КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1070
УДК 004.056.57

Чернігівський Іван Андрійович
аспірант
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0009-0003-4568-3212
i.chernihivskiy@gmail.com

Крючкова Лариса Петрівна
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

ТЕСТОВА ПОСЛІДОВНІСТЬ ВИЯВЛЕННЯ ТА ІЗОЛЯЦІЇ ЗАРАЖЕНИХ ВУЗЛІВ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Анотація. Сучасна інфокомунікаційна мережа (ІКМ) є розподіленою системою, базові елементи якої об'єднані в єдиний інформаційний простір. ІКМ часто зазнають різноманітних атак шкідливого програмного забезпечення (ШПЗ), саме тому вирішальним фактором, що впливає на ефективність функціонування інфокомунікаційної мережі, є ступінь захищеності вузлів ІКМ від впливу ШПЗ. Оскільки існуючі засоби захисту не завжди вчасно справляються з виявленням ознак зараження технічних засобів мережі, питання розробки і впровадження нових методів, моделей, алгоритмів та систем захисту інформації від зловмисного програмного забезпечення, яке не базується на виявленні сигнатур ШПЗ, є актуальним. Особливо важливим у зазначеному переліку є завдання своєчасного виявлення та ізоляції заражених вузлів інфокомунікаційної мережі. Метою статті є формування тестової послідовності для виявлення та ізоляції заражених вузлів інфокомунікаційної мережі. Для встановлення факту «зараженості» конкретного вузла ІКМ необхідно вилучити з нього інформаційні сліди та провести їх детальний аналіз, оскільки при цьому коректність відповіді визначення стану «заражено\не заражено» буде більше 50%. Побудова системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану ІКМ, дозволяє забезпечити необхідний рівень захищеності інформації. Запропонована тестова послідовність дозволяє виявляти заражені вірусами вузли ІКМ в циклі управління системи захисту та дозволяє оптимізувати час на оцінку одного вузла. Одночасне впровадження оптимізаційних рішень для кожного з етапів дозволить мінімізувати середній час на проходження тестової послідовності, що позитивно впливає на мінімізацію загальну часу на виявлення та ізоляцію заражених вузлів інфокомунікаційної мережі в циклі управління. Мінімізація середнього часу забезпечується: використанням лише мінімально необхідних цифрових слідів; використанням моделі ШІ у якості одного з компонентів модулю прийняття рішень та заздалегідь налаштованих правил оцінки цифрових слідів; застосуванням заздалегідь налаштованих правил для автоматичного здійснення керуючих дій щодо ізоляції зараженого вузла; розпаралеленням обчислень.

Ключові слова: кібербезпека; ІКМ; віруси; захист; ідентифікаційні ознаки; модель ШІ; захисні рішення.

ВСТУП

У сучасному світі успіх будь-якого підприємства вирішальною мірою визначається ефективністю його інформаційної інфраструктури. Сучасна інфокомунікаційна мережа (ІКМ) є розподіленою системою, базові елементи якої об'єднані в єдиний інформаційний

простір. Як показали дослідження [1], [2], існуючі ІКМ часто зазнають різноманітних атак шкідливого програмного забезпечення (ШПЗ). Особливим небезпекам наражаються ІКМ, що використовуються для контролю та управління технологічними процесами в системах критичної інфраструктури. Саме тому вирішальним фактором, що впливає на ефективність функціонування інфокомунікаційної мережі, є ступінь захищеності вузлів ІКМ (користувацьких комп'ютерів, ПК) від впливу ШПЗ.

Дослідження систем атак та захисту інформації згідно статистики [2], [3], [4] показали високий ступінь їхньої взаємозалежності, при цьому рівень технічного та програмного забезпечення зловмисників у більшості практичних випадків вищий. А також активне залучення ШІ до атак на інформаційні системи робить ці атаки простішими і дешевшими у застосуванні [5], [6]. У зв'язку з цим існуючі засоби захисту не завжди вчасно справляються з виявленням ознак зараження технічних засобів мережі, тому питання розробки і впровадження нових методів, моделей, алгоритмів та систем захисту інформації від зловмисного програмного забезпечення залишається актуальним і є спроби залучати ШІ до виконання задач кібербезпеки [7]. Особливо важливим у зазначеному переліку є завдання своєчасного виявлення та ізоляції заражених вузлів інфокомунікаційної мережі.

Аналіз досліджень і публікацій.

В роботі [8] виконано аналіз математичних моделей комп'ютерних вірусів і визначено, що моделі: *SI* (Suspected-Infected), *SIR*(Suspected-Infected- Recovered), *PSIDR* (Progressive Suspected-Infected-Detected-Recovered) найбільш точно описують процес поширення комп'ютерних вірусів в мережі.

В роботі [9] проведено порівняльні дослідження математичних моделей технології поширення комп'ютерних вірусів в інформаційно-телекомунікаційних мережах.

В роботі [10] удосконалено математичні моделі розповсюдження комп'ютерних вірусів в гетерогенній комп'ютерній мережі, що враховує її топологічні та архітектурні особливості і проведено порівняльні дослідження розроблених математичних моделей та побудовані порівняльні графіки залежності кількості заражених вузлів від часу функціонування комп'ютерної мережі при розповсюдженні епідемії.

В роботі [11] представлено аналіз нейромережевих моделей та методів розпізнавання комп'ютерних вірусів та процес створення такої нейромережевої моделі, яка може розпізнавати поліморфні віруси.

Аналіз розглянутих робіт показав, що їх метою є виявлення конкретних сімейств вірусів та моделювання процесу поширення комп'ютерних вірусів в ІКМ. Проте, досліджень потребує виявлення саме того, що «пропустили» наявні захисні рішення, виявлення конкретних заражених вузлів ІКМ та їх ізоляцію без наявності будь-якої інформації від захисних рішень.

Метою статті є формування тестової послідовності для виявлення та ізоляції заражених вузлів інфокомунікаційної мережі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

ІКМ можна класифікувати як складну динамічну багатопараметричну слабодетерміновану систему з розподіленими параметрами, в якій можуть виникати несподівані емерджентні властивості в результаті впливу комп'ютерних вірусів. Для досягнення необхідного рівня захищеності інформації має бути забезпечена здатність передбачати та запобігати появі цих властивостей на об'єкті захисту.

Для визначення того, чи конкретний вузол ІКМ має стан «заражено», необхідно вилучити з такого вузла інформаційні сліди та провести їх детальний аналіз, оскільки при цьому коректність відповіді визначення стану «заражено\не заражено» буде більше 50%.

Визначення тестової послідовності за допомогою інформації апріорі.

Необхідний рівень захищеності інформації забезпечується побудовою системи захисту у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану ІКМ. [1]. Інформаційна структура циклу управління захистом інформації в ІКМ представлена на рис. 1.

Рис.1. Інформаційна структура циклу управління захистом інформації в ІКМ.

Діагностика ІКМ становиться послідовною, як тільки ми вводимо фактор часу у вигляді порядку тестування, послідовність модулів, які необхідно пройти в певному порядку циклу управління – становляться тестовою послідовністю. Ціллю є діагностика того, чи є конкретний вузол ІКМ незараженим, і якщо це не підтверджується – ізолюємо такий вузол. Оскільки кожний наступний модуль використовує результати роботи попереднього модуля, їх взаємодію можна привести до вигляду графу або деревоподібної тестової схеми. Основними кроками побудови такої схеми є:

- визначити послідовність, яка б мінімізувала середню тривалість проходження тестової послідовності для пошуку зараженого вузла ІКМ та його ізоляції;
- на кожному етапі вибирати із послідовності модулі у відповідності до їх ролі в оцінці вузла та здійсненні керуючих дій.

На етапі виявлення наявності вірусних слідів можна вважати, що вузли ІКМ є статистично незалежними.

Метод захисту вузлів ІКМ на основі нейромережевих моделей в циклі управління представлено на рис. 2.

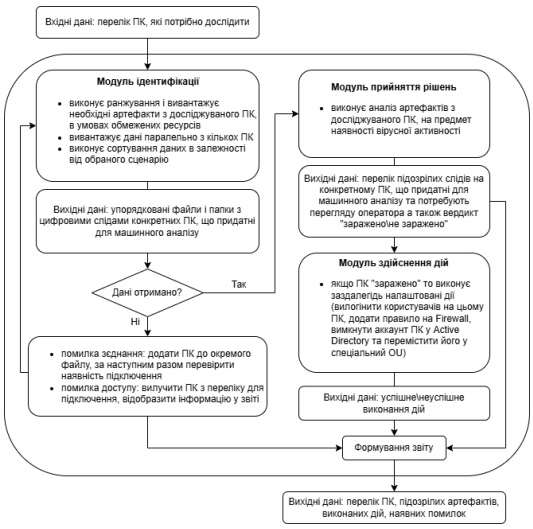

Рис. 2. Метод захисту вузлів ІКМ на основі нейромережевих моделей в циклі управління.

Згідно з циклом управління (рис. 1, 2) пропонується використовувати наступну тестову послідовність:

1. Вивантажити перелік ПК в ІКМ, які потрібно дослідити.
2. Визначити повну назву ПК (FQDN), якщо ПК більше не залишилось то завершити цикл.
3. Перевірити чи ПК онлайн (будемо вважати, що Forward\Reverse DNS, Firewall на ПК, мережеві доступи налаштовано правильно), якщо оффлайн – додати в окремий список і з інтервалом раз на 5хв перевіряти чи не з'явилась можливість підключитися. Якщо усі інші ПК перевірені то додати до окремого файлу із кодом помилки для майбутнього звіту і вилучити з поточного дослідження.
4. Перевірити чи є доступ на ПК, якщо відсутній то або виконати заздалегідь налаштовані дії (наприклад, спробувати використати інший обліковий запис для підключення) або додати до окремого файлу із кодом помилки для майбутнього звіту і вилучити з поточного дослідження.
5. Завантажити на ПК програми для проведення Forensic Triage і запустити їх з необхідними параметрами.
6. Вивантажити результати роботи програм для проведення Forensic Triage на окремий сервер, від найбільш релевантних до найменш.
7. Пересвідчитись, що на окремий сервер в локальній мережі відправлено всі результати програм.
8. Видалити програми, що було завантажено і їх результати з ПК.
9. На сервері, привести наявні цифрові сліди (результати роботи програм), що придатні для машинного аналізу у зрозумілий для ШІ вигляд.
10. Запустити локальну ШІ модель з необхідними параметрами і дочекатись виконання запиту.
11. Відфільтрувати нерелевантні дані, перевірити чи є остаточний вердикт від ШІ на предмет вірусного зараження.
12. Якщо зараження немає – додати інформацію про ПК до звіту, перейти до пункту 2.
13. Якщо зараження є – виконати заздалегідь налаштовані правила (вилогінити користувача, вимкнути акаунт ПК, тощо) додати інформацію про ПК та виявлені сліди до звіту, перейти до пункту 2.

Особливістю запропонованого методу тестування є те що кожний наступний крок тестової послідовності залежить від результату тестування попереднього, тобто встановлення чи взагалі передається інформація між модулями і яка саме, чи достатньо її для прийняття рішень і чи не виникло помилок. Варто зазначити, що тестування виконується для кожного наявного ПК в ІКМ.

При цьому:

- якщо система передає дані і не є зараженою – ніяких дій не виконується;
- якщо система не може передати дані або є зараженою –виконуються керуючі дії, направлені або на отримання інформації з ПК або ізоляції такого ПК від іншого сегменту мережі.

Маємо три стани системи:

1. Нічого апріорі невідомо про систему – в такому випадку необхідно систематично перевіряти ПК на можливість підключення до тих пір, доки система не почне віддавати дані або коли перевірка стане недоцільною.

2. Система онлайн, але не може віддати дані – в такому випадку доведеться розбиратись з конкретними причинами несправностей або виконувати заздалегідь налаштовані дії, для можливого усунення несправностей.

3. Відомо, що система може знаходитись лише в одному з N взаємовиключних станах, для кожного з таких станів будуть протестовані наявні дані до тих пір, поки не буде однозначно ідентифіковано стан системи «заражено \ не заражено».

Вказані три стани одночасно потребують все більше і більше інформації апріорі і все більше ресурсів під час виконання тестової послідовності, в результаті, система стає все більш складнішою.

Мінімізація середнього часу проходження тестової послідовності

Оскільки в розподіленій ІКМ активних вузлів може бути більше 100 та навіть більше 1000 важливого значення набуває час за який повністю буде перевірена ІКМ на наявність вірусної активності, додаткові проблеми розподіленої ІКМ описані в [1]. Таким чином, якщо навіть незначно зменшиться час на аналіз одного вузла – це матиме вплив на загальний час аналізу, тож треба проводити оптимізацію на всіх рівнях тестової послідовності, для кожного модулю.

Для оптимізації наявних рішень *на етапі ідентифікації стану ІКМ* (в основному це вивантаження цифрових артефактів та їх завантаження на сервер), доцільно розглянути кілька можливих шляхів [12]:

1. Зменшення кількості ПК, які потрібно дослідити.
2. Зменшення кількості цифрових слідів, які потрібно дослідити.
3. Автоматизувати процес за допомогою скриптів\програм.
4. Вважати зараженим тільки той ПК на якому спрацював АВ.
5. Вважати всі ПК зараженими, і перевстановити на всіх операційну систему без збереження профілів користувачів.

При цьому, кожний з цих методів має свої недоліки [12]:

1. При зменшенні кількості ПК ми не можемо точно сказати чи всі інші ПК не заражені.
2. При зменшенні кількості цифрових слідів, особливо якщо вірус затирає свої сліди або видаляється сам, ми не побачимо всі компоненти вірусу та сліди вірусної атаки на ПК, що дасть нам хибне уявлення про те, що ПК не був заражений.
3. Автоматизація завжди дає свій відсоток false-positive та false-negative, та при детальному аналізі цих подій і коригуванні правил для автоматичного розбору – витратиться стільки ж часу як при звичайному аналізі.
4. АВ зазвичай видалить тільки той компонент вірусу який знає сигнатурно або знайшов евристикою, та ніяк не зачепить інші «невидимі» (fully undetectable - FUD) частини.
5. Іноді переустановлення операційної системи є надмірним та неефективним рішенням, особливо якщо це будуть робити локальні адміністратори.

Згідно з даними MITRE ATT&CK Matrix визначено, що 252 відомих ШПЗ запускаються за допомогою техніки T1547 Registry Run Keys / Startup Folder, 184 відомих ШПЗ запускаються за допомогою техніки T1053 Scheduled Task, а інші техніки для автозапуску менш поширені [13], [14].

В роботі [12] визначено, що не має значення, який тип вірусу сховався на конкретному ПК та які механізми приховування від користувача вони реалізовують, якщо кожному з них важлива можливість отримати керування при перезапуску ПК. Це означає, що можна відкинути всі інші цифрові сліди та методи протидії вірусам, що «ховаються» та просто визначити перелік програм з автозавантаження. Зважаючи на

перелік поширених шляхів автозапуску у вірусів [15], використання відомих програм для автоматичного збору цифрових слідів, таких як Autoruns [16], [17], і використання інформації з таблиці мінімально необхідних артефактів (з наявністю таких цифрових слідів, де з ймовірністю 100% можна визначити вірусну активність), реляційної таблиці артефактів і врахування характеристик програм, якими можна знехтувати (відфільтрувавши певні дані), як представлено у роботі [12], дозволить значно знизити кількість помилок і зекономити час. При такій «грубій» оптимізації, де відкидається значна частина артефактів Windows і беруться не всі дані автозапуску, можна пропустити певну кількість вірусів, але при великій кількості досліджуваних ПК, зменшення часу, необхідного аналітику для аналізу кожного ПК стає більш пріоритетним. На думку авторів, достовірність визначення вірусної активності за розробленим алгоритмом становить від 60% до 100%. Крім того, 100% надійність виникає, якщо є будь-які записи у антивірусних виключеннях Windows Defender.

Для оптимізації наявних кроків *на етапі прийняття рішень* (в основному це оцінка того, чи знаходиться конкретний вузол ІКМ у стані незараженості), доцільно розглянути використання заздалегідь налаштованих правил і застосування моделей ШІ для аналізу цифрових слідів, оскільки людські ресурси дорожче коштують і збільшують час на виявлення (проте результати є більш точними).

Можливі ситуації, коли з наявних слідів статистичними методами зі 100% надійністю можна визначити вірусну активність, в такому випадку доцільно використовувати в автоматичному режимі прості правила (наприклад, шукати наявність записів у Windows Defender) перед відправленням цифрових слідів на обробку моделлю ШІ, оскільки тоді необхідність в обробці ШІ моделлю відпадає, що в свою чергу економить ресурси.

У роботі [18] проведено тестування 135 загальнодоступних нейромережевих моделей формату GGUF на предмет виявлення або невиявлення ними ознак вірусної активності та індикаторів компрометації і визначено як мінімум 43шт. доцільних для використання моделей ШІ, оскільки ці моделі формату GGUF менше ніж за 10хв. вірно визначили наявність вірусної активності на основі цифрових слідів з ПК, що були оформлені у вигляді промпту (див. рис. 3, 4).

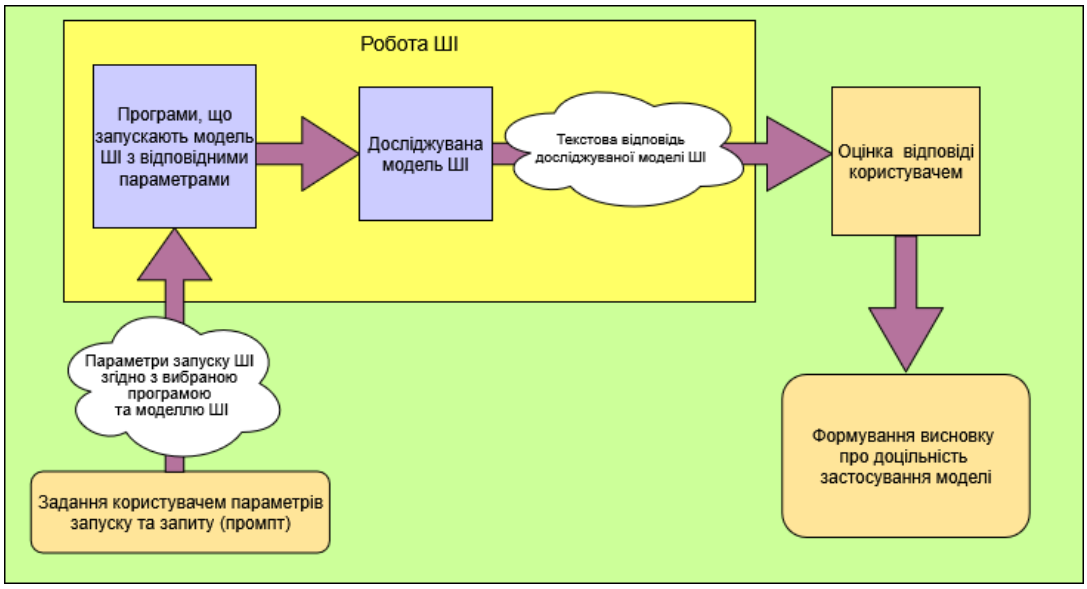

Рис. 3. Схема дослідження нейромережевих моделей

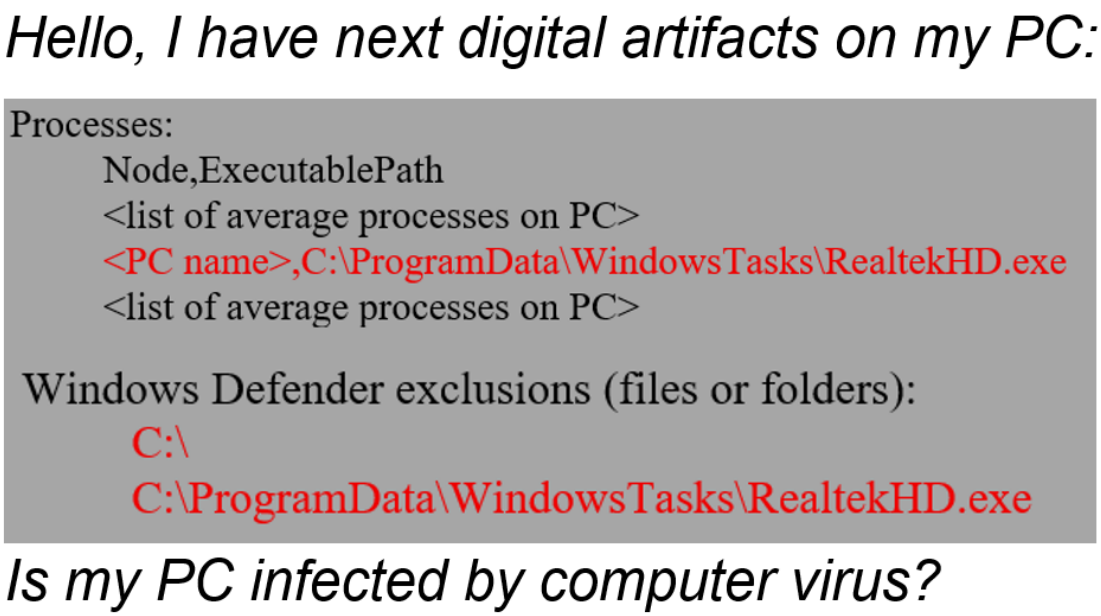

Рис. 4. Приклад структури промпту

Отже, вони можуть бути застосовані для вирішення задач виявлення заражених ПК на базі цифрових слідів в якості одного із компонентів кіберзахисту для зниження часу реагування на події інформаційної безпеки. Враховуючи, що кожна модель краще проявляє себе у специфічних умовах із різними сценаріями запуску, вибір моделі буде залежати від актуальних задач та наявних ресурсів. При цьому, якість відповідей ШІ класифікується наступним чином:

- ПК заражено і нейромережева модель це виявила,
- ПК заражено і нейромережева модель це не виявила,
- ПК не заражено і нейромережева модель це виявила,
- ПК не заражено і нейромережева модель це не виявила,
- ПК заражено і модель не змогла розпізнати стан,
- ПК не заражено і модель не змогла розпізнати стан.

Для оптимізації наявних кроків *на етапі здійснення керуючих дій* (в основному це вибір дій в залежності від того, чи знаходиться конкретний вузол ІКМ у стані незараженості та формування звіту), доцільно розглянути використання автоматизованих скриптів які виконують заздалегідь налаштовані правила та автоматично формують звіт (наприклад, примусово скинути пароль усім користувачам зараженого комп'ютера), оскільки це знизить час реагування на події інформаційної безпеки порівняно з ручним аналізом та діями.

Додатково, на кожному етапі доступно розпаралелення обчислень (рекомендується досліджувати ПК блоками з 5-10 ПК), що не прискорює отримання інформації про стан окремого ПК, але знижує чергу з ПК і оптимізує загальне очікування на обчислення, що позитивно впливає на загальну економію часу.

Отже, якщо одночасно впроваджувати ці оптимізаційні рішення для кожного з етапів, це дозволить мінімізувати середній час на проходження тестової послідовності, що позитивно впливає на мінімізацію загальну часу на дослідження ІКМ на предмет виявлення заражених вузлів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Побудова системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану ІКМ, дозволяє забезпечити необхідний рівень захищеності інформації.

Запропонована тестова послідовність дозволяє виявляти заражені вірусами вузли ІКМ в циклі управління системи захисту та дозволяє оптимізувати час на оцінку одного вузла.

Одночасне впровадження оптимізаційних рішень для кожного з етапів дозволить мінімізувати середній час на проходження тестової послідовності, що позитивно впливає на мінімізацію загальну часу на виявлення та ізоляції заражених вузлів інфокомунікаційної мережі в циклі управління.

Мінімізація середнього часу забезпечується:

- використанням лише мінімально необхідних цифрових слідів;
- використанням моделі ШІ у якості одного з компонентів модулю прийняття рішень та заздалегідь налаштованих правил оцінки цифрових слідів;
- застосуванням заздалегідь налаштованих правил для автоматичного здійснення керуючих дій щодо ізоляції зараженого вузла;
- розпаралеленням обчислень.

Подальші дослідження можуть бути зосереджені на вдосконаленні автоматизації аналізу відповіді ШІ та оптимізації модулів для постійного моніторингу ІКМ в автоматичному режимі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). A system approach to solving the problem of protecting information in an infocommunication network from the influence of computer viruses. *Cybersecurity: Education, Science, Technique*, 572–590. https://doi.org/10.28925/2663-4023.2025.27.781
2. Department for Science, Innovation and Technology. (2025). *Cyber security breaches survey 2025*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
3. CyberArrow. (2025). *Malware statistics: You need to know in 2025*. https://www.cyberarrow.io/blog/malware-statistics-you-need-to-know/
4. World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
5. Rando, J., Perez-Cruz, F., & Hitaj, B. (2023). *PassGPT: Password modeling and (guided) generation with large language models*. arXiv. https://doi.org/10.48550/arXiv.2306.01545
6. Coppolino, L., et al. (2025). The good, the bad, and the algorithm: The impact of generative AI on cybersecurity. *Neurocomputing*, *623*, Article 129406. https://doi.org/10.1016/j.neucom.2025.129406
7. Xu, H., et al. (2024). *Large language models for cyber security: A systematic literature review*. arXiv. https://doi.org/10.48550/arXiv.2405.04760
8. Davydov, V. V. (2012). Comparative analysis of computer virus distribution models in automated technological process control systems. *Information Processing Systems*, 3(101), 147–151.
9. Abu Taam Ghani Mohamad, A. A., Smirnov, A. A., Kovalenko, A. V., & Smirnov, S. A. (2014). Comparative studies of mathematical models of computer virus propagation technology in information and telecommunication networks. *Information Processing Systems*, (9), 105–110.
10. Semenov, S., & Davydov, V. (2012). Mathematical model of the spread of computer viruses in heterogeneous computer networks of automated technological process control systems. *Bulletin of NTU "KPI". Series: Informatics and Modeling*, 32, 163–171.
11. Tereykovsky, I. A., Korchenko, O. G., & Pogorelov, V. V. (2022). *Methods of recognizing cyberattacks: Recognizing computer viruses* (Textbook). Igor Sikorsky Kyiv Polytechnic Institute.

12. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). Effective solutions for rapid detection of compromised PCs in infocommunication networks. *Telecommunications and Information Technologies, 87*(2). https://doi.org/10.31673/2412-4338.2025.029875
13. MITRE ATT&CK®. (n.d.). *Boot or logon autostart execution: Registry run keys / startup folder (Sub-technique T1547.001)*. https://attack.mitre.org/techniques/T1547/001/
14. MITRE ATT&CK®. (n.d.). *Scheduled task/job: Scheduled task (Sub-technique T1053.005)*. https://attack.mitre.org/techniques/T1053/005
15. Daulaguphu, S. (n.d.). *Critical malware persistence mechanisms you must know*. Tech Zealots. https://tech-zealots.com/malware-analysis/malware-persistence-mechanisms/
16. Bencherchali, N. (n.d.). *Hunting malware with Windows Sysinternals – Autoruns*. Medium. https://nasbench.medium.com/hunting-malware-with-windows-sysinternals-autoruns-19cbfe4103c2
17. Microsoft. (n.d.). *Autoruns – Sysinternals*. Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
18. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). Testing neural network models to solve the problem of detecting infected PCs based on digital traces. *Cybersecurity: Education, Science, Technique, 1*(29), 800–817. https://doi.org/10.28925/2663-4023.2025.29.941

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Chernihivskyi Ivan
graduate student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0003-4568-3212
i.chernihivskiy@gmail.com

Kriuchkova Larysa
Doctor of technical sciences, professor
Professor of the Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

TEST SEQUENCE FOR DETECTION AND ISOLATION OF INFECTED NODES OF THE INFOCOMMUNICATION NETWORK

Abstract. A modern infocommunication network (ICN) is a distributed system, the basic elements of which are combined into a single information space. ICNs are often subjected to various attacks by malicious software (MSW), which is why the decisive factor affecting the effectiveness of the functioning of the infocommunication network is the degree of protection of ICN nodes from the influence of MSW. Since existing protection tools do not always cope with the detection of signs of infection of network hardware in a timely manner, the issue of developing and implementing new methods, models, algorithms and systems for protecting information from malicious software that is not based on the detection of MSW signatures is relevant. Of particular importance in this list is the task of timely detection and localization of infected nodes of the infocommunication network. The purpose of the article is to form a test sequence for the detection and localization of infected nodes of the infocommunication network. To establish the fact of "infection" of a specific ICN node, it is necessary to remove information traces from it and conduct their detailed analysis, since in this case the correctness of the response to determine the "infected\not infected" state will be more than 50%. Building an information protection system in the form of an automated control system aimed at ensuring support for the target ICN state allows to ensure the required level of information security. The proposed test sequence allows to detect ICN nodes infected with viruses in the control cycle of the protection system and allows to optimize the time for evaluating one node. Simultaneous implementation of optimization solutions for each of the stages will allow to minimize the average time for passing the test sequence, which has a positive effect on minimizing the total time for detecting and localizing infected nodes of the infocommunication network in the control cycle. Minimizing the average time is ensured by: using only the minimum necessary digital traces; using an AI model as one of the components of the decision-making module and pre-configured rules for evaluating digital traces; using pre-configured rules to automatically take control actions to locate an infected node; parallelizing calculations.

Keywords: cybersecurity; infocommunication network; viruses; protection; identification features; AI model; protective solutions.

REFERENCES

1. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). A system approach to solving the problem of protecting information in an infocommunication network from the influence of computer viruses. *Cybersecurity: Education, Science, Technique*, 572–590. https://doi.org/10.28925/2663-4023.2025.27.781
2. Department for Science, Innovation and Technology. (2025). *Cyber security breaches survey 2025*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
3. CyberArrow. (2025). *Malware statistics: You need to know in 2025*. https://www.cyberarrow.io/blog/malware-statistics-you-need-to-know/

4. World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
5. Rando, J., Perez-Cruz, F., & Hitaj, B. (2023). *PassGPT: Password modeling and (guided) generation with large language models*. arXiv. https://doi.org/10.48550/arXiv.2306.01545
6. Coppolino, L., et al. (2025). The good, the bad, and the algorithm: The impact of generative AI on cybersecurity. *Neurocomputing, 623*, Article 129406. https://doi.org/10.1016/j.neucom.2025.129406
7. Xu, H., et al. (2024). *Large language models for cyber security: A systematic literature review*. arXiv. https://doi.org/10.48550/arXiv.2405.04760
8. Davydov, V. V. (2012). Comparative analysis of computer virus distribution models in automated technological process control systems. *Information Processing Systems*, 3(101), 147–151.
9. Abu Taam Ghani Mohamad, A. A., Smirnov, A. A., Kovalenko, A. V., & Smirnov, S. A. (2014). Comparative studies of mathematical models of computer virus propagation technology in information and telecommunication networks. *Information Processing Systems*, (9), 105–110.
10. Semenov, S., & Davydov, V. (2012). Mathematical model of the spread of computer viruses in heterogeneous computer networks of automated technological process control systems. *Bulletin of NTU "KPI". Series: Informatics and Modeling*, 32, 163–171.
11. Tereykovsky, I. A., Korchenko, O. G., & Pogorelov, V. V. (2022). *Methods of recognizing cyberattacks: Recognizing computer viruses* (Textbook). Igor Sikorsky Kyiv Polytechnic Institute.
12. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). Effective solutions for rapid detection of compromised PCs in infocommunication networks. *Telecommunications and Information Technologies, 87*(2). https://doi.org/10.31673/2412-4338.2025.029875
13. MITRE ATT&CK®. (n.d.). *Boot or logon autostart execution: Registry run keys / startup folder (Sub-technique T1547.001)*. https://attack.mitre.org/techniques/T1547/001/
14. MITRE ATT&CK®. (n.d.). *Scheduled task/job: Scheduled task (Sub-technique T1053.005)*. https://attack.mitre.org/techniques/T1053/005
15. Daulaguphu, S. (n.d.). *Critical malware persistence mechanisms you must know*. Tech Zealots. https://tech-zealots.com/malware-analysis/malware-persistence-mechanisms/
16. Bencherchali, N. (n.d.). *Hunting malware with Windows Sysinternals – Autoruns*. Medium. https://nasbench.medium.com/hunting-malware-with-windows-sysinternals-autoruns-19cbfe4103c2
17. Microsoft. (n.d.). *Autoruns – Sysinternals*. Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
18. Chernigivskyi, I. A., & Kryuchkova, L. P. (2025). Testing neural network models to solve the problem of detecting infected PCs based on digital traces. *Cybersecurity: Education, Science, Technique, 1*(29), 800–817. https://doi.org/10.28925/2663-4023.2025.29.941