ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Чернігівського Івана Андрійовича на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей», поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Актуальність теми 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.

Найпоширенішими загрозами в інфокомунікаційних мережах є поширення комп'ютерних вірусів, оскільки вони можуть одночасно порушувати конфіденційність (Trojan, Spyware) цілісність (Exploit, Ransomware, Wiper) та доступність (Trojan, Ransomware, Wiper) інформації а загальна кількість комп'ютерних вірусів перевищує 1,5 млрд.; фішинг із використанням технології Deepfake, тому що кількість онлайн-діпфейків зросла на 550% з 2019 по 2023 рік; залучення штучного інтелекту (ШІ) для автоматизації кібератак у тому числі і для автоматичного виявлення та експлуатації вразливостей, оскільки це знижує час на підготовку та проведення атак.

Дослідження проблеми забезпечення кібербезпеки інформаційних систем та аналіз ШПЗ і цифрових слідів представлені у працях багатьох вчених, серед яких Яремчук Ю., Hintea D., Rogers M., Jusas V., Василенко М., Ричка Д., Bashir M., D. -Y. Kao, Shevchenko S., Skladannyi P., Davydov V., Abu Taam Ghani Mohamad, A. Smirnov, Терейковський І. А., Mahmoud Kalash та інші.

Проведений аналіз сучасних наукових досліджень показав, що більшість існуючих підходів використовують наявні фреймворки, математичні моделі, методи машинного навчання або звичайні алгоритми пошуку для аналізу стану вузлів ІКМ та визначення загроз. Проведення таких досліджень є результативним, оскільки вони зробили вагомий внесок у розвиток методів захисту інформації. Проте дані підходи зазвичай ґрунтуються на ШІ-аналізі конкретного потенційно шкідливого виконуваного файлу, надають перелік

неоптимальних цифрових слідів для ручного аналізу, не враховують роботу вузлів у розподіленій ІКМ, не надають конкретних практичних рекомендацій щодо вибору ШІ-моделей для автоматичного визначення стану зараженості вузла ІКМ, також наразі не запропоновано визначення стану вузла, коли ШПЗ може самоліквідуватись з вузла і буде відсутній виконуваний файл, не розглядаються можливості автоматично виявити атаку яку пропустило традиційне захисне рішення. Варто зазначити, що традиційні рішення захисту вузлів ІКМ можуть пропускати комп'ютерні віруси внаслідок недосконалості механізмів їх виявлення, що особливо критично під час багаторівневих кібератак.

Викладене обумовлює необхідність створення нових і вдосконалення існуючих методів захисту інформації в інфокомунікаційних мережах в умовах обмежених ресурсів, вдосконалення наявних методів ідентифікації ШПЗ на ПК для підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі. Перспективним шляхом є ефективний розподілу часу та ресурсів аналітика відділу інформаційної безпеки для своєчасного виявлення та запобігання загрозам.

Зв'язок роботи з науковими програмами, планами, темами. 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).

Мета і завдання дослідження. Метою дисертаційної роботи є синтез методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, здатного забезпечити підвищення ефективності протидії поширенню комп'ютерних вірусів в інфокомунікаційній мережі.

Для досягнення поставленої мети вирішено наступні наукові завдання:

- здійснено синтез методу захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів, здатного забезпечити економію часу і ресурсів на виявлення комп'ютерних вірусів та протидії їх поширенню в інфокомунікаційній мережі;

- обґрунтовано доцільність використання цифрових слідів у якості основної ідентифікаційної ознаки для оцінки стану вузлів ІКМ;

- розроблено модель для оптимізації кількості і розміру цифрових слідів, достатніх для ідентифікації стану вузлів ІКМ;

- шляхом тестування здійснено відбір релевантних нейромережевих моделей для аналізу вивантажених цифрових слідів;

- удосконалено метод вивантаження цифрових артефактів в умовах обмеженості ресурсів;

- виконано експериментальну перевірку ефективності запропонованого методу захисту вузлів ІКМ.

Об'єктом дослідження є процеси виявлення та блокування комп'ютерних вірусів у вузлах інфокомунікаційної мережі.

Предметом дослідження є методи і моделі виявлення комп'ютерних вірусів та захисту вузлів інфокомунікаційної мережі.

Методи дослідження. 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.

Наукова новизна одержаних результатів полягає в наступному:

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.

Практичне значення одержаних результатів полягає в тому, що в дослідженні запропоновано моделі та методи, які доцільно використовувати 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. 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.

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).

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені на наукових конференціях:

1. Чернігівський І. А., Захист інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів, Збірник тез XII Всеукраїнської науково-практичної конференції молодих учених 2025, 339ст.
2. Чернігівський І.А., Роль SIEM у побудові комплексного захисту інформаційно-телекомунікаційних систем, II International Scientific and Practical Conference Kharkiv, Ukraine 2024, 21ст.
3. Чернігівський І. А., Виявлення активності шкідливого програмного забезпечення у вузлах інфокомунікаційної мережі на основі нейромережевих моделей, XIII Всеукраїнська науково-технічна конференція з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті 2025« https://nuos.edu.ua/wp-content/uploads/2025/12/SPIBT-2025-Materiali.pdf
4. L. Kriuchkova, I. Tsmokanych, N. Mazur, I. Chernihivskyi, Spectral Characteristics of Intermodulation Emissions during High-Frequency Imposition, Cybersecurity Providing in Information and Telecommunication Systems, 2025, 449-462 ст. https://ceur-ws.org/Vol-3991/
5. I. Chernihivskyi, L. Kriuchkova, A method of generating data for further training artificial intelligence models aimed at solving cybersecurity problems, Cybersecurity Providing in Information and Telecommunication Systems, 2025, 246-256ст, https://ceur-ws.org/Vol-4145/

Публікації. Основні результати дисертації висвітлено у 12 наукових публікаціях, із них: 7 статей (усі у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 5 публікацій (з них 2 у співавторстві) публікації, у яких додатково висвітлено наукові результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Чернігівський І., Крючкова Л. (2025). Тестова послідовність виявлення та ізоляції заражених вузлів інфокомунікаційної мережі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 3(31), 652–662. https://doi.org/10.28925/2663-4023.2025.31.1070

2. Чернігівський І., Крючкова Л. (2025). Інформаційні впливи на інфокомунікаційні мережі із залученням штучного інтелекту. *Телекомунікаційні та інформаційні технології*, 3(88), 167-176. https://doi.org/10.31673/2412-4338.2025.038719

3. Чернігівський І., Крючкова Л. (2025). Тестування нейромережевих моделей для вирішення задачі виявлення заражених ПК на базі цифрових слідів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(29), 800–817. https://doi.org/10.28925/2663-4023.2025.29.941

4. Чернігівський І., Крючкова Л. (2025). Ефективні рішення для швидкого виявлення скомпрометованих ПК в інфокомунікаційних мережах. *Телекомунікаційні та інформаційні технології*, 2(87), 24–32. https://doi.org/10.31673/2412-4338.2025.029875

5. Чернігівський І., Крючкова Л. (2025). Системний підхід до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 572–590. https://doi.org/10.28925/2663-4023.2025.27.781

6. Чернігівський І., Крючкова Л. (2024). Тестування антивірусних рішень для корпоративного сегменту. *Безпека інформації*, 30(3), 407–413. https://doi.org/10.18372/2225-5036.30.20362

7. Чернігівський І., Богданов О., (2024). Типи цифрових криміналістичних артефактів в комп'ютерах під управлінням ос windows. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(24), 221–228. https://doi.org/10.28925/2663-4023.2024.24.221228

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Чернігівський І. А., Захист інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів, Збірник тез XII Всеукраїнської науково-практичної конференції молодих учених 2025, 339ст URL: https://zcit.kubg.edu.ua/index.php/journal/issue/view/13/23

2. Чернігівський І.А., Роль SIEM у побудові комплексного захисту інформаційно-телекомунікаційних систем, II International Scientific and Practical Conference Kharkiv, Ukraine 2024, 21 ст

3. Чернігівський І. А., Виявлення активності шкідливого програмного забезпечення у вузлах інфокомунікаційної мережі на основі нейромережевих моделей, XIII Всеукраїнська науково-технічна конференція з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті« 2025, 45ст URL: https://nuos.edu.ua/wp-content/uploads/2025/12/SPIBT-2025-Materiali.pdf

4. L. Kriuchkova, I. Tsmokanych, N. Mazur, I. Chernihivskyi, Spectral Characteristics of Intermodulation Emissions during High-Frequency Imposition, *Cybersecurity Providing in Information and Telecommunication Systems,* 2025, 449-462 ст. URL: https://ceur-ws.org/Vol-3991/paper32.pdf

5. I. Chernihivskyi, L. Kriuchkova, A method of generating data for further training artificial intelligence models aimed at solving cybersecurity problems, *Cybersecurity Providing in Information and Telecommunication Systems,* 2025, 246-256 ст, URL: https://ceur-ws.org/Vol-4145/paper16.pdf

Особистий внесок здобувача.

Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачем особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача. Безпосередньо автором розроблено метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей, запропоновано і реалізовано використання цифрових слідів у якості основної ідентифікаційної ознаки при оцінці зараженості вузлів ІКМ, запропоновано і реалізовано реляційну модель у вигляді таблиці артефактів, запропоновано і реалізовано застосування нейромережевих моделей для аналізу вивантажених цифрових слідів, вдосконалено метод вивантаження цифрових артефактів в умовах обмеженості ресурсів. Отримані результати можуть бути використані для зниження часу реагування на виникаючі інциденти в інфокомунікаційній мережі в умовах сучасних кіберзагроз.

У статті «Тестова послідовність виявлення та ізоляції заражених вузлів інфокомунікаційної мережі» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у створенні тестової послідовності, яка дозволяє виявляти заражені вірусами вузли ІКМ в циклі управління системи захисту та мінімізувати середній час на оцінку одного вузла, що загалом складає 80% тексту статті.

У статті «Інформаційні впливи на інфокомунікаційні мережі із залученням штучного інтелекту» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у визначенні найбільш небезпечних загроз та сценаріїв шкідливих інформаційних впливів із залученням ШІ, що загалом складає 70% тексту статті.

У статті «Тестування нейромережевих моделей для вирішення задачі виявлення заражених ПК на базі цифрових слідів» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у тому, що визначено критерії для моделі ШІ які будуть прийнятними для використання у корпоративному середовищі та проведено тестування 135 моделей формату GGUF на предмет виявлення або невиявлення ними ознак вірусної активності та індикаторів компрометації у промпті, що надавався користувачем, визначено перелік доцільних для використання моделей ШІ у форматі GGUF

для вирішення задач кібербезпеки, зокрема для виявлення заражених ПК на базі цифрових слідів, що загалом складає 80% тексту статті.

У статті «Ефективні рішення для швидкого виявлення скомпрометованих ПК в інфокомунікаційних мережах» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у тому, що визначено компонент/тактику, без яких сучасні комп'ютерні віруси зазвичай не працюють, запропоновано перелік програм для швидкого виявлення вірусів і скрипт оптимізації з використанням реляційної таблиці артефактів, які дозволяють скоротити кількість елементів, необхідних для подальших досліджень більш ніж у десять разів, що загалом складає 80% тексту статті.

У статті «Системний підхід до вирішення задачі захисту інформації в інфокомунікаційні мережі від впливу комп'ютерних вірусів» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у пропозиції будувати системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану ІКМ, створенні словника ознак для ідентифікації стану ІКМ на основі цифрових слідів, який є достатнім для прийняття рішень в циклах управління системи захисту інформації, що загалом складає 70% тексту статті.

У статті «Тестування антивірусних рішень для корпоративного сегменту» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у пропозиції набору тестів і програм які є достатніми для оцінки ефективності захисного рішення у корпоративному середовищі, визначено, що аналіз реакцій АВ на кілька ШПЗ з сімейства Ransomware цілком достатньо для отримання базового уявлення про евристичний модуль АВ та його можливість протидіяти новим загрозам, визначено критерії, за якими очікується спрацювання АВ на ШПЗ сімейства Ransomware, а також запропоновано скрипт, що імітує поведінку відомих Ransomware для тестування евристичного модулю АВ, що загалом складає 75% тексту статті.

У статті «Типи цифрових криміналістичних артефактів в комп'ютерах під управлінням ОС Windows» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у визначенні типів артефактів в ОС Windows та у визначенні, що для деяких задач буде достатньо лише невеликої кількості артефактів, які можна швидко зібрати для аналізу, що загалом складає 90% тексту статті.

У статті «Spectral Characteristics of Intermodulation Emissions during High-Frequency Imposition» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у пропозиції розглядати проблему захисту конфіденційної інформації від перехоплення методом високочастотного нав'язування із системних позицій, як проблему забезпечення електромагнітної сумісності технічних систем передачі, обробки та зберігання інформації, що загалом складає 10% тексту статті.

У статті «A method of generating data for further training artificial intelligence models aimed at solving cybersecurity problems» опублікованій у співавторстві, внесок Чернігівського І.А. полягає у пропонуванні методу формування навчальних даних для донавчання моделей ШІ, що забезпечує:

спеціалізацію конкретної моделі ШІ на виявлення основних ознак вірусної активності в наданих цифрових слідах; підвищення якості відповідей ШІ; зниження часу реагування на інциденти кібербезпеки. Пропозицію оформлення цифрових слідів для донавчання моделей ШІ у табличному вигляді з попередньою фільтрацією цифрових слідів на основі реляційної таблиці артефактів, що дозволяє скоротити кількість елементів, необхідних для подальших досліджень, що загалом складає 80% тексту статті.

Структура та обсяг дисертації. 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.

Оцінка мови та стилю дисертації. Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний і послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчесності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації.

На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії.

Дисертація Чернігівського Івана Андрійовича, на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях і міжнародних виданнях, що входять до наукометричних баз Scopus та Web of Science Core Collection та оприлюднювались на міжнародних науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Чернігівського Івана Андрійовича, на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає пп. 6–9 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 12.01.2022 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Чернігівського Івана Андрійовича та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3. Чернігівський Іван Андрійович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Чернігівського Івана Андрійовича, на тему «Метод захисту вузлів інфокомунікаційної мережі від комп'ютерних вірусів на основі нейромережевих моделей», до публічного захисту у разовій спеціалізованій вченій раді для присудження Чернігівському І.А. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Голова –
кандидат технічних наук, доцент
доцент кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Складанного П. ЗАСВІДЧУЮ
(ПІБ)
Нач. відд. каф. В.К.
(посада)