**РЕЦЕНЗІЯ**
на дисертаційну роботу
**Драгунцова Романа Ігоровича**
на тему «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності», представлену на здобуття ступеня доктора філософії
в галузі знань 12 – Інформаційні технології
за спеціальністю 122 – Комп’ютерні науки

**Актуальність теми дисертації**

Актуальність дисертаційного дослідження Р.І. Драгунцова зумовлена суттєвим ускладненням умов функціонування сучасних інформаційно-комунікаційних систем та процесів моніторингу, виявлення й реагування на інциденти кібербезпеки. Ефективність роботи операційних центрів кібербезпеки безпосередньо залежить від повноти, своєчасності та достовірності даних телеметрії, узгодженості відомостей про активи і стабільності інфраструктурних компонентів. В умовах воєнних впливів, пошкодження енергетичної та телекомунікаційної інфраструктури, масових відключень електропостачання та порушень каналів зв’язку виникає систематична деградація властивості спостережності інформаційних систем, що проявляється у фрагментації даних, переривчастості журналювання, затримках та втраті повідомлень про події.

Для комп’ютерних систем управління подіями безпеки залежність від фактичної доступності та достовірності вхідних даних є принциповою: деградація інфраструктури змінює склад доступної телеметрії, порушує надходження подій і створює умови для помилкової інтерпретації стану інформаційно-комунікаційної системи. В цьому сенсі розглядання та аналіз спостережності інформації як характеристики, що впливає на коректність подальших обчислювальних процедур є актуальним науковим завданням в галузі комп’ютерних наук, на вирішення якого насамперед спрямована дисертаційна робота, що подається на розгляд. На базі цього теоретичного здобутку в роботі також вирішено низку практичних завдань щодо підвищення ефективності процесів збору, обробки та аналізу інформації в комп’ютерних системах управління подіями безпеки за умов обмеженої спостережності.

**Ступінь обґрунтованості наукових положень, висновків і рекомендацій**

У дисертаційній роботі розв’язано науково-прикладну задачу підвищення ефективності процесів збору, обробки та аналізу інформації в комп’ютерних системах управління подіями безпеки за умов обмеженої спостережності,

спричиненої деградацією інформаційно-комунікаційної інфраструктури, неповнотою телеметрії та специфічними впливами військового часу.

Обґрунтованість висунутих положень, та висновків з отриманих результатів визначається послідовним переходом від аналізу умов функціонування комп'ютерних систем управління подіями безпеки до формалізованого опису втрати спостережності, розроблення методів, побудови прототипу та експериментальної перевірки. Для технічного дослідження суттєво, що запропоновані положення доведено до алгоритмічного й програмного представлення, придатного для перевірки за заданих сценаріїв деградації інфраструктури.

**Наукова новизна одержаних результатів**

Наукова новизна одержаних результатів на думку рецензента полягає в наступному.

1. Вперше розроблено 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 (виявлення, розслідування, атрибуція, реагування), а перехід у такий стан описується вимірюваними ознаками доступності джерел подій і узгодженості інвентарних даних.

2. Набув подальшого розвитку метод атрибутивного профілювання активів завдяки запропонованому вектору атрибутів, релевантних для оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури.

3. Вперше запропоновано багатоконтурну архітектуру спостережності, в якій виділено контури інвентаризації та злиття даних про активи, аналітики подій/інцидентів, активного реагування, атрибутивного профілювання та обчислення правил/метрик, а також візуалізації та звітності, що дозволило розробити прототип відповідного технічного рішення.

4. Розроблено методологію, орієнтовану на корекцію процесів обробки сигналів в операційних центрах кіберзахисту, спрямовану на виявлення та врахування деградації спостережності як необхідної умови коректної інтерпретації сигналів про кіберзагрози за умов воєнних впливів.

Цінним здобутком роботи в цілому є подання характеристик активів і стану спостережності у формі, придатній для подальшої машинної обробки. Введені атрибути використовуються не як описові ознаки, а як вхідні дані для правил обробки подій. Це забезпечує зв'язок між формальною частиною роботи та функціями прототипу.

Експериментальна частина підтверджує працездатність запропонованих методів у визначених умовах. Порівняння базового режиму з режимом, у якому враховується деградація спостережності, показує зміну якісних і кількісних характеристик обробки подій у напрямі, передбаченому постановкою задачі. Отримані результати достатні для підтвердження принципу роботи; питання оптимальності окремих ваг, порогів та обчислювальних процедур потребує окремого дослідження.

**Практичне значення одержаних результатів**

Практичне значення одержаних у дисертаційній роботі результатів полягає у можливості їх безпосереднього використання для підвищення ефективності функціонування операційних центрів кібербезпеки в умовах деградації інформаційно-комунікаційної інфраструктури та часткової втрати спостережності. Запропоновані автором методи дають змогу враховувати неповноту та недостовірність телеметрії, динамічність складу інфраструктури, стан каналів зв'язку й електроживлення, а також контекст загроз під час аналізу подій безпеки та прийняття рішень щодо реагування. Практично важливою є можливість застосування розроблених метрик і контролів для диференціації технічної недоступності компонентів та потенційної зловмисної активності, що сприяє зниженню кількості хибних спрацювань, зменшенню операційного навантаження на аналітиків і підвищенню обґрунтованості пріоритезації подій та інцидентів кібербезпеки.

**Оцінка змісту та структури дисертації, її завершеності й дотримання принципів академічної доброчесності**

Дисертація має загальний обсяг 179 сторінок, з яких 135 сторінок містять основний текст. Робота складається з вступу, чотирьох розділів, висновків, списку з 76 використаних джерел і двох додатків. Матеріал проілюстровано 24-ма рисунками та 9-тю таблицями.

Структура дисертації відповідає поставленій меті та семи завданням дослідження. Перші три завдання формують вихідну постановку: визначено існуючі методи обробки та аналізу подій, фактори повномасштабної війни і межі застосовності наявних підходів до протидії втраті спостережності. Четверте завдання реалізовано у формалізованій моделі впливу деградації інфраструктури. П'яте завдання одержало результат у вигляді методів підвищення спостережності та правил використання атрибутів активів. Шосте завдання завершено вимогами й багатоконтурною архітектурою спостережності. Сьоме завдання виконано шляхом створення експериментального стенду та перевірки розроблених методів.

Важливо, що технічна реалізація не підмінює наукову частину роботи. Архітектура і прототип використовуються для перевірки методів, а не як самостійне обґрунтування їх новизни. Така побудова відповідає характеру досліджень у галузі комп'ютерних систем, де формальний результат має бути співвіднесений із конкретною обчислювальною процедурою та можливістю її реалізації.

За поданим текстом дисертації, системою бібліографічних посилань та відомостями про особистий внесок здобувача підстав для висновку про некоректне використання результатів інших авторів не встановлено. Результати спільних публікацій супроводжуються визначенням особистого внеску здобувача. У вступі окремо зазначено використання інструменту штучного інтелекту для орфографічного, стилістичного та редакційного опрацювання тексту з покладенням відповідальності за прийняті правки на автора.

**Повнота викладення основних результатів у наукових публікаціях**

Основні положення дисертаційної роботи висвітлено у наукових публікаціях здобувача, безпосередньо пов'язаних із тематикою дослідження. Публікації охоплюють питання впливу деградації інфраструктури на кібербезпеку, спостережності інформації, динамічних компонентів інформаційно-комунікаційних систем, моніторингу під час відключень електропостачання та функціонування операційних центрів кіберзахисту в умовах повномасштабної війни.

Послідовність оприлюднення результатів відповідає розвитку дисертаційного дослідження: від постановки проблеми та аналізу факторів впливу до формалізації окремих характеристик, розроблення методів і їх експериментальної перевірки. Зміст опублікованих праць відповідає положенням, винесеним на захист.

Публікації засвідчують, що окремі положення роботи проходили наукове обговорення до їх об'єднання у дисертаційне дослідження. Для технічної роботи це є важливим, оскільки формування методів спирається на послідовну перевірку окремих складових, а не лише на кінцеву програмну реалізацію.

**Зауваження та дискусійні положення**

До зауважень та дискусійних моментів щодо дисертаційної роботи можна віднести наступне.

1. Під час оцінювання ефективності існуючих підходів до протидії втраті спостережності доцільно було б чіткіше задати набір критеріїв та умов, за якими здійснювалося порівняння.

2. Оскільки деякі параметри у запропонованих методах, такі як вагові коефіцієнти та порогові значення, встановлюються експертно, було б доцільно

оцінити стійкість цих методів по відношенню до варіацій даних параметрів, що дозволило б краще визначитися зі сферами їх застосування.

3. Не наведено кількісної оцінки обчислювальних витрат, потрібних для злиття даних про активи, перерахунок похідних атрибутів та розрахунків правил, які можуть виявитися суттєвими для великих інформаційно-комунікаційної системи.

4. Експериментальна перевірка запропонованих методів проведена у відносно обмеженому за масштабом модельному середовищі, а набір даних сформовано на основі експертної оцінки відтворення різних параметрів резервування, критичності та характеристик активів, що ускладнює оцінку статистичної відтворюваності отриманих результатів.

5. Текст дисертаційної роботи містить велику кількість помилок, насамперед, пунктуаційних та друкарських, також мають місце вади оформлення, зокрема:

– багато помилок у розділі ЗМІСТ та в нумерації пунктів у тексті;

– пропущені коми: в останньому абзаці підрозділу про актуальність, у формулюваннях наукового завдання та предмету дослідження, в четвертому пункті наукової новизни, в першому реченні пункту 2.4.14, в описі внеску здобувача в публікацію [9], і не тільки;

– зайві коми: у формулюванні об’єкту дослідження, в четвертому пункті наукової новизни, в другому реченні пункту 2.4.10;

– зайві крапки: в останньому рядку Таблиці 6, в другому реченні пункту 2.4.12, в останньому реченні підпункту 3.2.1.6;

– у формулюванні об’єкту дослідження пропущено дієслово "є";

– останнє слово в підрозділі про методи дослідження – "метології" замість "методології";

– в третьому пункті наукової новизни – "звітностіпрототипу" замість "звітності прототипу";

– в останньому рядку Таблиці 6 – "формуванняя" замість "формування";

– в другому реченні пункту 3.3.1 – "інформаціні" замість "інформаційні";

– в другому реченні підрозділу 4.3 – "Logstah" замість "Logstash";

– в останньому рядку Таблиці 7 – "Модуль визначення дескриптору загроз" замість "Модуль визначення дескриптора загроз";

– у передостанньому абзаці висновків до розділу 4 – "знижена н 74%" замість "знижена на 74%" тощо;

– на деяких рисунках – дуже дрібний текст.

Але згадані зауваження не є критичними та не зменшують загальну позитивну оцінку наукової та практичної значимості результатів дисертаційної роботи та рівня кваліфікації її автора.

**Загальний висновок про дисертаційну роботу**

Вважаю, що дисертаційна робота Драгунцова Романа Ігоровича на тему «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності» є завершеним самостійним науковим дослідженням, в якому розв'язано науково-прикладну задачу підвищення ефективності процесів збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки за умов обмеженої спостережності, спричиненої деградацією інформаційно-комунікаційної інфраструктури, неповнотою телеметрії та специфічними впливами військового часу.

За актуальністю, змістом, структурою, обґрунтованістю результатів та повнотою їх оприлюднення дисертаційна робота відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а здобувач Роман Ігорович Драгунцов заслуговує на присудження ступеня доктора філософії в галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

**Рецензент:**
Завідувач відділу математичного
та економетричного моделювання
Інституту проблем моделювання в
енергетиці ім. Г.Є. Пухова НАН України,
докт. техн. наук, ст. наук. співр. Сергій ГІЛЬГУРТ

М.П. «____» _____ 2026 року