Отримано
26.06.2026 р.
Голова СВР
ДФ 26.133.139
д.т.н., проф.

Голові спеціалізованої вченої ради
ДФ 26.133.139
У Київському столичному університеті
імені Бориса Грінченка
доктору технічних наук, професору,
професору кафедри інформаційної та
кібернетичної безпеки імені професора
Володимира Бурячка Факультету
інформаційних технологій та
математики Київського столичного
університету імені Бориса Грінченка
Гулаку Геннадію Миколайовичу

РЕЦЕНЗІЯ

ДОВЖЕНКО Надії Михайлівни, кандидата технічних наук, доцента, доцента кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка, на дисертацію **ЧЕРНІГІВСЬКОГО Івана Андрійовича** **«Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей»** подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

1. Актуальність дисертаційного дослідження

Інтенсивний розвиток інформаційних технологій та інфокомунікаційних мереж (ІКМ) призвів до впровадження передових технологій обробки і передачі даних та появи якісно нових послуг і сервісів в інформаційній сфері. Зазначене зумовило появу нових форм і способів несанкціонованого доступу до обчислювальних ресурсів ІКМ та призвело

до постійного щорічного зростання кількості і складності кібератак на інформаційні системи, спрямованих на порушення цілісності, конфіденційності і доступності інформації. При цьому складні атаки типу APT (Advanced Persistent Threat) не виявляються традиційним антивірусом і тому зловмисник може тривалий час перебувати в мережі не проявляючи своєї присутності активними діями, допоки його не буде виявлено. Загальновідомі тактики, вдосконалені штучним інтелектом, програми-вимагачі як послуга (RaaS) та передові методи соціальної інженерії випереджають традиційні засоби захисту.

Складність сучасних кіберзагроз, їх нелінійний характер розвитку, а також необхідність оперативного прийняття рішень у реальному часі зумовлюють потребу у створенні нових методів захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, оскільки традиційні рішення захисту вузлів ІКМ можуть пропускати комп'ютерні віруси внаслідок недосконалості механізмів їх виявлення, що особливо критично під час багаторівневих кібератак.

Саме тому, розробка методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей є важливою науковою задачею, що має теоретичну та практичну цінність.

2. Наукова новизна результатів дисертації

Наукова новизна результатів дисертаційного дослідження **Чернігівського Івана Андрійовича** зумовлена тим, що вперше запропоновано метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, побудований за принципом послідовного циклічного звернення до операторів ідентифікації, прийняття рішення та реалізації

керуючих дій, у якому ідентифікація стану вузла ІКМ здійснюється на основі вивантаження мінімально необхідної кількості цифрових слідів та їх аналізу нейромережевими моделями, що дозволяє забезпечити економію часу і ресурсів на виявлення комп'ютерних вірусів та протидії їх поширенню в інфокомунікаційній мережі. Вперше запропоновано і реалізовано використання цифрових слідів у якості основної ідентифікаційної ознаки при оцінці зараженості вузлів ІКМ, що забезпечує виявлення ШПЗ, пропущених традиційними рішеннями захисту кінцевих точок, та надає можливість вдосконалення наявного ешелонованого захисту ІКМ. Вперше запропоновано і реалізовано реляційну модель у вигляді таблиці артефактів, яка шляхом фільтрації дозволяє оптимізувати кількість і розмір цифрових слідів між наявними артефактами у вузлі і достатніми для ідентифікації стану, що забезпечує економію часу і ресурсів для виявлення наявності комп'ютерних вірусів у вузлах ІКМ. Вперше запропоновано і реалізовано застосування нейромережевих моделей для аналізу вивантажених цифрових слідів, що забезпечує підвищення швидкості реагування на виникаючі інциденти в ІКМ з великою кількістю вузлів. Набув подальшого розвитку метод вивантаження цифрових артефактів в умовах обмеженості ресурсів, який за рахунок оптимізації кількості і розміру цифрових слідів та їх ранжування забезпечує можливість формування уявлення про стан зараженості конкретного вузла на сервері ІКМ навіть у випадку переривання з'єднання під час передачі даних. Отримані результати розширюють існуючі підходи до виявлення комп'ютерних вірусів в ІКМ та підвищують ефективність управління кіберзагрозами.

3. Теоретичне і практичне значення результатів дисертації

Теоретичне значення результатів дисертаційного дослідження **Чернігівського Івана Андрійовича** полягає у подальшому розвитку наукових засад забезпечення кіберстійкості інфокомунікаційної мережі шляхом вивантаження мінімально необхідної кількості цифрових слідів та їх аналізу нейромережевими моделями, що дозволяє забезпечити економію часу і ресурсів на виявлення комп'ютерних вірусів та протидії їх поширенню в інфокомунікаційній мережі. У дисертаційній роботі запропоновано науково обґрунтований підхід до виявлення кіберінцидентів в розподілених ІКМ, який розширює існуючі підходи до оцінки стану вузла ІКМ за рахунок використання реляційної та нейромережевих моделей та врахування спрацювання антивірусного захисту на існуючі загрози. Отримані результати сприяють розвитку методологічних основ побудови ефективного захисту для забезпечення кіберстійкості ІКМ та формуванню наукових підходів до виявлення шкідливих впливів під час її функціонування. Таким чином, застосовані моделі та удосконалені методи створюють теоретичне підґрунтя для подальших досліджень у сфері кібербезпеки, зокрема щодо аналізу поведінки складних кіберзагроз, та розроблення ефективних механізмів реагування на кіберінциденти.

Практичне значення результатів дисертаційного дослідження полягає в тому, що в дослідженні запропоновано моделі та методи, які доцільно використовувати для підвищення кіберзахисту організацій навіть за наявності інших захисних рішень, за рахунок більш оперативного реагування на виникаючі загрози, а також автоматичного прийняття рішення та здійснення керуючих дій. Запропонований метод дозволяє знаходити вірусну активність там, де його пропустив традиційний антивірус

та навіть за умови самоліквідації вірусного файлу та підвищити ефективність реагування на кіберінциденти у системах управління інформаційною безпекою. Запропоновані моделі та методи можуть бути використані організаціями та державними структурами при розробці та удосконаленні оцінки захищеності інформації на вузлах ІКМ. Практичне значення отриманих результатів полягає у можливості їх застосування в різних галузях для вдосконалення методів захисту інформації від впливу комп'ютерних вірусів і більш ефективного використання часу аналітика при проведенні Forensic-аналізу ІКМ.

Теоретичні та практичні результати доцільно використовувати у науково-дослідній діяльності для створення нових методів аналізу інфокомунікаційних мереж, а також ввести у навчальний процес закладів вищої освіти під час викладання дисциплін з кібербезпеки, інформаційної безпеки та аналізу кіберінцидентів.

4. Наукова обґрунтованість результатів дослідження, наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність

Наукова обґрунтованість результатів дослідження підтверджується тим, що опрацьовано теоретичні наукові джерела, звіти міжнародних організацій та проведено їх аналіз. Наукові положення, висновки і результати, які представлені в дисертації **Чернігівського Івана Андрійовича**, є теоретично і емпірично обґрунтованими та достовірними. Для проведення досліджень в дисертаційній роботі використовувалися методи аналізу і синтезу систем; теорія інформації; теорія прийняття рішень; теорія алгоритмів; теорія ймовірностей; комп'ютерне та імітаційне моделювання. Загальні висновки дисертації логічні та повністю

розкривають хід дослідження, поставлені завдання та результати проведеної роботи.

5. Зв'язок теми дисертаційної роботи з науковими програмами, планами, фундаментальними та прикладними дослідженнями

Дисертаційна робота виконана відповідно до планів наукової та науково-технічної діяльності кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи №0122U200483 «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (м. Київ). Висновки та пропозиції, які отримані в дисертаційному дослідженні мають практичну цінність та прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 21.04.2026 року) та ТОВ «АШАН Україна Гіпермаркет» (акт від 10.03.2026).

6. Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності

Поставлене в дисертаційній роботі наукове завдання виконано здобувачем на належному науковому рівні. Мета дослідження сформульована чітко та логічно, визначені завдання є взаємопов'язаними й адекватними меті, а обрані методи дослідження є доцільними та достатніми для їх розв'язання. Зміст дисертаційної роботи свідчить про те, що **Чернігівський Іван Андрійович** володіє методологією наукової

діяльності, застосовує її при проведенні теоретичних та експериментальних досліджень, вміє формулювати наукові положення та узагальнювати одержані результати. Таким чином, здобувач оволодів повністю необхідними професійними та науково-дослідницькими компетентностями, що відповідають рівню доктора філософії.

7. Апробація результатів дисертації

Результати дисертаційного дослідження пройшли належну наукову апробацію та відображені в опублікованих наукових працях здобувача відповідно до мети та поставлених завдань. Основні результати дисертації висвітлено 12 наукових публікаціях, із них 3 – одноосібні, 9 – у співавторстві: 7 статей у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection. Основні теоретичні та практичні результати були представлені та обговорені на наукових 5 конференціях. У публікаціях, які виконані у співавторстві, вказано особистий внесок здобувача, що свідчить про самостійність виконання основних положень дисертаційного дослідження.

8. Структура та зміст дисертації, її самостійність, завершеність, відповідність вимогам щодо оформлення й обсягу

Зміст дисертаційної роботи **ЧЕРНІГІВСЬКОГО Івана Андрійовича** на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей» розкриває основні питання теми, відповідає меті та завданням дослідження. Дисертація складається зі вступу, чотирьох розділів, висновків, списку

використаних джерел із 135 найменувань на 11 сторінках і 3 додатки. Загальний обсяг роботи становить 244 сторінки, серед яких 197 сторінок – основного тексту, 58 рисунків і 43 таблиці. Зміст дисертаційної роботи є логічно побудованим, матеріал викладено послідовно, з дотриманням наукового стилю. Робота характеризується системністю викладення матеріалу, обґрунтованістю наукових положень, наявністю результатів експериментальних досліджень та їх аналізу.

9. Дотримання академічної доброчесності у дисертації та наукових публікаціях

Аналіз тексту дисертаційної роботи та наукових публікацій дозволяє зробити висновок, що **ЧЕРНІГІВСЬКИЙ Іван Андрійович** дотримувався принципів академічної доброчесності, в тексті не знайдено ознак плагіату, фабрикації чи фальсифікації результатів дослідження. Дисертаційна робота є оригінальним завершеним науковим дослідженням, що відповідає вимогам, які встановлені Міністерством освіти і науки України до оформлення дисертацій на здобуття наукового ступеня доктора філософії.

10. Дискусійні положення, недоліки та зауваження до дисертації

Зауважень щодо структури, основних положень та загального підходу до досліджень в дисертації **ЧЕРНІГІВСЬКОГО Івана Андрійовича** не виявлено. Позитивно оцінені наукові та практичні значення отриманих результатів дисертаційного дослідження, доцільно висловити окремі зауваження та рекомендації:

1. Доцільно було б включити в дослідження хмарні моделі ШІ такі як ChatGPT, Claude.

2. У частині, де викладено практичні результати дослідження, доцільно розширити перелік вивантажених цифрових слідів, оскільки зазвичай не настільки обмежені ресурси щоб боротись за кожний МБ.
3. В аналізі літературних джерел доцільно було б окремо представити сучасні дослідження у сфері застосування методів штучного інтелекту та окремо по цифровим слідам.

Зазначені зауваження не знижують загальної наукової та практичної цінності дисертаційної роботи та мають рекомендаційний характер.

11. Загальний висновок про рівень набуття здобувачем теоретичних знань, відповідних умінь, навичок та компетентностей

За результатами аналізу дисертаційної роботи можна зробити висновок, що **ЧЕРНІГІВСЬКИЙ Іван Андрійович** на високому рівні оволодів методологією наукової діяльності та набув необхідних теоретичних знань, умінь, навичок і професійних компетентностей. Здобувач продемонстрував належний рівень володіння методологією наукових досліджень, здатність самостійно формулювати наукові задачі, обґрунтовувати обрані підходи та узагальнювати отримані результати.

12. Загальна оцінка дисертації і наукових публікацій щодо їхнього наукового рівня та відповідності вимогам

Дисертаційна робота **ЧЕРНІГІВСЬКОГО Івана Андрійовича** на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей» є завершеним науковим дослідженням, яке за актуальністю, науковою новизною, достовірністю отриманих результатів та практичною цінністю відповідає вимогам

«Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», що затверджено Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, **ЧЕРНІГІВСЬКИЙ Іван Андрійович**, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензент:

кандидат технічних наук, доцент,
доцент кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
Київського столичного
університету імені Бориса Грінченка Надія ДОВЖЕНКО

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Н. Довженко (ПІБ)
ЗАСВІДЧУЮ
Начальник відділу кадрів (посада)

динамічністю, прихованістю та використанням легітимних утиліт і комбінованих впливів на інформаційні системи і критичну інфраструктуру, що ускладнює їх своєчасне виявлення та ідентифікацію. Це обумовлює необхідність розроблення нових підходів до виявлення таких впливів. Крім того, складні атаки типу APT (Advanced Persistent Threat) не виявляються традиційним антивірусом і тому зловмисник може тривалий час перебувати в мережі не проявляючи своєї присутності активними діями, допоки його буде виявлено. Загальновідомі тактики, вдосконалені штучним інтелектом, програми-вимагачі як послуга (RaaS) та передові методи соціальної інженерії випереджають традиційні засоби захисту. Складність сучасних кіберзагроз, їх нелінійний характер розвитку, а також необхідність оперативного прийняття рішень у реальному часі зумовлюють потребу у створенні нових методів захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів.

Таким чином, дисертаційна робота Чернігівського І.А., присвячена синтезу методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, здатного забезпечити підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі, є актуальним науковим дослідженням. Напрям дисертаційного дослідження Чернігівського І.А. безпосередньо пов'язаний із реалізацією ключових державних стратегічних документів, а саме: Доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

2. Зв'язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертаційна робота виконувалася відповідно до планів наукових досліджень на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в межах науково-дослідної роботи «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (номер державної реєстрації 0122U200483, КСУБГ, м. Київ). У межах зазначеної НДР здобувачем особисто було запропоновано і реалізовано низку ключових компонентів, що становлять основу дисертації, зокрема: метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, побудований за принципом послідовного циклічного звернення до операторів ідентифікації, прийняття рішення та реалізації керуючих дій; використання цифрових слідів у якості основної ідентифікаційної ознаки при оцінці зараженості вузлів ІКМ; реляційну модель у вигляді таблиці артефактів;

застосування нейромережевих моделей для аналізу вивантажених цифрових слідів; метод вивантаження цифрових артефактів в умовах обмеженості ресурсів.

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Аналіз змісту дисертаційної роботи свідчить, що визначені мета, завдання, об'єкт і предмет дослідження узгоджуються з темою дисертації та відображають ключові напрями наукових досліджень, виконаних автором.

Обґрунтованість наукових положень, висновків і рекомендацій забезпечується чіткою постановкою дослідницьких завдань, належним рівнем їх теоретичного й практичного опрацювання, а також коректним використанням відповідних методів для їх розв'язання, зокрема: аналізу і синтезу систем; теорія інформації; теорія прийняття рішень; теорія алгоритмів; теорія ймовірностей; комп'ютерне та імітаційне моделювання. Достовірність отриманих результатів підтверджується використанням реальних статистичних даних, результатами комп'ютерного та імітаційного моделювання, яке підтверджує переваги запропонованих рішень, та їх практичним впровадженням.

Наявні наукові праці та довідки щодо впровадження результатів дослідження засвідчують актуальність проведеного дослідження, професійний підхід здобувача до обрання дослідницької проблематики та високий рівень його наукової компетентності.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

У дисертаційній роботі отримано низку наукових результатів, що мають вагоме теоретичне та прикладне значення для розвитку підходів до захисту ІКМ. Зазначені результати відзначаються науковою новизною та відображають внесок автора у розв'язання актуальних наукових завдань у сфері кібербезпеки. Основні наукові результати, що визначають новизну роботи, полягають у наступному:

– вперше запропоновано метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, побудований за принципом послідовного циклічного звернення до операторів ідентифікації, прийняття рішення та реалізації керуючих дій, у якому ідентифікація стану вузла ІКМ здійснюється на основі вивантаження мінімально необхідної кількості цифрових слідів та їх аналізу нейромережевими моделями, що дозволяє забезпечити економію часу і ресурсів на виявлення комп'ютерних вірусів та протидії їх поширенню в інфокомунікаційній мережі;

– вперше запропоновано і реалізовано використання цифрових слідів у якості основної ідентифікаційної ознаки при оцінці зараженості вузлів ІКМ, що

забезпечує виявлення ШПЗ, пропущених традиційними рішеннями захисту кінцевих точок, та надає можливість вдосконалення наявного ешелонованого захисту ІКМ;

– вперше запропоновано і реалізовано реляційну модель у вигляді таблиці артефактів, яка шляхом фільтрації дозволяє оптимізувати кількість і розмір цифрових слідів між наявними артефактами у вузлі і достатніми для ідентифікації стану, що забезпечує економію часу і ресурсів для виявлення наявності комп'ютерних вірусів у вузлах ІКМ;

– вперше запропоновано і реалізовано застосування нейромережевих моделей для аналізу вивантажених цифрових слідів, що забезпечує підвищення швидкості реагування на виникаючі інциденти в ІКМ з великою кількістю вузлів;

– набув подальшого розвитку метод вивантаження цифрових артефактів в умовах обмеженості ресурсів, який за рахунок оптимізації кількості і розміру цифрових слідів та їх ранжування забезпечує можливість формування уявлення про стан зараженості конкретного вузла на сервері ІКМ навіть у випадку переривання з'єднання під час передачі даних.

Представлені результати свідчать про особистий внесок здобувача у розв'язання важливого наукового завдання – підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі.

5. Теоретична цінність і практична значущість наукових результатів

Теоретична цінність дисертаційного дослідження полягає у формуванні комплексного наукового підходу до забезпечення кіберстійкості ІКМ на основі синтезу методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, здатного забезпечити підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі. Теоретично доведено доцільність використання цифрових слідів для виявлення загроз, що забезпечує виявлення шкідливого впливу там, де його пропустив традиційний антивірус. Розроблений метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, побудований за принципом послідовного циклічного звернення до операторів ідентифікації, прийняття рішення та реалізації керуючих дій, у якому визначення стану вузла ІКМ здійснюється на основі вивантаження мінімально необхідної кількості цифрових слідів та їх аналізу нейромережевими моделями, створює наукове підґрунтя для побудови інтелектуальних систем, здатних прогнозувати, виявляти та знешкоджувати дестабілізуючі впливи на вузли інфокомунікаційної мережі в умовах активної протидії виявленню з боку кіберзлочинців.

Практична значущість отриманих результатів визначається можливістю їх застосування в різних галузях для вдосконалення методів захисту інформації від

впливу комп'ютерних вірусів і більш ефективного використання часу аналітика при проведенні Forensic-аналізу ІКМ, зокрема:

– імплементація запропонованого методу захисту вузлів ІКМ дозволяє виявити вірусну активність на одному вузлі ІКМ за 6хв роботи з достовірністю від 60% до 100%. Зокрема, 100% достовірність забезпечується за наявності будь-яких записів у антивірусних виключеннях Windows Defender;

– словник ознак для ідентифікації стану вузлів ІКМ і запропоновані таблиці артефактів є достатніми для прийняття рішень в циклах управління;

– рекомендовані програми для швидкого виявлення вірусів і скрипт оптимізації з використанням реляційної таблиці артефактів дозволяють скоротити кількість елементів, необхідних для подальших досліджень більш ніж у десять разів;

– удосконалений метод вивантаження цифрових артефактів в умовах обмеженості ресурсів, за рахунок оптимізації кількості і розміру цифрових слідів та їх ранжування забезпечує можливість формування уявлення про стан зараженості конкретного вузла на сервері ІКМ навіть у випадку переривання з'єднання під час передачі даних.

Наукові положення та практичні рекомендації у дисертаційному досліджені прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 21.04.2026 року) та ТОВ «АШАН Україна Гіпермаркет» (акт від 10.03.2026), а також використовуються в освітньому процесі Київського столичного університету імені Бориса Грінченка. Результати роботи можуть бути використані при розробці перспективних систем кіберзахисту об'єктів критичної інфраструктури України.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

Основні наукові результати та положення дисертаційного дослідження Чернігівського І.А. повною мірою висвітлено у 12 наукових публікаціях, що відповідає чинним вимогам МОН України щодо оприлюднення змісту дисертацій на здобуття ступеня доктора філософії. До переліку опублікованих праць входять 7 статей у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті, що індексуються в базі Scopus, 5 публікацій за результатами виступів та обговорень на наукових конференціях різних рівнів. Аналіз публікацій за темою роботи підтверджує особистий внесок здобувача у кожній праці. Зміст опублікованих праць цілком відповідає основним положенням дисертації, що дозволяє зробити висновок про належне та повне оприлюднення результатів проведеного наукового дослідження.

7. Відсутність (наявність) порушення академічної доброчесності

Аналіз дисертаційної роботи та оприлюднених наукових праць за темою дослідження засвідчує відсутність ознак порушення вимог академічної доброчесності. За результатами перевірки встановлено, що дисертаційна робота є результатом самостійних досліджень здобувача. Робота не містить елементів плагіату, фальсифікації, фабрикації чи неправомірних запозичень. Усі використані ідеї, результати, методичні положення та тексти інших авторів мають належні посилання на відповідні першоджерела і використані автором виключно для підкріплення власних наукових висновків. Дисертаційна робота відповідає нормам законодавства України про авторське право і суміжні права. Матеріал викладено з дотриманням вимог наукової етики, що відображає прагнення автора до надання достовірної інформації про результати власної наукової діяльності. Таким чином, можна зробити обґрунтований висновок про повне дотримання Чернігівським І.А. принципів академічної доброчесності.

8. Дискусійні положення та зауваження до дисертації

Оцінюючи дисертаційну роботу Чернігівського І.А. як ґрунтовне та завершене наукове дослідження, доцільно висловити низку дискусійних положень та зауважень:

1. У роботі не розглянуто питання впливу людського фактора та можливих нештатних подій на сервері на ефективність функціонування запропонованого методу.
2. У роботі не розглядається аналіз цифрових слідів із журналів операційної системи та дослідження вмісту оперативної пам'яті (RAM), незважаючи на те, що ці джерела часто містять важливі відомості для виявлення та розслідування інцидентів інформаційної безпеки.
3. У роботі не проведено оцінювання впливу запропонованого методу донавчання на здатність моделей виявляти зараження вузлів ІКМ та не здійснено порівняння їхньої ефективності з моделями, які не пройшли такого донавчання.

Висловлені зауваження та дискусійні положення не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

9. Загальна оцінка дисертаційної роботи, її відповідність встановленим вимогам

Дисертаційна робота Чернігівського Івана Андрійовича на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей» є завершеним науковим дослідженням, виконаним

автором самостійно на високому науковому рівні. Сукупність отриманих автором нових теоретичних положень, удосконалених методів та розроблених математичних моделей у своїй єдності розв'язує актуальне наукове завдання – підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі. Дисертаційна робота Чернігівського І.А. за своєю актуальністю, рівнем наукової новизни, теоретичною та практичною значущістю результатів повністю відповідає вимогам, встановленим у «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. Враховуючи високий науковий рівень виконаного дослідження, вважаю, що здобувач Чернігівський Іван Андрійович заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент:

завідувач кафедри
інженерії програмного забезпечення
та кібербезпеки
Державного торговельно-економічного
університету
доктор філософії, доцент Альона ДЕСЯТКО

Підпис Десятко Альона засвідчую
Начальник відділу кадрів