**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 роботи обумовлюється потребою в обробці та аналізі інформації за умов, коли частина відомостей про стан інформаційно-комунікаційної системи відсутня, надходить із запізненням або не узгоджується з інвентарними даними. Для комп’ютерних систем управління подіями безпеки така ситуація змінює умови застосовності існуючих алгоритмів виявлення та аналізу подій.

В роботі деградація інфраструктури розглядається як фактор, що змінює спостережність інформації. Така постановка завдання дослідження є коректною для спеціальності 122 Комп’ютерні науки, оскільки спрямоване на методи збору, аналізу та консолідації розподіленої інформації, а саме формалізацію стану системи, побудову моделі впливу, визначення параметрів активів, алгоритмічне використання цих параметрів та перевірку запропонованих рішень засобами комп’ютерного моделювання.

Фактори повномаштабної війни підкреслюють виразність поставленого завдання дослідження, але отримані результати мають ширшу застосовність до розподілених інформаційно-комунікаційних систем, що працюють за неповної або нестійкої телеметрії.

**Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.**

Структура дослідження є послідовною з точки зору математичного та комп’ютерного моделювання: вихідні фактори та обмеження переводяться у формалізовані ознаки, визначаються методи їх використання, після чого виконується програмна реалізація й обчислювальний експеримент. Відповідність між постановкою задачі, структурою моделі, алгоритмами і дослідною перевіркою простежується по всій роботі.

Наукова новизна здобутих результатів полягає в такому:

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. Дістав 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.

Наукові положення обґрунтовуються функціональним і порівняльним аналізом, формалізацією, математичним та комп’ютерним моделюванням, методами синтезу й архітектурного проєктування, експериментальним методом та імітаційним моделюванням. Вибір цих методів відповідає змісту поставлених завдань.

Формалізована модель встановлює структурні залежності між деградацією інфраструктури, втратою спостережності та якістю процесів обробки подій. Її адекватність у межах роботи підтверджується узгодженістю з реалізованими сценаріями та результатами функціонування прототипу.

**Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.**

Зміст дисертації відповідає меті та завданням, сформульованим у вступі. Перші три завдання виконують функцію постановки та обмеження предметної області: визначено існуючі методи обробки і аналізу подій, фактори впливу повномасштабної війни та ефективність наявних підходів до протидії втраті спостережності. Четвертому завданню відповідає формалізована модель впливу деградації інфраструктури на спостережність інформації. П’ятому - розроблені методи підвищення спостережності. Шостому - вимоги та архітектура системи, що реалізує розроблені методи. Сьомому - склад експериментального стенду та результати перевірки.

Системність дослідження виявляється у послідовності, де кожний наступний етап використовує результат попереднього. Введені у формальній частині атрибути присутні у структурі даних прототипу; правила, що спираються на ці атрибути, перевіряються в експерименті.

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. Формальна оцінка текстових збігів має здійснюватися відповідно до процедури академічної доброчесності установи.

**Мова та стиль викладення результатів.**

Мова дисертації відповідає науковому стилю. Основні терміни використано відповідно до вступу та предмета дослідження: «спостережність інформації», «втрата спостережності», «деградація інфраструктури», «телеметрія», «інвентарні дані», «атрибутивне профілювання активів», «вектор атрибутів», «дескриптор загроз», «багатоконтурна архітектура спостережності».

Виклад матеріалу є послідовним, а використана термінологія загалом узгоджена з предметом дослідження.

**Оприлюднення результатів дисертаційної роботи.**

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.

Наявні публікації дають змогу простежити формування основних положень роботи у часі та їх апробацію в науковому середовищі. Наукові результати, винесені на захист, мають відповідне відображення у публікаціях здобувача.

**Недоліки та зауваження до дисертаційної роботи.**

1. У роботі запропоновано використовувати відкриту модульну архітектуру. Водночас потребує додаткового обґрунтування вибір критерії оцінки варіантів аррхітектурних стилів, оцінка за критеріями варіантів архітектуриних стилів та пояснення чому саме віддано пріоритет відкритій модульній архітектурі.

2. Потребує уточнення співвідношення між переривчастістю журналювання та фрагментацією видимості: не цілком визначено, чи розглядається перше поняття як часовий прояв втрати даних від окремого джерела, а друге — як системний стан неповного охоплення активів і сегментів.

3. Не цілком розкрито, яким чином формалізація стану спостережності забезпечує його вимірюваність. Доцільно чіткіше показати зв'язок між формальним поданням параметрів, визначеними показниками та процедурою їх обчислення.

4. Потребує конкретизації поняття «традиційні методи кореляції». Доцільно визначити, які саме підходи, розглянуті в роботі, віднесено до традиційних, і за якими ознаками здійснено таку класифікацію.

5. У тексті дисертації наявні орфографічні та друкарські помилки, які не впливають на зміст роботи.

Зазначені зауваження мають уточнювальний і редакційний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та можуть бути враховані під час її доопрацювання.

**Висновок про дисертаційну роботу.**

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 науковим дослідженням. Сформульовані у вступі завдання мають відповідні результати в основній частині роботи, а застосовані методи дослідження відповідають характеру цих завдань.

За актуальністю, рівнем формалізації, обґрунтованістю наукових результатів, їх новизною та практичним значенням дисертаційна робота відповідає вимогам чинного законодавства України, передбаченим Порядком присудження ступеня доктора філософії, затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. № 44. Роман Ігорович Драгунцов заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

**Рецензент:**

Старший науковий співробітник відділу математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, кандидат технічних наук _____ Григорій КРАВЦОВ

М.П. «____» _____ 2026 року