Отримано
10.04.2026 р
Голова спеціалізованої
вченої ради ДФ 26.133.114
д.т.н., проф. Коршун Н.В.

Голові спеціалізованої вченої ради
ДФ 26.133.114
У Київському столичному університеті
імені Бориса Грінченка
доктору технічних наук, професору,
професору кафедри інформаційної та
кібернетичної безпеки імені професора
Володимира Бурячка Факультету
інформаційних технологій та
математики Київського столичного
університету імені Бориса Грінченка
Коршун Наталії Володимирівні

РЕЦЕНЗІЯ

РЗАЄВОЇ Світлани Леонідівни, кандидата технічних наук, доцента, доцента кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка, на дисертацію **НЕГОДЕНКА Віталія Петровича «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф»** подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

1. Актуальність теми дослідження

Сучасні інформаційні системи військового призначення функціонують в умовах постійного впливу кіберзагроз, які характеризуються високою динамікою розвитку, складною структурою та значним потенціалом деструктивного впливу на процеси управління. У зв'язку з цим забезпечення кібербезпеки військових інформаційних систем є одним із ключових завдань системи національної безпеки та оборони держави.

Особливого значення набуває проблема прогнозування критичних станів інформаційних систем та забезпечення їх стійкості в умовах кіберконфліктів. Традиційні підходи до аналізу ризиків і реагування на кіберінциденти часто базуються на статичних або лінійних моделях, які не дозволяють точно описувати нелінійні процеси, характерні для сучасних інформаційних систем. Саме тому, використання математичної теорії катастроф і теорії конфліктів для моделювання процесів забезпечення кібербезпеки військових інформаційних систем є перспективним напрямом розвитку наукових досліджень. Застосування таких підходів дозволяє виявляти критичні переходи станів системи, прогнозувати можливі сценарії розвитку кіберінцидентів та забезпечувати прийняття обґрунтованих управлінських рішень.

Виявлені невирішені питання вказують на те, що тема дисертаційної роботи Негоденко В.П. є актуальною, своєчасною та має важливе теоретичне і практичне значення для розвитку систем кібербезпеки.

2. Зв'язок теми дисертаційної роботи з науковими програмами, планами, фундаментальними та прикладними дослідженнями

Дисертація виснувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ).

Також результати досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 09.12.2025 року), Інституту програмних систем Національної академії наук України (акт від 09.12.2025 року), військової частини А2393 (довідка від 05.02.2026.) та Військового інституту телекомунікацій та інформатизації імені Героїв Крут (акт від 22.03.2026).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їх достовірність

Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі, є достатньо обґрунтованими та логічно узгодженими між собою, що підтверджується аналізом значної кількості наукової та технічної літератури, а також використанням методів теорії конфліктів, теорії катастроф, кластерного аналізу, теорії функцій, теорії алгоритмів, теорії складності алгоритмів, теорії ймовірностей та математичної статистики, а також методів математичного, комп'ютерного та імітаційного моделювання.

Достовірність отриманих результатів підтверджується проведенням експериментальних досліджень, аналізом отриманих даних та порівнянням результатів із відомими підходами до забезпечення кібербезпеки інформаційних систем. Всі практичні і теоретичні результати дослідження апробовано на конференціях та опубліковано в наукових статтях. Перелік наукових праць Негоденко В.П. та довідки щодо впровадження результатів дослідження підтверджують фаховий підхід здобувача до обрання теми роботи та високий рівень наукової компетентності.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

Представлені в дисертації Негоденко Віталія Петровича положення, підходи, структура, постановка завдання та їх вирішення, узагальнені висновки розкривають авторську ідею і самостійно виконану наукову працю, в якій обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

– вперше запропоновано математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик», що дозволяє прогнозувати перехід системи до небезпечного стану, яка відрізняється від лінійних моделей оцінювання ризиків тим, що враховує нелінійну динаміку змін станів інформаційної системи та дозволяє виявляти передкризові режими функціонування системи. Використання запропонованої моделі збільшує в 2,5 рази час попередження про перехід стану системи до критичного;

– удосконалено метод кластеризації загроз та уразливостей, який на відміну від методу k-means, враховує часову динаміку кіберінцидентів, що забезпечує високу часову узгодженість (0,985), а використання ковзних часових рядів дозволяє зменшити шум в даних приблизно 85%, що зменшує суб'єктивність експертних оцінок і підвищує об'єктивність управління ризиками у військових інформаційних системах;

– вперше запропоновано модель прогнозування критичних переходів, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції теорії катастроф у SIEM-системи. На відміну від традиційних підходів моніторингу кіберінцидентів, запропонована модель забезпечує виявлення нестійкі режими функціонування системи та формування сигналів про перехід системи до критичного стану.

Використання даної моделі дозволяє SIEM-системі за 2-3 дні сформувати попередження про перехід інформаційної системи до критичного стану;

– набув подальшого розвитку метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів та катастроф. Запропонований метод забезпечує комплексне виявлення, класифікацію та прогнозування критичних станів на 15-25% в порівнянні з методами машинного навчання (SVM, Random Forest), що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів.

Таким чином, мета дослідження щодо підвищення кіберстійкості військових інформаційних систем за рахунок розробки моделей та методів забезпечення кібербезпеки на основі застосування математичної теорії катастроф та теорії конфліктів для аналізу та моделювання складної нелінійної динаміки функціонування систем під впливом кіберзагроз і прогнозування критичних переходів їх станів досягнута.

5. Теоретична цінність і практична значущість наукових результатів

Наукові положення, висновки та рекомендації дисертаційної роботи Негоденко Віталія Петровича мають теоретичну цінність та практичну важливість.

Теоретична цінність дисертаційної роботи полягає у розвитку наукових засад забезпечення кібербезпеки інформаційних систем за допомогою математичних моделей аналізу критичних станів систем на основі методів теорії катастроф і теорії конфліктів. Запропонований підхід дозволяє описати процеси взаємодії між загрозами та механізмами захисту, визначати критичні режими функціонування інформаційних систем та розширює існуючі наукові підходи до моделювання кіберстійкості в умовах динамічного розвитку кіберзагроз. Отримані результати створюють

теоретичне підґрунтя для подальшого розвитку методів прогнозування критичних станів і оцінювання стійкості інформаційних систем.

Практичне значення отриманих результатів полягає у можливості використання розроблених моделей і методів прогнозування критичних станів для підвищення рівня кіберстійкості інформаційних систем та ефективності функціонування систем управління інформаційною безпекою в умовах зростання інтенсивності кіберзагроз. Запропоновані рішення можуть бути використані підрозділами кібербезпеки для своєчасного виявлення ознак втрати стійкості систем, підтримки прийняття управлінських рішень щодо реагування на кіберінциденти та оцінювання стану захищеності інформаційно-комунікаційних систем. Отримані результати сприяють підвищенню надійності функціонування інформаційних систем державного і військового сектору в умовах сучасних кіберзагроз.

Запропоновані рішення використані в наукових дослідженнях Інституту програмних систем Національної академії наук України, які пов'язані з аналізом кіберінцидентів та кіберзагроз, моделюванням процесів інформаційної безпеки, прогнозуванням критичних станів інформаційних систем та розробкою методів підвищення кіберстійкості інформаційних систем. Крім того, розробки інтегровані в освітній процес Київського столичного університету імені Бориса Грінченка, а також використані при відпрацюванні наукової продукції при розробці оперативного завдання у Військовому інституті телекомунікацій та інформатизації імені Героїв Крут.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

Основні результати дисертації висвітлено у 8 наукових публікаціях, із них усіх у співавторстві: 6 статті (з них 3 у співавторстві) у наукових

виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті (з них усі у співавторстві) у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях відповідно до мети та поставлених завдань.

Основні положення дисертаційної роботи були апробовані на науково-практичних конференціях, що підтверджує їх наукову та практичну значущість.

7. Відсутність (наявність) порушення академічної доброчесності

Аналіз змісту дисертації, а також публікацій Негоденко В.П. вказують на відсутність ознак порушення вимог академічної доброчесності. Дисертаційна робота містить посилання на джерела інформації у випадку використання ідей, розробок, тверджень, відомостей, а також відповідає нормам законодавства про авторське право і суміжні права. В дисертації Негоденко В.П. надає достовірну інформацію про результати вдасної наукової діяльності, а також про використані методи та моделі досліджень та інформаційні ресурси.

8. Дискусійні положення та зауваження до дисертації

Принципових зауважень щодо структури, основних положень та концепції дисертації Негоденко В.П. не виявлено.

Позитивно оцінюючи результати дисертаційного дослідження, слід звернути увагу на окремі зауваження та рекомендації до окремих положень дисертації.

1. У роботі запропоновано математичну модель прогнозування критичних станів інформаційних систем на основі теорії катастроф типу «Метелик». Було б доцільно більш детально описати процедуру

калібрування параметрів моделі, зокрема вибір початкових значень параметрів, критерії збіжності алгоритму оптимізації та провести аналіз чутливості моделі до зміни вагових коефіцієнтів кіберінцидентів.

2. Метод кластеризації загроз і уразливостей військових інформаційних систем, запропонований у роботі, враховує часову динаміку розвитку кіберінцидентів. Разом з тим залишилося недостатньо висвітленим питання вибору параметрів кластеризації (розмір часових вікон, кількість кластерів, критерій зупинки алгоритму), тому було б доцільно докладніше описати процедуру налаштування цих параметрів.

3. У роботі на Рис. 3.2 наведено схему математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою, яка включає модулі збору даних, математичного моделювання та підтримки прийняття рішень. Було б доцільно більш детально описати механізм взаємодії між зазначеними модулями, зокрема порядок передачі даних між ними та вимоги до часових характеристик обробки інформації.

4. В тексті дисертаційної роботи виявлено певні неточності та помилки технічного характеру:

- розділ 4 на стр. 186 у визначенні показників матриці помилок використано позначення TN (Tru Negative) та TP (Tru Positive), де, ймовірно, малося на увазі True Negative та True Positive;
- розділ 4 на стр. 187 у формулі часу попередження $EWT = t_m - t_{pr}$ не зазначено одиниці вимірювання часу та умови застосування показника, що доцільно було б уточнити;

Наведені зауваження мають рекомендаційний характер і не знижують загальної позитивної оцінки дисертаційної роботи.

9. Загальна оцінка дисертаційної роботи, її відповідність встановленим вимогам

Дисертаційна робота Негоденка Віталія Петровича на тему: «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф» є завершеним науковим дослідженням, яке за актуальністю, науковою новизною, обґрунтованістю результатів і практичною значущістю відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», що затверджено Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, **Негоденко Віталій Петрович**, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензент:
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Київського столичного університету
імені Бориса Грінченка Світлана РЗАЄВА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
КОД ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
ЗАСВІДЧУЮ
(ПІБ)
(посада)