1–8. DOI: 10.1109/FIE.2017.8190713.
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework (ECSF). – Athens : ENISA, 2022. URL: https://www.enisa.europa.eu/topics/skills-framework/ecsf.
4. Russo E., Costa G., Armando A. Building next generation cyber ranges with CRACK. Computers & Security. – 2020. – Vol. 95. – Article 101837. DOI: 10.1016/j.cose.2020.101837.
5. Besson P.-V., Viet Triem Tong V., Guette G. та ін. URSID: Automatically refining a single attack scenario into multiple cyber range architectures. Foundations and Practice of Security (FPS 2023). Lecture Notes in Computer Science. Cham : Springer, 2024. DOI: 10.1007/978-3-031-57537-2_8.
6. Xiang X., Ma C., Zeng L. та ін. Uncovering multi-step attacks with threat knowledge graph reasoning. Security and Safety. – 2025. – Vol. 4. – Article 2024019. DOI: 10.1051/sands/2024019.

Удосконалення процедур цифрової криміналістики в системах реагування на інциденти кібербезпеки

УДК 004.056.55

Мар'яна Мельник[1], Віктор Чешун[2], Дмитро Чешун[3]

[1,2]Хмельницький національний університет, [3]Хмельницький фаховий економіко-технологічний коледж Університету економіки і підприємництва
[1]melnyk.masia@gmail.com, [2]cheshunvn@khmnu.edu.ua,
[3]dmytro.cheshun@gmail.com

Сучасний етап розвитку цифрового суспільства характеризується тотальною інтеграцією інформаційних технологій у процеси державного управління та функціонування критичної інфраструктури, що водночас створює безпрецедентні ризики для національної безпеки.

Аналіз поточної ситуації [1-3] дозволяє виявити суттєві недоліки в існуючих підходах до реагування, серед яких найгострішими є низький рівень автоматизації моніторингу подій безпеки та відсутність єдиної методології збору цифрових доказів. Більшість установ сьогодні стикаються з проблемою фрагментарності журналів подій та невідповідністю процедур вилучення артефактів міжнародним стандартам, що часто унеможливлює проведення глибокого технічного аналізу та встановлення реальних причин інцидентів. Досвід масштабних атак останніх років підтверджує, що без впровадження проактивних методів виявлення та структурованих алгоритмів розслідування об'єкти критичної інфраструктури залишаються вразливими до тривалої прихованої присутності зловмисників у їхніх внутрішніх мережах.

Мета дослідження полягає у розробці та практичному обґрунтуванні системного підходу до розслідування кіберінцидентів, який би забезпечував цілісність процесу криміналістики від моменту первинної фіксації аномалії до формування підсумкової аналітичної звітності. Автори поставили за ціль створити гнучку модель, що поєднує сучасні технічні засоби автоматизованого аналізу телеметрії з чіткими організаційними регламентами взаємодії між

різними суб'єктами кібербезпеки. Важливим аспектом дослідження є адаптація вимог міжнародних стандартів ISO/IEC 27035 [4] та рекомендацій NIST [5,6] до специфічних умов функціонування українських державних інформаційних систем. Для досягнення поставленої мети розв'язано низку наукових і практичних завдань, зокрема моделювання процесів збереження цифрових артефактів, визначення оптимального стеку програмних інструментів із відкритим кодом та побудова тестового середовища для верифікації запропонованих підходів у реальних сценаріях складних кібератак.

Отримані результати дослідження базуються на розробці оригінального інтегрованого методу, що об'єднує кілька технологічних платформ у єдину логічну систему реагування та аналізу. Оригінальність полягає у формуванні двох взаємодоповнюючих моделей, де перша регламентує збереження та відновлення цифрових доказів за принципом суворого дотримання ланцюга зберігання, а друга визначає чіткі алгоритми взаємодії учасників розслідування на локальному, галузевому та національному рівнях.

Основними деталізованим етапами реалізації методу є реагування на інциденти, робота з доказами і взаємодія учасників. На етапі реагування впроваджено ієрархічний підхід, де кожен інцидент проходить фази ідентифікації, локалізації, аналізу та «навчання». Акцент зроблено на безперервності – результати розслідування обов'язково мають оновлювати бази індикаторів компрометації (IoC). Для роботи з доказами регламентовано порядок збору волатильних даних (RAM) та створення посекторних копій дисків; використання хеш-функцій (SHA-256) гарантує недоторканність доказів для можливого подальшого судового розгляду. Взаємодія передбачає 4-рівневу систему обміну інформацією (локальний–галузевий–національний–міжнародний), що дозволяє оперативно попереджати інші об'єкти про нові загрози через платформу MISP.

Практична реалізація методу була успішно здійснена з використанням стеку технологій та відповідних їм інструментів: Wazuh для моніторингу кінцевих точок та виявлення аномалій у реальному часі; ELK Stack (Elasticsearch, Logstash, Kibana) для централізованого збору та візуалізації терабайтів логів; TheHive для управління процесами розслідування інцидентів; MISP для автоматизованого оперативного обміну індикаторами загроз серед спільноти фахівців; криміналістичний софт включно з Autopsy (аналіз файлових систем), Volatility (аналіз оперативної пам'яті), Wireshark (мережева форензика).

Пропонований підхід може стати корисним для створення внутрішніх регламентів CSIRT-підрозділів, забезпечуючи швидке відновлення систем та недопущення повторних атак. Автоматизація через Wazuh дозволила скоротити час реакції на типові вектори атак (фішинг, несанкціонований доступ) на 30-40%. Алгоритм фіксації артефактів забезпечує повну реконструкцію дій атакуючого (dwell time, використані скрипти, канали витоку даних). Використання інструментів із відкритим кодом робить метод економічним і доступним для державних установ з обмеженим фінансуванням.

1. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA). 2025. URL: https://urli.info/1uHEw (date of access: 8.05.2026).

2. Річний звіт 2025: системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://urli.info/1uHEt (дата звернення: 8.05.2026).
3. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://urli.info/1pmEF (дата звернення: 8.05.2026).
4. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. International Organization for Standardization. 2023. URL: https://urli.info/1uHEW (date of access: 12.12.2025).
5. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://urli.info/1uHEA (date of access: 8.05.2026).
6. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. National Institute of Standards and Technology. https://urli.info/1pmEm (date of access: 8.05.2026).

Огляд підходів використання DGA алгоритмів

УДК 004.056

Петро Венгерський[1], Юрій Шпак[2]

Львівський національний університет імені Івана Франка,
[1]petro.venherskyy@lnu.edu.ua, [2]Yurii.Shpak@lnu.edu.ua

Сучасні кібератаки дедалі частіше використовують алгоритми генерації доменів (Domain Generation Algorithms, DGA) для забезпечення стійкого зв’язку шкідливого програмного забезпечення з серверами управління (C&C) [1]. Традиційні методи захисту, зокрема «чорні списки» (blacklisting) або статичні IP-адреси, є малоефективними проти DGA, оскільки зловмисники можуть генерувати сотні або тисячі нових доменів щодня, роблячи блокування неактуальним ще до його впровадження.

У зв’язку зі швидкою еволюцією кіберзагроз, зокрема переходом від випадкових наборів символів до словникових DGA, глибоке розуміння того, як і де застосовуються ці алгоритми, є важливим для розробки проактивних систем виявлення індикаторів компрометації [1].

В роботі проводиться системний огляд основних підходів до використання DGA-алгоритмів, проаналізувати механізми їхньої роботи («як вони використовуються») та ідентифікувати ключові вектори їх застосування зловмисниками («де саме»)[2].

На відміну від більшості робіт, які фокусуються переважно на методах виявлення (за допомогою машинного навчання чи аналізі DNS-трафіку), дане дослідження систематизує самі підходи до використання DGA з точки зору архітектури атаки. Проводиться аналіз еволюції вибору початкового "зерна" (seed) та генерації доменів залежно від типу загрози, що дозволяє краще зрозуміти тактичні цілі зловмисників.