Отримано
22.06.2026
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

РЗАЄВОЇ Світлани Леонідівни, кандидата технічних наук, доцента, доцента кафедри комп'ютерних наук 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 теми дослідження

Сучасні інфокомунікаційні мережі (ІКМ) функціонують в умовах постійного впливу кіберзагроз, які характеризуються постійним зростанням кількості і складності кібератак на ІКМ та деструктивного впливу на процеси управління. У зв'язку з цим забезпечення цілісності, конфіденційності і доступності інформації, що циркулює в ІКМ є одним із ключових завдань системи національної кібербезпеки.

Особливого значення набуває проблема виявлення складних атак типу APT (Advanced Persistent Threat) в умовах кіберконфліктів. Традиційні

рішення захисту вузлів ІКМ можуть пропускати комп'ютерні віруси внаслідок недосконалості механізмів їх виявлення, що особливо критично під час багаторівневих кібератак. А у наявних дослідженнях, виявлення вірусів за допомогою ШІ зазвичай здійснюється шляхом сканування виконуваного файлу, що не завжди можна використати для наявного захисту інфокомунікаційних мереж.

Саме тому, розробка методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей є перспективним напрямом розвитку наукових досліджень. Застосування таких підходів дозволяє виявляти шкідливі впливи там, де їх пропустив традиційний антивірус, що знижує час реагування на інциденти інформаційної безпеки.

Виявлені невирішені питання вказують на те, що тема дисертаційної роботи Чернігівського І.А. є актуальною, своєчасною та має важливе теоретичне і практичне значення для розвитку систем кібербезпеки.

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

Дисертація виконувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики 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).

Також результати 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).

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

Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі, є достатньо обґрунтованими та логічно узгодженими між собою, що підтверджується аналізом значної кількості наукової та технічної літератури, а також використанням методів аналізу і синтезу систем; теорія інформації; теорія прийняття рішень; теорія алгоритмів; теорія ймовірностей; комп'ютерне та імітаційне моделювання.

Достовірність отриманих результатів підтверджується проведенням експериментальних досліджень, аналізом отриманих даних та порівнянням результатів. Всі практичні і теоретичні результати дослідження апробовано на конференціях та опубліковано в наукових статтях. Перелік наукових праць Чернігівського І.А. та довідки щодо впровадження результатів дослідження підтверджують фаховий підхід здобувача до обрання теми роботи та високий рівень наукової компетентності.

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

Представлені в дисертації Чернігівського Івана Андрійовича положення, підходи, структура, постановка завдання та їх вирішення, узагальнені висновки розкривають авторську ідею і самостійно виконану наукову працю, в якій обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

– 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.

Таким чином, мета дослідження щодо синтезу методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, здатного забезпечити підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі досягнута.

5. Теоретична цінність і практична значущість наукових результатів

Наукові положення, висновки та рекомендації дисертаційної роботи Чернігівського Івана Андрійовича мають теоретичну цінність та практичну важливість.

Теоретична цінність дисертаційної роботи полягає у подальшому розвитку наукових засад забезпечення кіберстійкості інфокомунікаційної мережі шляхом вивантаження мінімально необхідної кількості цифрових слідів та їх аналізу нейромережевими моделями. Запропонований підхід дозволяє дозволяє забезпечити економію часу і ресурсів на виявлення комп'ютерних вірусів та протидії їх поширенню в інфокомунікаційній мережі та розширює існуючі наукові підходи до забезпечення кіберстійкості в умовах динамічного розвитку кіберзагроз. Отримані результати створюють теоретичне підґрунтя для подальших досліджень у сфері кібербезпеки, зокрема щодо аналізу поведінки складних кіберзагроз, та розроблення ефективних механізмів реагування на кіберінциденти.

Практичне значення отриманих результатів полягає у можливості використання моделей і методів для підвищення кіберзахисту на підприємстві навіть за наявності інших захисних рішень, за рахунок більш оперативного реагування на виникаючі загрози, а також автоматичного прийняття рішення та здійснення керуючих дій. Запропоновані рішення можуть бути використані працівниками відділу інформаційної безпеки для своєчасного виявлення та реагування на виникаючі кіберінциденти в ІКМ. Отримані результати сприяють підвищенню ефективності функціонування

інформаційних систем організацій та державних структур в умовах сучасних кіберзагроз.

Запропоновані рішення інтегровані в освітній процес Київського столичного університету імені Бориса Грінченка, 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. 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. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях відповідно до мети та поставлених завдань.

Основні положення дисертаційної роботи були апробовані на науково-практичних конференціях, що підтверджує їх наукову та практичну значущість.

7. Відсутність (наявність) порушення академічної доброчесності

Аналіз змісту дисертації, а також публікацій Чернігівського І.А. вказують на відсутність ознак порушення вимог академічної доброчесності. Дисертаційна робота містить посилання на джерела інформації у випадку використання ідей, розробок, тверджень, відомостей, а також відповідає нормам законодавства про авторське право і суміжні права. В дисертації

Чернігівський І.А. надає достовірну інформацію про результати власної наукової діяльності, а також про використані інформаційні ресурси.

8. Дискусійні положення та зауваження до дисертації

Принципових зауважень щодо структури, основних положень та концепції дисертації Чернігівського І.А. не виявлено.

Позитивно оцінюючи результати дисертаційного дослідження, слід звернути увагу на окремі зауваження та рекомендації до окремих положень дисертації.

1. Доцільно було б у дослідженні більш детально приділити увагу тому, скільки системних ресурсів витрачається на вивантаження і аналіз артефактів, а також провести експериментальні дослідження на кількох ПК.
2. Зазначаючи актуальність і сучасність дослідження, варто зауважити, що у автора є фрагменти коду з утилітою wmic, проте зараз актуальна Windows 11 і код на ній може не запуститися.
3. У вступі автором недостатньо детально обґрунтовано актуальність теми, оскільки не наведено аналіз інцидентів інформаційної безпеки за тривалий ретроспективний період (2010–2020 роки), що обмежує можливість оцінювання довгострокових тенденцій розвитку кіберзагроз.

Наведені зауваження мають рекомендаційний характер і не знижують загальної позитивної оцінки 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, яке за актуальністю, науковою новизною, обґрунтованістю

результатів і практичною значущістю 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 комп'ютерних наук
Київського столичного
університету імені Бориса Грінченка Світлана РЗАЄВА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
ЗАСВІДЧУЮ
(ПІБ)
(посада)