Голові разової спеціалізованої
вченої ради PhD 17297
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ
29016, м. Хмельницький,
вул. Інститутська, 11

**ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА**

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

## 1. Актуальність теми дисертаційної роботи

В умовах активної цифровізації та зростання складності комп'ютерних атак особливої актуальності набуває підвищення ефективності захисту корпоративних мереж. Сучасні кіберзагрози характеризуються різноманітністю способів реалізації та здатністю зловмисників долати наявні механізми захисту, що зумовлює необхідність удосконалення систем і засобів протидії комп'ютерним атакам, зокрема методів організації, зберігання та використання історичних даних.

Історичні дані про функціонування систем кіберзахисту є важливим джерелом інформації для виявлення загроз, аналізу попередніх атак і прийняття ефективних захисних рішень. Водночас постійне збільшення їх обсягів, поступова втрата актуальності та обмеженість обчислювальних ресурсів ускладнюють процеси зберігання, вибору й оптимізації даних. З огляду на концепцію «піраміди болю зловмисника» важливого значення набуває вдосконалення підсистем пам'яті засобів протидії комп'ютерним атакам, зокрема шляхом застосування адаптивних механізмів та обманних технологій.

Основна суперечність полягає в необхідності забезпечення повноти й тривалості зберігання історичних даних для ефективного виявлення кіберзагроз за одночасної потреби оптимізації їх обсягів, зменшення ресурсних витрат і забезпечення оперативного доступу до актуальної інформації. Розв'язання цієї суперечності потребує розроблення нових і вдосконалення наявних методів та засобів роботи з історичними даними.

Актуальність дисертаційного дослідження не викликає сумнівів, оскільки воно спрямоване на вирішення важливої наукової задачі підвищення ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам у корпоративних мережах. Результати

дослідження мають наукове та практичне значення для вдосконалення технологій кіберзахисту й підвищення стійкості корпоративних інформаційних систем до сучасних загроз.

Отже, тема дисертації є актуальною і відповідає теоретичному змісту предметної області стандарту вищої освіти зі спеціальності 123 Комп'ютерна інженерія.

**2. 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.

**3. Наукова новизна отриманих результатів**

До основних наукових результатів дисертаційної роботи варто віднести такі:

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.

## 4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації відображає її зміст і відповідає спеціальності 123 Комп'ютерна інженерія.

У вступі обґрунтовано вибір теми дисертаційного дослідження, визначено наукову задачу, що полягає в підвищенні ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам у корпоративних мережах. Висвітлено перспективні напрями її розв'язання з урахуванням глибини горизонту використання даних, наведено основні наукові результати, їх практичне значення, відомості про апробацію та впровадження.

У першому розділі здійснено аналіз сучасних систем і засобів протидії комп'ютерним атакам у корпоративних мережах, методів виявлення кіберзагроз і зловмисного програмного забезпечення. Розглянуто наявні підходи до зберігання, вибору й оптимізації історичних даних та їх вплив на ефективність виявлення комп'ютерних атак.

У другому розділі розроблено моделі організації підсистем пам'яті з історичними даними та моделі застосування обманних технологій у засобах протидії комп'ютерним атакам. Удосконалено архітектуру підсистем пам'яті шляхом поєднання автоматизованого керування життєвим циклом даних, урахування особливостей апаратно-програмних засобів їх зберігання, глибини горизонту використання та механізмів самонавчання для протидії повторюваним атакам.

У третьому розділі запропоновано методи організації зберігання, оптимізації та вибору історичних даних. Метод організації зберігання передбачає їх поділ на початкові, накопичувані та використані з урахуванням

результатів попереднього застосування. Метод оптимізації ґрунтується на механізмах самонавчання та адаптивного управління даними відповідно до ресурсних, структурних і функціональних критеріїв. Метод вибору даних базується на інтегральній оптимізаційній функції, яка враховує глибину горизонту, семантичну значущість і попередній досвід використання даних.

У четвертому розділі розроблено методику оцінювання ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам. Наведено постановку та результати експериментальних досліджень, а також представлено відповідний засіб зберігання, вибору й оптимізації історичних даних у корпоративних мережах.

Завершують роботу узагальнення отриманих результатів та додаткові матеріали, необхідні для ознайомлення з програмними засобами й експериментами. Впровадження підтверджено документами, розміщеними у додатках.

## 5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність

Сформульовані в дисертаційній роботі наукові положення, висновки та рекомендації є достатньо обґрунтованими, що забезпечується комплексним підходом до розв'язання поставленої наукової задачі, використанням сучасних методів дослідження та результатами експериментальної перевірки запропонованих рішень.

Обґрунтованість отриманих результатів підтверджується розробленням удосконаленої архітектури засобів зберігання історичних даних систем протидії комп'ютерним атакам, яка поєднує автоматизоване керування життєвим циклом даних, урахування особливостей апаратно-програмних засобів, глибини горизонту використання інформації та механізмів самонавчання.

Вагоме значення мають запропоновані методи організації зберігання, оптимізації та вибору історичних даних. Зокрема, метод організації зберігання передбачає розподіл даних на початкові, накопичувані та використані з оцінюванням ефективності їх застосування на основі марковських моделей, динамічних баєсівських мереж і статистичних методів. Поєднання оптимізаційних процедур із механізмами самонавчання забезпечує адаптивне управління інформаційними масивами, зменшення їх надлишковості та підвищення оперативності доступу до необхідних даних.

Запропонований метод вибору історичних даних ґрунтується на інтегральній оптимізаційній функції, що враховує глибину горизонту, семантичну значущість і попередній досвід використання інформації. Це створює передумови для підвищення точності відбору релевантних даних та адаптації засобів кіберзахисту до змін інформаційного середовища.

Достовірність наукових результатів підтверджується наведеними в

дисертації результатами експериментальних досліджень, які засвідчують ефективність запропонованих архітектурних і методичних рішень щодо вдосконалення процесів зберігання, вибору та оптимізації історичних даних.

Отже, представлені в дисертації наукові положення, висновки та рекомендації мають належне теоретичне й експериментальне обґрунтування та спрямовані на підвищення ефективності функціонування систем і засобів протидії комп'ютерним атакам у корпоративних мережах.

## 6. Практичні результати роботи

У дисертаційній роботі запропоновано архітектуру засобів зберігання історичних даних систем протидії комп'ютерним атакам, яка поєднує автоматизоване керування життєвим циклом даних, урахування особливостей апаратно-програмного забезпечення, інтелектуальне визначення глибини горизонту використання інформації та механізми самонавчання для вибору даних під час виявлення повторюваних атак.

Важливими результатами дослідження є розроблені методи організації зберігання, оптимізації та вибору історичних даних. Метод організації зберігання передбачає їх розподіл на початкові, накопичувані та використані з урахуванням результативності попереднього застосування на основі марковських моделей, динамічних баєсівських мереж і статистичних методів. Запропонований метод оптимізації, що поєднує адаптивне управління даними та механізми самонавчання, сприяє зменшенню інформаційної надлишковості й підвищенню швидкодії доступу до даних, зокрема в підсистемах пам'яті та обманних системах.

Метод вибору історичних даних базується на інтегральній оптимізаційній функції з урахуванням глибини горизонту, семантичної значущості та попереднього досвіду використання інформації. Застосування механізмів самонавчання забезпечує адаптивне формування й коригування сукупностей даних відповідно до змін умов функціонування корпоративних мереж.

Результати експериментальних досліджень, наведені в дисертації, підтверджують ефективність запропонованих архітектурних рішень і методів, зокрема щодо підвищення оперативності доступу до історичних даних, точності вибору релевантної інформації та адаптивності систем протидії комп'ютерним атакам. Це свідчить про практичну значущість отриманих результатів для вдосконалення засобів забезпечення кібербезпеки корпоративних мереж.

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).

## 7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях

Дисертаційна робота складається з анотації, змісту, переліку скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та п'яти додатків. Повний обсяг роботи становить 245 сторінку друкованого тексту, з них анотація займає 14 сторінок, зміст 2 сторінки, перелік скорочень 1 сторінку, вступ, розділи та висновки викладено на с. 16-195, список зі 122 використаних джерел займає 14 сторінок, додатки 36 сторінок. Дисертація містить 12 рисунків та 10 таблиць. Оформлення дисертації відповідає вимогам.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами дисертаційного дослідження опубліковано 11 наукових праць, у тому числі 4 статті у наукових фахових виданнях України категорії Б, 7 праці 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 твір (програму). Комп'ютерна програма «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).

Усі наукові положення і результати дисертації повністю викладено в опублікованих працях. Згідно аналізу наукових статей в фахових наукових журналах категорії Б встановлено, що в них чітко опубліковано основні чотири наукові результати та в них відсутній самоплагіат в контексті оприлюднення наукових результатів.

## 8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи характеризується послідовністю, логічністю та структурованістю викладення матеріалу, написаний українською мовою із дотриманням норм наукового стилю та використанням усталеної фахової термінології. Зміст роботи належним чином проілюстровано схемами, рисунками та таблицями, які сприяють кращому розумінню представлених положень, результатів досліджень і наукових висновків. Мова викладу є чіткою, зрозумілою та грамотною, а стиль і загальне оформлення дисертації відповідають встановленим вимогам до наукових праць такого рівня.

**9. Зауваження та дискусійні положення щодо змісту дисертації**

1. Потребує додаткового обґрунтування вибір критеріїв оцінювання ефективності запропонованих методів. У роботі використовуються показники ймовірності виявлення атак, часу доступу до даних, інформаційної надлишковості та часу реагування. Однак бажано пояснити, чому саме ці показники є достатніми для комплексної оцінки та чи враховуються інші характеристики, зокрема частота хибнопозитивних спрацювань і пропускна здатність системи.

2. Недостатньо чітко розмежовано ефективність запропонованих методів зберігання даних та ефективність системи виявлення комп'ютерних атак загалом. Оскільки результативність виявлення залежить також від алгоритмів аналізу, сенсорів і характеристик атак, доцільно було б детальніше пояснити, яким чином у експерименті ізолюється саме внесок розроблених методів роботи з історичними даними.

3. Потребує уточнення процедура формування експериментального набору даних. У дисертації зазначено використання журналів подій, мережних пакетів, сигнатур і поведінкових характеристик кіберінцидентів, однак доцільно конкретизувати обсяги вибірок, кількість сценаріїв атак, їх типи, часові характеристики та принципи формування навчальної й тестової частин.

4. Не повною мірою розкрито методику забезпечення відтворюваності експериментальних результатів. Бажано було б докладніше описати конфігурацію експериментального середовища, апаратні характеристики, параметри програмного забезпечення, початкові налаштування моделей та процедуру повторення експериментів іншими дослідниками.

5. Потребує додаткового статистичного обґрунтування отриманих експериментальних результатів. У роботі розглядається підвищення ефективності системи, однак доцільно уточнити кількість повторних експериментів, спосіб оцінювання варіативності результатів, довірчі інтервали та критерії статистичної значущості отриманих відмінностей.

6. Практичне застосування запропонованих методів потребує додаткового аналізу стійкості до цілеспрямованого впливу зловмисника. Зокрема, доцільно розглянути можливість маніпулювання історичними даними, навмисного формування хибних подій, впливу на механізми самонавчання та спроб порушення функціонування підсистеми пам'яті. Такий аналіз дозволив би повніше оцінити надійність запропонованого рішення в реальних умовах корпоративної мережі.

7. Недостатньо деталізовано оцінювання ресурсних витрат на реалізацію запропонованої архітектури. Впровадження механізмів самонавчання, марковських моделей, динамічних баєсівських мереж та адаптивної оптимізації може потребувати додаткових обчислювальних ресурсів. Бажано було б визначити накладні витрати за CPU, RAM, дисковими ресурсами та мережевим

трафіком, а також оцінити їх співвідношення з отриманим приростом ефективності.

Однак, зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

**10. Висновки щодо дисертації в цілому**

На основі викладеного вище вважаю, що дисертація Паюка Вадима Павловича на тему «Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах», що подана на здобуття ступеня доктора філософії, є завершеною самостійною науковою працею, у якій отримано нові науково обґрунтовані результати, що в сукупності розв'язують актуальну науково-прикладну задачу вдосконалення методів і засобів роботи з історичними даними та підвищення ефективності протидії комп'ютерним атакам у корпоративних мережах. За актуальністю, науковою новизною, практичною цінністю, змістом та оформленням дисертація 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, № 1240 від 07.10.2026), а її автор, Паюк Вадим Павлович, заслуговує на присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Західноукраїнського національного
університету _____ Степан ІВАСЬЄВ

Підпис _____
Завіряю:
НАЧАЛЬНИК
ЗАГАЛЬНОГО ВІДДІЛУ _____