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

ВІДГУК

офіційного опонента **СМІРНОВА Олексія Анатолійовича,** доктора технічних наук, професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету на дисертацію **ЧЕРНІГІВСЬКОГО Івана Андрійовича** на тему **«Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей»** подану на здобуття доктора філософії за спеціальністю 125 Кібербезпека

1. Актуальність теми дослідження.

Сучасний інформаційний простір неможливо уявити без інфокомунікаційних мереж (ІКМ). Оскільки в них знаходиться конфіденційна інформація то ці мережі стали об'єктом складних кібератак, спрямованих на порушення цілісності, конфіденційності і доступності інформації. Такі атаки постійно вдосконалюються а їх кількість зростає щорічно.

Проте більшість традиційних методів забезпечення кібербезпеки орієнтовані на звичайні загрози, що робить їх не ефективними у реаліях кібервійни, оскільки вони не враховують інтелектуальний характер цих атак та можливості кіберзлочинців активно протидіяти виявленню їх шкідливих впливів. Така ситуація вимагає більш просунутих механізмів захисту інформації, застосування методів і моделей, що здатні працювати в режимі реального часу та забезпечувати виявлення шкідливих впливів там, де їх пропущено традиційними рішеннями. Впровадження таких методів і моделей сприяє створенню комплексного захисту інформації, зокрема можливість підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі, автономне виявлення та реагування на інциденти інформаційної безпеки.

Таким чином, впровадження методів та моделей забезпечення кібербезпеки ІКМ на основі синтезу методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів стає необхідним елементом методологічної основи концепції інформаційної безпеки, що й визначає актуальність даного дослідження.

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

Дисертація виконана на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка відповідно до теми науково-дослідної роботи та індивідуального плану аспіранта Київського столичного університету імені Бориса Грінченка. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

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

Зміст дисертаційної роботи повною мірою розкриває тему наукового дослідження та відповідає визначеним меті, завданням, об'єкту та предмету дослідження. Розроблені автором і викладені у дисертаційній роботі наукові положення, висновки та рекомендації є аргументованими та обґрунтованими, сформульовані чітко, логічно і послідовно.

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості та достовірності, оскільки при її підготовці:

1) опрацьовано значну кількість літературних джерел зарубіжних і вітчизняних вчених, проаналізовано нормативно-правове забезпечення та приділено значну увагу дослідженню та можливості впровадження іноземного досвіду;

2) використано широкий спектр загальнонаукових і спеціальних методів дослідження – індукції і дедукції, логічного узагальнення, аналізу і синтезу систем, теорії інформації, теорії прийняття рішень, теорії алгоритмів, теорії ймовірностей, комп'ютерне та імітаційне моделювання;

3) вміло використано значний масив статистичного і фактологічного матеріалу, який якісно опрацьовано, систематизовано у вигляді таблиць та візуалізовано за допомогою рисунків, що забезпечує високу наочність отриманих висновків.

Перелік наукових праць та довідки щодо впровадження результатів дослідження засвідчують фаховий підхід здобувача до обрання дослідницької проблематики та високий рівень його наукової компетентності. Викладене вище дає можливість висловити позитивний висновок стосовно наукового рівня, достовірності подання в дисертації матеріалу, теоретичних обґрунтувань і аргументації всіх положень, практичного значення висновків і рекомендацій.

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

Представлені в дисертації положення, концептуальні засади, структура, постановка завдань та їх вирішення, узагальнені висновки є результатом реалізації авторських ідей і самостійно виконаної наукової праці. У дисертаційній роботі Чернігівського І.А. обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

1) 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;

2) 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;

3) 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;

4) 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;

5) 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 створюють науково-методологічне підґрунтя для розробки доктрин кібербезпеки сучасної армії та є фундаментом для впровадження адаптивних стратегій управління ризиками, здатних ефективно протидіяти динамічній еволюції загроз у цифровому просторі ведення бойових дій.

5. Теоретична цінність і практична значущість наукових результатів.

Дисертаційна робота Чернігівського І.А. має фундаментальне значення для галузі, а її висновки та розробки пропонують нові підходи до розв'язання

актуальних завдань кібербезпеки, що підтверджує як теоретичну, так і практичну цінність проведеного дослідження.

Теоретичне значення дослідження 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.

Практична цінність дисертаційної роботи Чернігівського І.А. є беззаперечною, що підтверджується наступними результатами:

1) запропонований метод дозволяє забезпечити підвищення швидкості реагування на виникаючі інциденти, економію часу і ресурсів на виявлення комп'ютерних вірусів, протидію поширення ШПЗ в ІКМ та є швидшим на 90% порівняно із повним ручним аналізом та ізоляцією зараженого вузла ІКМ, оскільки витрачає близько 6хв на аналіз одного вузла ІКМ;

2) запропонована реляційна модель у вигляді таблиці артефактів, шляхом фільтрації дозволяє оптимізувати кількість і розмір цифрових слідів за критерієм «необхідна достатність – мінімум часу», що забезпечує економію часу і ресурсів на виявлення наявності комп'ютерних вірусів у вузлах ІКМ;

3) відібрані 43 моделі ШІ, що відповідають запропонованим критеріям оцінки нейромережевих моделей, є доцільними для застосування при вирішенні задач кібербезпеки, зокрема для виявлення заражених ПК на базі цифрових слідів;

4) Реалізований метод вивантаження цифрових слідів повністю відпрацьовує за 2хв 40сек (що швидше на 81.1%, ніж Cedarpelta) та має розмір артефактів 89.4МБ (що менше Cedarpelta на 48% та KAPE на 88%) при однаковій релевантності даних, при цьому за перші 1хв 28сек сформовано 67КБ артефактів, яких достатньо для первинного перегляду. Застосування меншої кількості цифрових артефактів та їх аналіз нейромережевими моделями критично важливо для зменшення когнітивного навантаження на аналітиків інформаційної безпеки.

Практичні рішення наукових досліджень 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).

Сформульовані в дисертації висновки та пропозиції можуть бути використані в організаціях будь-якого типу власності, де є інформаційно-комунікаційні мережі.

6. Повнота викладення наукових результатів дисертації в опублікованих працях.

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 5 наукових конференціях.

Аналіз публікацій автора дозволяє зробити висновок про повноту викладення основних наукових положень дисертаційного дослідження у науковій літературі. Також зазначено особистий внесок здобувача у тих публікаціях, які виконано у співавторстві.

7.Відсутність (наявність) порушення академічної доброчесності.

Комплексний аналіз дисертації та наукових публікацій автора підтверджує повне дотримання принципів академічної доброчесності. У роботі забезпечено належне цитування джерел при використанні сторонніх ідей та розробок, що повністю відповідає нормам авторського права. Автор демонструє сумлінний підхід до представлення результатів власних досліджень, методик та використаних ресурсів. Усі посилання на першоджерела є верифікованими та коректними, а ознак навмисного спотворення інформації не виявлено.

8.Дискусійні положення та недоліки дисертаційної роботи.

Високо оцінюючи наукове дослідження автора, варто водночас зосередити увагу на окремих положеннях роботи, що потребують глибшого обґрунтування та додаткової аргументації.

1. Автор вказав, що метод відслідковування слідів вірусів та їх вивантаження є більш точним на відміну від антивірусу, проте зазначений метод відсікає значну частину слідів, таким чином не можна знайти ШПЗ яке ховається, наприклад руткіт.

2. Незважаючи на те, що ідентифікується вірусна активність, залишається незрозумілим яким чином захищаються вузли, якщо лише констатується факт зараження.

3. Автор обрав лише один варіант вірусу для побудови таблиці артефактів та формування таблиці первинних даних для донавчання нейромережевих моделей.

Вказані недоліки не носять принципового характеру та не впливають на загальну позитивну оцінку представленої до захисту дисертаційної роботи, оскільки в основному носять дискусійний характер та спрямовують дисертанта на дослідження зазначеної проблематики. Також слід зауважити, що наявність дискусійних питань, насамперед, характеризує складність, актуальність і багатоаспектність досліджуваної теми та власний підхід до її розгляду дисертантом.

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, самостійним науковим дослідженням, яке має теоретичне і практичне значення та характеризується науковою новизною. Результати роботи можуть бути використані при формуванні положень систем управління інформаційною безпекою та

управління ризиками, що відповідають сучасним викликам гібридних загроз. Виконане дослідження має достатньо високий теоретичний, методичний та практичний рівні, послідовне та логічне представлення матеріалу, необхідну повноту розкриття виконаних розробок.

Дисертація за формою і змістом відповідає вимогам викладеним 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 року №44.

ЧЕРНІГІВСЬКИЙ Іван Андрійович, автор дисертаційної роботи на тему: «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей», заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Офіційний опонент
завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
“ ___ ” _____ 2026 року