КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1162
УДК 004.056:004.9:343.98

Ларченко Марина Олександрівна
кандидат юридичних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка», Чернігів, Україна;
доцент кафедри права та соціально-філософських наук
Ніжинський державний університет імені Миколи Гоголя, Ніжин, Україна.
ORCID: 0000-0002-2643-980X
urlinka2006@gmail.com

ЦИФРОВЕ ПРОФІЛЮВАННЯ КІБЕРЗЛОЧИНЦІВ НА ОСНОВІ АРТЕФАКТІВ ОПЕРАТИВНОЇ ПАМ'ЯТІ

Анотація. У статті досліджено можливості використання аналізу артефактів оперативної пам'яті комп'ютерних систем для виявлення ознак кіберзлочинної діяльності та формування моделей поведінки зловмисників у цифровому середовищі. Запропоновано підхід до реконструкції технічних дій під час кіберінциденту на основі комплексного аналізу дампів оперативної пам'яті, що дозволяє ідентифікувати активні процеси, мережеві з'єднання, взаємодію системних об'єктів та фрагменти виконуваного програмного коду. Методика дослідження передбачає структурний аналіз процесів операційної системи, виявлення аномальних параметрів запуску, дослідження ієрархії процесів та аналіз мережевої активності, зафіксованої у пам'яті системи. На основі отриманих результатів здійснено реконструкцію послідовності дій зловмисника, що включає запуск допоміжних процесів, встановлення мережевого з'єднання із віддаленими вузлами, інжекцію коду та виконання шкідливих команд. У результаті узагальнення виявлених артефактів сформовано модель поведінкових патернів кіберзлочинної активності, яка відображає взаємозв'язок між технічними діями зловмисника та цифровими слідами у структурі оперативної пам'яті. Отримані результати свідчать про те, що аналіз артефактів оперативної пам'яті може бути ефективним інструментом цифрової криміналістики для виявлення складних кіберінцидентів, реконструкції механізмів атак та формування поведінкових профілів кіберзлочинців. Запропонований підхід може використовуватися у практиці розслідування кіберзлочинів, а також для підвищення ефективності систем виявлення та аналізу кіберзагроз.

Ключові слова: цифрова криміналістика; оперативна пам'ять; дампи пам'яті; аналіз артефактів; кіберзлочини; поведінкове профілювання; кіберінциденти; інформаційна безпека.

ВСТУП

Активна цифровізація суспільних відносин, розвиток інформаційно-комунікаційних технологій та широке впровадження цифрових сервісів у державному управлінні, бізнесі й повсякденному житті супроводжуються одночасним зростанням кількості та складності кіберзлочинів. Сучасні кіберінциденти дедалі частіше характеризуються використанням складних технічних засобів, спеціалізованого шкідливого програмного забезпечення, а також застосуванням різноманітних методів приховування слідів протиправної діяльності. У таких умовах ефективність розслідування кіберзлочинів значною мірою залежить від здатності фахівців з цифрової криміналістики оперативно виявляти, фіксувати та інтерпретувати цифрові сліди, що виникають у процесі функціонування комп'ютерних систем.

Особливе значення у цьому контексті має аналіз оперативної пам'яті комп'ютерних систем. На відміну від традиційних носіїв інформації, оперативна пам'ять містить значну кількість тимчасових даних, що відображають поточний стан операційної системи, активні процеси, мережеві з'єднання, фрагменти виконуваного програмного коду та інші цифрові артефакти. У пам'яті можуть зберігатися залишкові дані шкідливих програм, ключі шифрування, фрагменти мережевого трафіку, токени автентифікації, дані про взаємодію процесів та інші відомості, що мають суттєве доказове значення для встановлення обставин кіберінциденту.

У практиці цифрової криміналістики дослідження дампів оперативної пам'яті поступово стає важливим інструментом відтворення подій, пов'язаних із кіберзлочинною діяльністю. Аналіз таких

даних дозволяє не лише виявляти шкідливі процеси або ознаки несанкціонованого втручання у роботу інформаційних систем, але й отримувати більш глибоке розуміння механізмів здійснення кібератак. Водночас цифрові артефакти, що зберігаються в оперативній пам'яті, можуть містити інформацію про особливості використаних інструментів, послідовність дій зловмисника, характер взаємодії з системними компонентами та іншими ресурсами.

У цьому контексті особливої актуальності набуває концепція цифрового профілювання кіберзлочинців, яка передбачає формування узагальнених моделей поведінки правопорушників на основі аналізу цифрових слідів їх діяльності. Такий підхід дозволяє розглядати технічні дії зловмисника не лише як окремі епізоди втручання в інформаційну систему, а як елементи певної поведінкової моделі, що може бути використана для подальшої атрибуції кібератак, виявлення повторюваних сценаріїв кіберзлочинної діяльності та вдосконалення методів розслідування.

Постановка проблеми. Незважаючи на значний розвиток інструментів цифрової криміналістики, сучасні підходи до аналізу дампів оперативної пам'яті здебільшого зосереджені на технічному вилученні окремих артефактів або ідентифікації шкідливого програмного забезпечення. Більшість існуючих методик спрямовані на виявлення конкретних технічних індикаторів компрометації, таких як підозрілі процеси, інжекції коду, аномальні модулі або незвичні мережеві з'єднання. Водночас ці підходи часто не передбачають системної інтерпретації отриманих даних у контексті поведінкових характеристик зловмисника.

Фактично значна кількість цифрових артефактів, що містяться у дампах оперативної пам'яті, розглядається лише як ізольовані технічні індикатори, хоча їх комплексний аналіз може надати значно ширшу інформацію про спосіб дій правопорушника. Зокрема, послідовність запуску процесів, використання певних інструментів, особливості взаємодії із системними компонентами або мережевими ресурсами можуть відображати характерні поведінкові патерни, притаманні окремим категоріям кіберзлочинців.

У зв'язку з цим виникає потреба у формуванні підходів, які дозволяли б використовувати дані оперативної пам'яті не лише для технічного виявлення ознак кібератак, але й для побудови моделей поведінки зловмисників. Такі моделі можуть сприяти підвищенню ефективності аналізу цифрових доказів, покращенню процесу атрибуції кіберінцидентів та розширенню можливостей прогнозування подальших дій правопорушників.

Отже, науковою проблемою, що потребує вирішення, є відсутність системного підходу до використання артефактів оперативної пам'яті для цифрового профілювання кіберзлочинців. Розроблення методів аналізу таких артефактів з урахуванням їх поведінкових характеристик може стати важливим напрямом розвитку цифрової криміналістики та підвищити ефективність розслідування кіберзлочинів.

Аналіз останніх досліджень і публікацій. Проблематика аналізу оперативної пам'яті у цифровій криміналістиці протягом останніх років привертає значну увагу дослідників у сфері кібербезпеки. Це пов'язано з тим, що значна частина сучасних кіберзагроз реалізується з використанням технік, які залишають мінімальну кількість слідів на постійних носіях інформації, але водночас формують численні артефакти у оперативній пам'яті комп'ютерних систем. У зв'язку з цим дослідження методів вилучення та інтерпретації даних з дампів пам'яті розглядається як один із ключових напрямів розвитку цифрової криміналістики.

Сучасні дослідження у цій сфері зосереджені насамперед на вдосконаленні інструментів аналізу пам'яті та автоматизації процесу виявлення цифрових артефактів. Зокрема, у роботі A. Case та G. G. Richard III розглянуто сучасний стан інструментів аналізу пам'яті та подальший розвиток фреймворку Volatility 3, який забезпечує модульний підхід до дослідження дампів пам'яті та підтримує розширений аналіз процесів, мережевих з'єднань і структур операційної системи [1]. Автори підкреслюють, що розвиток таких інструментів відкриває можливості для більш детального дослідження цифрових артефактів, проте більшість практичних застосувань обмежується технічним вилученням інформації без глибокої поведінкової інтерпретації отриманих даних.

Окремий напрям сучасних досліджень пов'язаний із використанням методів машинного навчання для автоматизованого аналізу даних оперативної пам'яті. Наприклад, у дослідженні S. Garfinkel та співавторів розглядаються перспективи застосування алгоритмів аналізу даних для автоматичного виявлення аномальних процесів і шкідливих артефактів у пам'яті комп'ютерних систем [2]. Автори зазначають, що поєднання цифрової криміналістики з методами аналізу великих даних дозволяє суттєво підвищити ефективність виявлення складних кіберзагроз, однак практична реалізація таких підходів потребує формалізації моделей поведінки зловмисників.

Важливим напрямом досліджень є також аналіз так званих fileless-атак, які виконуються без створення традиційних файлів на диску та переважно функціонують у пам'яті операційної системи. У роботах M. Sikorski та A. Honig розглядаються сучасні техніки використання пам'яті для приховування

шкідливого коду та механізми їх виявлення у процесі цифрової криміналістичної експертизи [3]. Дослідники підкреслюють, що такі атаки формують специфічні артефакти у структурі процесів та пам'яті операційної системи, аналіз яких може надати важливу інформацію про інструменти та методи діяльності кіберзлочинців.

У сучасних публікаціях також приділяється увага питанню атрибуції кіберінцидентів та аналізу поведінкових характеристик зловмисників. Так, у дослідженні E. Casey розглядається концепція поведінкового аналізу у цифровій криміналістиці та підкреслюється, що цифрові артефакти можуть використовуватися не лише для відновлення подій кіберінциденту, але й для формування профілів кіберзлочинців на основі характерних технічних дій, які вони здійснюють у процесі атаки [4].

Попри значну кількість досліджень, більшість сучасних робіт зосереджена або на технічних аспектах вилучення даних з оперативної пам'яті, або на виявленні конкретних типів шкідливого програмного забезпечення. Водночас питання системного використання артефактів оперативної пам'яті для формування моделей цифрового профілювання кіберзлочинців залишається недостатньо розробленим. Зокрема, у науковій літературі обмежено представлені підходи, що поєднують методи аналізу пам'яті з концепціями поведінкового аналізу у кіберпросторі. Це свідчить про наявність наукової потреби у розробленні методів інтерпретації артефактів оперативної пам'яті у контексті цифрового профілювання зловмисників та формування моделей їхньої поведінки під час здійснення кіберзлочинів.

Метою статті є розроблення підходу до цифрового профілювання кіберзлочинців на основі аналізу артефактів оперативної пам'яті комп'ютерних систем з метою виявлення характерних поведінкових патернів зловмисників під час здійснення кіберінцидентів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Цифрова криміналістика як міждисциплінарна галузь досліджує методи виявлення, фіксації, аналізу та інтерпретації цифрових слідів, що виникають у процесі функціонування інформаційних систем [5]. У межах цієї галузі особливе місце посідає дослідження оперативної пам'яті комп'ютерних систем, оскільки саме вона відображає поточний стан операційної системи, активні процеси, мережеві взаємодії та інші елементи, які можуть містити важливу інформацію про перебіг кіберінциденту [6]. На відміну від постійних носіїв інформації, дані оперативної пам'яті є високодинамічними та можуть змінюватися упродовж дуже короткого часу, що зумовлює як їхню криміналістичну цінність, так і складність аналізу.

У структурі сучасних операційних систем оперативна пам'ять використовується для зберігання виконуваного програмного коду, системних структур ядра, даних прикладних процесів, буферів мережевих з'єднань, а також тимчасових даних, які виникають під час виконання різних операцій. У процесі функціонування системи ці елементи формують сукупність цифрових артефактів, які можуть відображати як легітимну активність користувачів, так і ознаки несанкціонованого втручання. До таких артефактів належать, зокрема, записи про активні та завершені процеси, завантажені модулі та бібліотеки, об'єкти міжпроцесної взаємодії, мережеві сокети, структури керування потоками виконання, а також залишкові фрагменти програмного коду, що виконувалися у пам'яті.

З точки зору цифрової криміналістики аналіз оперативної пам'яті ґрунтується на реконструкції внутрішніх структур операційної системи на основі даних, отриманих із дампа пам'яті. Такий підхід передбачає використання спеціалізованих інструментів, які дозволяють відтворювати інформацію про процеси, драйвери, мережеві з'єднання та інші системні об'єкти [7]. У результаті формується структуроване уявлення про стан інформаційної системи на момент фіксації пам'яті, що створює можливість для подальшого криміналістичного аналізу.

Одним із важливих аспектів дослідження артефактів оперативної пам'яті є їх інтерпретація у контексті поведінки суб'єкта, який здійснює певні дії у системі. У криміналістиці загалом широко використовується концепція поведінкового профілювання, яка передбачає виявлення характерних ознак діяльності правопорушника на основі аналізу слідів його поведінки. У цифровому середовищі така концепція трансформується у підхід цифрового профілювання, що базується на аналізі технічних дій, які здійснюються у процесі використання інформаційних систем.

У контексті кіберзлочинної діяльності поведінкові характеристики можуть проявлятися у виборі інструментів, послідовності виконання команд, способах взаємодії з операційною системою, використанні мережевих протоколів та інших технічних аспектах функціонування програмного середовища. Відповідно, цифрові артефакти, що зберігаються у пам'яті комп'ютерних систем, можуть містити інформацію про ці характеристики та відображати специфіку діяльності зловмисника.

Особливу роль у цьому процесі відіграють так звані поведінкові патерни, під якими розуміють повторювані послідовності технічних дій, що виникають у процесі реалізації кібератак [8]. Такі патерни можуть включати характерні комбінації процесів, специфічні способи завантаження модулів у пам'ять,

використання механізмів інжекції коду, а також особливості встановлення мережевих з'єднань. Виявлення та систематизація подібних ознак дозволяє формувати узагальнені моделі поведінки кіберзлочинців, які можуть бути використані для аналізу нових кіберінцидентів.

Таким чином, теоретичною основою дослідження є поєднання підходів цифрової криміналістики, аналізу оперативної пам'яті та концепції поведінкового профілювання у кіберпросторі. Використання цих підходів у комплексі створює передумови для переходу від суто технічного вилучення артефактів пам'яті до їх системної інтерпретації з метою виявлення характерних моделей діяльності кіберзлочинців. Це, у свою чергу, дозволяє підвищити ефективність аналізу цифрових доказів та розширити можливості атрибуції кіберінцидентів.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження спрямована на виявлення та інтерпретацію цифрових артефактів оперативної пам'яті з метою формування поведінкових характеристик кіберзлочинців. В основу дослідження покладено підхід, який передбачає послідовне виконання етапів отримання дампів оперативної пам'яті, їх криміналістичного аналізу, систематизації виявлених артефактів та подальшої інтерпретації отриманих даних у контексті поведінкових моделей зловмисників.

На першому етапі здійснюється отримання дампів оперативної пам'яті комп'ютерних систем, які потенційно містять сліди кіберінцидентів. Фіксація пам'яті виконується за допомогою спеціалізованих інструментів цифрової криміналістики, що дозволяють здійснювати копіювання вмісту оперативної пам'яті без істотного впливу на стан системи. У результаті формується бінарний образ пам'яті, який відображає стан операційної системи, активні процеси, завантажені модулі, мережеві з'єднання та інші елементи системного середовища на момент фіксації.

Другий етап дослідження передбачає структурний аналіз отриманих дампів пам'яті. Для цього застосовуються спеціалізовані програмні засоби аналізу пам'яті, які дозволяють реконструювати внутрішні структури операційної системи та відтворити інформацію про системні об'єкти. У межах цього етапу здійснюється ідентифікація активних і завершених процесів, аналіз завантажених динамічних бібліотек та драйверів, дослідження мережевих з'єднань, а також виявлення аномальних або підозрілих об'єктів. Особлива увага приділяється виявленню ознак інжекції коду, використання безфайлових механізмів виконання програм, а також інших технік приховування шкідливої активності.

На третьому етапі проводиться виділення та систематизація цифрових артефактів, що можуть свідчити про діяльність зловмисника. До таких артефактів належать записи про процеси, які мають нетипові параметри запуску, аномальні мережеві з'єднання, підозрілі модулі у пам'яті, невідповідності у структурі системних об'єктів, а також залишкові фрагменти виконуваного коду. Для кожного виявленого артефакту фіксуються його основні характеристики, включаючи часові параметри, взаємозв'язки з іншими процесами та місце розташування у структурі пам'яті.

Наступний етап дослідження полягає у встановленні взаємозв'язків між виявленими артефактами. На цьому етапі проводиться аналіз послідовності технічних дій, що могли бути здійснені у системі під час реалізації кібератаки. Зокрема, досліджується взаємодія між процесами, механізми завантаження модулів у пам'ять, структура мережевих з'єднань та інші елементи системної активності. Такий підхід дозволяє перейти від аналізу окремих технічних індикаторів до реконструкції загальної логіки дій зловмисника.

У процесі дослідження отримані дані також піддаються узагальненню з метою формування поведінкових характеристик кіберзлочинців. Для цього проводиться групування виявлених артефактів за типами дій, які вони відображають. Наприклад, окремі групи можуть характеризувати використання інструментів віддаленого доступу, виконання команд через інтерпретатори системних оболонок, встановлення мережевих тунелів або застосування технік приховування шкідливих процесів. Аналіз таких груп дозволяє виявляти повторювані патерни діяльності, які можуть бути використані для формування узагальнених моделей поведінки зловмисників.

Для підвищення наочності результатів дослідження передбачено використання методів візуалізації отриманих даних. Зокрема, взаємозв'язки між процесами, модулями та мережевими з'єднаннями можуть бути представлені у вигляді графових моделей, де вузли відображають окремі системні об'єкти, а ребра – їх взаємодію. Крім того, послідовність дій, що відбуваються у системі, може бути відображена у вигляді часових діаграм або схем процесної активності. Така візуалізація дозволяє більш чітко продемонструвати структуру виявлених артефактів та їх роль у реалізації кіберінциденту.

Таким чином, запропонована методика дослідження базується на поєднанні криміналістичного аналізу оперативної пам'яті, систематизації цифрових артефактів та інтерпретації отриманих даних у контексті поведінкових моделей кіберзлочинців. Такий підхід дозволяє не лише виявляти технічні ознаки

кібератак, але й формувати більш глибоке розуміння механізмів їх реалізації та особливостей діяльності зловмисників у цифровому середовищі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах проведеного дослідження було здійснено комплексний аналіз артефактів оперативної пам'яті комп'ютерних систем з метою виявлення характерних ознак діяльності кіберзлочинців та формування моделей їх поведінки у цифровому середовищі. Особливість такого підходу полягає у тому, що оперативна пам'ять відображає поточний стан операційної системи та програмного середовища у конкретний момент часу, що дозволяє отримати інформацію про процеси, які виконуються, активні мережеві з'єднання, завантажені модулі та інші елементи системної активності. На відміну від традиційного аналізу постійних носіїв інформації, який здебільшого дозволяє дослідити вже завершені дії користувачів або програм, аналіз оперативної пам'яті дає змогу виявити активні механізми функціонування шкідливого програмного забезпечення, що є особливо важливим у випадках використання безфайлових технік атак.

Отримані результати свідчать про те, що оперативна пам'ять містить значний обсяг даних, які можуть використовуватися для ідентифікації ознак компрометації інформаційної системи. Серед таких даних особливе значення мають структури, що описують процеси операційної системи, таблиці дескрипторів об'єктів, інформація про потоки виконання, завантажені динамічні бібліотеки, мережеві сокети, а також фрагменти виконуваного коду. Аналіз зазначених структур дозволяє не лише встановити факт несанкціонованого втручання у роботу системи, але й реконструювати логіку технічних дій, які були виконані зловмисником під час реалізації кібератаки. Таким чином, оперативна пам'ять виступає своєрідним «знімком» стану інформаційної системи, що містить комплексну інформацію про її функціонування.

На першому етапі дослідження було здійснено структурний аналіз дампів оперативної пам'яті з метою виявлення активних процесів та системних об'єктів, які функціонували у системі на момент фіксації пам'яті. Для цього використовувалися методи реконструкції структур операційної системи, що дозволяють відновити інформацію про таблиці процесів, потоки виконання, дескриптори відкритих файлів та інші елементи системного середовища. У результаті аналізу було отримано повний перелік процесів, які виконувалися у системі, а також встановлено їх ієрархічні зв'язки, параметри запуску та взаємодію з іншими компонентами операційної системи.

Проведений аналіз показав, що у структурі пам'яті можуть міститися як легітимні системні процеси, так і процеси, які мають ознаки аномальної або підозрілої активності. До легітимних процесів належать стандартні компоненти операційної системи, що відповідають за управління ресурсами, взаємодію з користувачем та виконання системних функцій. Водночас у деяких випадках можуть бути виявлені процеси, які маскуються під легітимні системні служби або використовують схожі назви для приховування своєї присутності у системі.

Аналіз артефактів пам'яті дозволив виділити низку характерних ознак, які можуть свідчити про наявність підозрілої активності. Однією з таких ознак є невідповідність між ім'ям процесу та шляхом його розташування у файловій системі. Наприклад, процес може мати назву, ідентичну до одного з системних компонентів операційної системи, однак фактичний шлях до виконуваного файлу може вказувати на розташування у тимчасових каталогах або директоріях користувача. Така невідповідність може свідчити про використання технік маскування шкідливого програмного забезпечення.

Ще однією важливою ознакою підозрілої активності є відсутність цифрового підпису виконуваного файлу або використання підпису, який не відповідає виробнику програмного забезпечення. У сучасних операційних системах більшість легітимних системних компонентів мають цифрові підписи, що дозволяє перевірити їх походження. Відсутність такого підпису або використання невідомого сертифіката може свідчити про те, що відповідний процес був створений стороннім програмним забезпеченням.

Крім того, у процесі дослідження було встановлено, що підозрілі процеси часто мають нетипові параметри запуску або взаємодіють із системними ресурсами у спосіб, який не характерний для стандартних програм операційної системи. Зокрема, такі процеси можуть ініціювати встановлення мережевих з'єднань із зовнішніми вузлами, завантажувати додаткові модулі у пам'ять або створювати нові потоки виконання у контексті інших процесів. Подібна активність може бути пов'язана з використанням технік віддаленого керування системою або виконанням шкідливих команд.

Особливу увагу під час аналізу було приділено дослідженню взаємодії процесів між собою. У багатьох випадках кіберзлочинці використовують легітимні системні процеси як середовище для виконання шкідливого коду. Це може реалізовуватися шляхом інжекції коду у пам'ять іншого процесу

або створення нових потоків виконання у його адресному просторі. У результаті такі процеси можуть виконувати шкідливі функції, залишаючись зовні схожими на стандартні компоненти операційної системи. Виявлення подібних ознак можливе саме завдяки детальному аналізу структури оперативної пам'яті та взаємозв'язків між процесами.

Важливим результатом проведеного етапу дослідження стало встановлення того, що структурний аналіз дампів пам'яті дозволяє не лише ідентифікувати окремі підозрілі процеси, але й визначити їх роль у загальній архітектурі кіберінциденту. Зокрема, було встановлено, що деякі процеси можуть виконувати функції початкового проникнення у систему, інші – забезпечувати встановлення мережевого з'єднання із зовнішнім сервером, а окремі компоненти можуть відповідати за виконання шкідливих команд або передачу даних.

Приклад структури активних процесів операційної системи та їх ієрархічних зв'язків представлено на рисунку 1.

Структура активних процесів операційної системи

Рис.1. Приклад структури активних процесів у системі (parent–child relationship), виявленої під час аналізу оперативної пам'яті

Подальший аналіз отриманих дампів оперативної пам'яті дозволив встановити характер взаємодії між процесами, які функціонували у системі під час реалізації кіберінциденту. Особливу увагу було приділено дослідженню механізмів створення нових процесів, передачі керування між ними, а також особливостей їх запуску та функціонування у системному середовищі. У межах проведеного дослідження було встановлено, що аналіз взаємозв'язків між процесами є важливим інструментом для реконструкції послідовності технічних дій, виконаних зловмисником під час реалізації атаки.

У результаті аналізу було виявлено випадки створення дочірніх процесів із нетиповими параметрами запуску, що може свідчити про використання спеціалізованих механізмів виконання команд або застосування технік прихованого запуску програмного коду. Зокрема, у деяких випадках батьківські процеси, які належать до стандартних компонентів операційної системи, ініціювали запуск виконуваних файлів, що не входять до складу системного програмного забезпечення або розташовані у нетипових каталогах файлової системи. Така поведінка може бути ознакою використання механізмів віддаленого виконання команд або інжекції коду у контексті легітимних системних процесів.

Крім того, у процесі дослідження було встановлено, що окремі дочірні процеси запускалися з параметрами командного рядка, які не відповідають типовим сценаріям використання відповідних програм. Подібні параметри можуть включати виклик системних утиліт із передачею спеціальних аргументів, виконання скриптів або ініціювання з'єднання із зовнішніми мережевими ресурсами. Такі ознаки можуть свідчити про використання технік так званого «living-off-the-land», коли зловмисник застосовує стандартні інструменти операційної системи для реалізації шкідливої активності, що дозволяє значною мірою ускладнити її виявлення засобами традиційного антивірусного захисту.

Окрему увагу під час аналізу було приділено дослідженню ієрархічних зв'язків між процесами. Встановлено, що структура процесів у пам'яті операційної системи відображає чітку систему батьківських і дочірніх відносин, що дозволяє простежити походження кожного виконуваного процесу. Завдяки цьому стає можливим відтворення послідовності запуску програм та визначення процесу, який ініціював виконання підозрілого модуля. У випадках кіберінцидентів саме цей аспект дозволяє встановити початкову точку проникнення шкідливого програмного забезпечення у систему.

Для наочного представлення такого механізму на рисунку 2 наведено граф взаємодії процесів, що демонструє типовий ланцюг запуску підозрілих виконуваних модулів через легітимні системні процеси операційної системи. Така модель дозволяє відобразити послідовність створення дочірніх процесів, а

також виділити елементи, які можуть свідчити про реалізацію шкідливого програмного забезпечення у системі.

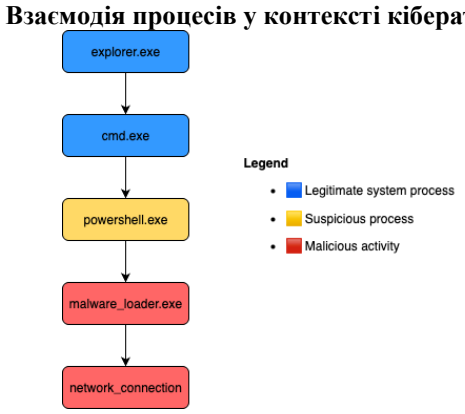

Рис. 2. Граф взаємодії процесів в контексті реалізації кібератаки

Важливим результатом проведеного дослідження стало також виявлення аномальних мережевих з'єднань, які були зафіксовані у структурі оперативної пам'яті досліджуваних систем. Оперативна пам'ять містить інформацію про активні мережеві сесії, включаючи параметри встановлених TCP та UDP-з'єднань, ідентифікатори процесів, що ініціювали відповідні з'єднання, а також адреси віддалених вузлів. Аналіз зазначених структур дозволяє встановити мережеву активність системи навіть у тих випадках, коли відповідні записи відсутні у системних журналах або були видалені зловмисником.

У ході дослідження було встановлено наявність мережевих з'єднань із зовнішніми вузлами, які не входять до стандартної інфраструктури досліджуваної інформаційної системи. Зокрема, деякі процеси ініціювали мережеві сесії із віддаленими IP-адресами, що належать до географічно віддалених регіонів або використовуються для розміщення серверів керування шкідливими мережами. Подібні з'єднання можуть використовуватися для встановлення каналів віддаленого керування зараженою системою, передачі викрадених даних або отримання додаткових команд від оператора шкідливого програмного забезпечення.

Крім того, у структурі пам'яті були виявлені ознаки використання нестандартних мережевих портів та короткочасних мережевих сесій, що можуть свідчити про спроби приховати мережеву активність шляхом використання динамічних каналів зв'язку. Така поведінка є характерною для сучасних шкідливих програм, які намагаються мінімізувати час існування мережевого з'єднання та уникати фіксації у системних журналах або мережевих засобах моніторингу. Візуалізація розміщена на рисунку 3.

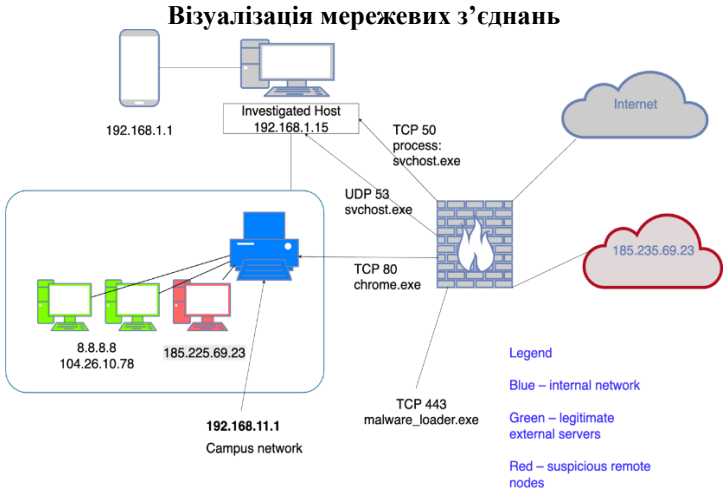

Рис. 3. Візуалізація мережевих з'єднань, зафіксованих у пам'яті досліджуваної системи

У процесі подальшого аналізу пам'яті також було виявлено фрагменти виконуваного програмного коду, які не відповідали жодному легітимному модулю операційної системи або встановленого

програмного забезпечення. Такі артефакти можуть бути результатом застосування технік інжекції коду, коли шкідливий код завантажується безпосередньо у пам'ять процесу без створення окремого виконуваного файлу на диску. Подібні методи широко використовуються у сучасних кіберзагрозах, оскільки дозволяють уникнути виявлення традиційними засобами антивірусного захисту.

Дослідження відповідних сегментів пам'яті показало, що підозрілий код може розміщуватися у динамічно виділених областях адресного простору процесу, які не пов'язані з легітимними модулями або бібліотеками. Такі області можуть мати характерні ознаки, зокрема наявність виконуваних інструкцій у пам'яті, що була виділена як область даних, або невідповідність між правами доступу до сегмента пам'яті та його фактичним використанням.

Виявлення подібних структур у пам'яті є важливим індикатором компрометації інформаційної системи, оскільки свідчить про наявність механізмів прихованого виконання шкідливого коду. Крім того, аналіз таких фрагментів може дозволити дослідникам отримати додаткову інформацію про функціональні можливості шкідливого програмного забезпечення, його алгоритми роботи та можливі канали взаємодії із зовнішнім середовищем.

На рисунку 4 представлено схематичну модель адресного простору процесу операційної системи із виділенням області пам'яті, у якій було виявлено фрагмент інжектованого коду. Виявлена область не належить до жодного легітимного модуля або бібліотеки та характеризується наявністю виконуваних інструкцій у сегменті пам'яті, який призначений для зберігання даних. Подібна невідповідність може свідчити про використання техніки інжекції коду у контексті процесу.

Схематичне відображення адресного простору процесу

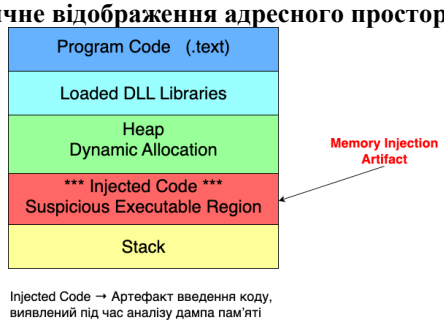

Рис. 4. Схематичне відображення адресного простору процесу із виділенням області пам'яті, у якій виявлено інжектований виконуваний код

Аналіз сукупності виявлених артефактів оперативної пам'яті дозволив здійснити реконструкцію ймовірної послідовності технічних дій, які могли бути виконані зловмисником під час реалізації кіберінциденту. Такий підхід ґрунтується на зіставленні різних типів цифрових артефактів, що містяться у дампі пам'яті, зокрема інформації про активні процеси, мережеві з'єднання, завантажені модулі, фрагменти виконуваного коду та інші структурні елементи операційної системи. Системний аналіз цих даних дозволяє не лише зафіксувати факт компрометації інформаційної системи, але й відтворити логічну структуру атаки, що є важливим для подальшого розслідування кіберінцидентів.

У ході дослідження було встановлено, що початковий етап атаки може бути пов'язаний із запуском допоміжного процесу або виконанням скрипту через системний інтерпретатор команд. Подібний механізм часто використовується у випадках, коли зловмисник отримує первинний доступ до системи через уразливість програмного забезпечення, компрометацію облікових даних або застосування соціальної інженерії. У таких ситуаціях виконання початкової команди може здійснюватися через стандартні системні утиліти або інтерпретатори сценаріїв, що дозволяє зловмиснику використовувати легітимні механізми операційної системи для подальшого розгортання атаки.

Подальший аналіз показав, що після виконання початкового сценарію у системі може створюватися окремий допоміжний процес, який виконує функцію підготовки середовища для наступних етапів атаки. Такий процес може здійснювати перевірку системної конфігурації, визначати рівень доступу користувача, аналізувати мережеві параметри або готувати механізми для встановлення віддаленого з'єднання. Подібні дії дозволяють зловмиснику оцінити можливості подальшого проникнення у систему та адаптувати інструменти атаки до конкретного середовища.

Наступним етапом атаки, відповідно до отриманих результатів, є встановлення мережевого з'єднання із віддаленим сервером, який може виконувати функції командно-керуючого центру або використовуватися для передачі додаткових компонентів шкідливого програмного забезпечення. Аналіз артефактів оперативної пам'яті показав, що такі з'єднання можуть ініціюватися одразу після запуску

допоміжного процесу або після виконання низки підготовчих дій у системі. При цьому у структурі пам'яті фіксуються параметри відповідних мережевих сесій, що дозволяє встановити IP-адреси віддалених вузлів, використовувані мережеві порти та процеси, які ініціювали відповідні з'єднання.

Після встановлення мережевого з'єднання у системі може відбуватися завантаження додаткових компонентів шкідливого програмного забезпечення безпосередньо у оперативну пам'ять. Такий підхід дозволяє уникнути створення виконуваних файлів на постійних носіях інформації, що значною мірою ускладнює виявлення атаки традиційними засобами антивірусного захисту. Завантажені у пам'ять модулі можуть виконувати різні функції, включаючи забезпечення віддаленого керування системою, збір конфіденційної інформації, виконання команд оператора або підготовку подальших етапів кібератаки.

Важливою особливістю таких атак є використання технік інжекції коду, коли шкідливі інструкції впроваджуються у адресний простір легітимних системних процесів. У результаті цього відповідні процеси можуть виконувати шкідливі функції без створення нових виконуваних файлів, що ускладнює виявлення підозрілої активності. Аналіз пам'яті дозволяє виявити подібні механізми за рахунок дослідження структури сегментів пам'яті та визначення аномальних областей, у яких міститься виконуваний код. Візуалізація на рисунку 5 дозволяє наочно продемонструвати еволюцію атаки у часі та встановити взаємозв'язок між окремими технічними діями.

Хронологія реконструкції кібератаки

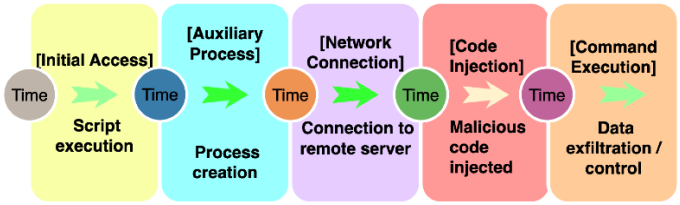

Рис. 5. Часова діаграма послідовності дій під час кіберінциденту (стрічка часу)

У результаті узагальнення отриманих даних було сформовано модель поведінкових патернів, характерних для досліджуваного типу кіберзлочинної активності. Формування такої моделі ґрунтується на аналізі повторюваних технічних ознак, які проявляються у різних кіберінцидентах та можуть бути пов'язані з використанням однакових інструментів або схожих методів реалізації атак. До таких ознак належать характер запуску процесів, специфіка використання системних утиліт, особливості мережевої активності, а також структура розміщення шкідливого коду у пам'яті процесів.

Сформована модель поведінкових патернів відображає взаємозв'язок між технічними діями зловмисника та відповідними цифровими артефактами, які залишаються у структурі оперативної пам'яті системи. Наприклад, запуск підозрілого процесу може супроводжуватися появою нетипових параметрів командного рядка, встановленням нових мережевих з'єднань або створенням додаткових потоків виконання у межах інших процесів. Подібні взаємозв'язки дозволяють дослідникам ідентифікувати характерні поведінкові моделі та використовувати їх для виявлення аналогічних атак у майбутньому.

Особливу цінність така модель має у контексті цифрового профілювання кіберзлочинців. Аналіз поведінкових патернів дозволяє встановити характер використаних інструментів, технічний рівень підготовки зловмисника, а також можливі методи маскування його діяльності. У деяких випадках повторюваність певних технічних прийомів може свідчити про використання однакових наборів інструментів або належність кількох кіберінцидентів до діяльності однієї й тієї ж злочинної групи.

Модель поведінкового профілювання на основі артефактів пам'яті

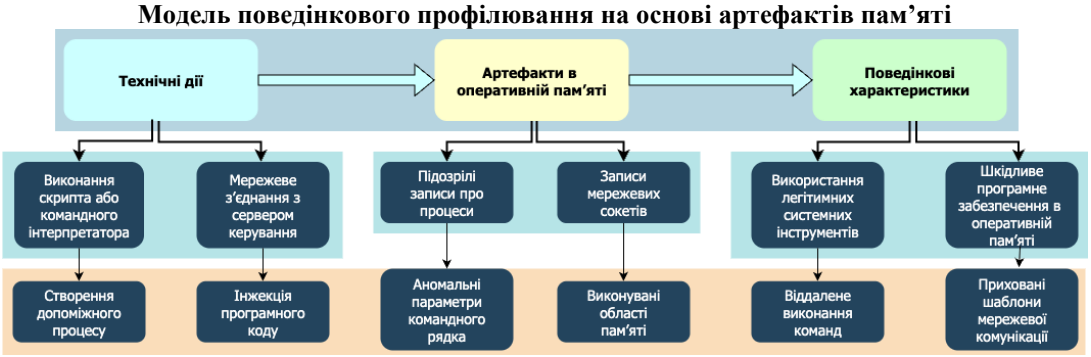

Рис. 6. Узагальнена модель поведінкового профілю кіберзлочинця

Схема на рисунку 6 демонструє взаємозв'язок між технічними діями зловмисника, відповідними артефактами у пам'яті та сформованими поведінковими характеристиками. Схема побудована у вигляді багаторівневої моделі, де перший рівень відображає конкретні технічні дії у системі, другий рівень – цифрові артефакти, що залишаються у пам'яті, а третій рівень – узагальнені поведінкові характеристики, які можуть використовуватися для формування профілю потенційного кіберзлочинця.

Таким чином, результати проведеного дослідження свідчать про те, що аналіз артефактів оперативної пам'яті дозволяє отримати комплексну інформацію про технічні дії зловмисників у межах інформаційної системи. Систематизація та інтерпретація таких артефактів створює можливість переходу від простого виявлення технічних індикаторів компрометації до формування структурованих моделей поведінки кіберзлочинців. Застосування подібних моделей може істотно підвищити ефективність розслідування кіберзлочинів, а також сприяти розвитку сучасних методів цифрової криміналістики, орієнтованих на аналіз поведінкових характеристик зловмисників у цифровому середовищі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження встановлено, що артефакти оперативної пам'яті комп'ютерних систем становлять важливе джерело інформації для аналізу кіберінцидентів та можуть бути ефективно використані не лише для технічного виявлення ознак компрометації інформаційних систем, але й для формування поведінкових характеристик кіберзлочинців. На відміну від традиційних підходів цифрової криміналістики, які здебільшого орієнтовані на дослідження даних постійних носіїв інформації, аналіз оперативної пам'яті дозволяє отримати більш детальне уявлення про поточний стан системи, активні процеси, мережеві взаємодії та інші елементи, що безпосередньо відображають дії користувачів або програмного забезпечення у момент реалізації кіберінциденту.

У межах дослідження було обґрунтовано теоретичні засади використання артефактів оперативної пам'яті для цифрового профілювання кіберзлочинців. Показано, що у структурі пам'яті можуть міститися різноманітні цифрові сліди, зокрема записи про активні та завершені процеси, інформація про завантажені модулі та драйвери, дані про мережеві з'єднання, а також фрагменти виконуваного програмного коду. Сукупність таких артефактів дозволяє реконструювати логіку функціонування інформаційної системи на момент фіксації пам'яті та виявити характерні ознаки несанкціонованої діяльності.

Результати дослідження підтвердили, що системний аналіз взаємозв'язків між процесами, модулями та мережевими з'єднаннями, зафіксованими у дампах оперативної пам'яті, дозволяє встановлювати послідовність технічних дій, які могли бути виконані зловмисником під час реалізації кібератаки. Зокрема, такі дії можуть включати запуск допоміжних процесів, використання інтерпретаторів системних команд, встановлення мережевих каналів зв'язку з віддаленими вузлами, а також застосування технік інжекції коду або безфайлового виконання шкідливих програм. Виявлення подібних ознак дозволяє не лише ідентифікувати факт втручання у роботу інформаційної системи, але й визначити характер використаних інструментів та методів реалізації кібератаки.

Важливим результатом дослідження стало формування підходу до інтерпретації цифрових артефактів оперативної пам'яті у контексті поведінкових моделей кіберзлочинців. Показано, що технічні дії, які виконуються зловмисниками у процесі реалізації кібератак, формують певні повторювані патерни, що можуть бути виявлені шляхом аналізу структури процесів, механізмів взаємодії між системними об'єктами та особливостей мережевої активності. Узагальнення таких патернів створює передумови для побудови моделей цифрового профілювання, які можуть бути використані у процесі розслідування кіберзлочинів, аналізу нових кіберінцидентів та підвищення ефективності атрибуції кібератак.

Запропонована у роботі методика дослідження передбачає поєднання інструментів криміналістичного аналізу пам'яті, систематизації цифрових артефактів та подальшої інтерпретації отриманих даних з урахуванням поведінкових характеристик зловмисників. Такий підхід дозволяє перейти від фрагментарного аналізу окремих технічних індикаторів компрометації до комплексного дослідження структури кіберінциденту та механізмів його реалізації. Крім того, використання методів візуалізації взаємозв'язків між системними об'єктами сприяє більш наочному представленню отриманих результатів та полегшує інтерпретацію складних структур даних, що містяться у дампах оперативної пам'яті.

Практичне значення отриманих результатів полягає у можливості використання запропонованого підходу під час проведення цифрових криміналістичних досліджень, аналізу кіберінцидентів та розроблення інструментів автоматизованого виявлення ознак кіберзлочинної діяльності. Формування поведінкових моделей на основі артефактів оперативної пам'яті може бути корисним як для

правоохоронних органів, що здійснюють розслідування кіберзлочинів, так і для фахівців з кібербезпеки, які займаються моніторингом та аналізом загроз у корпоративних або державних інформаційних системах.

Перспективи подальших досліджень у цьому напрямі пов'язані з удосконаленням методів автоматизованого аналізу артефактів оперативної пам'яті та інтеграцією таких методів із сучасними технологіями обробки великих даних і машинного навчання. Зокрема, перспективним є створення систем, здатних автоматично виявляти поведінкові патерни кіберзлочинців на основі аналізу великої кількості дампів пам'яті та формувати узагальнені моделі кіберзлочинної активності.

Крім того, подальшого дослідження потребує питання стандартизації підходів до інтерпретації артефактів оперативної пам'яті у цифровій криміналістиці, а також розроблення уніфікованих методик їх використання у процесі розслідування кіберінцидентів. Важливим напрямом є також дослідження можливостей інтеграції аналізу пам'яті з іншими джерелами цифрових доказів, зокрема журналами подій операційних систем, мережевим трафіком та даними систем моніторингу безпеки.

Таким чином, результати проведеного дослідження підтверджують перспективність використання артефактів оперативної пам'яті для цифрового профілювання кіберзлочинців та свідчать про доцільність подальшого розвитку цього напряму у межах цифрової криміналістики та кібербезпеки. Запропонований підхід створює основу для формування нових методів аналізу кіберінцидентів, спрямованих на глибше розуміння механізмів кіберзлочинної діяльності та підвищення ефективності протидії кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Case, A., & Richard, G. G., III. (2023). Memory forensics: The path forward. *Digital Investigation, 45*, Article 301522. https://doi.org/10.1016/j.diin.2016.12.004
2. Garfinkel, S. L. (2023). Digital forensics research: The next 10 years. *Digital Investigation, 44*, 64-73. https://doi.org/10.1016/j.diin.2010.05.009
3. Sikorski, M., & Honig, A. (2024). *Practical malware analysis: The hands-on guide to dissecting malicious software* (Updated ed.). No Starch Press. https://j.twirpx.link/file/1487771/
4. Casey, E. (2023). *Handbook of digital forensics and investigation* (2nd ed.). Academic Press. https://dokumen.pub/handbook-of-digital-forensics-and-investigation-0123742676-9780123742674.html
5. National Institute of Standards and Technology. (2023). *Guide to integrating forensic techniques into incident response* (Special Publication 800-86). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
6. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2023). *The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory* (Reprint ed.). Wiley. https://elhacker.info/manuales/Análisis%20forense/The_Art_of_Memory_Forensics.pdf
7. Volatility Foundation. (2025). *Volatility 3 framework documentation*. https://volatility3.readthedocs.io
8. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2023). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78,* 544-546. https://doi.org/10.1016/j.future.2017.07.060

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Maryna Larchenko
Candidate of Law, Associate Professor, Associate Professor of the Department of Cybersecurity and Mathematical Modeling, National University "Chernihiv Polytechnic", Chernihiv, Ukraine
Associate Professor of the Department of Law and Social and Philosophical Sciences
Mykola Gogol Nizhyn State University, Nizhyn, Ukraine.
ORCID: 0000-0002-2643-980X
urlinka2006@gmail.com

DIGITAL PROFILING OF CYBERCRIMINALS BASED ON WORKING MEMORY ARTIFACTS

Abstract. The article explores the possibilities of using the analysis of working memory artifacts of computer systems to identify signs of cybercriminal activity and form models of behavior of attackers in the digital environment. An approach to reconstructing technical actions during a cyber incident is proposed based on a comprehensive analysis of RAM dumps, which allows identifying active processes, network connections, interaction of system objects, and fragments of executable program code. The research methodology involves structural analysis of operating system processes, detection of anomalous startup parameters, study of process hierarchy, and analysis of network activity recorded in the system memory. Based on the results obtained, a sequence of actions of the attacker was reconstructed, which includes launching auxiliary processes, establishing a network connection with remote nodes, code injection, and execution of malicious commands. As a result of generalizing the detected artifacts, a model of behavioral patterns of cybercriminal activity was formed, which reflects the relationship between the attacker's technical actions and digital traces in the RAM structure. The results obtained indicate that the analysis of RAM artifacts can be an effective digital forensics tool for detecting complex cyber incidents, reconstructing attack mechanisms, and forming behavioral profiles of cybercriminals. The proposed approach can be used in the practice of investigating cybercrimes, as well as to improve the efficiency of cyber threat detection and analysis systems.

Keywords: digital forensics; RAM; memory dumps; artifact analysis; cybercrimes; behavioral profiling; cyber incidents; information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Case, A., & Richard, G. G., III. (2023). Memory forensics: The path forward. *Digital Investigation, 45*, Article 301522. https://doi.org/10.1016/j.diin.2016.12.004
2. Garfinkel, S. L. (2023). Digital forensics research: The next 10 years. *Digital Investigation, 44*, 64-73. https://doi.org/10.1016/j.diin.2010.05.009
3. Sikorski, M., & Honig, A. (2024). *Practical malware analysis: The hands-on guide to dissecting malicious software* (Updated ed.). No Starch Press. https://j.twirpx.link/file/1487771/
4. Casey, E. (2023). *Handbook of digital forensics and investigation* (2nd ed.). Academic Press. https://dokumen.pub/handbook-of-digital-forensics-and-investigation-0123742676-9780123742674.html
5. National Institute of Standards and Technology. (2023). *Guide to integrating forensic techniques into incident response* (Special Publication 800-86). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
6. Ligh, M. H., Case, A., Levy, J., & Walters, A. (2023). *The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory* (Reprint ed.). Wiley. https://elhacker.info/manuales/Análisis%20forense/The_Art_of_Memory_Forensics.pdf
7. Volatility Foundation. (2025). *Volatility 3 framework documentation*. https://volatility3.readthedocs.io
8. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2023). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78,* 544-546. https://doi.org/10.1016/j.future.2017.07.060

Отримано редакцією журналу / Received: 22.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26