

ВІДГУК

офіційного опонента 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 дисертаційної роботи зумовлена умовами функціонування сучасних розподілених інформаційно-комунікаційних систем. Стан окремого активу у таких системах встановлюється за сукупністю подій, мережною зв'язністю та інвентарними даними. Відмова електроживлення, деградація каналу зв'язку або зміна топології можуть призвести до втрати частини телеметрії без фактичного порушення безпеки самого активу. Для комп'ютерних мереж ця проблема має системний характер. Один і той самий результат на рівні центральної системи (відсутність подій чи недоступність активу) може мати різні причини: втрати живлення, порушення маршрутизації, розриву каналу, відмови джерела подій або реалізації кіберзатаки. Тому розроблення методів, які враховують стан інфраструктури ІКС під час обробки та аналізу подій безпеки, а також комп'ютерних систем управління ними є обґрунтованим напрямом дослідження.

Тема відповідає спеціальності 122 Комп'ютерні науки, оскільки стосується методів збору й аналізу інформації, формування структур даних про активи, алгоритмів обробки подій, розробки та реалізації архітектури технічного рішення, а також експериментальної перевірки у розподіленому середовищі.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Достовірність результатів забезпечується узгодженням формальної, архітектурної та експериментальної частин роботи. Автор використовує дані про активи, мережні сегменти, резервування, доступність джерел подій та інші атрибути, що можуть бути одержані у реальних інформаційно-комунікаційних системах. Розроблені правила перевіряються на сценаріях втрати електроживлення, деградації каналів зв'язку, відновлення та накладання сигналів про кіберзагрози.

Наукова новизна здобутих результатів полягає в такому:

1. Вперше розроблено постановку задачі підвищення спостережності інформації у контексті деградації мережної 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.

З позиції проєктування, побудови та експлуатації комп'ютерних мереж особливо важливо, що в багатоконтурній архітектурі спостережності відокремлено інвентаризацію і злиття даних про активи від аналітики подій та активного реагування. Такий розподіл функцій відповідає практиці побудови розподілених систем і спрощує інтеграцію з різними джерелами телеметрії.

Експеримент підтверджує працездатність методів у мережних сценаріях, де центральна комп'ютерна система управління втрачає частину інформації про активи або сегменти. Отриманий результат важливий тим, що обробка подій виконується з урахуванням причини деградації, а не лише факту недоступності.

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

Структура дисертації відповідає логіці розроблення технічного методу для розподіленої системи. На початковому етапі визначено умови, за яких наявні методи обробки подій втрачають ефективність. Далі сформовано

модель впливу деградації інфраструктури, розроблено методи підвищення спостережності, встановлено вимоги до технічного рішення й виконано експериментальну перевірку.

Сім завдань, наведених у вступі, мають відповідні результати. Особливо важливим є зв'язок між завданням розроблення архітектури системи управління та завданням експериментальної перевірки, а саме реалізований стенд відтворює основні функції багатоконтурної архітектури спостережності й використовує ті самі атрибути, які визначено в методичній частині.

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.

Дисертація написана українською мовою. Стиль викладення матеріалу – науковий. Термінологія є науковою та професійною, у цілому відповідає предметній області спеціальності та предмету дослідження. Водночас у тексті роботи доречно послідовно використовувати терміни «інформаційно-комунікаційна система», «спостережність інформації», «телеметрія», «джерело подій», «інвентарні дані», «актив», «мережевий сегмент», «деградація інфраструктури», «атрибутивне профілювання активів». Для мережних і хмарних компонентів слід уникати різних назв одного й того самого явища чи сутності, якщо вони не мають окремого технічного значення. Окремі редакційні помилки та відхилення від вимог оформлення, зокрема, оформлення таблиць, порушення нумерації формул у розділі 2, потребують виправлення у фінальній версії.

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 етапу постановки проблеми та аналізу факторів впливу до формалізації окремих характеристик, розроблення методів і їх експериментальної перевірки. Зміст опублікованих праць відповідає положенням, винесеним на захист.

Тематика публікацій охоплює як загальні умови функціонування операційних центрів кіберзахисту, так і питання спостережності інформаційно-комунікаційної інфраструктури та моніторингу під час порушення електроживлення. Це відповідає предмету дисертації та підтверджує апробацію основних положень.

Недоліки та зауваження до дисертаційної роботи.

1. Деградація каналів зв'язку у експерименті представлена переважно значною або повною втратою зв'язності. Для розподілених комп'ютерних мереж доцільно окремо перевірити режими зі зростанням затримки, втратою пакетів, нестійким маршрутом, наявністю петель маршрутизації і запізненою доставкою подій без повного розриву каналу.

2. Багатоконтурна архітектура спостережності передбачає застосування у різних інформаційно-комунікаційних системах, однак експериментальний стенд переважно відтворює класичну сегментовану комп'ютерну мережу. Перевірка на віртуалізованих та хмарних ресурсах посилила б обґрунтованість висновків щодо динамізму активів.

3. У моделі використовуються відомості про резервування каналів зв'язку та електроживлення. Доцільно детальніше визначити порядок врахування складних мережних топологій, у яких доступність активів залежить від кількох послідовних або резервних маршрутів.

4. Не наведено окремої оцінки продуктивності злиття даних і правил обробки подій при значному збільшенні кількості активів, мережних сегментів та інтенсивності телеметрії. Для практичного використання у великих розподілених системах така перевірка є важливою.

5. Частина показників експерименту характеризує автоматизовану обробку подій у лабораторному стенді комп'ютерної системи управління. Їх не слід без додаткового обґрунтування ототожнювати з часовими показниками повного операційного процесу, в якому бере участь аналітик.

Зауваження стосуються переважно розширення набору мережних режимів і масштабування стенду. Вони не змінюють позитивної оцінки одержаних результатів.

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, у якому методи підвищення спостережності інформації доведено до архітектури технічного рішення та експериментальної перевірки.

Робота має наукову новизну, відповідає предметній області спеціальності і містить результати, придатні для подальшого розвитку систем збору й аналізу подій у розподілених інформаційно-комунікаційних системах.

Вважаю, що дисертаційна робота відповідає вимогам чинного законодавства України, передбаченим пунктами 6–9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Роман Ігорович Драгунцов заслуговує на присудження ступеня доктора філософії у галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент:

Завідувач кафедри
кібербезпеки та захисту інформації
Державного університету
«Житомирська політехніка»,
кандидат технічних наук, доцент
10 вересня 2026 року

Андрій ЄФІМЕНКО