Отримано
дд.04.2026 р.
Голова спеціалізованої
вченої ради ДФ 26.133.114
д.т.н., проф. Я.В. Коршунов

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

ВІДГУК

офіційного опонента доктора технічних наук, професора, професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка **ТОЛЮПИ Сергія Васильовича** на дисертаційну роботу **НЕГОДЕНКА Віталія Петровича** на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф», представлену на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

1. Актуальність теми дисертації.

У сучасних умовах цифровізації оборонної сфери військові інформаційні системи стають критично важливим елементом забезпечення національної безпеки та ефективності ведення бойових дій. Їх функціонування безпосередньо впливає на прийняття управлінських рішень, координацію сил і засобів, а також на досягнення інформаційної переваги. Умови функціонування сучасних військових інформаційних систем суттєво ускладнилися: вони розглядаються як багаторівневі, динамічні комплекси, що працюють під постійним впливом навмисної протидії. Це підвищує вимоги до їхньої стійкості, здатності до адаптації та збереження працездатності, оскільки такі системи є пріоритетною ціллю для складних і багаторівневих кібератак, що можуть призводити до дестабілізації управління, втрати даних і зриву військових операцій. Сучасні кіберконфлікти характеризуються високою динамічністю, прихованістю та використанням комбінованих впливів на інформаційні системи і критичну

інфраструктуру, що ускладнює їх своєчасне виявлення та ідентифікацію. Це обумовлює необхідність розроблення нових підходів до моделювання кіберпротиборства, які враховують конфліктний характер взаємодії сторін. Крім того, традиційні методи забезпечення кібербезпеки часто базуються на реактивних підходах і не забезпечують адекватного врахування нелінійних процесів розвитку кіберінцидентів, які можуть мати властивості різких стрибкоподібних змін стану систем, що виникають під впливом сукупності внутрішніх і зовнішніх факторів

Таким чином, дисертаційна робота Негоденка В.П., присвячена розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі теорії конфліктів та катастроф для моделювання динаміки загроз та підтримки прийняття рішень щодо підвищення кіберстійкості, є актуальним та вчасним науковим дослідженням. Напрям дисертаційного дослідження Негоденка В.П. безпосередньо пов'язаний із реалізацією ключових державних стратегічних документів, а саме: Доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

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

Дисертаційна робота виконувалася відповідно до планів наукових досліджень на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в межах науково-дослідної роботи «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (номер державної реєстрації 0122U200483, КСУБГ, м. Київ). У межах зазначеної НДР здобувачем особисто було розроблено низку ключових компонентів, що становлять основу дисертації, зокрема: математичну модель впливу кіберінцидентів на стійкість систем управління безпекою з використанням апарату теорії катастроф; удосконалений метод кластеризації загроз та уразливостей, який враховує часову динаміку подій; модель прогнозування критичних переходів станів, призначену для інтеграції в архітектуру SIEM-систем; метод підтримки прийняття рішень для забезпечення кіберстійкості військових систем на основі синтезу теорій конфліктів та катастроф.

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

Аналіз змісту дисертаційної роботи свідчить, що визначені мета, завдання, об'єкт і предмет дослідження узгоджуються з темою дисертації та відображають ключові напрями наукових досліджень, виконаних автором.

Обґрунтованість наукових положень, висновків і рекомендацій забезпечується чіткою постановкою дослідницьких завдань, належним рівнем їх теоретичного й практичного опрацювання, а також коректним використанням відповідних методів для їх розв'язання, зокрема: математичного апарату теорій конфліктів та катастроф, методів кластерного аналізу, теорії функцій та алгоритмів, а також методів теорії ймовірностей та математичної статистики. Достовірність отриманих результатів підтверджується використанням реальних статистичних даних, результатами комп'ютерного та імітаційного моделювання, яке підтверджує переваги запропонованих рішень, та практичним впровадженням.

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

У дисертаційній роботі отримано наукові результати, що мають вагоме теоретичне та прикладне значення для розвитку підходів до захисту інформаційних систем оборонного призначення. Зазначені результати відзначаються науковою новизною та відображають внесок автора у розв'язання актуальних наукових завдань у сфері кібербезпеки. Основні наукові результати, що визначають новизну роботи, полягають у наступному:

– 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;

– удосконалено метод кластеризації загроз та уразливостей, який на відміну від методу k-means, враховує часову динаміку кіберінцидентів, що забезпечує високу часову узгодженість, а використання ковзних часових рядів дозволяє зменшити шум в даних, 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 і 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, що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів.

Представлені результати свідчать про особистий внесок здобувача у розв'язання важливого наукового завдання – підвищення рівня захищеності та живучості військових інформаційних систем в умовах інтенсивної кіберпротидії.

5. Теоретична цінність і практична значущість наукових результатів

Теоретична цінність дисертаційного дослідження полягає у формуванні комплексного наукового підходу до забезпечення кіберстійкості військових інформаційних систем (ВІС) на основі синтезу математичних теорій конфліктів та катастроф. Робота розширює теоретичну базу кібербезпеки за рахунок обґрунтування використання катастрофи типу «Метелик» для моделювання нелінійної динаміки змін станів системи, що дозволяє ідентифікувати передкризові режими та точки біфуркації, які не фіксуються традиційними лінійними моделями. Теоретично доведено доцільність врахування часової агрегації подій у методах кластеризації загроз, що забезпечує перехід від аналізу окремих інцидентів до оцінки цілісних режимів функціонування системи управління безпекою. Розроблений метод підтримки прийняття рішень створює наукове підґрунтя для побудови інтелектуальних систем, здатних прогнозувати дестабілізаційні процеси в умовах активної кіберпротидії.

Практична значущість отриманих результатів визначається можливістю їх застосування для підвищення живучості та захищеності інформаційного простору Збройних Сил України, зокрема:

– імплементація моделі прогнозування критичних переходів у SIEM-системи дозволяє отримувати попередження про можливі збої за 2–3 дні до їх настання;

– удосконалений метод кластеризації забезпечує автоматизацію аналізу великих масивів даних у реальному часі, що підвищує точність визначення стану системи у 2 рази;

– запропонований метод підтримки прийняття рішень дозволяє знизити рівень хибних спрацювань системи захисту на 62%, що суттєво підвищує ефективність роботи аналітиків центрів моніторингу.

Наукові положення та практичні рекомендації дисертації впроваджені в діяльність військової частини А2393, Інституту програмних систем НАН України, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, а також використовуються в освітньому процесі Київського столичного університету імені Бориса Грінченка. Результати роботи можуть бути використані при розробці перспективних систем кіберзахисту об'єктів критичної інфраструктури України.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

Основні наукові результати та положення дисертаційного дослідження Негоденка В.П. повною мірою висвітлено у 13 наукових публікаціях, що відповідає чинним вимогам МОН України щодо оприлюднення змісту дисертацій на здобуття ступеня доктора філософії. До переліку опублікованих праць входять 6 наукових статей у наукових фахових видань України, 2 публікації у матеріалах CEUR Workshop Proceedings, що індексуються в базі Scopus, 5 публікацій за результатами виступів та обговорень на наукових конференціях різних рівнів. Аналіз публікацій за темою роботи підтверджує особистий внесок здобувача у кожній праці. Зміст опублікованих праць цілком відповідає основним положенням дисертації, що дозволяє зробити висновок про належне та повне оприлюднення результатів проведеного наукового дослідження.

7. Відсутність (наявність) порушення академічної доброчесності

Аналіз дисертаційної роботи та оприлюднених наукових праць за темою дослідження засвідчує відсутність ознак порушення вимог академічної доброчесності. За результатами перевірки встановлено, що дисертаційна робота є результатом самостійних досліджень здобувача. Робота не містить елементів плагіату, фальсифікації, фабрикації чи неправомірних запозичень. Усі використані ідеї, результати, методичні положення та тексти інших авторів мають належні посилання на відповідні першоджерела і використані автором виключно для підкріплення власних наукових висновків. Дисертаційна робота відповідає нормам законодавства України про авторське право і суміжні права. Матеріал викладено з дотриманням вимог наукової етики, що відображає прагнення автора до надання достовірної інформації про результати власної

наукової діяльності. Таким чином, можна зробити обґрунтований висновок про повне дотримання Негоденком В.П. принципів академічної доброчесності.

8. Дискусійні положення та зауваження до дисертації

Оцінюючи дисертаційну роботу Негоденка В.П. як ґрунтовне та завершене наукове дослідження, доцільно висловити низку дискусійних положень та зауважень:

1. У розробленій математичній моделі на основі катастрофи типу «Метелик» використано п'ять ключових категорій кіберінцидентів як параметрів керування. Варто було б надати більш детальне обґрунтування вибору саме цих показників порівняно з іншими типами загроз, що згадуються в роботі (наприклад, спуфінг або фішинг), а також описати механізм динамічного перерахунку вагових коефіцієнтів у разі раптової зміни інтенсивності окремих векторів атак.

2. При обґрунтуванні удосконаленого методу кластеризації загроз та уразливостей автор використовує ковзні часові вікна тривалістю 14 днів зі зсувом у 7 днів. Хоча ці параметри підтверджені експериментально, у роботі не в повній мірі розкрито можливість адаптації довжини вікна до інтенсивності потоку подій безпеки, яка у військових системах може коливатися від 100 до 100 000 щоденно, що могло б вплинути на точність виявлення дуже коротких у часі передкризових станів.

3. Запропонована модель прогнозування критичних переходів призначена для інтеграції в SIEM-системи. Проте в тексті дисертації недостатньо уваги приділено технічним аспектам обчислювальної складності реалізації розроблених алгоритмів у режимі реального часу, особливо в умовах обмежених ресурсів кінцевих вузлів військових інформаційних систем.

4. В описі методу підтримки прийняття рішень автор проводить порівняння з алгоритмами машинного навчання (SVM, Random Forest). Було б доцільно надати більш детальні рекомендації щодо налаштування порогових значень τ для різних сценаріїв бойового застосування системи, оскільки надмірна чутливість моделі може призвести до збільшення кількості хибних спрацювань у динамічному конфліктному середовищі.

Висловлені зауваження та дискусійні положення не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку 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, виконаним автором самостійно на високому науковому рівні. Сукупність отриманих автором нових теоретичних положень, удосконалених методів та розроблених математичних моделей у своїй єдності розв'язує актуальне наукове завдання – підвищення рівня кіберстійкості військових інформаційних систем в умовах нелінійної динаміки загроз та активної кіберпротидії. Дисертаційна робота Негоденка В.П. за своєю актуальністю, рівнем наукової новизни, теоретичною та практичною значущістю результатів повністю відповідає вимогам, встановленим у пп. 6-9 «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 також «Вимогам до оформлення дисертації», затверджених наказом Міністерства освіти і науки України від 12 січня 2017 року №40.

Враховуючи високий науковий рівень виконаного дослідження, вважаю, що здобувач Негоденко Віталій Петрович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

ОФІЦІЙНИЙ ОПОНЕНТ.
Професор кафедри кібербезпеки та захисту інформації
Факультету інформаційних технологій
Київського національного
університету імені Тараса Шевченка
доктор технічних наук, професор Сергій ТОЛЮПА

Підпис засвідчую
Вчений секретар НДЧ
Карауьна Н В
2025 р.