Голові разової спеціалізованої
вченої ради PhD 17297
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ

РЕЦЕНЗІЯ

на дисертаційну роботу Паюка Вадима Павловича
на тему «Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах», подану
на здобуття ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.

Актуальність дисертаційного дослідження визначається інтенсивним розвитком цифрових технологій, посиленням кіберзагроз і зростанням складності комп'ютерних атак на корпоративні мережі. За таких умов особливого значення набуває вдосконалення систем кіберзахисту, зокрема механізмів накопичення, зберігання та використання історичних даних, необхідних для своєчасного виявлення загроз, аналізу дій зловмисників і формування ефективних рішень щодо протидії атакам.

Важливим напрямом підвищення результативності засобів кібербезпеки є модернізація підсистем пам'яті з урахуванням концепції «піраміди болю зловмисника», використання обманних технологій та інтелектуальних механізмів управління інформацією. Водночас збільшення обсягів накопичених даних, зниження їх актуальності з часом та обмеженість обчислювальних ресурсів потребують розроблення адаптивних підходів до організації зберігання, оптимізації й вибору інформації з урахуванням глибини горизонту її використання.

Наукова проблема полягає в необхідності узгодження вимог щодо повноти та довготривалого збереження історичних даних із потребою скорочення їх надлишковості, раціонального використання ресурсів і забезпечення швидкого доступу до актуальної інформації. Вирішення зазначеної суперечності передбачає вдосконалення архітектури підсистем пам'яті та створення ефективних методів зберігання, вибору й оптимізації історичних даних.

Отже, тема дисертації є своєчасною, науково обґрунтованою та практично значущою, оскільки спрямована на підвищення ефективності систем протидії комп'ютерним атакам у корпоративних мережах. Напрям дослідження узгоджується із сучасними тенденціями розвитку інформаційних технологій і кібербезпеки, а його результати становлять інтерес для подальших наукових розробок у сфері

інтелектуального аналізу даних, виявлення кіберзагроз і захисту корпоративних інформаційних систем.

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980); держбюджетної науково-дослідної теми №1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (ДР № 0126U002082), в яких автор дисертації був виконавцем.

Формулювання наукової задачі, мети й завдань дослідження.

У дисертаційній роботі належним чином визначено наукову задачу, мету, об'єкт і предмет дослідження, які взаємопов'язані між собою та відповідають обраному напряму наукового пошуку. Основна наукова задача полягає у підвищенні ефективності процесів зберігання, вибору та оптимізації історичних даних, що використовуються системами й засобами протидії комп'ютерним атакам у корпоративних мережах.

Метою дослідження є вдосконалення процесів роботи з історичними даними шляхом розроблення відповідних архітектурних рішень і методів їх організації, що сприятиме підвищенню результативності функціонування засобів кіберзахисту.

Об'єкт дослідження охоплює процеси організації зберігання, вибору та оптимізації історичних даних систем протидії комп'ютерним атакам у корпоративних мережах. Предметом дослідження виступають методи організації зазначених процесів, спрямовані на забезпечення ефективного використання накопиченої інформації.

Відповідно до поставленої мети в дисертації розглянуто комплекс взаємопов'язаних завдань, що передбачають дослідження сучасних підходів до зберігання й оброблення історичних даних, розроблення моделей організації підсистем пам'яті, вдосконалення їх архітектури, створення методів зберігання, оптимізації та вибору даних із застосуванням механізмів самонавчання, а також експериментальну перевірку ефективності запропонованих рішень.

Слід відзначити логічну послідовність і взаємоузгодженість сформульованих положень, які забезпечують цілісність дисертаційного дослідження. Визначені мета та завдання відповідають змісту роботи, а їх реалізація спрямована на розв'язання актуальної наукової задачі вдосконалення інформаційного забезпечення систем протидії комп'ютерним атакам у корпоративних мережах.

Загалом формулювання наукової задачі, мети, об'єкта та предмета дослідження є логічно узгодженими, відповідають змісту дисертаційної роботи й відображають її спрямованість на вдосконалення методів і засобів протидії комп'ютерним атакам у корпоративних мережах.

Наукова новизна отриманих автором результатів полягає в наступному:

1) удосконалено архітектуру засобів зберігання даних для систем і засобів протидії КА, в якій на відміну відомих, здійснено поєднання автоматичного

керування життєвим циклом всіх даних або їх частини, особливостей апаратно-програмних засобів для зберігання даних, інтелектуалізації щодо глибини горизонту для даних, самонавчання при виборі даних для типових повторюваних КА, що дає змогу підвищити оперативність та точність при надані даних системам протидії КА, а також забезпечити ефективність їх зберігання з урахування глибини горизонту;

2) вперше розроблено метод організації зберігання даних у системах та засобах протидії комп'ютерним атакам, особливістю якого є поділ даних на початкові, накопичувані та використані, а також врахування історичного аспекту їх застосування шляхом збереження результатів оцінювання ефективності використання даних із застосуванням марковських моделей, динамічних баєсівських мереж та статистичних методів, що забезпечує опис динаміки станів системи, врахування причинно-наслідкових залежностей і узагальнення накопиченого досвіду для підвищення ефективності повторного використання даних, адаптивності систем та автономності їх функціонування в умовах тривалої експлуатації;

3) розроблено новий метод оптимізації даних на основі самонавчання засобів підсистеми пам'яті систем та засобів протидії КА, який, на відміну від існуючих, забезпечує комплексну адаптивну оптимізацію початкових, накопичених, використаних та даних обманних систем з урахуванням критеріїв ресурсної ефективності, структури даних, шарового розміщення, апаратно-мережного розподілу та специфіки функціонування обманних систем, що дозволяє зменшити надлишковість інформаційних масивів, підвищити швидкодію доступу до даних, покращити інформативність інформаційного середовища, ефективність накопичення знань про дії зловмисника та адаптивність систем і засобів протидії КА до змін умов функціонування;

4) розроблено новий метод вибору даних, який, на відміну від відомих, що базуються на статичному оцінюванні ознак або фіксованих моделях ранжування, використовує інтегральну оптимізаційну функцію з урахуванням глибини горизонту, семантичної значущості та попереднього досвіду використання, доповнену механізмом самонавчання для адаптивного формування та корекції інтегрованих сукупностей даних, що дозволило підвищити точність відбору, зменшити інформаційну надлишковість і забезпечити динамічну адаптацію до змін середовища.

Короткий аналіз основного змісту дисертації.

Дисертаційна робота характеризується логічною побудовою, послідовністю викладення матеріалу та комплексним підходом до розв'язання наукової задачі підвищення ефективності зберігання, вибору й оптимізації історичних даних систем протидії комп'ютерним атакам у корпоративних мережах.

У вступі обґрунтовано актуальність теми, визначено мету, наукову задачу та напрями дослідження, висвітлено наукову новизну, практичне значення, апробацію і впровадження результатів.

У першому розділі проаналізовано сучасні системи протидії комп'ютерним атакам, методи виявлення кіберзагроз та наявні підходи до зберігання, вибору й оптимізації історичних даних. Визначено основні проблеми та перспективи вдосконалення відповідних засобів кіберзахисту.

У другому розділі розроблено моделі організації підсистем пам’яті та застосування обманних технологій. Удосконалено архітектуру засобів зберігання історичних даних шляхом інтеграції автоматизованого керування їх життєвим циклом, урахування глибини горизонту використання інформації та механізмів самонавчання.

У третьому розділі запропоновано методи організації зберігання, адаптивної оптимізації та вибору історичних даних. Їх особливістю є врахування попереднього досвіду використання інформації, застосування механізмів самонавчання та інтегральної оптимізаційної функції для підвищення релевантності даних і раціонального використання ресурсів.

У четвертому розділі представлено методику оцінювання ефективності розроблених рішень, результати експериментальних досліджень та програмний засіб реалізації запропонованих методів.

У висновках систематизовано основні результати дослідження, а в додатках наведено допоміжні матеріали та документи щодо їх впровадження.

Загалом структура і зміст дисертації відповідають поставленій меті та завданням, а отримані результати мають теоретичне і практичне значення для вдосконалення засобів і систем кіберзахисту корпоративних мереж.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові положення, висновки та рекомендації дисертаційної роботи характеризуються належним рівнем обґрунтованості, що забезпечується комплексним підходом до розв’язування наукової задачі, застосуванням сучасного математичного апарату та експериментальною перевіркою запропонованих рішень.

Важливим результатом дослідження є вдосконалення архітектури засобів зберігання історичних даних з урахуванням їх життєвого циклу, глибини горизонту використання та механізмів самонавчання. Розроблені методи зберігання, оптимізації та вибору даних базуються на марковських моделях, динамічних баєсівських мережах, статистичних методах та інтегральній оптимізаційній функції, що сприяє підвищенню ефективності управління інформаційними ресурсами.

Наведені в дисертації результати експериментальних досліджень підтверджують результативність запропонованих підходів щодо зменшення інформаційної надлишковості, підвищення оперативності доступу до даних та адаптивності засобів кіберзахисту. Отже, отримані наукові результати є теоретично аргументованими, експериментально підтвердженими та мають практичне значення для вдосконалення систем протидії комп’ютерним атакам у корпоративних мережах.

Практичне значення отриманих результатів.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (акт від 30.06.2026, м. Хмельницький), ПП «Авіві» (акт від 29.06.2026, м. Хмельницький), а також в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп’ютерної інженерії та інформаційних систем для спеціальності F7 Комп’ютерна інженерія, зокрема в курсах «Безпека та захист

комп’ютерних систем», «Моделювання та методи оптимізації в наукових та експериментальних дослідженнях», «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп’ютерних систем та мереж» (акт від 26.06.2026 м.Хмельницький).

Крім того, запропоновані методи є основою для розроблення нових засобів методи організації зберігання, вибору й оптимізації історичних даних і можуть бути використані розробниками систем протидії комп’ютерним атакам. Результати роботи деталізовані, що дає змогу здійснювати їх відтворюваність.

Особистий внесок здобувача

Здобувачем розроблено моделі та методи організації зберігання, вибору й оптимізації історичних даних, удосконалено архітектуру підсистем пам’яті засобів протидії комп’ютерним атакам із застосуванням механізмів самонавчання. Отримані результати спрямовані на підвищення ефективності використання інформаційних ресурсів, удосконалення засобів виявлення кіберзагроз та забезпечення захисту корпоративних мереж.

Основні наукові результати дисертаційної роботи отримані здобувачем самостійно. За темою дослідження опубліковано 11 наукових праць, зокрема 4 статті у фахових виданнях України категорії «Б» та 7 праць у матеріалах міжнародних наукових конференцій, що індексуються в наукометричній базі Scopus. Крім того, одержано свідоцтво про реєстрацію авторського права на комп’ютерну програму «SECMON», призначену для зберігання, оптимізації та вибору історичних даних у системах протидії комп’ютерним атакам.

Наведені результати свідчать про наукову та практичну значущість виконаного дослідження, а також належне оприлюднення його основних положень. Самоплагіату в наукових статтях не виявлено. Всі основні наукові результати роботи опубліковані в різних наукових статтях.

Апробація матеріалів дисертації.

Основні положення та результати дисертаційної роботи доповідались і обговорювались на міжнародних наукових конференціях та семінарах: 1nd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, June 10-12, 2020); 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 24–26, 2021); 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 28, 2024); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS, Khmelnytskyi, Ukraine, June 28, 2024); 1st International Workshop on Advanced Applied Information Technologies: 29 (AdvAIT, Khmelnytskyi, Ukraine and Zilina, Slovakia, December 5, 2024); 14th International Conference on Dependable Systems, Services and Technologies (IEEE, DeSSerT, Athens, Greece, October 11-13, 2024); 6th International Workshop on Intelligent Information Technologies & S).

Структура та обсяг дисертації.

Оформлення дисертації відповідає нормативним вимогам.

Дисертаційна робота складається з анотації, змісту, переліку скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та п’яти додатків. Повний обсяг роботи становить 245 сторінок друкованого тексту, з них анотація займає 13 сторінок, зміст 2 сторінки, перелік скорочень 1 сторінку, вступ, розділи та висновки викладено на 150 сторінках, список зі 122 використаних джерел займає 14 сторінок, додатки 36 сторінок. Дисертація містить 12 рисунків та 10 таблиць.

Зауваження.

1. Недостатньо чітко обґрунтовано вибір критеріїв оцінювання історичних даних. У роботі використовуються характеристики актуальності, інформативності, надлишковості, вартості обробки та контекстної відповідності даних. Водночас недостатньо розкрито принципи визначення вагових коефіцієнтів цих характеристик та їх впливу на кінцевий результат. Це ускладнює оцінювання об’єктивності сформованих інтегральних показників і можливості їх застосування в корпоративних мережах із різними умовами функціонування.

2. Не достатньо конкретизовано умови застосування марковської властивості до процесів використання історичних даних. Оскільки комп’ютерні атаки можуть характеризуватися складною багатоступеневою поведінкою, доцільно додатково пояснити, наскільки адекватним є припущення про залежність майбутнього стану системи лише від поточного стану, а також чи враховується вплив більш ранніх подій.

3. Потребує деталізації механізм формування станів марковської моделі. Важливим є пояснення того, за якими ознаками визначаються стани системи, як формується матриця переходів, яким чином оцінюються ймовірності переходів і як здійснюється оновлення моделі після появи нових сценаріїв комп’ютерних атак.

4. Недостатньо розкрито процедуру формування та оновлення динамічних баєсівських мереж. Доцільно уточнити, чи структура мережі є фіксованою або адаптивною, як визначаються причинно-наслідкові зв’язки між змінними та яким чином забезпечується коректність моделі за зміни характеру комп’ютерних атак.

5. Потребує додаткового пояснення взаємозв’язок між запропонованими моделями організації пам’яті та моделями обманних технологій. У дисертації ці напрями об’єднані в загальну архітектуру, проте було б доцільно чіткіше визначити, які саме дані обманних систем використовуються під час формування історичних масивів та як їх включення впливає на ефективність виявлення атак.

6. Не повною мірою обґрунтовано критерії визначення актуальності історичних даних. У роботі враховуються глибина горизонту, семантична значущість і попередній досвід використання, однак доцільно уточнити, чи враховується швидкість зміни характеру загроз, поява нових тактик зловмисників та можливість втрати релевантності раніше накопичених даних.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий рівень проведеного дослідження і не знижують його наукової та практичної цінності.

Загальний висновок.

Вважаю, що дисертаційна робота Паюка Вадима Павловича на тему «Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі знань 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі вдосконалення методів і засобів роботи з історичними даними та підвищення ефективності протидії комп'ютерним атакам у корпоративних мережах.

Дисертаційна робота «Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням відповідає вимогам пп. 6, 7, 8, 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 (зі змінами, внесеними згідно з постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Паюк Вадим Павлович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент,
кандидат технічних наук,
доцент, доцент кафедри комп'ютерної інженерії
та інформаційних систем,
Хмельницького національного
університету Підпис дійсний Відділ кадрів Марія КАПУСТЯН

«Підпис Марії КАПУСТЯН засвідчую»:
Проректор з наукової роботи
Хмельницького національного
університету Олег СИНЮК