of cybersecurity level determining for the critical information infrastructure of the state. CEUR Workshop Proceedings. 2020. Vol. 2616. P. 332-341. URL: https://ceur-ws.org/Vol-2616/paper28.pdf
- 8. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Sotnichenko, Y. Experimental Cybersecurity Level Determination in the Civil Aviation Critical Infrastructure. IEEE International Conference on Problems of Infocommunications Science and Technology. 2021. P. 757-764. DOI: https://doi.org/10.1109/PICST51311.2020.9467987.
- 9. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., Polozhentsev, A. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. CEUR Workshop Proceedings, 2022. Vol. 3156. P. 390-399. URL: https://ceur-ws.org/Vol-3156/paper29.pdf
- 10. Polozhentsev, A., Gnatyuk, S., Berdibayev, R., Sydorenko, V., Zhyharevych, O. Novel Cyber Incident Management System for 5G-based Critical Infrastructures. IDAACS. 2023, P. 1037-1041. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348645.
- 11. Lutskyi, M., Sydorenko, V., Polozhentsev, A., Apenko, N., Sydorenko, S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. CEUR Workshop Proceedings. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf
- 12. Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., Brzhanov, R. Method of Forming the Functional Security Profile for the Sectoral Information and Telecommunication Systems. CEUR Workshop Proceedings. 2021. Vol. 3179. P. 272-283. URL: https://ceur-ws.org/Vol-3179/Paper_25.pdf
- 13. Yarotskiy, S., Sydorenko, V., Lelechenko, A., Kolisnyk, O., Polozhentsev, A. Method of Determining the Importance Factor of IT Security Projects Investment Attractiveness in Critical Infrastructures. CEUR Workshop Proceedings. 2023. Vol. 3550. P. 181-190. URL: https://ceur-ws.org/Vol-3550/paper15.pdf
- 14. 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. 2022. Vol. 3347. P. 234-245. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf
- 15. Gnatyuk, S., Sydorenko, V., Polozhentsev, A. Method for Cybersecurity Level Evaluation in the Civil Aviation Critical Infrastructure. Lecture Notes in Networks and Systems. 2023. Vol. 736. P. 206-218, DOI: https://doi.org/10.1007/978-3-031-38082-2_16.
- 16. 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. 2024. Vol. 3654. P. 343-354. URL: https://ceur-ws.org/Vol-3654/paper29.pdf
- 17. 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. 2023. Vol. 3421. P. 206-213. URL: https://ceur-ws.org/Vol-3421/short6.pdf
- 18. Lutskyi, M., Gnatyuk, S., Sydorenko, V., Yarotskiy, S., Polozhentsev, A. Study on the Evaluating the Degree of Investment Attractiveness of IT-Projects. DESSERT. 2023. P 1-7. DOI: https://doi.org/10.1109/DESSERT61349. 2023.10416440
- 19. Semenchenko, A., Gurkovskyi, V., Romanenko, Y., Sydorenko, V., Kudrenko, S., Polozhentsev, A. Ukraine on the Road to the European Digital Market: Status and Tools for Implementing the European Digital Economy and Society Index in Ukraine. CEUR Workshop Proceedings. 2022. Vol. 3296. P. 18-28. URL: https://ceur-ws.org/Vol-3296/paper2.pdf
- 20. Lutskyi, M., Gnatyuk, S., Verkhovets, O., Polozhentsev, A. Information Flows Formalization for BSD Family Operating Systems Security Against Unauthorized Investigation. Lecture Notes on Data Engineering and

Communications Technologies. 2023. Vol. 178. P. 235-246. DOI: https://doi.org/10.1007/978-3-031-35467-0_16.
- 21. Gnatyuk, S., Berdibayev, R., Sydorenko, V., Polozhentsev, A., Ryabyy, M. Enterprise Service Bus Construction in SOA Architecture for SIEM Implementation in Critical Information Infrastructure. CEUR Workshop Proceedings. 2022. Vol. 3288. P. 11-20. URL: https://ceur-ws.org/Vol-3288/paper2.pdf
- 22. Сидоренко В., Положенцев А., Юдін О., Жигаревич О. «Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем» АВІА-2023: XVI міжнар. наук.-техніч. конф., 18-20 квітня 2023 р.: тези доп., Київ: НАУ, 2023. С. 16.14-16.17.
- 23. 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.
- 24. А. Положенцев, В. Сидоренко, «Метод визначення рівня кібербезпеки об'єктів критичної інфраструктури держави», Матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів «ПОЛІТ-2018. Сучасні проблеми науки», м. Київ, 4-6 квітня 2018 р., с. 102-103, 2018.
- 25. С. Гнатюк, В. Сидоренко, А. Положенцев. «Визначення показників рівня кібербезпеки об'єктів критичної інфраструктури авіаційної галузі». Матеріали VII Всеукр. наук.-практ. конф. «Перспективні напрямки захисту інформації», 30 серпня-03 вересня 2021 р.: тези доп. – Одеса, 2021. – С. 150-153
- 26. Ж. Алімсеітова, А. Положенцев. «Аналіз підходів до визначення терміну «критична інфраструктура» у різних країнах світу». Матеріали VI Міжн. наук.-практ. конф. «ITSEC», 17-19 травня 2016.: тези доп. – Київ, 2021. С. 62.
- 27. А. Положенцев. «Методи ведення кібервійни як потенційна загроза критичним авіаційним інформаційним системам». Матеріали IV Всеукраїнської наук.-практ. конф. молодих учених і студентів з міжнародною участю «Проблеми та перспективи розвитку авіації та космонавтики». тези доп., 28-29 жовтня 2015. К. С. 106
- 28. А. Положенцев. «Поняття кібервійни та їх прояв у сучасному світі». Матеріали наук.-практ. конф."Перспективні напрями захисту інформації": тези доп., 7-8 вересня 2015р., Одеса. – С. 79-80.
- 29. . Положенцев. «Інформаційна війна». Матеріали XV Міжн. наук.-практ. конф. молодих учених і студентів «Політ. Сучасні проблеми науки»:, 8-9 квітня 2015р.: тези доп. міжнар. наук.-практ. конф. – К., 2015. – С. 139.
- 30. В.О. Гнатюк, А.А. Положенцев. «Метод оцінки ефективності роботи груп реагування на кіберінциденти». Матеріали II всеукр. наук.-пр. конф. «Перспективні напрями захисту інформації». – м. Одеса, 03-07 вересня 2016 р. – Одеса: ОНАЗ, 2016. – С. 56-58.

Наукова (науково-технічна) продукція: технології; програмні продукти, програмно-технологічна документація; аналітичні матеріали

Соціально-економічна спрямованість: підвищення стану захищеності критичної інформаційної інфраструктури шляхом розробки та вдосконалення методів управління іт-інцидентами та оцінки ризиків.

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Сидоренко Вікторія Миколаївна

2. Viktoria Sydorenko

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, 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. Мартинюк Ганна Вадимівна
2. Hanna Martyniuk

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Маріупольський державний університет

Код за ЄДРПОУ: 26593428

Місцезнаходження: пр. Повітряних Сил, буд. 31, Київ, 03037, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Охріменко Тетяна Олександрівна
2. Tetiana Okhrimenko

Кваліфікація: к. т. н., с.д., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Савченко Аліна Станіславівна
2. Alina Savchenko

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Одарченко Роман Сергійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні	Одарченко Роман Сергійович
Відповідальний за підготовку облікових документів	Довженко Олена Андріївна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна