ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

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

Публічна презентація проведена на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету «07» жовтня 2026 р., протокол № 7.

1. Актуальність теми дослідження. Зловмисники при здійсненні комп'ютерних атак (КА) на корпоративні мережі (КМ) стикаються з протидією їм різних апаратно-програмних та програмних систем, що відображено в класифікації індикаторів компрометації піраміди болю зловмисника. Долаючи перешкоди при проникненні в КМ зловмисники витрачають багато ресурсів та часу і в цьому процесі для них зростають складності, які пов'язані з проведенням КА. На кожному рівні піраміди болю зловмисника для забезпечення безпеки та захисту КМ використовуються різні апаратно-програмні та програмні засоби і системи. Всі вони залежать від даних щодо свого попереднього функціонування, які формують підсистему пам'яті з історичними даними. В залежності від етапу, на якому розміщуються засоби та системи протидії КА організація їх пам'яті з історичними даними є різною. Зловмисники розуміють ієрархію засобів та систем у співвіднесенні до рівнів піраміди болю зловмисника, а також особливо щодо організації в них підсистем пам'яті з історичними даними. Вважаючи елементи чи підсистеми пам'яті одними з основних джерел попереднього досвіду функціонування для протидії КА, зловмисники прагнуть обходити не стільки сенсори засобів та систем протидії КА, а саме пам'яті з історичними даними щодо функціонування таких засобів та систем. Тому, організація елементів чи підсистем пам'яті з історичними даними щодо функціонування потребує постійного удосконалення за різними рівнями та формами, зокрема і з використанням обманних технологій, які активно інтегруються в апаратно-програмні та програмні засоби і системи протидії КА на КМ, для заплутування зловмисників під час проведення ними КА. Це дало б змогу підвищити рівень кібербезпеки в КМ за рахунок змінюваної організації елементів чи підсистем пам'яті з історичними

даними щодо попереднього функціонування систем і засобів та з використанням відповідних обманних технологій. Ще однією з проблем, які потребують вирішення в контексті зберігання даних, є проблема оптимізації таких даних, бо їх кількість накопичується швидко і частина з них рідко використовується.

В процесі функціонування систем та засобів протидії КА в КМ виникає потреба вибору даних з наявних або їх модифікація для використання при виникненні певних подій в КМ. Такий вибір має забезпечуватись з урахуванням глибини горизонту, що потребує оцінювання актуальності даних. Для вирішення таких проблем із зберіганням, оптимізацією та вибором даних необхідно розробляти нові підходи для забезпечення їх ефективного впливу на процес протидії КА і КМ.

Протиріччя полягає в тому, що системи та засоби протидії КА в КМ повинні забезпечувати повноту, тривалість і історичність зберігання даних для ефективного аналізу та виявлення загроз, але водночас змушені обмежувати обсяги зберігання і тривалість використання даних через втрату їх актуальності, обмеженість обчислювальних ресурсів та необхідність адаптивної обробки, яка може змінювати або витісняти раніше накопичені дані.

Тому, важливою та актуальною науковою задачею є підвищення ефективності зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах за рахунок удосконалення архітектури та методів організації зберігання, вибору та оптимізації історичних даних.

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. Наукові положення, висновки і рекомендації дисертації забезпечуються коректним використанням сучасного математичного апарату, методів теорії ймовірностей, математичної статистики, марковських моделей, динамічних баєсівських мереж, методів оптимізації та інтелектуального аналізу даних при розв'язанні задач організації зберігання, вибору та оптимізації даних у системах і засобах протидії комп'ютерним атакам. Достовірність отриманих результатів підтверджується обґрунтованістю

удосконаленої архітектури засобів зберігання даних для систем і засобів протидії КА, яка забезпечує автоматичне керування життєвим циклом даних, врахування особливостей апаратно-програмного середовища, глибини горизонту даних та механізмів самонавчання для вибору інформації при типових повторюваних комп'ютерних атаках.

Отримані теоретичні результати узгоджуються з результатами експериментальних досліджень, що підтверджує адекватність запропонованих моделей, методів і архітектурних рішень, а також їх ефективність при практичному застосуванні у системах і засобах протидії комп'ютерним атакам.

Наукова новизна отриманих 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.

4. Теоретичне та практичне значення результатів дисертації. 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. 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 баєсівських 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 баєсівських 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.

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.

5. Використання результатів роботи. 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).

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі.

Повнота викладення матеріалів дисертації в роботах, опублікованих автором. За результатами проведених досліджень основні наукові результати опубліковано у чотирьох наукових статтях у фахових виданнях України. Апробацію результатів дисертації засвідчено публікацією сімох праць у матеріалах міжнародних наукових конференцій, з яких дві проіндексовано в наукометричній базі Scopus. Отримано одне свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму).

У роботах, які опубліковані у співавторстві, автору належать основні ідеї, теоретична та практична розробка положень, відображених у характеристиці наукової новизни отриманих результатів, а саме: розроблено моделі даних та метод організації зберігання даних в системах та засобах протидії КА з урахуванням історичного досвіду їх використання; розроблено архітектуру засобів підсистеми пам'яті систем та засобів протидії КА в корпоративних мережах на основі використання історичних даних для прийняття рішень та метод вибору даних з урахуванням глибини горизонту, самонавчання та попереднього досвіду використання; розроблено метод оптимізації даних на основі самонавчання засобів підсистеми пам'яті; розроблено методику застосування багатофакторного аналізу з метою зменшення кількості показників в задачах виявлення ЗПЗ; здійснення порівняльного аналізу альтернативних подань програмного коду та формування експериментальних сценаріїв; здійснено вибір методів машинного навчання до задач аналізу програмного коду та систематизація характеристик програмних систем; здійснено постановку експерименту щодо вразливостей застосунків;– розроблено алгоритм захисту критичної інформації в корпоративних мережах для реалізації засобів; розробка експериментів для перевірки роботи модуля шифрування для різних станів системи централізованого керування; розроблено метод виявлення вставок в програмний код на основі дослідження аномалій при

його виконанні в комп'ютерних мережах; розроблено програмне забезпечення організації зберігання, оптимізації та вибору даних в системах та засобах протидії КА з урахуванням історичного досвіду їх використання.

У роботах, які опубліковані у співавторстві, співавторам належать такі результати: запропоновано концепцію організації зберігання даних в системах та засобах протидії КА з урахуванням історичного досвіду їх використання (Савенко Б.); запропоновано концепцію архітектури засобів підсистеми пам'яті систем та засобів протидії КА в корпоративних мережах на основі використання історичних даних для прийняття рішень (Каштальян А.); запропоновано концепцію оптимізації даних на основі самонавчання засобів підсистеми пам'яті (Савенко Б.); запропоновано підхід до застосування багатофакторного аналізу з метою зменшення кількості показників в задачах виявлення ЗПЗ (Гейдарова О. В., Косенков В. Д.), верифіковано застосування багатофакторного аналізу з метою зменшення кількості показників в задачах виявлення ЗПЗ (Савенко О.С.); [розроблення підходу до побудови графових моделей коду для задачі виявлення вразливостей, визначення схеми перетворення таких моделей у вхідні дані для нейронних мереж і обґрунтування переваг графового представлення порівняно з лінійним (Сєргєєв Є.), здійснено постановку завдання дослідження та участь у аналізі результатів (Саченко А.), інтерпретація результатів експериментів (Kwiecien A., Нічепорук А.); розроблення підходу до аналізу поведінкових характеристик програмних систем з використанням методів машинного навчання для виявлення та прогнозування вразливостей, а також адаптація отриманих положень для формування показників ризику (Сєргєєв Є.), участь у зборі та систематизації даних для завдання дослідження (Нічепорук А., Гуральник О.), верифікація результатів дослідження (Kwiecien A.); здійснено формування вимог до сучасних статичних методів аналізу безпеки, розроблення підходів для підвищення ефективності SAST-засобів у контексті SQL-ін'єкцій, вдосконалення методу статичного тестування безпеки застосунків у контексті вразливостей SQL Injection (Сєргєєв Є.), визначено стратегію тестування безпеки застосунків в корпоративних мережах (Дрозд А.), визначено концепцію здійснення тестування застосунків в корпоративних системах (Савенко О.); розроблено метод захисту критичної інформації в корпоративних мережах (Гуральник О.), здійснено верифікацію моделі подання критичної інформації (Kwiecien A.), здійснено постановку експерименту щодо надійності захисту критичної інформації (Клейн О., Лигун О.); запропонована концепція перевірки ефективності централізованої системи (Стецюк М.), проведено аналіз множини механізмів захисту ОС (Возний К.), здійснено постановку експерименту для дослідження ефективності застосування централізованої системи безпеки ОС (Kvassay M.), розроблено модель централізованої системи безпеки, як інформаційної технології для синтезу архітектури ОС, захищеної від витоку конфіденційної інформації (Стецюк Ю.);

розроблено показники для застосування багатофакторного аналізу ЗПЗ (Нічепорук А.); розроблено концепцію дослідження щодо виявлення вставок в програмний код на основі дослідження аномалій при його виконанні в комп'ютерних мережах (Савенко О., Нічепорук А.), здійснено верифікацію моделі вставок в програмний код на основі дослідження аномалій при його виконанні в комп'ютерних мережах (Каштальня А., Савенко Б.); здійснено постановку завдання щодо архітектури та завдань програмного забезпечення організації зберігання, оптимізації та вибору даних в системах та засобах протидії КА з урахуванням історичного досвіду їх використання (Савенко Б.), розроблено модулі програмного забезпечення організації зберігання, оптимізації та вибору даних в системах та засобах протидії КА з урахуванням історичного досвіду їх використання (Нічепорук А., Каштальян А.).

Результати дисертації опубліковано в повному обсязі.

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету.

Наукові керівники:

доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Каштальян Антоніна Сергіївна;

доктор філософії, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Савенко Богдан Олегович.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Паюка В.П. є результатом самостійних досліджень здобувача і не містить елементів плагіату та неправомірних запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідні джерела.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

Дотримання академічної доброчесності. Дисертаційну роботу Паюка В.П. перевірено на текстові збіги відповідно до встановленого в Хмельницькому національному університеті порядку. За результатами аналізу звіту подібності встановлено, що робота є результатом самостійних досліджень здобувача, не містить елементів академічного плагіату та неправомірних запозичень; використані ідеї, результати й тексти інших авторів супроводжуються належними посиланнями.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 12 праць, у тому числі 4 статей у наукових фахових виданнях України, 7 публікації у матеріалах міжнародних наукових конференцій, з яких 7 проіндексовано у наукометричній базі Scopus, та отримано 1 свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму).

Список публікацій здобувача за темою дисертації.

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Паюк В.П., Савенко Б О. Організація зберігання даних в системах та засобах протидії комп'ютерним атакам з урахуванням історичного досвіду їх використання. Вимірювальна та обчислювальна техніка в технологічних процесах. 2026. № 2. С. 321–336. DOI: https://doi.org/10.31891/2219-9365-2026-86-39

2. Paiuk, V., & Kashtalian, A. (2026). Selection of data in systems and tools for computer attack defense taking into account the historical aspect of their use . Computer Systems and Information Technologies, (3), 186–204. https://doi.org/10.31891/csit-2026-3-19

3. Паюк В. П., Савенко Б О. Оптимізація зберігання даних в системах та засобах протидії комп'ютерним атакам з урахуванням історичного аспекту їх використання. Вимірювальна та обчислювальна техніка в технологічних процесах. 2026. № 3. С. 217–236. DOI: https://doi.org/10.31891/2219-9365-2026-87-26

4. Паюк В. П., Гейдарова О. В., Косенков В. Д., Савенко О. С. Застосування багатофакторного аналізу з метою виявлення незадокументованих закладок програмного забезпечення в локальних комп'ютерних мережах. Вісник Хмельницького національного університету. Технічні науки. 2020. № 5. С. 280-285. DOI 10.31891/2307-5732-2020-289-5-280-285

Праці, які засвідчують апробацію матеріалів дисертації

5. Sierhieiev Y., Paiuk V., Sachenko A., Nicheporuk A., Kwiecien A. A graph-based vulnerability detection method. (2024) *CEUR Workshop Proceedings*, 3675, pp. 388-401. The 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2024) : CEUR-Workshop Proceedings. Vol. 3675. (Khmelnytskyi, March 2024). Khmelnytskyi, 2024. Pp. 343-355. URL: https://ceur-ws.org/Vol-3675/

6. Sierhieiev Y., Paiuk V., Nicheporuk A., Kwiecien A., Huralnyk O. Detection and prediction of the vulnerabilities in software systems based on behavioral analysis with machine learning. The 1th Proceedings of the 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS 2024) Khmelnytskyi, Ukraine, June 28, 2024 : CEUR-Workshop Proceedings. Vol. 3736. 2024. Pp. 239-254. URL: https://ceur-ws.org/Vol-3736/

7. Sierhieiev Y., Savenko O., Paiuk V., Drozd A. Effectiveness and improvement of Static Application Security Testing (SAST) in the context of SQL Injection vulnerabilities // Proceedings of 2024 IEEE 14th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2024, Athens, Greece, October 11-13, 2024). DOI: 10.1109/DESSERT65323.2024.11122171

8. Huralnyk O., Kwiecien A., Paiuk V., Klein O., Lyhun O. Method and Means of Critical Information Processing in Corporate Networks. Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security, Aprile 04, 2025, Khmelnytskyi, Ukraine. Pp. 314-328. URL: https://ceur-ws.org/Vol-3963/paper25.pdf

9. Stetsyuk Y., Stetsyuk M., Voznyi K., Paiuk V., Kvassay M. A model of a centralized security system, as an information technology for the synthesis of an OS architecture protected against the leakage of confidential information. 1st International Workshop on Advanced Applied Information Technologies: (AdvAIT-2024), Khmelnytskyi, Ukraine and Zilina, Slovakia, December 5, 2024. Vol. 3899. P. 224-233. URL: https://ceur-ws.org/Vol-3899/paper20.pdf

10. Paiuk V., Kosenkov V., Savenko O., Nicheporuk A., Geidarova O. Application of multifactor analysis for the purpose of detecting malicious software implants of the software in local computer networks. 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2021. Ceur Workshop Proceedings. Vol. 2853. Pp. 517–526. URL: https://ceur-ws.org/Vol-2853/paper46.pdf

11. Nicheporuk A., Paiuk V., Savenko B., Savenko O., Geidarova O. Detecting Software Malicious Implant Based on Anomalies Research on Local Area Networks. Ceur Workshop Proceedings, 1nd International Workshop on Intelligent Information Technologies and Systems of Information Security, June 10-12, 2020. Khmelnytskyi, Ukraine 2020, Vol. 2623. Pp. 194–207. URL: https://ceur-ws.org/Vol-2623/paper18.pdf

Публікації, які додатково відображають наукові результати дисертації

12. Свідоцтво про реєстрацію авторського права на твір (програму) № 150528 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») / Нічепорук А. О., Паюк В.П., Савенко Б.О., Каштальян А.С. Дата реєстрації 03.09.2026.

8. Апробація дисертації. Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідались на таких конференціях: 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: (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 & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, April 04, 2025).

9. Оцінка мови, стилю та оформлення дисертації. Дисертацію написано грамотною українською мовою. Стиль викладення матеріалів дослідження, наукових положень, висновків і рекомендацій є послідовним, логічним та забезпечує належне сприйняття змісту роботи. Дисертацію оформлено відповідно до вимог, передбачених наказом Міністерства освіти і науки України від 12.01.2017 № 40 (зі змінами, внесеними наказом Міністерства освіти і науки України від 31.05.2019 № 759) «Про затвердження Вимог до оформлення дисертації».

ВВАЖАТИ, що дисертаційна робота Паюка Вадима Павловича
(прізвище, ініціали здобувача)
«Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах»,
(назва)
яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю 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», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 123 Комп'ютерна інженерія.
(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Методи та засоби зберігання, вибору та оптимізації історичних даних систем і засобів протидії комп'ютерним атакам в корпоративних мережах»,

(назва роботи)

подану Паюком Вадимом Павловичем

(прізвище, ім'я, по батькові)

на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації,
доктор філософії, доцент,
завідувачка кафедри КІС _____ Ольга ПАВЛОВА
(науковий ступінь, вчене звання, посада) підпис Ім'я ПРІЗВИЩЕ

Підпис дійсний
Відділ кадрів

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВІДДІЛ КАДРІВ
Ідентифікаційний код 02071294