Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U002070

Особливі позначки: відкрита

Дата реєстрації: 29-05-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Личик Владислав Васильович
2. Vladyslav V. Lychyk

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

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: Кібербезпека

Дата захисту:

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 14181

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 28.17, 44.29.29, 50.37.23, 28.31

Тема дисертації:

1. Моделювання кіберстійкості критичної інфраструктури на прикладі енергетичного об’єкта

2. Modeling Cyber Resilience of Critical Infrastructure Applied to an Energy Facility

Реферат:

1. У дисертаційній роботі формалізовано понятійний апарат кіберстійкості (кіберрезильєнтності) та обґрунтовано його концептуальну відмінність від класичної кібербезпеки. На основі критичного аналізу провідних міжнародних фреймворків доведено, що існуючі підходи здебільшого базуються на парадигмі Data-driven, обмеження якої не дозволяють здійснювати прогнозування та динамічну адаптацію системи в умовах сучасних кіберінцидентів. Також у роботі обґрунтовано та здійснено концептуальний перехід від якісних доменів кіберстійкості до кількісних моделей високого рівня шляхом розроблення метамоделі IT-мережі енергетичного об’єкта (парадигма Model-driven). Здійснено метамоделювання категорій кіберстійкості на основі архітектури MOF (Meta-Object Facility) із вираженням концепцій мовою UML. Таке структурне моделювання забезпечило строгий перехід від абстрактних якісних показників до обчислювальної моделі предметної області (енергетичного сектору), що створило необхідний базис для

подальшого застосування інструментів ймовірнісного оцінювання параметрів та розрахунку функціональних станів системи, зокрема баєсових мереж, та підтвердило гіпотезу про необхідність ускладнення контролера об’єкта критичної інфраструктури. Досліджено проблему зниження невизначеності під час кібератак на енергооб’єкт. Показано, що для раннього виявлення загроз ефективним є використання баєсових мереж, де апріорні розподіли ймовірностей будуються за допомогою баз даних вразливостей (CVE) із застосуванням метрик CVSS. Проведений аналіз чутливості моделі за методом К’єрульфа та ван дер Гааг довів її низьку чутливість до похибок апріорних параметрів. У ході дисертаційного дослідження розроблено метод активної протидії кібератакам для мережі енергетичного об’єкта в реальному часі на основі інтеграції баєсових графів атак (BAG) у структуру частково спостережуваних марковських процесів прийняття рішень (POMDP). Запропонований метод дозволяє уникнути надмірних витрат на перманентне блокування критичних сегментів мережі, фокусуючись на оптимальному розподілі ресурсів та найбільш ймовірних векторах атаки. Показано, що ключовим фактором мінімізації збитків є не лише жорсткість реагування, а й доступність та безпосередня вартість верифікації загрози, що перетворює стратегію захисту з реактивної на проактивну точкову ліквідацію. У ході експериментального моделювання проведено порівняльний аналіз чотирьох стратегій кіберзахисту, які концептуально різняться підходами до прийняття рішень, значенням фактора дисконтування (п) та варіативністю доступних контрзаходів. Завдяки застосуванню розробленого алгоритму в середовищі pomdp-solve було синтезовано оптимальну політику протидії. У ході проведення експериментальних досліджень практично доведено неефективність прямої імплементації високодеталізованих сценаріїв кібератак для формування об'ємної вибірки даних. Практична апробація засвідчила, що, незважаючи на результативність таких сценаріїв під час натурного тестування безпосередньо на об’єкті критичної інфраструктури, їх застосування стикається з критичними обмеженнями при моделюванні. Побудовано експериментальне середовище та проведено симуляційне моделювання для апробації запропонованих підходів. За результатами досліджень установлено, що зведення складного простору топології технологічної мережі (SCADA-систем) до 6 макро-станів на основі моделі Cyber Kill Chain забезпечило обчислювальну досяжність політики POMDP шляхом подолання проблеми експоненційного зростання розмірності простору станів. Доведено, що введення низьковартісних операцій розвідки радикально змінює поведінку автономного агента, забезпечуючи перехід від «реактивного стримування» до «превентивної ліквідації». Для експериментальної апробації запропонованих рішень та отримання репрезентативної вибірки даних використано фреймворк автоматизованої емуляції кібератак MITRE Caldera. За результатами масштабного моделювання (виконання понад 800 модулів деструктивних впливів) розроблено матрицю впливу контрзаходів («Дія vs Стан») та побудовано матрицю ефективності контрзаходів (Countermeasure Efficiency). На основі отриманих емпіричних даних експериментально підтверджено здатність розробленої оптимальної політики протистояти високоагресивним сценаріям цілеспрямованих атак із гарантованим збереженням критичної функціональності IT-мережі. Отримані результати підтвердили, що удосконалення функції винагороди шляхом її жорсткої прив'язки до фізичних коефіцієнтів деградації цільової функції переводить завдання кіберзахисту в площину мінімізації економічних збитків. Установлено, що впровадження розробленої оптимальної політики дозволило знизити сукупну вартість кіберінциденту. Симуляційне моделювання засвідчило абсолютний приріст загальної кіберстійкості мережі на 27,58% порівняно з базовою стратегією. Проактивні дії автономного агента дозволили скоротити загальні функціональні втрати енергетичного об'єкта у 6,7 раза , що беззаперечно доводить високу ефективність математичної моделі адаптивного захисту.

2. The dissertation formalizes the conceptual apparatus of cyber resilience and substantiates its conceptual difference from classical cybersecurity. Based on a critical analysis of leading international frameworks, it is proven that existing approaches are mostly based on a Data-driven paradigm, the limitations of which do not allow for forecasting and dynamic system adaptation under the conditions of modern cyber incidents. The study also justifies and executes a conceptual transition from qualitative cyber resilience domains to high-level quantitative models by developing a metamodel of the energy facility's IT network (Model-driven paradigm). The metamodeling of cyber resilience categories was carried out based on the MOF architecture, expressing concepts in UML. Such

structural modeling ensured a rigorous transition from abstract qualitative indicators to a computational model of the problem domain (energy sector), creating the necessary basis for the subsequent application of probabilistic parameter estimation tools and the calculation of the system's functional states, in particular, Bayesian networks, and confirmed the hypothesis regarding the increased complexity of the critical infrastructure facility's controller. The problem of reducing uncertainty during cyberattacks on an energy facility was investigated. It is shown that Bayesian networks are effective for early threat detection, where prior probability distributions are constructed using vulnerability databases (CVE) with the application of CVSS metrics. A sensitivity analysis of the model using the Kjærulff and van der Gaag method proved its low sensitivity to errors in prior parameters. During the dissertation research, a method for active real-time cyberattack countermeasures for an energy facility network was developed, based on the integration of BAG into the framework of POMDP. The proposed method avoids the excessive costs of permanently blocking critical network segments, focusing on the optimal allocation of resources and the most probable attack vectors. Minimizing losses depends on response rigidity and the availability and cost of threat verification, shifting defense from reactive to proactive targeted elimination. During the experimental modeling, a comparative analysis of four cyber defense strategies was conducted, which conceptually differ in decision-making approaches, the value of the discount factor (□), and the variability of available countermeasures. Through the application of the developed algorithm in the pomdp-solve environment, an optimal countermeasure policy was synthesized. Experiments demonstrated the inefficiency of directly implementing highly detailed cyberattack scenarios to generate large datasets. Practical testing showed that, despite the effectiveness of such scenarios during field testing directly at a critical infrastructure facility, their application faces critical limitations in modeling. Thus, an experimental environment was built, and simulation modeling was conducted to test the proposed approaches. Based on the research results, it was established that the reduction of the complex topology space of the technological network (SCADA systems) to 6 macro-states based on the Cyber Kill Chain model ensured the computational tractability of the POMDP policy by overcoming the problem of the exponential growth of the state space dimensionality. It is proven that the introduction of low-cost reconnaissance operations radically changes the behavior of the autonomous agent, ensuring a transition from "reactive containment" to "preventive elimination". For the experimental validation of the proposed solutions and obtaining a representative data sample, the MITRE Caldera automated cyberattack emulation framework was used. Based on the results of large-scale modeling (involving the execution of over 800 destructive impact modules), a Countermeasure Impact Matrix («Action vs. State») and a Countermeasure Efficiency Matrix were developed. Based on the obtained empirical data, the ability of the developed optimal policy to withstand highly aggressive targeted attack scenarios with guaranteed preservation of the IT network's critical functionality was experimentally confirmed. The obtained results confirmed that improving the reward function by strictly linking it to physical degradation coefficients of the target function shifts the task of cyber defense into the realm of minimizing economic losses. It was established that the implementation of the developed optimal policy allowed reducing the total cost of a cyber incident. Simulation modeling demonstrated an absolute increase in the overall cyber resilience of the network by 27.58% compared to the baseline strategy. The proactive actions of the autonomous agent reduced the overall functional losses of the energy facility by a factor of 6.7, which indisputably proves the high efficiency of the adaptive defense mathematical model.

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. Гальчинський, Л., & Личик, В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, (2 (8), С. 27-33. URL: https://doi.org/10.32689/maup.it.2023.2.3
- 2. Личик, В. В. (2025). Адаптивний підхід до реагування на порушення кіберстійкості об'єктів критичної інфраструктури. Комп'ютерно-інтегровані технології: освіта, наука, виробництво, (59), С. 16-28. URL: https://doi.org/10.36910/6775-2524-0560-2025-59-02
- 3. Личик В., Гальчинський Л., Косарик Д. (2025). Пом'якшення впливу кібератак, таких як атаки, що змінюють навантаження. Теоретична і прикладна кібербезпека (Theoretical and Applied Cybersecurity - TACS), (7), С. 71-81. URL: https://doi.org/10.20535/tacs.2664-29132025.1.327873
- 4. Личик В. В., Гальчинський Л.Ю. (2025). Використання моделі мереж Баєса для раннього оцінювання загроз кібератак об'єкта електроенергетики. Інститут проблем реєстрації інформації НАН України. Реєстрація, зберігання і оброб. даних. 2025, Т. 27, № 2. С. 70-85. URL: https://doi.org/10.35681/1560-9189.2025.27.2.345591
- 5. Личик В. В., Гальчинський Л. Ю. Пошук оптимальної політики забезпечення кіберстійкості енергетичного об'єкта на основі частково спостережуваних процесів. Матеріали XXV Міжнародної науково-практичної конференції ІТБ-2025 (м. Київ, Україна, 11 грудня 2025 р.) / Інститут проблем реєстрації інформації НАН України. Київ : Інжиніринг, 2025. С. 126–129. ISBN: 978-617-8180-04-1. URL: https://drive.google.com/file/d/1wMZcK5J8LJdnqUP-KLwBmVSgZuqtCAuJ/view
- 6. Личик В.В., Фролов П.А. Імітація кібератаки та кількісний обрахунок кіберстійкості для об'єкту критичної інфраструктури. Матеріали XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики" КПІ ім. Ігоря Сікорського (14 – 17 травня 2025 р., м. Київ, Україна). С. 200-202. URL: http://conf.ipt.kpi.ua/arxiv/2025-2/
- 7. Оцінювання кіберстійкості розподільчої системи енергетичного об'єкту критичної інфраструктури на основі мереж Байєса. Личик В.В., Гальчинський Л.Ю. // III Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2025). 29 травня 2025 р. С. 109-112. URL: https://is.ipt.kpi.ua/pdf/TACS-25el.pdf
- 8. Апробація моделей кіберстійкості для функції розподілу енергосистеми. Личик В.В., Гальчинський Л.Ю. // XXIV Міжнародна науково-практична конференція «Інформаційні технології та безпека» (ІТБ-2024) від Інституту проблем реєстрації інформації Національної академії наук України, 19 грудня 2024 р. С. 103-106. URL: http://dwl.kiev.ua/its-ua/itb-2024_merged.pdf
- 9. Личик В.В. & Нечаєв О.О. (2024). Порівняльна характеристика методологій та метрик кіберстійкості для об'єктів критичної інфраструктури. 5th International Scientific and Practical Conference «Modern directions and movements in science» (June 16-18, 2024; Luxembourg, Grand Duchy of Luxembourg). URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/6502
- 10. Розробка метамоделі для забезпечення кіберстійкості об'єктів критичної інфраструктури різних рівнів. Личик В.В., Гальчинський Л.Ю. // Друга Всеукраїнська науково-практична конференція "Theoretical and Applied Cybersecurity" (TACS-2024), 30 травня 2024 р. С. 111-114. URL: http://www.is.ipt.kpi.ua/pdf/T24.pdf
- 11. Метамоделювання кіберстійкості для об'єктів критичної інфраструктури. Личик В.В., Гальчинський Л.Ю. // XV Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» від Національної академії Служби безпеки України, 21 березня 2024 р.
- 12. Оцінювання кібервідмовостійкості для об'єктів критичної інфраструктури. Личик В.В., Гальчинський Л.Ю. // XXIII Міжнародна науково-практична конференція «Інформаційні технології та безпека» (ІТБ-2023) від Інституту проблем реєстрації інформації Національної академії наук України, 30 листопада 2023 р. С. 122-125. URL: http://dwl.kiev.ua/its-ua/itb-2023_merged.pdf

- 13. Проблематика підбору метрик для оцінки кібервідмовостійкості. Личик В.В., Гальчинський Л.Ю. // Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023» («Survivability & Resilience – 2023») від Інституту проблем реєстрації інформації НАН України та Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 19 жовтня 2023р. С. 65-68. URL: https://ipme.kiev.ua/wp-content/uploads/2023/11
- 14. Проблематика підбору метрик кіберстійкості для оцінки об'єктів різних рівнів. Личик В.В., Гальчинський Л.Ю // Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023). 26 травня 2023 р.
- 15. Необхідність пошуку рішення комплексного підходу до забезпечення кіберстійкості об'єктів критичної інфраструктури. Личик В.В., Гальчинський Л.Ю. // XIV Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» від Національної академії Служби безпеки. 30 березня 2023 р. С. 507-510. URL: https://nasbu.edu.ua/uploads/p_57_92088934.pdf

Наукова (науково-технічна) продукція: пристрої; технології; методи, теорії, гіпотези; методичні документи; програмні продукти, програмно-технологічна документація; аналітичні матеріали; політики протидії, набори контрзаходів, план та програма кіберзахисту об'єктів критично інфраструктури.

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг; забезпечення інформаційної безпеки для об'єктів критичної інфраструктури.

Охоронні документи на ОПІВ:

Комп'ютерні програми

Розробка автоматизованого програмного забезпечення для оцінки рівня кіберстійкості об'єктів критичної інфраструктури.

Компіляції даних (бази даних)

Генерація сценаріїв та формування політик протидій для забезпечення кіберстійкості об'єктів критичної інфраструктури.

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Гальчинський Леонід Юрійович

2. Leonid Y. Galchynsky

Кваліфікація: к.т.н., доцент, 05.13.03

Ідентифікатор ORCID ID: 0000-0002-3805-1474

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Гончар Сергій Феодосійович

2. Serhii Honchar

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

Ідентифікатор ORCID ID: 0000-0002-9978-8998

Додаткова інформація:

Повне найменування юридичної особи: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України

Код за ЄДРПОУ: 05516949

Місцезнаходження: вул. Генерала Наумова, Київ, 03164, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Лаптєв Олександр Анатолійович

2. Oleksandr A. Laptiev

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-4194-402X

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, Київ, 01033, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Прогонов Дмитро Олександрович

2. Dmytro O. Progonov

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

Ідентифікатор ORCID ID: 0000-0002-1124-1497

Додаткова інформація: http://www.researcherid.com/rid/G-9658-2017; http://www.scopus.com/inward/authorDetails.url?authorID=57201682654&partnerID=MN8TOARS

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Коломицев Михайло Володимирович

2. Mykhailo Kolomytsev

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

Ідентифікатор ORCID ID: 0000-0001-8460-3041

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Новіков Олексій Миколайович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Новіков Олексій Миколайович

Відповідальний за підготовку облікових документів Личик Владислав Васильович

Реєстратор Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна