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 стрімкого розвитку інформаційних технологій, цифровізації бізнес-процесів та зростання складності комп'ютерних атак особливого значення набуває забезпечення надійного захисту корпоративних мереж. Сучасні кіберзагрози характеризуються різноманітністю методів реалізації, високим рівнем адаптивності та здатністю зловмисників долати наявні механізми захисту. Це зумовлює необхідність постійного вдосконалення апаратно-програмних і програмних систем протидії комп'ютерним атакам, зокрема в частині організації, зберігання, оброблення та використання історичних даних про їхнє функціонування.

Важливу роль у забезпеченні кібербезпеки корпоративних мереж відіграють системи та засоби протидії комп'ютерним атакам, функціонування яких ґрунтується на аналізі поточних подій і використанні накопиченого досвіду виявлення та нейтралізації загроз. Відповідно до концепції «піраміди болю зловмисника», ефективність захисних механізмів значною мірою визначається рівнем складності їх подолання та можливістю своєчасного виявлення індикаторів компрометації. На різних рівнях цієї ієрархії застосовуються відповідні засоби захисту, які відрізняються функціональним призначенням, архітектурою та особливостями організації підсистем пам'яті з історичними даними.

Історичні дані, що накопичуються в процесі функціонування систем кіберзахисту, є важливим інформаційним ресурсом для аналізу попередніх атак,

виявлення закономірностей поведінки зловмисників, прогнозування потенційних загроз та формування ефективних захисних рішень. Водночас зростання обсягів таких даних, неоднорідність їх структури, поступова втрата актуальності та обмеженість обчислювальних ресурсів ускладнюють процеси їх зберігання, вибору й оптимізації. Особливої уваги потребує забезпечення можливості оперативного використання релевантних історичних даних залежно від характеру подій у корпоративній мережі та визначеного часового горизонту їх аналізу.

Додатковим чинником, що актуалізує зазначену проблематику, є необхідність підвищення стійкості систем протидії комп'ютерним атакам до цілеспрямованих дій зловмисників, спрямованих на обхід або компрометацію механізмів захисту. У цьому контексті перспективним напрямом є вдосконалення архітектури підсистем пам'яті, застосування адаптивних механізмів організації історичних даних, а також інтеграція обманних технологій, здатних ускладнювати реалізацію атак і підвищувати результативність захисних заходів.

Водночас існує об'єктивна суперечність між необхідністю забезпечення повноти, достовірності та тривалого зберігання історичних даних для ефективного виявлення кіберзагроз і потребою в обмеженні їх обсягів, скороченні витрат обчислювальних ресурсів та своєчасному вилученні інформації, що втратила актуальність. Подолання цієї суперечності потребує розроблення нових і вдосконалення наявних методів зберігання, вибору та оптимізації історичних даних з урахуванням особливостей функціонування систем і засобів протидії комп'ютерним атакам у корпоративних мережах.

З огляду на викладене, дисертаційне дослідження, присвячене розробленню та вдосконаленню методів і засобів зберігання, вибору й оптимізації історичних даних систем протидії комп'ютерним атакам у корпоративних мережах, є актуальним, своєчасним і має важливе наукове та практичне значення. Його спрямованість на підвищення ефективності використання історичних даних, удосконалення механізмів їх організації та забезпечення адаптивності систем кіберзахисту відповідає сучасним потребам розвитку інформаційної безпеки корпоративних інформаційних систем.

Актуальність обраної теми дисертаційного дослідження не викликає сумнівів, оскільки розв'язання поставленої наукової задачі спрямоване на вдосконалення методів і засобів роботи з історичними даними та підвищення ефективності протидії комп'ютерним атакам у корпоративних мережах. Отримані результати можуть мати вагоме значення для подальшого розвитку

методологічних і технологічних засад забезпечення кібербезпеки корпоративних мереж.

Таким чином, тема дисертації є актуальною і відповідає предметній області 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 наданні 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

У вступі представлено обґрунтування актуальності наукової задачі, що полягає у підвищенні ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах шляхом удосконалення архітектури та методів організації зберігання, вибору та оптимізації історичних даних. Перспективним напрямком досліджень для підвищення ефективності протидії комп'ютерним атакам в корпоративних мережах визначено організацію зберігання, оптимізацію та вибір історичних даних з врахуванням глибини горизонту. Продемонстровано зв'язок тематики дослідження з напрямками наукових досліджень науковців за цим спрямуванням, представлено основні наукові результати роботи, їх практичне використання, перелік підприємств та установ, в яких впроваджено результат роботи.

У першому розділі проведено аналіз предметної області дослідження, існуючих систем протидії комп'ютерним атакам в корпоративних мережах, методів, що застосовуються для виявлення комп'ютерних атак та зловмисного програмного забезпечення, а також методів зберігання, оптимізації та вибору історичних даних з урахуванням їх впливу на показники виявлення комп'ютерних атак.

У другому розділі визначено область дослідження, розроблено моделі організації пам'яті з історичними даними щодо функціонування систем та засобів протидії КА, моделі обманних технологій в системах та засобах протидії КА, удосконалено архітектуру засобів підсистеми пам'яті систем та засобів протидії КА в корпоративних мережах на основі використання історичних даних

для прийняття рішень. При розробленні архітектури засобів 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 комп'ютерних атак.

У третьому розділі представлено розроблені такі методи: 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; метод оптимізації даних на основі самонавчання засобів підсистеми пам'яті систем та засобів протидії комп'ютерним атакам, який 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; метод вибору даних, який 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.

У четвертому розділі представлено методику оцінювання ефективності засобів зберігання, вибору та оптимізації історичних даних систем та засобів протидії комп'ютерним атакам. Також, представлено постановку та результати експерименту і засіб зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в 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 у дисертації наукові положення, висновки та рекомендації є аргументованими. Вони спираються на розроблену архітектуру засобів зберігання даних для систем і засобів протидії КА, особливістю якої є поєднання автоматичного керування життєвим циклом даних, врахування особливостей апаратно-програмних засобів зберігання, інтелектуалізації глибини горизонту даних та механізмів самонавчання при виборі даних для типових повторюваних

КА. Розроблено метод організації зберігання даних у системах і засобах протидії КА, який забезпечує поділ даних на початкові, накопичувані та використані, а також врахування історичних аспектів їх застосування на основі оцінювання ефективності використання даних із використанням марковських моделей, динамічних бассівських мереж і статистичних методів.

Розроблено метод організації зберігання даних у системах і засобах протидії КА, який забезпечує поділ даних на початкові, накопичувані та використані, а також врахування історичних аспектів їх застосування на основі оцінювання ефективності використання даних із використанням марковських моделей, динамічних бассівських мереж і статистичних методів. Синтез методів оптимізації та самонавчання в архітектурі підсистем пам'яті систем і засобів протидії КА дав змогу реалізувати адаптивне керування процесами оптимізації початкових, накопичених, використаних даних та даних обманних систем. Це забезпечило зниження надлишковості інформаційних масивів, підвищення швидкодії доступу до даних та покращення інформативності інформаційного середовища для підтримки процесів виявлення і протидії комп'ютерним атакам. Також розроблено метод вибору даних, який базується на використанні інтегральної оптимізаційної функції з урахуванням глибини горизонту, семантичної значущості та попереднього досвіду використання даних, доповнений механізмом самонавчання для адаптивного формування та коригування інтегрованих сукупностей даних. Це дозволило підвищити точність відбору даних, зменшити інформаційну надлишковість і забезпечити динамічну адаптацію систем і засобів протидії КА до змін умов функціонування.

6. Практичні результати роботи

Розроблено архітектуру засобів зберігання даних для систем і засобів протидії КА, особливістю якої є поєднання автоматичного керування життєвим циклом даних, врахування особливостей апаратно-програмних засобів зберігання, інтелектуалізації глибини горизонту даних та механізмів самонавчання при виборі даних для типових повторюваних КА.

За результатами проведених експериментальних досліджень встановлено, що розроблені архітектурні рішення та методи забезпечують ефективне функціонування засобів зберігання даних в умовах динамічної зміни параметрів інформаційного середовища, підвищують оперативність надання даних системам протидії КА, покращують точність вибору релевантної інформації та забезпечують підвищення загальної ефективності функціонування систем і засобів протидії КА.

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 сторінок друкованого тексту, з них анотація займає 13 сторінок, зміст 2 сторінки, перелік скорочень 1 сторінку, вступ, розділи та висновки викладено на с. 16-196, список зі 122 використаних джерел займає 14 сторінок, додатки 36 сторінок. Дисертація містить 12 рисунків та 10 таблиць.

За результатами аналізу тексту дисертаційної роботи не виявлено ознак неправомірного запозичення текстових фрагментів, привласнення наукових результатів інших дослідників або використання їхніх напрацювань без належного посилання на відповідні інформаційні джерела. Усі використані в роботі наукові положення та результати інших авторів супроводжуються відповідними бібліографічними посиланнями, що свідчить про дотримання принципів академічної доброчесності та вимог до оформлення наукових досліджень.

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 твір (програму) Україна. 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. В опублікованих наукових статтях плагіату і самоплагіату не виявлено.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності, українською мовою, з використанням усталеної термінології. Дисертація містить достатню кількість ілюстративного матеріалу: схем, рисунків, таблиць. Мова викладу, стиль та оформлення роботи відповідають вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

1. Потребує уточнення механізм самонавчання запропонованих методів. Бажано конкретизувати змінювані параметри на етапі самонавчання та дані, які використовуються для коригування моделей, а також щодо визначення досягнення прийнятного результату та механізмів, які запобігають накопиченню помилкових рішень.

2. Недостатньо розглянуто проблему негативного впливу помилкових або некоректних історичних даних на процес самонавчання. У корпоративних мережах можуть накопичуватися неповні, застарілі або хибно класифіковані події. Доцільно було б деталізувати механізми контролю якості даних, їх верифікації та виключення з процесу адаптивного навчання.

3. Потребує додаткового обґрунтування інтегральна оптимізаційна функція методу вибору даних. У роботі враховуються кілька критеріїв, однак важливим є пояснення способу визначення їх вагових коефіцієнтів, впливу кожного критерію на кінцевий результат і можливості адаптивного коригування ваг залежно від характеру комп'ютерної атаки.

4. Не повною мірою розкрито проблему конфлікту між актуальністю, інформативністю та ресурсною вартістю зберігання даних. Зокрема, дані, які рідко використовуються, можуть містити критично важливу інформацію про рідкісні або складні атаки. Доцільно уточнити, як запропонований метод запобігає втраті таких даних у процесі оптимізації.

5. Потребує уточнення математичний критерій оптимізації історичних даних. Бажано детальніше пояснити, яким чином у запропонованому методі забезпечується баланс між скороченням інформаційної надлишковості, швидкістю доступу, обсягом пам'яті та ефективністю виявлення комп'ютерних атак, а також як визначаються граничні значення відповідних критеріїв.

6. Не повною мірою розкрито механізм адаптації запропонованих методів до нових, раніше невідомих комп'ютерних атак. Метод вибору історичних даних використовує попередній досвід та механізм самонавчання. Водночас виникає питання щодо рівня ефективності такого підходу у випадку появи атак, які не мають аналогів у накопиченій історії. Орієнтація на повторювані сценарії може обмежувати здатність системи виявляти принципово нові або модифіковані атаки.

7. Недостатньо досліджено вплив розподіленого зберігання даних на узгодженість історичної інформації. Для корпоративних мереж із територіально розподіленими вузлами важливими є затримки передавання, синхронізація, дублювання даних та можливість тимчасової недоступності окремих вузлів. Доцільно було б детальніше розглянути ці аспекти.

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), 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 безпеки інформації та
телекомунікацій Національного університету
«Дніпровська політехніка» Олександра ГЕРАСІНА

Підпис Герасіної
засвідчую:
вчений секретар
Вченої ради

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ДНІПРОВСЬКА ПОЛІТЕХНІКА» * І.К. 02070743 *