Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U002732

Особливі позначки: відкрита

Дата реєстрації: 07-07-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Дженюк Наталія Володимирівна
2. Nataliia V. Dzheniuk

Кваліфікація:

Ідентифікатор ORCHID ID: 0000-0003-0758-7935

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 125 Кібербезпека (12 Інформаційні технології)

Дата захисту: 28-08-2025

Спеціальність за освітою: Електронні обчислювальні машини

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 10013

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

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

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56

Тема дисертації:

1. Моделі синтезу систем безпеки соціокіберфізичних систем
2. Models of the synthesis of security systems of socio-cyberphysical systems

Реферат:

1. Дисертаційна робота спрямована на розв’язання актуальної науково-технічної задачі – підвищення рівня захищеності інформаційних ресурсів соціокіберфізичних систем шляхом розробки та впровадження моделей та методів захищеності інформації соціокіберфізичних систем на основі побудови багатоконтурної системи захисту інформації. Метою дисертаційної роботи є розробка математичних моделей та методів захищеності інформації соціокіберфізичних систем на основі багатоконтурної системи захисту інформації, спрямованої на підвищення рівня захищеності інформаційних ресурсів. Об’єкт дослідження – процес забезпечення захисту інформації у соціокіберфізичних системах на основі моделі багатоконтурної системи

захисту інформації. Предмет дослідження – моделі синтезу систем безпеки соціокіберфізичних систем. За результатами дослідження отримано такі наукові результати: 1. Вперше запропоновано математичну модель функціонування системи безпеки соціокіберфізичних систем в умовах загроз з ознаками гібридності та синергізму, яка встановлює залежність між структурою соціокіберфізичної системи та стратегією поведінки зовнішнього середовища, яка відрізняється врахуванням ознак гібридності та синергізму цільових (змішаних) атак. 2. Вперше розроблено математичну модель безпеки інформаційних взаємодій у соціокіберфізичних системах на основі комплексного аналізу поведінки користувачів та інформаційних потоків, в якому враховується взаємодія соціальних, кібернетичних та фізичних компонентів системи. 3. Вперше розроблено метод проектування безперервного функціонування системи безпеки соціокіберфізичних систем, який забезпечує формалізований підхід до опису ризиків та загроз для інформаційних активів, який відрізняється можливістю здійснювати контроль рівня безпеки з необхідним рівнем послуг безпеки. 4. Удосконалено класифікатор загроз безпеці інформаційних ресурсів соціокіберфізичних систем на основі комплексного підходу, який поєднує аналіз мережевих вразливостей, соціальної інженерії та кіберфізичних атак, який відрізняється врахуванням рівня критичності загроз, їх зв'язку з компонентами безпеки та відповідними послугами захисту. 5. Набула подальшого розвитку концепція багатоконтурної безпеки соціокіберфізичних систем, в якій враховуються загрози внутрішнього та зовнішнього контурів за кожною з платформ (соціальні мережі, кіберпростір, кіберфізичні системи) з урахуванням форми власності елементів і технологій соціокіберфізичних систем. Практичне значення отриманих результатів: – розроблена модель функціонування системи безпеки, що пов'язує структуру соціокіберфізичної системи із стратегією поведінки зовнішнього середовища, показала існування оптимальної стратегії поведінки зовнішнього середовища та оптимальної первинної структури системи; – розроблена модель безпеки інформаційних взаємодій у соціокіберфізичних системах показала, що асинхронна взаємодія між агентами прискорює утворення стійких кластерів інформаційного впливу на 15–20% порівняно з синхронною; – практична реалізація розробленого методу проектування безперервного функціонування системи безпеки соціокіберфізичних систем дозволяє виявляти загрози у реальному часі та мінімізувати ризики їх впливу на функціонування системи. Найшвидше виявляються DDoS-атаки, SQL-ін'єкції, фішингові атаки та ботнети (1.2–1.4 сек), тоді як аномалії у промислових системах потребують більше часу на аналіз (2.0–2.3 сек) через складність обробки фізичних параметрів. Найвищу точність методів виявлення (99%) демонструють методи контролю промислових систем. Високий рівень точності (97–98%) мають методи розпізнавання голосових маніпуляцій та шифрувальників (ransomware), що підтверджує ефективність використання нейромереж та алгоритмів машинного навчання; – запропоноване удосконалення класифікатора загроз безпеки інформаційних ресурсів соціокіберфізичних систем (електронний доступ: http://skl.khpi.edu.ua) забезпечує можливість оперативної онлайн-оцінки загроз з урахуванням соціальних, кібернетичних та фізичних чинників. Це дозволяє визначати критичні вузли інфраструктури соціокіберфізичних систем, оцінювати потенціал превентивних заходів, а також формувати інтегральну оцінку поточного рівня захищеності системи в умовах динамічно змінюваного середовища. За результатами дослідження підтверджено практичну та теоретичну цінність розроблених моделей та методів, надано практичні рекомендації щодо їх застосування.

2. The dissertation aims at solving the actual scientific and technical problem: increasing the level of protection of information resources of socio-cyber-physical systems by developing and introducing models and methods of information security of socio-cyber-physical systems based on the construction of a multi-loop information protection system. The purpose of the dissertation is to develop mathematical models and methods of information security of socio-cyber-physical systems based on a multi-loop information protection system aimed at increasing the level of protection of information resources. The object of research is the process of ensuring information protection in socio-cyber-physical systems based on the model of a multi-loop information protection system. Subject of research – models for synthesizing security systems of socio-cyber-physical systems. The following scientific results were obtained as a result of the study: 1. For the first time, a mathematical model of the functioning of the security system of socio-cyber-physical systems in conditions of threats with signs of hybridity and synergism establishing a relationship between the structure of the socio-cyber-physical system and the

strategy of behavior of the external environment is distinguished by taking into account the signs of hybridity and synergism of target (mixed) attacks has been proposed. 2. For the first time, a mathematical model of security of information interactions in socio-cyber-physical systems on the basis of a comprehensive analysis of user behavior and information flows taking into account the interaction of social, cybernetic and physical components of the system has been developed. 3. For the first time, a method for designing the continuous functioning of the security system of socio-cyber-physical systems provides a formalized approach to describing risks and threats to information assets, characterized by the ability to control the level of security with the necessary level of security services has been developed. 4. The classification of threats to the security of information resources of socio-cyber-physical systems has been improved on the basis of an integrated approach that combines the analysis of network vulnerabilities, social engineering and cyber-physical attacks, which is distinguished by taking into account the level of criticality of threats, their connection with security components, relevant security services. 5. The concept of multi-loop security of socio-cyber-physical systems taking into account the threats of internal and external contours for each of the platforms (social networks, cyberspace, cyber-physical systems), taking into account the ownership of elements and technologies of socio-cyber-physical systems has been further developed. Practical significance of the results: – the developed model of the functioning of the security system connecting the structure of the socio-cyber-physical system with the strategy of behavior of the external environment showed the existence of an optimal strategy of behavior of the external environment and an optimal primary structure of the system; – the developed model of information interaction security in socio-cyber-physical systems showed that asynchronous interaction between agents accelerates the formation of stable clusters of information influence by 15-20% compared to synchronous; – practical implementation of the developed method of designing the continuous functioning of the security system of socio-cyber-physical systems allows us to identify threats in real time and minimize the risks of their impact on the functioning of the system. DDoS attacks, SQL injections, phishing attacks and botnets (1.2-1.4 seconds) are most quickly detected, while anomalies in industrial systems require more analysis time (2.0-2.3 seconds) due to the complexity of processing physical parameters. The highest accuracy of detection methods (99%) is demonstrated by methods for monitoring industrial systems. A high level of accuracy (97-98%) has methods of recognizing voice manipulations and ransomware, which confirms the effectiveness of using neural networks and machine learning algorithms; – the proposed improvement of the classification of threats to the security of information resources of socio-cyber-physical systems (electronic access: http://skl.khpi.edu.ua) provides the possibility of operational online assessment of threats, taking into account social, cybernetic and physical factors. This allows us to determine the critical nodes of the infrastructure of socio-cyber-physical systems, assess the potential of preventive measures, and also form an integral assessment of the current level of system security in a dynamically changing environment. By results of the study practical and theoretical value of the developed models and methods have been confirmed, practical recommendations for their application have been provided.

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:

- Дженюк Н.В. Методологічні основи захисту в соціокіберфізичних системах. Сучасний захист інформації, Київ: Державний університет інформаційно-комунікаційних технологій, 2024. 4(60), С. 16-29. DOI: 10.31673/2409-7292.2024.040002.
- Dzheniuk N., Yevseiev S., Milevskyi S., Voropay N., Korolov R. Sociocyberphysical system wireless air network topology synthesis model. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30 No. 1. P. 51-57.

DOI: 10.18372/2225-5036.30.18603.
- Захаржевський А.Г., Толкачов М.Ю., Дженюк Н.В., Погасій С.С., Глухов С.І. Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації. Київ: Державний університет інформаційно-комунікаційних технологій, 2024. № 1(57). С. 57–68. doi: 10.31673/2409-7292.2024.010007.
- Serkov O., Dzheniuk N., Kasilov O., Sokol G., Tolkachov M., Arutiunian D. Інтелектуальна безпровідна система зв'язку. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2024. Т. 3 (77). С. 206-210. doi: 10.26906/SUNZ.2024.3.206.
- Dzheniuk N., Yevseiev S., Lazurenko B., Serkov O., Kasilov O. A Method of Protecting Information in Cyberphysical Space. Advanced Information Systems. 2023. Vol. 7, N. 4. P. 80-85. doi: 10.20998/2522-9052.2023.4.11.
- Yevseiev S., Milov O., Dzheniuk N., Tolkachov M., Voitko T., Prygara M., Shpak O., Voropay N., Volkov A., & Lezik O. Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies. Kharkiv, 2023. 5(9 (125), P. 53–74. doi: 10.15587/1729-4061.2023.289467.
- Tolkachov M., Dzheniuk N., Yevseiev S., Lysetskyi Y., Shulha V., Grod I., Faraon S., Ivanchenko I., Pasko I., & Balagura D. Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, Kharkiv, 2024. 5(9 (131), P. 63–78. doi: 10.15587/1729-4061.2024.313158.
- Serkov A., Jammine A., Kudii D., Dzheniuk N., Nait-Abdesselam Farid, Lazurenko B. Security Models and Methods of Socio-Cyberphysical Systems. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). Ankara: IEEE, 2023. Paper ID 105. doi: 10.1109/ismsit58785.2023.10304955.
- Dzheniuk N., Milevskyi S., Lazurenko B., Serkov A., Zakharzhevskyi A. Sociocyberphysical Security Systems Synthesis Models. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). Ankara: IEEE, 2023. Paper ID 111. doi: 10.1109/ISMSIT58785.2023.10304965.
- Толкачов М. Ю., Дженюк Н. В. Підхід до побудови систем безпеки корпоративної мережі. XI Наукова конференція «Наукові підсумки 2022 року». Харків, Україна, 2022. С. 18. e-ISBN 978-617-7319-62-6
- Дженюк Н.В., Толкачов М.Ю. Формування класифікатора загроз на основі комплексування із загрозами методів соціальної інженерії. VII Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення. 1 листопада 2023 р. Кропивницький: ЦНТУ, 2023. 135 с. (С. 21)
- Дженюк Н.В., Воропай Н.І., Король О.Г., Стрельнікова А.Ю. Модель безпеки соціокіберфізичної системи. Міжнародна науково-практична конференція «Виклики і загрози для критичної інфраструктури». Київ, Україна, 2023. С. 16-18.
- Толкачов М.Ю., Дженюк Н.В. Побудова багатоконтурної системи безпеки мереж за впливу соціологічних складових навантаження. XII Наукова конференція «Наукові підсумки 2023 року». Збірка наукових праць. Харків. Технологічний центр, 2023. 98 С., с. 56. e-ISBN 978-617-8360-00-9.
- Дженюк Н.В., Кулікова Д.В, Пархоменко І.П. Модель безпеки інформаційних взаємодій у соціокіберфізичних системах. XXXII Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я MicroCAD-2024», Харків, 2024. С. 1384.
- Дженюк Н.В. Модель аналізу інформаційних потоків в соціокіберфізичних системах. XIII Наукова конференція «Наукові підсумки 2024 року». Харків. Технологічний центр. 2024. С. 45. e-ISBN 978-617-8360-11-5.
- Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Dzheniuk, N. et. al. (2023). Models of socio-cyber-physical systems security. Monography. Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
- Дженюк Н.В.. Євсеєв С.П., Лазуренко Б.О., Серков О.А., Хвостенко В.С., Корчагін М.В., Орєхов С.В., Лезік О.В., Корсунов С.І., Воропай Н.І. Спосіб формування топології мобільної безпровідної повітряної мережі. Патент України на корисну модель № 156381 U МПК H04B 1/12, / u 202301793 заявл. 18.04.2023, опубл.

20.06.24, Бюл. № 25.

Наукова (науково-технічна) продукція: технології; методи, теорії, гіпотези

Соціально-економічна спрямованість: підвищення захищеності інформації в соціокіберфізичних системах

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0123U101018, 0123U101020

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Король Ольга Григорівна
2. Olga H. Korol

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCHID ID: 0000-0002-8733-9984

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii A. Smirnov

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

Ідентифікатор ORCHID ID: 0000-0001-9543-874X

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

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Казакова Надія Феліксівна
2. Nadiia Kazakova

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCHID ID: 0000-0003-3968-4094

Додаткова інформація:

Повне найменування юридичної особи: Одеський національний університет імені І. І. Мечникова

Код за ЄДРПОУ: 02071091

Місцезнаходження: вул. Дворянська, буд. 2, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Копп Андрій Михайлович
2. Andrii M. Корр

Кваліфікація: д.філософ, доц., 122

Ідентифікатор ORCHID ID: 0000-0002-3189-5623

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Ткачов Андрій Михайлович
2. Andrii M. Tkachov

Кваліфікація: к. т. н., старший науковий співробітник, 20.02.12

Ідентифікатор ORCHID ID: 0000-0003-1428-0173

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Кучук Георгій Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Кучук Георгій Анатолійович
Відповідальний за підготовку облікових документів	Дженюк Наталія Володимирівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна