ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Негоденко Віталія Петровча на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Актуальність теми дослідження.

Глобальна інформаційна еволюція та інтенсифікація відповідних процесів перетворили інформацію на ключовий стратегічний ресурс військових інформаційно-телекомунікаційних (ІТ) систем. Згідно із звітом оперативного центру реагування на кіберінциденти Державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України за 2024 та 2025 роки найактивнішими виявленими кластерами кіберзагроз були UAC-0010, UAC-0006 та UAC-0050 (за класифікацією CERT-UA) саме на державні органи та сили оборони. Усвідомлення критичної важливості захисту інформаційного простору підкріплюється значними бюджетними асигнуваннями для реалізації відповідних інфраструктурних проєктів на міжнародній арені. Прогнозується, що світовий ринок військової кібербезпеки зросте з 19,2 мільярда доларів у 2024 році до 66,3 мільярда доларів до 2034 року, що відображає зростаючу важливість безпечного зв'язку в сучасній війні. Все це детермінує об'єктивну необхідність розробки цілісних систем кіберзахисту та гарантування безпеки критичних даних у ІТ-системах командування та управління, моніторингу розвідки, програмного забезпечення для логістичних дій, комунікаційних мережах та інструментах управління полем бою. Здійснюється перехід до програмно-визначеної безпечної архітектури, інтеграції штучного інтелекту для прогнозування та реагування на загрози.

Підтвердження зазначеного відображається у державних нормативних документах, зокрема наказом 692/нм від 15 жовтня 2025 року відповідно до статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах», пункту 4 Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затверджений постановою Кабінету Міністрів України від 18 червня 2025 року №712, підпункт 113 пункту 4 Положення про Міністерство оборони України від 26 листопада 2014 року №671 та з метою підвищення інформаційної безпеки та кібербезпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України було затверджено Галузевий профіль безпеки систем, де обробляється відкрита, конфіденційна або службова інформація. Даний Галузевий профіль безпеки систем відповідає вимогам міжнародних стандартів і національного законодавства з урахуванням особливостей оборонної галузі.

Відповідно до сучасних вимог сьогодення військові ІТ системи побудовані за принципом стійкості, що забезпечує безперервність та безпеку операцій при дії кіберзагроз за рахунок резервування, розділення мереж та шифруванні ліній зв'яку. Але при цьому зростає також розвиток складності самих загроз, які вже більш адаптивні, складні для виявлення та мають комплексно багаторівневу зону атаки. Статичні моделі та класичні методи захисту інформації не завжди враховують динамічний і конфліктний вплив загроз на уразливості інформаційної системи, тому доцільно застосовувати теорію конфліктів, яка дозволяє описати поведінку реагування на кіберзагрози, а також оцінити ефективність різних стратегій щодо забезпечення безпеки інформаційних систем.

Очевидно, що функціонування складних інформаційних систем не є лінійним, характеризується виникненням критичних станів, що можуть зумовити стохастичні переходи від нормативного режиму до стадії часткової або повної відмови. У зазначеному контексті ефективним інструментарієм для розв'язання даної проблеми є математична теорія катастроф, яка дозволяє не тільки виявляти, але і прогнозувати виникнення критичних точок, нестійкості та дестабілізації системи під впливом загроз.

Таким чином, існує необхідність вирішення актуального наукового завдання, сутність якого полягає у дослідженні та розвитку моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів з метою аналізу динаміки кіберзагроз, прогнозування критичних переходів станів системи та підвищення її кіберстійкості.

Дослідження проблеми забезпечення кібербезпеки інформаційних систем та підвищення їх кіберстійкості представлені у працях багатьох вчених, серед яких В. Бурячок, О. Корченко, О. Юдін, С. Гуцалюк, М. Опірський, Л. Крючкова, R. Ross, V. Pillitteri, U. Franke, J. Brynielsson, T. Alpcan, T. Basar, M. H. Manshaei, R. Thom, E. Zeeman, S. Wiggins, J.P. Hubaux, Q. Zhu, D. Nicol, W. Sanders, K. Trivedi та інші.

Проведений аналіз сучасних наукових досліджень показав, що більшість існуючих підходів використовують статистичні методи, методи машинного навчання або класичні моделі для аналізу та прогнозування стану інформаційних систем при дії загроз. Безперечно, проведення таких досліджень є доцільним та результативним, адже вони зробили вагомий внесок у розвиток наявної бази захисту інформації. Проте дані підходи не враховують конфліктну взаємодію між джерелами кібератак та системою захисту інформаційної системи, а також складну нелінійну динаміку функціонування інформаційних систем, що призводить до виникнення критичних станів системи та втрати їх стійкості.

Таким чином, необхідно вирішити актуальне наукове завдання, яке полягає в розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів для моделювання динаміки кіберзагроз, прогнозування критичних

переходів станів інформаційної системи та підтримки прийняття рішень щодо підвищення її кіберстійкості.

Зв'язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності 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).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в підвищенні 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.

У відповідності до поставленої мети для вирішення наукового завдання в роботі визначено та розв'язано такі *часткові завдання*:

- проаналізовано сучасні підходи забезпечення кібербезпеки військових інформаційних систем та визначено особливості нелінійної динаміки їх станів під впливом кіберінцидентів;
- обґрунтовано доцільність застосування математичної теорії катастроф та теорії конфліктів для моделювання динаміки станів інформаційних системи під впливом кіберінцидентів;
- розроблено математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик» та проведено оцінку її ефективності щодо впливу кіберінцидентів на стійкість систем;
- удосконалено метод кластеризації загроз та уразливостей інформаційних систем та проведено порівняльну оцінку його ефективності з класичними методами кластеризації;
- розроблено модель прогнозування критичних переходів станів інформаційної системи при інтеграції з SIEM- системою та проведено оцінку ефективності її застосування для раннього виявлення нестійких режимів функціонування системи;
- удосконалено метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який включає інтеграцію математичних моделей, методів аналізу та прогнозування на основі теорії конфліктів для моделювання протидії кіберзагрозам та теорії катастроф для прогнозування критичних станів системи;
- проведено оцінку ефективності удосконаленого методу підтримки прийняття рішень шляхом імітаційного моделювання сценаріїв реагування на кіберінциденти.

Об'єктом дослідження є процес функціонування військових інформаційних систем в умовах деструктивних кібервпливів.

Предметом дослідження є моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф для аналізу та прогнозування критичних переходів станів інформаційних систем.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися методи теорії конфліктів, методи теорії катастроф, методи кластерного аналізу; теорія функцій, теорія алгоритмів, теорія складності алгоритмів, теорії ймовірностей та математичної статистики; математичне, комп'ютерне та імітаційне моделювання.

Наукова новизна одержаних результатів полягає в подальшому розвитку і обґрунтуванні методів прогнозування та підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем на основі теорії конфліктів, теорії катастроф та методу кластерного аналізу.

1.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.

2. 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.

3. 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.

4. 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.

Практичне значення одержаних результатів полягає в тому, що в дослідженні запропоновано моделі та методи аналізу та прогнозування критичних станів військових інформаційних систем, які доцільно використовувати для підвищення ефективності попередження та виявлення кіберінцидентів, а також підтримки прийняття рішення під час реагування на кіберзагрози. Розроблену модель прогнозування критичних переходів станів інформаційної системи при інтеграції в SIEM-систему можливо впровадити у центри моніторингу кібербезпеки військових інформаційних систем для формування попередження за 2-3 дні про можливі переходи інформаційної системи до критичних станів, що дозволить швидко реагувати на кіберзагрози. Удосконалений метод кластеризації загроз та уразливостей сприяє автоматизації обробки та аналізу великих масивів даних у режимі реального часу, що дозволяє підвищити точність визначення режимів функціонування системи у 2 рази для об'єктивної оцінки рівня загроз. Запропонований метод підтримки прийняття рішень дозволяє зменшити кількість хибних спрацювань системи на 62% та підвищити ефективність реагування на кіберінциденти у системах управління інформаційною безпекою військових інформаційних систем.

Результати досліджень прийняті до впровадження в діяльність військової частини А2393, Інституту програмних систем Національної академії наук України та Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені на наукових конференціях:

1. XI Всеукраїнська науково-практична конференція молодих учених «Інформаційні технології – 2024», 2024 (м. Київ).
2. II Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024 (м. Київ).
3. XIII Міжнародна конференція «ITSec»-2024 Безпека інформаційних технологій, 2024 (м. Львів).
4. XII Всеукраїнської науково-практична конференціія молодих учених, 2025 (м. Київ).
5. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'II), 2025 (м. Київ).

Публікації. Основні результати дисертації висвітлено у 13 наукових публікаціях, із них 3 – одноосібні, 5 – у співавторстві: 6 статей (з них 3 у співавторстві, зараховано як 4,5 публікації) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 7 публікацій (з них 5 у співавторстві) у яких додатково висвітлено наукові результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Шевченко, С., Складанний, П., Негоденко, О., **Негоденко, В.** (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка,* 2(18), 150–162. https://doi.org/10.28925/2663-4023.2022.18.150162

2. **Негоденко, В.** (2023). Дослідження інформаційних конфліктів у системі навчання ЗСУ за допомогою імітаційного моделювання. *Кібербезпека: освіта, наука, техніка*, 4(20), 164–173, https://doi.org/10.28925/2663-4023.2023.20.164173

3. Шевченко, С., Жданова, Ю., Спасітєлєва, С., Мазур, Н., Складанний П., **Негоденко, В.** (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 3(23), 258–273. https://doi.org/10.28925/2663-4023.2024.23.258273.

4. **Негоденко, В**. (2024). Застосування математичної теорії катастроф для забезпечення стійкості системи управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка,* 2(26), 212–222. https://doi.org/10.28925/2663-4023.2024.26.692

5. Nehodenko, O., Shevchenko, S., **Nehodenko, V**., Zolotukhina, O. (2025). The Integration of Catastrophe Theory into Decision-Making Models for Information Security Management Systems. *Телекомунікаційні та інформаційні технології*, 2025, 4(2025), 20–28. https://doi.org/10.31673/2412-4338.2025.048903

6. Негоденко, В. (2025). Моделювання критичних станів в SIEM-системі на основі теорії катастроф. *Телекомунікаційні та інформаційні технології*, 2(2025), 118–125. https://doi.org/10.31673/2412-4338.2025.028289

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Skladannyi, P., Nehodenko, O., Shevchenko, S., Zolotukhina, O., & **Nehodenko, V.** (2022). Modified delta maintainability model of object-oriented software. Paper presented at the CEUR Workshop Proceedings, 3288, pp. 117–124. (Scopus).

2. **Негоденко, В.** Кластерний аналіз для прогнозування кібератак в інформаційних системах. (2024). *На XI Всеукраїнській науково-практичній конференції молодих учених «Інформаційні технології – 2024»*, 248–250.

3. **Негоденко В.**, Негоденко, О. (2024). Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах. *На XIII Міжнародній конференції «ITSec».Безпека інформаційних технологій*, 157–159.

4. **Nehodenko, V.** Impact of cyber incidents on the resilience of the information security management system. *На II Міжнародній науково-практичній конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»*, 226–229.

5. **Негоденко, В**., Шевченко, С., Негоденко, О. Прогнозування кіберінцидентів у SIEM-системі на основі теорії катастроф. *На XII*

Всеукраїнській науково-практичній конференції молодих учених «Інформаційні технології – 2025» (IT-2025), 300–302.

6. **Nehodenko, V.,** Shevchenko, S., Zolotukhina, O., Nehodenko, O., Zhdanova, Y. (2025). Model of an intelligent decision support system to ensure cyber resilience of military information systems. Paper presented at the CPITS'II Workshop Proceedings, 4145, 307–315.

7. Shevchenko, S., Zolotukhina, O., Nehodenko, O., Zhdanova, Y., Spasiteleva, S., **Nehodenko, V.** (2025). Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems. Paper presented at the CEUR Workshop Proceedings, 3991, 311–322. (Scopus).

Особистий внесок здобувача.

Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачем особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача. Безпосередньо автором розроблено математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою на основі катастрофи типу «Метелик», модель прогнозування критичних переходів станів інформаційної системи з інтеграцією в SIEM-систему, удосконалений метод кластеризації кіберінцидентів із врахуванням їх часової динаміки та інтегральних показників стану системи, а також метод підтримки прийняття рішень щодо забезпечення кіберстійкості інформаційних систем. Отримані результати можуть бути використані для підвищення ефективності функціонування систем управління інформаційною безпекою в умовах сучасних кіберзагроз.

У статті «Дослідження прикладних аспектів теорії конфліктів у системах безпеки» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведені аналізу щодо застосування теорії конфліктів для моделювання процесів протидії загрозам у системах безпеки, підготовці висновків щодо використання практичних результатів дослідження, що загалом складає 40% тексту статті.

У статті «Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведенні аналізу і описі етапів задачі кластеризації, вибору міри відстані та міри подібності для об'єктів, які вивчаються, що загалом складає 40% тексту статті.

У статті «The Integration of Catastrophe Theory into Decision-Making Models for Information Security Management Systems» опублікованій у співавторстві, внесок Негоденко В.П. полягає у розробці алгоритму реагування системи прийняття рішень на основі теорії катастроф та визначенні сценаріїв для симуляції з різними параметрами за допомогою Python, що загалом складає 70% тексту статті.

У статті «Modified delta maintainability model of object-oriented software» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведенні

практичної валідації модифікованої дельта-моделі шляхом аналізу програмних продуктів з відкритим вихідним кодом, що загалом складає 30% тексту статті.

У тезах «Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах», опублікованій у співавторстві, внесок Негоденко В.П. полягає у розробці моделі прогнозування критичних переходів станів військових інформаційних систем на основі теорії катастроф, яка інтегрована в SIEM-систему для підвищення рівня кіберстійкості, що загалом складає 40% тексту статті.

У тезах «Прогнозування кіберінцидентів у SIEM-системі на основі теорії катастроф» опублікованій у співавторстві, внесок Негоденко В.П. полягає в дослідженні інформаційних конфліктів у системі навчання військ та обґрунтуванні використання імітаційного моделювання для їх аналізу і мінімізації, що загалом складає 45% тексту статті.

У статті «Model of an intelligent decision support system to ensure cyber resilience of military information systems», опублікованій у співавторстві, внесок Негоденко В.П. полягає у розробці математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик» та визначенні умов виникнення критичних станів системи, що загалом складає 55% тексту статті.

У статті «Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems» опублікованій у співавторстві, внесок Негоденко В.П. полягає в дослідженні проблеми впровадження штучного інтелекту в системах безпеки, встановлені ключових відмінностей між оборонним, наступальним та спрямованим га протидію ШІ в кібербезпеці, що загалом складає 30% тексту статті.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 189 найменувань на 21 сторінці і 6 додатків. Загальний обсяг роботи становить 239 сторінок, серед яких 184 сторінок – основного тексту, 34 рисунків і 22 таблиць.

Оцінка мови та стилю дисертації. Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний і послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчесності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації.

На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії.

Дисертація Негоденко Віталія Петровича, на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях і міжнародних виданнях, що входять до наукометричних баз Scopus та Web of Science Core Collection та оприлюднювались на міжнародних науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Негоденко Віталія Петровича, на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає 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 12.01.2022 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Негоденко Віталія Петровича та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3.Негоденко Віталій Петрович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Негоденко Віталія Петровича, на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф», до публічного захисту у разовій спеціалізованій вченій раді для присудження Негоденко В.П. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Голова –
доктор технічних наук, професор
професор кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Геннадій ГУЛАК