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 теми дисертаційного дослідження зумовлена стрімким розвитком інформаційно-комунікаційних технологій, зростанням масштабів, різноманітності та складності комп'ютерних атак, а також підвищенням вимог до кіберстійкості корпоративних мереж. У сучасних умовах ефективна протидія кіберзагрозам передбачає не лише своєчасне виявлення зловмисної активності, а й здатність систем захисту накопичувати, зберігати, аналізувати та використовувати історичні дані для встановлення закономірностей у поведінці зловмисників, прогнозування можливого розвитку атак і формування обґрунтованих захисних рішень. У зв'язку з цим особливої актуальності набуває вдосконалення методів і засобів організації історичних даних у системах протидії комп'ютерним атакам.

Важливим напрямом розв'язання зазначеної проблеми є вдосконалення підсистем пам'яті засобів кіберзахисту на основі врахування концепції «піраміди болю зловмисника», використання адаптивних механізмів структуризації та зберігання інформації, а також інтеграції обманних технологій. Такий підхід дає змогу підвищити інформативність накопичуваних даних, забезпечити їх відповідність актуальним сценаріям атак і створити передумови для ефективнішого виявлення зловмисної діяльності. Водночас безперервне збільшення обсягів інформації, неоднакова тривалість її актуальності, обмеженість обчислювальних і запам'ятовувальних ресурсів та необхідність оперативного отримання потрібних відомостей ускладнюють функціонування відповідних підсистем. Це зумовлює потребу в розробленні адаптивних підходів до визначення складу, строків зберігання, пріоритетності та обсягів історичних даних залежно від їхньої цінності для виявлення й аналізу комп'ютерних атак.

Основна наукова суперечність полягає в необхідності забезпечення повноти, доступності та достатньої глибини зберігання історичних даних,

необхідних для виявлення багатоступеневих і тривалих комп’ютерних атак, за одночасної потреби мінімізувати інформаційну надлишковість, раціонально використовувати обмежені обчислювальні та запам’ятовувальні ресурси й забезпечувати оперативний доступ до найбільш релевантної інформації. Усунення цієї суперечності потребує вдосконалення архітектурних рішень, а також розроблення методів адаптивної організації, відбору, зберігання та оптимізації історичних даних з урахуванням їхньої інформаційної цінності, часових характеристик і перспектив подальшого використання в процесах протидії комп’ютерним атакам.

Спрямованість дослідження в предметній області спеціальності «Комп’ютерна інженерія» визначається тим, що розглянута проблема не обмежується питаннями розроблення алгоритмів виявлення кіберзагроз або аналізу інформації, а безпосередньо стосується вдосконалення архітектури та функціональних компонентів комп’ютерних систем, у яких реалізуються процеси накопичення, структуризації, зберігання, оброблення й передавання даних. Зокрема, дослідження передбачає розгляд підсистем пам’яті як складових програмно-апаратної інфраструктури кіберзахисту, визначення принципів їхньої взаємодії з іншими компонентами системи, оптимізацію використання ресурсів зберігання та обчислення, а також забезпечення необхідної продуктивності й адаптивності функціонування в умовах змінного навантаження та впливу комп’ютерних атак. Отже, основний аспект роботи полягає у вдосконаленні архітектурно-функціональної організації комп’ютерних систем протидії атакам шляхом розроблення відповідних методів і засобів керування їхніми інформаційними та обчислювальними ресурсами.

Таким чином, обрана тема дисертаційної роботи є актуальною та має важливе наукове і практичне значення, оскільки спрямована на підвищення ефективності функціонування систем протидії комп’ютерним атакам у корпоративних мережах завдяки вдосконаленню принципів організації та використання історичних даних. Очікувані результати дослідження сприятимуть підвищенню оперативності доступу до релевантної інформації, раціоналізації використання ресурсів комп’ютерних систем, покращенню інформаційного забезпечення процесів виявлення кіберзагроз і підвищенню загального рівня кіберстійкості корпоративної мережевої інфраструктури.

Тематика дисертаційного дослідження відповідає сучасним науково-технічним напрямам розвитку комп’ютерної інженерії, пов’язаним із проєктуванням та вдосконаленням архітектури комп’ютерних систем, організацією підсистем зберігання й оброблення даних, оптимізацією використання апаратних і програмних ресурсів та забезпеченням надійності функціонування розподілених обчислювальних середовищ. Практичне застосування отриманих результатів можливе під час розроблення й модернізації програмно-апаратних засобів кіберзахисту корпоративних мереж, побудови адаптивних підсистем зберігання історичних даних, а також виконання науково-дослідних і дослідно-конструкторських робіт, спрямованих на підвищення

ефективності та надійності комп’ютерних систем в умовах протидії сучасним кіберзагрозам.

Зв’язок роботи з науковими програмами, планами, темами.

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 чітко сформульовано наукову задачу, яка полягає у підвищенні ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп’ютерним атакам у корпоративних мережах. Її розв’язання передбачає вдосконалення архітектури підсистем пам’яті та розроблення методів організації й адаптивного використання історичних даних з урахуванням особливостей функціонування засобів кіберзахисту.

Мета дисертаційного дослідження полягає в підвищенні ефективності зберігання, вибору та оптимізації історичних даних шляхом удосконалення відповідних архітектурних рішень і методів їх організації. Визначена мета узгоджується з актуальністю теми та спрямована на вирішення важливої науково-прикладної задачі у сфері кібербезпеки корпоративних мереж.

Об’єктом дослідження визначено процес організації зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп’ютерним атакам у корпоративних мережах, а предметом – методи реалізації зазначених процесів.

Для досягнення поставленої мети дослідження спрямоване на аналіз наявних підходів до організації історичних даних, удосконалення архітектури засобів їх зберігання, розроблення методів оптимізації та вибору даних з урахуванням глибини горизонту, а також експериментальне оцінювання ефективності запропонованих рішень.

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 має логічну структуру, а її зміст характеризується послідовним викладенням теоретичних положень, розроблених моделей і методів та результатів експериментальних досліджень, спрямованих на підвищення ефективності зберігання, вибору й оптимізації історичних даних систем протидії комп'ютерним атакам у корпоративних мережах.

У вступі розкрито актуальність обраної теми, сформульовано наукову задачу, визначено мету та основні напрями дослідження. Представлено наукові результати, їх практичну значущість, а також відомості щодо апробації та впровадження отриманих розробок.

Перший розділ присвячено дослідженню сучасного стану систем і засобів протидії комп’ютерним атакам, аналізу методів виявлення кіберзагроз і шкідливого програмного забезпечення. Особливу увагу приділено підходам до організації зберігання та використання історичних даних, визначенню їх переваг і обмежень, що стало підґрунтям для подальших досліджень.

У другому розділі представлено моделі організації підсистем пам’яті та використання обманних технологій у системах кіберзахисту. Запропоновано вдосконалену архітектуру засобів зберігання історичних даних, яка передбачає автоматизоване управління їх життєвим циклом, урахування характеристик апаратно-програмного забезпечення, глибини горизонту використання інформації та застосування механізмів самонавчання.

Третій розділ містить основні методологічні розробки, спрямовані на вдосконалення процесів зберігання, оптимізації та вибору історичних даних. Запропоновано метод організації зберігання з розподілом інформації за особливостями її накопичення та використання, метод адаптивної оптимізації із застосуванням механізмів самонавчання, а також метод вибору релевантних даних на основі інтегральної оптимізаційної функції. Зазначені рішення спрямовані на раціональне використання інформаційних ресурсів та підвищення оперативності функціонування систем протидії комп’ютерним атакам.

У четвертому розділі викладено методику оцінювання ефективності запропонованих рішень, описано організацію та результати експериментальних досліджень. Представлено засіб зберігання, вибору й оптимізації історичних даних, призначений для використання в системах протидії комп’ютерним атакам у корпоративних мережах.

У висновках узагальнено основні наукові та практичні результати дослідження. Додатки містять матеріали, що доповнюють основний зміст роботи, зокрема відомості про програмні засоби, експериментальні дослідження та документи, які підтверджують впровадження отриманих результатів.

Загалом зміст дисертаційної роботи відповідає поставленій меті та визначеним завданням дослідження. Матеріал викладено послідовно, із належним взаємозв’язком між теоретичними положеннями, запропонованими методами та їх експериментальним дослідженням, що свідчить про комплексний характер виконаної наукової роботи.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові положення, висновки та рекомендації дисертаційної роботи є достатньо обґрунтованими, що підтверджується системним підходом до розв’язання поставленої наукової задачі, використанням сучасних методів дослідження та результатами експериментальної перевірки.

Обґрунтованість отриманих результатів забезпечується розробленням удосконаленої архітектури засобів зберігання історичних даних, яка враховує їх життєвий цикл, глибину горизонту використання, особливості апаратно-програмного забезпечення та механізми самонавчання.

Запропоновані методи організації зберігання, оптимізації та вибору історичних даних ґрунтуються на застосуванні марковських моделей, динамічних баєсівських мереж, статистичних методів та інтегральної оптимізаційної функції. Їх використання сприяє зменшенню інформаційної надлишковості, підвищенню оперативності доступу до даних та адаптивності систем кіберзахисту.

Достовірність наукових результатів підтверджується наведеними в дисертації експериментальними дослідженнями. Загалом отримані результати мають належне теоретичне й експериментальне обґрунтування та практичне значення для підвищення ефективності 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).

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 використанням механізмів самонавчання. Запропоновано методику багатофакторного аналізу для виявлення зловмисного програмного забезпечення, досліджено методи машинного навчання для аналізу мані результати спрямовані на підвищення ефективності кіберзахисту корпоративних мереж.

Отримані результати спрямовані на вдосконалення методів захисту корпоративних мереж, підвищення ефективності використання історичних даних та розвиток інтелектуальних засобів виявлення кіберзагроз.

Основні наукові результати дисертаційної роботи отримані здобувачем самостійно. За результатами дисертаційного дослідження опубліковано 11 наукових праць, у тому числі 4 статті у наукових фахових виданнях України категорії Б, 7 праць у матеріалах міжнародних наукових конференцій, з яких 7 опубліковано у виданнях, що індексуються наукометричною базою Scopus, а також одержано свідоцтво про реєстрацію авторського права на комп'ютерну програму «Програмне забезпечення зберігання, оптимізації і вибору даних в системах та засобах протидії комп'ютерним атакам з урахуванням історичного аспекту їх використання та глибини горизонту» («SECMON») (№150528 від

03.09.2026). Самоплагіату в наукових статтях в фахових наукових журналах не встановлено.

Апробація матеріалів дисертації.

Основні положення та результати дисертаційної роботи доповідались і обговорювались на семи міжнародних наукових конференціях та семінарах, матеріали яких проіндексовані в наукометричній базі Scopus: 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.

Дисертаційна робота має завершену структуру та складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох основних розділів, загальних висновків, списку використаних джерел і семи додатків. Така побудова роботи забезпечує послідовне та логічно узгоджене висвітлення поставлених наукових завдань, обґрунтування запропонованих наукових положень, розкриття змісту проведених досліджень і представлення отриманих результатів.

Повний обсяг дисертаційної роботи становить 245 сторінок друкованого тексту. Зокрема, анотація викладена на 13 сторінках, зміст займає 2 сторінки, перелік умовних скорочень – 1 сторінку. Вступ, чотири розділи основної частини та загальні висновки розміщені на 150 сторінках. Список використаних джерел налічує 122 найменування та займає 14 сторінок, що свідчить про опрацювання відповідної наукової, нормативно-технічної та інформаційної бази за тематикою дослідження. Обсяг додатків становить 36 сторінок, вони містять додаткові матеріали, які доповнюють основний виклад дисертації та сприяють повнішому представленню отриманих наукових і практичних результатів.

Ілюстративний матеріал дисертації представлений 12 рисунками та 10 таблицями, які забезпечують наочність викладення теоретичних положень, структурних і функціональних взаємозв’язків, а також результатів проведених досліджень.

Оформлення дисертаційної роботи здійснено відповідно до встановлених нормативних вимог щодо структури, обсягу та представлення наукових результатів.

Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. Недостатньо чітко розмежовано поняття «історичні дані», «початкові дані», «накопичувані дані» та «використані дані». У роботі запропоновано класифікацію даних за етапами їх життєвого циклу, однак потребує додаткового уточнення, за якими формальними критеріями здійснюється перехід даних між відповідними категоріями та чи є ці категорії взаємовиключними.

2. Потребує уточнення поняття «глибина горизонту» історичних даних. У дисертації цей параметр використовується як один із ключових факторів організації, оптимізації та вибору даних, проте доцільно чіткіше визначити його фізичний та інформаційний зміст, одиниці вимірювання, спосіб обчислення і відмінність від традиційних понять часової глибини зберігання та актуальності інформації.

3. Недостатньо обґрунтовано універсальність запропонованої архітектури підсистеми пам’яті. Архітектура орієнтована на системи протидії комп’ютерним атакам у корпоративних мережах, однак не до кінця зрозуміло, наскільки запропоновані рішення адаптуються до різних типів систем кіберзахисту, зокрема SIEM, IDS/IPS, EDR та NDR, які мають різні вимоги до обсягів даних і швидкості їх оброблення.

4. Не повною мірою розкрито механізм взаємодії запропонованої підсистеми пам’яті з наявними засобами кіберзахисту. Було б доцільно деталізувати інтерфейси взаємодії, протоколи обміну даними, порядок передавання результатів аналізу та механізми інтеграції з уже функціонуючими корпоративними системами безпеки.

5. Потребує додаткового обґрунтування використання марковських моделей та динамічних баєсівських мереж. У роботі застосовуються обидва підходи для врахування історичного аспекту використання даних, проте бажано чіткіше визначити, які саме процеси моделюються кожним із них, чому обрано саме ці математичні апарати та які переваги вони мають порівняно з альтернативними моделями.

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,
завідувач кафедри кібербезпеки
Хмельницького національного
університету _____ Юрій КЛЬОЦ

Підпис дійсний
Відділ кадрів

«Підпис Юрія КЛЬОЦА засвідчую»:
Проректор з наукової роботи
Хмельницького національного
університету _____ Олег СИНЮК