Облікова картка ДіР

Image not found or type unknow

I. Загальні відомості

Державний обліковий номер: 0225U000752

Державний реєстраційний номер: 0123U101018

Особливі позначки: відкрита

Дата реєстрації: 18-01-2025

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка моделей соціо-кіберфізичних систем

Початок етапу: 01.2023

Закінчення етапу: 01.2025

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577076634

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380577076634

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7706 - безплатно (договір про науково-технічне співробітництво, тощо)

VII. Відомості про ДіР

Назва роботи українською:

Моделювання соціо-кіберфізичних систем

Назва роботи англійською:

Modelling of socio-cyber-physical systems

Реферат українською:

Об'єктом дослідження є багатоконтурна система безпеки інформаційних взаємодій у соціокіберфізичних системах. Дії з адаптації та еволюції повинні бути оцінені до їх реалізації в керованій системі, щоб забезпечити стійкість до відмови при мінімізації ризиків. Отже, дизайн соціокіберфізичних систем повинен забезпечувати не тільки надійну автономність, а й експлуатаційну стійкість до відмов та безпеки. Пропонований підхід грунтується на комплексуванні цільових (змішаних) загроз на основі синтезу технічних кіберзагроз із методами соціальної інженерії. Такий підхід забезпечує можливість формувати динамічну модель безпеки на основі аналізу взаємодії різних агентів у соціокіберфізичних системах, що дозволяє підвищити рівень протидії цільовим (змішаним) кіберзагрозам. Наведені результати моделювання ґрунтуються на запропонованій класифікації загроз методів соціальної інженерії, що дозволяє кіберзловмісникам забезпечити ймовірність реалізації цільових загроз до 95–98 %. Запропоновано класифікацію загроз на основі методів соціальної інженерії дозволити сформувати додатковий параметр об'єктивності цільових загроз з урахуванням їх комплексування та синергії. При цьому представлена модель дозволити своєчасно забезпечити знання про можливість реалізації цільової атаки та своєчасно вжити превентивних заходів протидії. Такий підхід дозволить покращити комплекс заходів захисту, а також своєчасно сформувати підвищення рівня протидії персоналу компанії (організації, підприємства тощо) загрозам соціальної інженерії. Мета роботи – розробка моделей соціо-кіберфізичних систем, спрямованих на побудову систем безпеки та підвищення рівня її ефективності у кібер- просторі.

Реферат англійською:

The object of the study is a multi-circuit information interaction security system in sociocyberphysical systems. However, adaptation and evolution actions must be evaluated before their implementation in a managed system to ensure fault tolerance while minimizing risks. Therefore, the design of sociocyberphysical systems must provide not only reliable autonomy, but also operational fault tolerance and security. The proposed approach is based on the integration of targeted (mixed) threats based on the synthesis of technical cyber threats with social engineering methods. This approach provides the opportunity to form a dynamic security model based on the analysis of the interaction of various agents in socio-cyber-physical systems, which allows to increase the level of counteraction to targeted (mixed) cyber threats. The presented modeling results are based on the proposed classification of threats of social engineering methods, which allows cyber attackers to ensure the probability of implementation of targeted threats up to 95–98%. The proposed classification of threats based on social engineering methods allows to form an additional parameter of the objectivity of targeted threats, taking into account their integration and synergy. At the same time, the presented model allows to provide timely knowledge about the possibility of implementing a targeted attack and to take timely preventive countermeasures. This approach will allow to improve the set of protection measures, as well as to timely form an increase in the level of counteraction of the company's personnel (organization, enterprise, etc.) To social engineering threats. The aim of the study is the development of models of socio-cyber-physical systems aimed at building security systems and increasing the level of their effectiveness in the conditions of work in cyberspace.

Індекс УДК: 519.711.3, , 620.9.001.5; 620.9.001.57; 620.9.001.5:51-7; 620.9.001.5:007, 002:651.928(083.73)

Коди тематичних рубрик: 28.17.19, 28.29.63.15, 44.01.77

Керівники роботи

Власне Прізвище Ім'я По-батькові: Мілов Олександр Володимирович

Науковий ступінь: д.т.н.

Вчене звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Система захищеності інформаційних взаємодій у соціокіберфізичних системах.

Назва НТП англійською: Information interaction security system in socio-cyber-physical systems.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Кібербезпека

Реєстраційний номер картки технології:

Опис НТП: Розроблено систему захищеності інформаційних взаємодій у соціокіберфізичних системах. На основі запропонованої моделі забезпечується розуміння причинно-наслідкових зв'язків, що існують у соціальній компоненті соціокіберфізичних систем, а також забезпечується аналіз кластерів агентів системи у вигляді байєсівської мережі. Такий підхід формування системи безпеки дозволить враховувати синтез технологій та каналів взаємодії циркулюючої інформації в соціокіберфізичних системах. Для кожної платформи соціокіберфізичних систем пропонується формувати внутрішній та зовнішній контури безпеки, що дозволить враховувати взаємодію інформаційних потоків, як усередині платформи, так і зовні.

Соціально-економічна спрямованість НТП: Розробка моделей соціо-кіберфізичних систем

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 01.2023

Закінчення етапу: 01.2025

Споживачі продукції: Державні установи, наукові заклади, бізнес-компанії та оборонний сектор.

Перспективні ринки: Перспективними ринками є IT, енергетика, транспорт, медицина, оборона та фінансовий сектор.

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. Murr P., Yevseiev S. Milevskyi S., Melnyk M., Katsalap V., Pribyliev Y., Rzayev K., Bryla A., Shpak O., Fedorka P. (2023). Development of an error correction method using perfect binary arrays. Eastern-European Journal of Enterprise Technologies, 4(9 (124), 45–53. DOI: 10.15587/1729-4061.2023.285540 (індексується базою Scopus)

2. Korol O., Mykytyn G., Milevskyi S., Lozova I., Solnyshkova S., Husarova I., Hrebeniuk A., Vlasov A., Sukhoteplyi V., Balagura D. (2024). Development of the sociocyberphysical systems` multi-contour security methodology. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 34–51. DOI: 10.15587/1729- 4061.2024.298844 (індексується базою Scopus)

3. Serhii Yevseiev, Maksym Tolkachov, Darshan Shetty, Stanislav Milevskyi, Vladyslav Khvostenko, Anna Strelnikova, Sergii Golovashych The concept of building security of the network with elements of the semiotic approach ScienceRise, No. 1 (84), 2023, P. 24–34 DOI: 10.21303/2313-8416.2023.002828 (закордонне видання)

4. Мілевський С. Розробка класифікатора загроз у соціокіберфізичних системах// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 118-123 DOI: 10.18372/2225-5036.29.18070

5. Мілевський С. Моделі безпеки соціокіберфізичних систем // Ukrainian Information Security Research Journal, 2023, vol. 25, issue 4, pp. 191-197 DOI: 10.18372/2410-7840.25.18224

6. Dzheniuk N., Lazurenko B., Serkov A., Zakharzhevskyi A., Milevskyi S. Sociocyberphysical Security Systems Synthesis Models 7th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2023 - Proceedings, DOI: 10.1109/ISMSIT58785.2023.10304965 (індексується базою Scopus)

7. Molodetska K., Veretiuk S., Milevskyi S., Rahimova I., Khvostenko V. Information Influence on the Virtual Community: Implementation Features and Method of Detection in Social Internet Services 7th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2023 - Proceedings, DOI: 10.1109/ISMSIT58785.2023.10305001 (індексується базою Scopus)

8. Yevseiev S., Murr P., Korol O., Milevskyi S., Melnyk M. and others Development of a Sociocyberphysical Systems Cyber Threats Classifier 7th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2023 - Proceedings, DOI: 10.1109/ISMSIT58785.2023.10304895 (індексується базою Scopus)

9. Herasymov S., Soroka V., Yevseiev S., Milevskyi S., Pohasii S. Phase- Modulated Signals Synthesis Method to Control Information Transmission Channels 2023 IEEE 4th KhPI Week on Advanced Technology, KhPI Week 2023 - Conference Proceedings, DOI: 10.1109/KhPIWeek61412.2023.10312859 (індексується базою Scopus)

10. 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 (2024) Eastern-European Journal of Enterprise Technologies, 5 (9(131)), pp. 63 – 78 DOI: 10.15587/1729-4061.2024.313158

11. Yevseiev S., Khokhlachova Y., Ostapov S., Laptiev O., Korol O., Milevskyi S., Milov O., Pohasii S., Melenti Y., Hrebeniuk V., Havrylova A., Herasmov S., Korolev R., Barabash O., Sobchuk V., Kyrychok R., Shuklin G., Akhramovych V., Savchenko V., Golovashych R., Lezik O., Opirskyy I., Voitko O., Yerhidzei K., Mykus S., Pribyliev Y., Prokopenko O., Vlasov A., Nataliia D., Tolkachov M. (2023) Models of Socio-Cyber- Physical Systems Security, pp. 1 - 168 DOI: 10.15587/978-617-7319-72-5

12. Serkov A., Jammine A., Kudii D., Nataliia D., Farid N.-A., Bogdan L. Security Models and Methods of Socio-Cyberphysical Systems (2023) 7th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2023 - Proceedings DOI: 10.1109/ISMSIT58785.2023.10304955

13. Dzheniuk N., Yevseiev S., Lazurenko B., Serkov O., Kasilov O. A METHOD OF PROTECTING INFORMATION IN CYBER-PHYSICAL SPACE (2023) Advanced Information Systems, 7 (4), pp. 80 - 85 DOI: 10.20998/2522-9052.2023.4.11

14. Yevseiev S., Milov O., Dzheniuk N., Tolkachov M., Voitko T., Prygara M., Voropay N., Shpak O., Volkov A., Lezik O. DEVELOPMENT OF A MULTI-LOOP SECURITY SYSTEM OF INFORMATION INTERACTIONS IN SOCIO-

CYBERPHYSICAL SYSTEMS (2023) Eastern-European Journal of Enterprise Technologies, 5 (9(125)), pp. 53 - 74 DOI: 10.15587/1729-4061.2023.289467

15. Milov O., Rahimova I., Havrylova A., Golovashych S., Aksonova I., Pecherytsia D. Cybersecurity of SMART Technologies Using Deep Learning Methods (2024) ISMSIT 2024 - 8th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings DOI: 10.1109/ISMSIT63511.2024.10757295

16. Shmatko O., Yevseiev S., Milov O., Sporyshev K., Opirskyy I., Glukhov S., Rudenko Y., Nalyvaiko A., Dakov S., Sampir O. DEVELOPMENT OF A MODEL OF THE INFORMATION AND ANALYTICAL SYSTEM FOR MAKING DECISIONS ON DETECTING FAILURES OF INFORMATION TRANSMISSION CHANNELS (2024) Eastern-European Journal of Enterprise Technologies, 3 (9(129)), pp. 28 - 36 DOI: 10.15587/1729-4061.2024.306179

17. Yevseiev S., Milov O., Zviertseva N., Pribyliev Y., Lezik O., Komisarenko O., Nalyvaiko A., Pogorelov V., Katsalap V., Husarova I. DEVELOPMENT OF THE CONCEPT FOR DETERMINING THE LEVEL OF CRITICAL BUSINESS PROCESSES SECURITY (2023) Eastern-European Journal of Enterprise Technologies, 1 (9(121)), pp. 21 - 40 DOI: 10.15587/1729-4061.2023.274301

X. Заключні відомості

Керівник юридичної особи Марченко Андрій Петрович
д. т. н., 05.05.03

Перелік осіб-виконавців

Ахієзер Олена Борисівна
(к. т. н., 01.05.02)

Букатич Ілля Вадимович

Дженюк Наталія Володимирівна

Дунаєв Сергій Володимирович

Жигалов Михайло Олександрович

Меленті Євген Олександрович
(к.т.н., 05.12.17)

Мілевський Станіслав Валерійович
(к. е. н., 08.03.02)

Печериця Дмитро Вікторович Дмитро Вікторович

Погасій Сергій Сергійович
(к. е. н., 08.00.03)

Сокол Владислав Євгенович
(к.т.н., 05.13.06)

Стеценко Вадим Олегович

Толкачов Максим Юрійович

Уманський Олександр Григорович

Відповідальний за підготовку облікових документів Гуренко Ю.І.

Телефон +38 (050) 609-83-92

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

