Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U005285

Особливі позначки: відкрита

Дата реєстрації: 21-09-2026

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Драгунцов Роман Ігорович
2. Roman Drahuntsov

Кваліфікація: 122

Ідентифікатор ORCID ID: 0000-0002-1781-7530

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: 01-10-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України

Код за ЄДРПОУ: 25198635

Місцезнаходження: пр. Академіка Палладіна , Київ, 03142, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 16897

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

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

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

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.03

Тема дисертації:

1. МЕТОДИ ЗБОРУ, ОБРОБКИ ТА АНАЛІЗУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ В УМОВАХ ОБМЕЖЕНОЇ СПОСТЕРЕЖНОСТІ

2. Methods for the Collection, Processing, and Analysis of Information in Computer Systems for Security Event Management under Conditions of Limited Observability

Реферат/анотація:

1. У дисертації розв’язано науково-прикладну задачу підвищення спостережності інформаційних систем у процесах моніторингу та реагування на інциденти кібербезпеки за умов обмеженої спостережності, спричиненої воєнними впливами і деградацією інфраструктури, зокрема масовими відключеннями електропостачання та зв’язку. Розроблено методологічний апарат формалізації «втрати спостережності» як вимірюваної властивості активу; запропоновано методи атрибутивного профілювання активів і контролю на основі метрик; сформовано високорівневі вимоги та архітектуру технічної реалізації методів. Метою роботи є підвищення ефективності процесів збору та аналізу інформації в комп’ютерних системах управління подіями безпеки шляхом їх удосконалення в умовах деградації інфраструктури інформаційно-

комунікаційних систем. Об'єктом дослідження є процеси збору, аналізу інформації про події та інциденти, а також прийняття рішень в операційних центрах кіберзахисту в розподілених інформаційних системах, які зазнають деградації доступності та спостережності внаслідок зовнішніх впливів. Предметом дослідження є методи збору та аналізу інформації в операційних центрах кіберзахисту, спрямовані на підвищення спостережності інформаційних систем. Вперше розроблено формалізовану постановку задачі підвищення спостережності інформації у контексті деградації інфраструктури, у якій «втрата спостережності» визначається як стан системи, за якого зменшується повнота та/або достовірність телеметрії до рівня, що порушує коректність виконання щонайменше одного класу процедур операційного центру кіберзахисту, а перехід у такий стан описується вимірюваними ознаками доступності джерел подій і узгодженості інвентарних даних. Дістав подальшого розвитку метод атрибутивного профілювання активів, у якому для кожного активу формується вектор атрибутів, релевантних для оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури. Виконано проєктування архітектури прототипу технічного рішення підвищення спостережності, в якій виділено контури інвентаризації та злиття даних про активи, аналітики подій/інцидентів, активного реагування, атрибутивного профілювання та обчислення правил/метрик, візуалізації та звітності. Розроблено методологію корекції процесів обробки сигналів в операційних центрах кіберзахисту, спрямовану на виявлення та врахування деградації спостережності як умови коректної інтерпретації сигналів про кіберзагрози за умов воєнних впливів. Розділ 1 присвячено аналізу впливу сучасних умов функціонування інформаційно-комунікаційних систем на спостережність інформації. Систематизовано фактори військового часу, що порушують повноту, своєчасність і достовірність телеметрії, та визначено їх вплив на процеси виявлення, аналізу і реагування. Розділ 2 присвячено розробці методів підвищення спостережності інформації в умовах деградації інфраструктури. Побудовано дескриптивну модель впливу деградації електроживлення, каналів зв'язку, джерел телеметрії та інвентаризаційного контексту. Запропоновано атрибутивне профілювання активів і злиття інвентарних даних, визначено правила та метрики оцінювання втрати спостережності, введено атрибути динамізму активу і дескриптора загроз та сформовано принципи побудови контролів для розрізнення технічної деградації й потенційної активності агента загроз. Розділ 3 присвячено розробці вимог, архітектури та прототипу технічного рішення. Сформовано проєкт відкритої модульної архітектури, визначено склад її підсистем і модулів, вимоги до інтеграції та даних, а також сформовано склад експериментального стенду. Розділ 4 присвячено експериментальній перевірці ефективності розроблених методів. Виконано порівняння базового режиму обробки подій і режиму із застосуванням запропонованої методології на сценаріях масової втрати електроживлення, деградації каналів зв'язку, відновлення після деградації та накладання зловмисної активності на тлі технічної недоступності. Результати підтвердили зменшення кількості хибних інтерпретацій, підвищення точності класифікації, зниження операційного шуму та покращення пріоритезації подій. Актуальність тематики визначається залежністю процесів обробки, аналізу та реагування на події та інциденти безпеки від безперервного збору телеметрії та стабільності інфраструктурних компонентів, тоді як у воєнних умовах знижується доступність джерел журналювання, деградують канали доставлення подій та зростає динамічність інфраструктури. Це зумовлює потребу формалізації «якості спостережності» як вимірюваної величини. Практична значимість полягає у можливості безпосереднього впровадження запропонованих методів у процеси операційних центрів кібербезпеки шляхом інтеграції модулів інвентаризації та злиття даних про активи, атрибутивного профілювання та обчислення контролів/метрик з наявними компонентами технологічних платформ обробки та аналізу подій безпеки.

2. The dissertation addresses the applied scientific problem of improving information system observability in cybersecurity incident monitoring and response under limited observability caused by wartime impacts and infrastructure degradation. A methodological framework for formalizing “loss of observability” as a measurable asset property, methods for attribute-based asset profiling and metric-based control, and a prototype architecture of the technical solution have been developed. The aim of the research is to improve the efficiency of information collection and analysis in computer security event management systems under infrastructure degradation. The object of the research is the processes of collecting and analyzing information on events and incidents and

decision-making in cybersecurity operations centers within distributed information systems affected by degradation of availability and observability. The subject of the research is methods of information collection and analysis in cybersecurity operations centers aimed at improving information system observability. For the first time, a formalized problem statement for improving information observability under infrastructure degradation has been developed, in which “loss of observability” is defined as a system state where telemetry completeness and/or reliability decreases to a level that disrupts the correct execution of at least one class of cybersecurity operations center procedures. The transition to this state is described by measurable indicators of event source availability and inventory data consistency. The method of attribute-based asset profiling has been further developed by forming, for each asset, a vector of attributes relevant to assessing observability and risks of telemetry interpretation under infrastructure degradation. A prototype architecture for improving observability has been designed, comprising asset inventory and data fusion, event/incident analytics, active response, attribute-based profiling and rule/metric computation, visualization and reporting. A methodology for correcting signal processing in cybersecurity operations centers has been developed to detect and account for observability degradation when interpreting cyber threat signals under wartime impacts. Chapter 1 analyzes wartime factors affecting telemetry completeness, timeliness, and reliability and their impact on detection, analysis, and response processes. Chapter 2 develops a descriptive model of infrastructure degradation, attribute-based asset profiling and inventory data fusion, rules and metrics for assessing loss of observability, asset dynamicity and threat descriptor attributes, and principles for distinguishing technical degradation from potential threat actor activity. Chapter 3 defines the requirements, open modular architecture, prototype, integration requirements, and experimental testbed. Chapter 4 experimentally compares baseline event processing with the proposed methodology under scenarios of power loss, communication degradation, recovery, and malicious activity against technical unavailability. The results confirmed reduced incorrect interpretations and operational noise, and improved classification accuracy and event prioritization. The relevance of the research is determined by the degradation of telemetry collection and infrastructure availability under wartime conditions, which requires formalization of “observability quality” as a measurable quantity. The practical significance lies in integrating the proposed asset inventory, data fusion, attribute-based profiling, and control/metric computation methods with existing security event processing and analysis platforms.

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:

- R. Drahuntsov, A. Symonov, O. Potenko, O. Dybach, and V. Zubok, “Cybersecurity monitoring during power outages: Use cases for enhanced infrastructure observability and potential implications for NPP combined events,” Nuclear and Radiation Safety, no. 3(107), pp. 17–29, 2025, doi: 10.32918/nrs.2025.3(107).02.
- R. Drahuntsov and V. Zubok, “Modeling of cyber threats related to massive power outages and potential countermeasures,” Elektronnoe Modelirovanie, vol. 45, no. 3, pp. 116–128, 2023, doi: 10.15407/emodel.45.03.116.
- R. Drahuntsov and V. Zubok, “Dynamic infrastructure components and system visibility during cybersecurity incident response,” Cybersecurity: Education, Science, Technique, no. 1(29), pp. 493–507, 2025, doi: 10.28925/2663-4023.2025.29.891.
- O. Popov and R. Drahuntsov, “Ключові виклики для операційних центрів кібербезпеки в умовах повномасштабної війни,” Information Technology and Society, no. 3(18), 2025, doi: 10.32689/maup.it.2025.3.19.

- R. Drahuntsov and V. Zubok, “Methods for maintaining the observability of information and communication infrastructure in conditions of full-scale war,” Elektronnoe Modelirovanie, vol. 48, no. 1, pp. 72–86, 2026, doi: 10.15407/emodel.48.01.072.
- R. Drahuntsov and V. Zubok, “A method for reducing the uncertainty caused by a power outage during a cyber incident response,” in CEUR Workshop Proc., vol. 3887, pp. 226–236, 2024. [Online]. Available: ceur-ws.org/Vol-3887/paper20.pdf. Accessed: Feb. 24, 2026.
- V. Yu. Zubok and R. S. Drahuntsov, “Проєкція принципів національної системи стійкості та резильєнтність критичної інформаційної інфраструктури,” in Proc. Sci.-Pract. Conf. “Резильєнтність критичної інфраструктури – 2023”, Kyiv, Ukraine, Jun. 21, 2023, pp. 104–108. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/06/Матеріали-конференції-Critical-Infrastructure-Resilience---2023.pdf. Accessed: Feb. 24, 2026.
- V. Yu. Zubok and R. S. Drahuntsov, “Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання,” in Proc. V Sci.-Pract. Conf. “Безпека енергетики в епоху цифрової трансформації” (БЕЕЦТ-2023), Kyiv, Ukraine, 2023, pp. 38–42. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали-конференції-БЕЕЦТ-2023.pdf. Accessed: Feb. 24, 2026.
- R. Drahuntsov and V. Zubok, “Особливості атак з використанням соціального графу та підходи до захисту,” in Proc. 2nd All-Ukrainian Sci.-Pract. Conf. “Theoretical and Applied Cybersecurity” (TACS-2024), Kyiv, Ukraine, 2024. [Online]. Available: is.ipt.kpi.ua/pdf/T24.pdf. Accessed: Feb. 24, 2026.
- V. V. Zubok, R. S. Drahuntsov, and V. Yu. Zubok, “Резильєнтність ERP-систем в умовах енергетичної кризи,” in Proc. Sci.-Pract. Conf. “Кібербезпека енергетики”, Kyiv, Ukraine, 2024, pp. 13–16. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/06/Матеріали-КБЕ-2024.pdf. Accessed: Feb. 24, 2026.
- R. I. Drahuntsov, “Особливості інцидентів інформаційної безпеки з залученням шкідливого ПЗ в умовах кібервійни – аналіз та реагування,” in Proc. Conf. Materials (v.2), Kyiv, Ukraine, 2024, pp. 65–68. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2024/05/Матеріали-конференції-2024-v-2.pdf. Accessed: Feb. 24, 2026.
- R. I. Drahuntsov and V. Yu. Zubok, “Проблематика інтеграції джерел виявлення технічних вразливостей в розрізі підтримки кіберстійкості критичної інфраструктури,” in Proc. XLIII Sci.-Tech. Conf. Young Scientists and Specialists (PIMEE NAS of Ukraine), Kyiv, Ukraine, May 14, 2025, pp. 29–31. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Materialy-KMV-2025.pdf. Accessed: Feb. 24, 2026.
- R. I. Drahuntsov, “Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури,” in Proc. Sci.-Pract. Conf. “Кібербезпека енергетики” (КБЕ-2025), Kyiv, Ukraine, 2025. [Online]. Available: ipme.kiev.ua/wp-content/uploads/2025/05/Матеріали-КБЕ-2025-1.pdf. Accessed: Feb. 24, 2026.
- R. I. Drahuntsov, “Процедури threat hunting в сучасному SOC – ключові підходи та проблематика оцінки покриття,” in Proc. Conf. “Цифрова трансформація кібербезпеки”, pp. 40–42, 2025. [Online]. Available: duikt.edu.ua/uploads/p_2779_36484696.pdf. Accessed: Feb. 24, 2026.
- R. I. Drahuntsov and V. Yu. Zubok, “Застосування великих мовних моделей для автоматичної ідентифікації окремих атрибутів поверхні атаки активів в кібербезпеці,” in Proc. Sci.-Pract. Conf. “ШІБ-2025”. [Online]. Available: ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-sib-2025/. Accessed: Feb. 24, 2026.

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

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Планується до впровадження

Зв'язок з науковими темами: 0123U102744

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Зубок Віталій Юрійович

2. Vitalii Y. Zubok

Кваліфікація: д. т. н., с.д.

Ідентифікатор ORCID ID: 0000-0002-6315-5259

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович

2. Oleksandr H. Korchenko

Кваліфікація: д. т. н., професор, член-кор. НАН України, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3376-0631

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Єфіменко Андрій Анатолійович

2. Andrii A. Yefimenko

Кваліфікація: к. т. н., доц.

Ідентифікатор ORCID ID: 0000-0003-2128-4797

Додаткова інформація:

Повне найменування юридичної особи: Державний університет "Житомирська політехніка"

Код за ЄДРПОУ: 05407870

Місцезнаходження: вул. Чуднівська, Житомир, Житомирський р-н., 10005, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: 04r5xzk86

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Кравцов Григорій Олексійович

2. Hryhorii O. Kravtsov

Кваліфікація: к. т. н., 01.05.02

Ідентифікатор ORCID ID: 0000-0003-1915-4897

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. Гільгурт Сергій Якович

2. Serhii Y. Hilhurt

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.05

Ідентифікатор ORCID ID: 0000-0003-1647-1790

Додаткова інформація: Web of Science Researcher ID: Q-6850-2018; Scopus Author ID: 57373650100; https://scholar.google.com.ua/citations?user=L4JS3tQAAAAJ

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Мохор Володимир Володимирович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Мохор Володимир Володимирович
Відповідальний за підготовку облікових документів	Драгунцов Роман Ігорович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна