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.

У ході огляду визначено основні підходи до того, як використовуються DGA:

- Псевдовипадкові генератори (PRNG): Використовують математичні функції та динамічне "зерно" (наприклад, поточну дату або публічні параметри) для створення великого обсягу доменів, які виглядають як випадковий набір літер та цифр.
- Словникові DGA (Dictionary-based): Комбінують легітимні слова з вбудованих словників, щоб імітувати звичайний трафік і обходити системи лексичного аналізу.
- Механізм відвернення уваги: Програма генерує тисячі DNS-запитів, але справжнім сервером управління виявляється лише один із них, що перевантажує системи моніторингу захисників.
- Щодо того, де саме вони використовуються:
- Управління ботнетами та троянами (C&C): Як основний або резервний канал зв'язку.
- Програми-вимагачі (Ransomware): Для передачі ключів шифрування на сервери зловмисників.
- Фішингові кампанії (наприклад, через SMS): Для швидкої генерації нових посилань з метою уникнення спам-фільтрів [2].

Використання алгоритмів генерації доменів стало стандартом для сучасного шкідливого ПЗ завдяки здатності забезпечувати стійкість ворожої інфраструктури. Аналіз DGA демонструє еволюцію від простої псевдовипадкової генерації до складних словникових та адаптивних алгоритмів. Розуміння специфіки їх використання, особливо в системах C&C та фішингових кампаніях, є важливою основою для створення нового покоління систем кіберзахисту.

У роботі систематизовано основні підходи до застосування алгоритмів генерації доменів у сучасних кібератаках, охарактеризовано псевдовипадкові та словникові DGA, а також механізми відвернення уваги захисників. Показано, що ефективність DGA визначається не лише кількістю згенерованих доменів, а й узгодженістю з тактикою атаки: від вибору «зерна» до імітації легітимної DNS-поведінки. Отримані результати підкреслюють необхідність поєднання технічних засобів виявлення з аналізом контексту застосування алгоритмів у ланцюгу компрометації. Подальші дослідження доцільно спрямувати на вдосконалення класифікації DGA-варіантів та інтеграцію таких знань у проактивні системи кіберзахисту.

1. "Large Language Models for Effective Detection of Algorithmically Generated Domains: A Comprehensive Review," *Computer Modeling in Engineering & Sciences (CMES)*, Tech Science Press, 2024. https://www.techscience.com/CMES/v144n2/63716/html
2. "An end-to-end framework for private DGA detection as a service," PubMed Central (PMC), 2024. https://pmc.ncbi.nlm.nih.gov/articles/PMC11355532/