ЗАТВЕРДЖУЮ
Заступник директора з науково-організаційної роботи Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, д.т.н., с.н.с.

Володимир АРТЕМЧУК

«06» червня 2026 р.

ВИТЯГ З ПРОТОКОЛУ № 3

засідання розширеного науково-технічного семінару
відділу математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України

м. Київ «04» червня 2026 р.

ПРИСУТНІ 14 осіб:

- Душеба Валентина Віталіївна, к.т.н., доцент
- Зубок Віталій Юрійович, д.т.н., ст.д.
- Гільгурт Сергій Якович, д.т.н.
- Шкарупило Вадим Вікторович, д.т.н., професор
- Кравцов Григорій Олексійович, к.т.н.
- Артемчук Володимир Олександрович, д.т.н.
- Самойлов Віктор Дмитрович, д.т.н., професор
- Мохор Володимир Володимирович, д.т.н., професор, чл.-кор. НАН України
- Плетяний Ігор Васильович, к.т.н.
- Потенко Олександр Сергійович, к.т.н.
- Цуркан Василь Васильович, к.т.н., доцент
- Дмитро Павлович Сінько, аспірант
- Кравчук Олександр Анатолійович, аспірант
- Тарановський Артем Олександрович, аспірант

ГОЛОВУВАЛА: к.т.н., доцент Душеба В.В., завідувачка відділу математичного та комп'ютерного моделювання ІПМЕ ім. Г.Є. Пухова НАН України.

ПОРЯДОК ДЕННИЙ:

СЛУХАЛИ:

1. Повідомлення аспіранта 4-го року навчання ІПМЕ ім. Г.Є. Пухова НАН України **Драгунцова Романа Ігоровича** за матеріалами дисертаційної

роботи «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки, освітньо-наукова програма «Комп'ютерні науки».

Тему дисертаційної роботи «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності» затверджено на засіданні Вченої ради ІПМЕ ім. Г.Є. Пухова НАН України (протокол № 13 від 29.12.2022).

Науковим керівником затверджений доктор технічних наук, старший дослідник Зубок Віталій Юрійович.

2. Запитання до здобувача.

Запитання за темою дисертації ставили:

- Душеба Валентина Віталіївна, кандидат технічних наук, доцент
- Гільгурт Сергій Якович, доктор технічних наук, професор
- Самойлов Віктор Дмитрович, доктор технічних наук, професор
- Шкарупило Вадим Вікторович, доктор технічних наук, професор
- Кравцов Григорій Олексійович, кандидат технічних наук, старший дослідник

3. Виступи за обговореною роботою.

В обговоренні дисертації взяли участь:

- Душеба Валентина Віталіївна, кандидат технічних наук, доцент
- Гільгурт Сергій Якович, доктор технічних наук, професор
- Самойлов Віктор Дмитрович, доктор технічних наук, професор
- Шкарупило Вадим Вікторович, доктор технічних наук, професор
- Кравцов Григорій Олексійович, кандидат технічних наук, старший дослідник

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. Актуальність теми дослідження

Процеси моніторингу та реагування на інциденти кібербезпеки в операційних центрах кіберзахисту (Security Operations Center, SOC) залежать від безперервності надходження телеметрії, узгодженості відомостей про активи та стабільності інфраструктурних компонентів. Воєнні впливи, масові порушення електроживлення і зв'язку, фізичне руйнування або втрата контролю над інформаційно-комунікаційною інфраструктурою спричиняють переривчастість журналювання, затримки доставлення подій, фрагментацію видимості та прискорення змін складу систем.

За умов неповної або суперечливої телеметрії традиційні правила кореляції не забезпечують однозначного розрізнення технічної недоступності активу та активності агента загроз. Наслідками є збільшення частки хибнопозитивних і хибнонегативних інтерпретацій, зміна пріоритетів

розслідування та прийняття дій реагування на основі неповного контексту. У дисертації спостережність інформації розглянуто як характеристику системи, що визначає можливість відновлення її внутрішнього стану за доступними вихідними сигналами.

Наявні підходи до резервування електроживлення і каналів зв'язку, географічного розподілення компонентів, використання хмарної інфраструктури та моніторингу доступності знижують ризик відмови окремих вузлів, але не формалізують стан втрати спостережності та не визначають порядок використання такого стану під час обробки подій безпеки. Тому актуальним є розвиток методів збору, обробки та аналізу інформації, які враховують повноту і достовірність телеметрії, динамічність активів, резервування, географічний контекст і профіль загроз.

2. Зв'язок роботи з науковими програмами, планами, темами

Тематика дисертаційної роботи відповідає пріоритетним напрямам розвитку науки і техніки в Україні. Роботу виконано відповідно до плану наукових досліджень Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, зокрема в межах науково-дослідних робіт «Кіберризики та кіберзахищеність топології розподілених інформаційних систем в глобальному кіберпросторі» (державний реєстраційний номер 0123U102744) та «Розроблення науково-обґрунтованих критеріїв та принципів побудови системи кіберзахисту об'єктів атомної енергетики» (державний реєстраційний номер 0123U100909).

3. Наукова новизна отриманих результатів

За результатами дисертаційного дослідження отримано такі наукові результати:

- вперше розроблено постановку задачі підвищення спостережності інформації у контексті деградації інфраструктури, у якій втрата спостережності визначається як стан системи, за якого повнота та/або достовірність телеметрії зменшується до рівня, що порушує коректність виконання щонайменше одного класу процедур операційного центру кіберзахисту: виявлення, розслідування, атрибуції або реагування; перехід у такий стан описано вимірюваними ознаками доступності джерел подій та узгодженості інвентаризаційних даних;
- дістав подальшого розвитку метод атрибутивного профілювання активів завдяки формуванню вектора атрибутів, релевантних для оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури, зокрема атрибутів динамізму, резервування, географічної приналежності, дескриптора загроз та часової актуальності спостережень;
- вперше запропоновано багатоконтурну архітектуру підвищення спостережності, у якій виділено контури інвентаризації та злиття даних про активи, аналітики подій та інцидентів, активного реагування, атрибутивного профілювання і обчислення правил та метрик, а також

візуалізації та звітності; на її основі розроблено прототип технічного рішення;

– 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 воєнних впливів і масштабної деградації інформаційно-комунікаційної інфраструктури.

4. Теоретичне та практичне значення результатів роботи

Теоретичне значення результатів полягає у розвитку формального апарату оцінювання спостережності комп'ютерних систем управління подіями безпеки. Запропоновано причинно-наслідкове відображення між ризиковими факторами, порушеними доменами керованості та операційними метриками; формалізовано стан втрати спостережності; визначено атрибутивне подання активу, придатне для оцінювання якості телеметрії та корекції правил кореляції. Розроблена методологія доповнює методи виявлення зловмисної активності процедурами встановлення причин технічної деградації та оцінювання допустимості аналітичних висновків.

Практичне значення результатів полягає у можливості використання розробленої методології, архітектурних вимог і програмного прототипу під час проєктування та модернізації технологічних платформ операційних центрів кіберзахисту. Запропоновані модулі підтримують багатоджерельну інвентаризацію активів, обчислення динамізму та дескриптора загроз, формування синтетичних подій втрати спостережності, контекстно-залежну кореляцію, оцінювання достатності резервування і пріоритезацію аналітичних дій.

Експериментальна перевірка засвідчила, що використання запропонованих методів зменшило загальну кількість сигналів з 217 до 59, кількість хибнопозитивних спрацювань зі 119 до 14, а кількість високопріоритетних і критичних сигналів — зі 146 до 38. Середня точність класифікації зросла з 0,429 до 0,765, середня повнота — з 0,776 до 0,916, значення F1-міри — з 0,551 до 0,832. Середній час виявлення (Mean Time to Detect, MTTD) зменшився з 84,3 с до 60,0 с.

5. Апробація та використання результатів дисертації

Результати дисертаційного дослідження апробовано під час доповідей та обговорень на наукових і науково-практичних заходах: ITS-2023: Information Technologies and Security; науково-практичній конференції «Резильєнтність критичної інфраструктури – 2023»; IV та V науково-практичних конференціях «Безпека енергетики в епоху цифрової трансформації»; II Всеукраїнській науково-практичній конференції «Theoretical and Applied Cybersecurity»; конференціях «Кібербезпека енергетики» 2024 та 2025 років; XLIII науково-технічній конференції молодих учених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України; конференції «Цифрова трансформація кібербезпеки»; науково-практичній конференції «Штучний інтелект і безпека».

Програмний прототип і експериментальний стенд використано для відтворення сценаріїв масової втрати електроживлення, деградації каналів зв'язку, відновлення після деградації та накладання зловмисної активності на фон технічної недоступності. Результати експериментів використано для перевірки правил диференціації причин втрати спостережності, алгоритмів пріоритезації та оцінювання якості класифікації.

6. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи дисертацію Драгунцова Романа Ігоровича визнано самостійною завершеною науковою працею, яка не містить ознак академічного плагіату, фабрикації або фальсифікації результатів. Використані положення, результати та тексти інших авторів супроводжуються посиланнями на відповідні джерела.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача

За результатами дослідження опубліковано 15 наукових праць за темою дисертації, з них 5 статей у наукових періодичних виданнях та 10 праць, що засвідчують апробацію результатів наукового дослідження.

Статті у наукових періодичних виданнях:

1. Drahuntsov R., Symonov A., Potenko O., Dybach O., Zubok V. Cybersecurity Monitoring During Power Outages: Use Cases for Enhanced Infrastructure Observability and Potential Implications for NPP Combined Events. Nuclear and Radiation Safety. 2025. No. 3(107). P. 17–29. DOI: 10.32918/nrs.2025.3(107).02.

   Особистий внесок здобувача: збір та аналіз референсних даних; визначення проблем спостережності інформації в досліджуваних умовах та референтних інфраструктурах; розроблення методів і контролів виявлення порушення спостережності та зменшення невизначеності за умов деградації інфраструктури.

2. Драгунцов Р.І., Зубок В.Ю. Моделювання загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання та потенційні заходи протидії. Електронне моделювання. 2023. Vol. 45, No. 3. P. 116–128. DOI: 10.15407/emodel.45.03.116.

   Особистий внесок здобувача: аналіз загроз і ризиків для інформаційно-комунікаційних систем, пов'язаних з атаками на енергосистему; порівняльний аналіз контрзаходів; формування підходів до моделювання загроз з урахуванням масштабних відключень електропостачання.

3. Драгунцов Р.І., Зубок В.Ю. Динамічні інфраструктурні компоненти та видимість системи під час реагування на інциденти кібербезпеки. Cybersecurity: Education, Science, Technique. 2025. No. 1(29). P. 493–507. DOI: 10.28925/2663-4023.2025.29.891.

Особистий внесок здобувача: ідентифікація ключових класів динамічних інфраструктурних компонентів; аналіз характеру впливу деградації енергетичної інфраструктури на динамічні компоненти інформаційно-комунікаційних систем та спостережність під час реагування на інциденти.

4. Попов О.О., Драгунцов Р.І. Ключові виклики для операційних центрів кібербезпеки в умовах повномасштабної війни. Інформаційні технології та суспільство. 2025. № 3(18). DOI: 10.32689/maup.it.2025.3.19.

Особистий внесок здобувача: збір статистичних даних; визначення специфічних факторів впливу воєнного часу на процеси обробки інформації в операційних центрах кіберзахисту; аналіз впливу руйнування енергетичної та телекомунікаційної інфраструктури, окупації та втрати об'єктів інформаційної інфраструктури і кібервійни на операційні показники.

5. Драгунцов Р.І., Зубок В.Ю. Методи підтримки спостережності інформаційно-комунікаційної інфраструктури в умовах повномасштабної війни. Електронне моделювання. 2026. Vol. 48, No. 1. P. 72–86. DOI: 10.15407/emodel.48.01.072.

Особистий внесок здобувача: аналіз наявних підходів до протидії погіршенню спостережності; формування дескриптивної моделі впливів воєнного часу на обробку подій безпеки; розроблення принципу зменшення невизначеності, атрибута динамізму та дескриптора загроз для об'єктів інформаційно-комунікаційної системи.

Наукові праці, що засвідчують апробацію результатів дослідження:

6. Drahuntsov R., Zubok V. A Method for Reducing the Uncertainty Caused by a Power Outage During a Cyber Incident Response. CEUR Workshop Proceedings. 2024. Vol. 3887. P. 226–236. URL: https://ceur-ws.org/Vol-3887/paper20.pdf.

Особистий внесок здобувача: визначення факторів впливу деградації енергетичної та комунікаційної інфраструктури на реагування; визначення класів операційних помилок за неповної телеметрії; розроблення алгоритму спрощення представлення інформаційно-комунікаційної системи під час реагування.

7. Зубок В.Ю., Драгунцов Р.І. Проєкція принципів національної системи стійкості та резильєнтність критичної інформаційної інфраструктури. Резильєнтність критичної інфраструктури – 2023: матеріали науково-практичної конференції. Київ, 21 червня 2023 р. С. 104–108.

Особистий внесок здобувача: дослідження нормативної бази у сфері кіберстійкості критичної інформаційної інфраструктури та систематизація вимог, релевантних для предмета дисертації.

8. Зубок В.Ю., Драгунцов Р.І. Особливості розслідування та реагування на інциденти кібербезпеки в умовах масових відключень електропостачання. Безпека енергетики в епоху цифрової трансформації: матеріали V науково-практичної конференції. Київ, 2023. С. 38–42.

Особистий внесок здобувача: дослідження підходів до обробки сигналів про інциденти в системах аналізу подій безпеки; оцінювання впливу деградації інфраструктури на процеси реагування.

9. Драгунцов Р.І., Зубок В.Ю. Особливості атак з використанням соціального графу та підходи до захисту. Theoretical and Applied Cybersecurity (TACS-2024): матеріали II Всеукраїнської науково-практичної конференції. Київ, 2024.

Особистий внесок здобувача: збір статистичних даних про атаки із застосуванням соціальної інженерії; визначення графового подання ланцюжка атаки та ризиків непрямих соціотехнічних впливів.

10. Зубок В.В., Драгунцов Р.І., Зубок В.Ю. Резильєнтність ERP-систем в умовах енергетичної кризи. Кібербезпека енергетики: матеріали науково-практичної конференції. Київ, 2024. С. 13–16.

Особистий внесок здобувача: оцінювання впливу деградації енергетичної інфраструктури на спостережність систем планування ресурсів підприємства та формування вимог до підтримання їх операційної стійкості.

11. Драгунцов Р.І. Особливості інцидентів інформаційної безпеки з залученням шкідливого програмного забезпечення в умовах кібервійни: аналіз та реагування. Матеріали конференції. Київ, 2024. Ч. 2. С. 65–68.

Особистий внесок здобувача: праця виконана здобувачем одноосібно; визначено особливості аналізу та реагування на інциденти зі шкідливим програмним забезпеченням за умов кібервійни.

12. Драгунцов Р.І., Зубок В.Ю. Проблематика інтеграції джерел виявлення технічних вразливостей в розрізі підтримки кіберстійкості критичної інфраструктури. XLIII науково-технічна конференція молодих учених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України. Київ, 14 травня 2025 р. С. 29–31.

Особистий внесок здобувача: збір статистичних відомостей про засоби управління вразливостями; визначення проблем інтеграції джерел; формування математичного подання зростання складності процесу управління вразливостями.

13. Драгунцов Р.І. Алгоритм управління ризиками кібербезпеки в умовах знищення енергетичної інфраструктури. Кібербезпека енергетики – 2025: матеріали науково-практичної конференції. Київ, 2025.

Особистий внесок здобувача: праця виконана здобувачем одноосібно; розроблено алгоритм урахування деградації енергетичної інфраструктури під час управління ризиками кібербезпеки.

14. Драгунцов Р.І. Процедури Threat Hunting в сучасному SOC: ключові підходи та проблематика оцінки покриття. Цифрова трансформація кібербезпеки: матеріали конференції. 2025. С. 40–42.

Особистий внесок здобувача: праця виконана здобувачем одноосібно; систематизовано процедури проактивного пошуку загроз і сформульовано підхід до оцінювання покриття технік агента загроз.

15. Драгунцов Р.І., Зубок В.Ю. Застосування великих мовних моделей для автоматичної ідентифікації окремих атрибутів поверхні атаки активів в кібербезпеці. Штучний інтелект і безпека – 2025: матеріали науково-практичної конференції. Київ, 2025.

Особистий внесок здобувача: розроблення концепції застосування великих мовних моделей для визначення дескриптора загроз активу та оцінювання можливостей їх інтеграції у процес управління активами.

ВВАЖАТИ:

Дисертаційну роботу Драгунцова Романа Ігоровича «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки, завершеною самостійною науковою працею. За науковим рівнем, новизною отриманих результатів, теоретичним і практичним значенням, змістом та оформленням робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії та напряму освітньо-наукової програми «Комп'ютерні науки» ІПМЕ ім. Г.Є. Пухова НАН України.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності», подану Драгунцовим Романом Ігоровичем на здобуття ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України утворити разову спеціалізовану вчену раду у складі:

Голова ради:

Мохор Володимир Володимирович, член-кореспондент НАН України, доктор технічних наук, професор, радник при дирекції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Рецензенти:

Кравцов Григорій Олексійович, кандидат технічних наук, старший науковий співробітник, старший науковий співробітник відділу математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України;

Гільгурт Сергій Якович, доктор технічних наук, старший науковий співробітник, завідувач відділу математичного та економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Опоненти:

Корченко Олександр Григорович, член-кореспондент НАН України, доктор технічних наук, професор, перший проректор Державного університету інформаційно-комунікаційних технологій;

Єфіменко Андрій Анатолійович, кандидат технічних наук, доцент, виконувач обов'язків завідувача кафедри кібербезпеки та захисту інформації Державного університету «Житомирська політехніка».

Головуюча на засіданні,
к.т.н., доцент, завідувачка відділу математичного та комп'ютерного моделювання ІПМЕ ім. Г.Є. Пухова НАН України
ІПМЕ ім. Г.Є. Пухова НАН України — Валентина Душеба

Гарант освітньо-наукової програми,
член-кореспондент НАН України,
д.т.н., проф., радник при дирекції
ІПМЕ ім. Г.Є. Пухова НАН України — Володимир МОХОР

Учений секретар
ІПМЕ ім. Г.Є. Пухова НАН України,
к.т.н. — Вікторія ЧЬОЧЬ