Лайчук А.А., магістрант
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ ІНТЕГРОВАНОГО ПІДХОДУ В ЦИФРОВІЙ КРИМІНАЛІСТИЦІ ДЛЯ АНАЛІЗУ ДАНИХ І ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У сучасному цифровому середовищі кіберзлочинність зростає стрімкими темпами: за оцінками Cybersecurity Ventures, глобальні збитки від кіберзлочинів у 2024 році сягнули 9,5 трлн доларів США, що робить цифрову криміналістику критично важливою дисципліною [2]. Зловмисники дедалі частіше використовують шкідливе програмне забезпечення для крадіжки даних і фінансового шахрайства, як це було під час атак програм-вимагачів WannaCry (2017) та REvil (2021), які завдали багатомільярдних збитків і паралізували роботу організацій по всьому світу.

Цифрова криміналістика займається виявленням, збереженням, аналізом і документуванням цифрових доказів. Зародившись наприкінці 1970-х років у відповідь на зростання комп'ютерних злочинів, вона набула широкого розвитку з поширенням персональних комп'ютерів та Інтернету [3]. Сучасні методи цифрової криміналістики дозволяють відтворювати події кіберінцидентів навіть у складних сценаріях, коли зловмисники застосовують механізми маскування чи шифрування даних.

Інтегрований підхід до цифрової криміналістики передбачає поєднання різних методів та інструментів для глибокого аналізу цифрових даних, виявлення загроз та забезпечення цілісності доказової бази. Його ефективність зумовлена можливістю аналізу інцидентів на основі різних джерел даних і методів. Наприклад, використання мережевого аналізу у поєднанні з реверс-інжинірингом допомагає не лише виявити шкідливий трафік, а й зрозуміти механізми його поширення та функціонування, що суттєво прискорює реагування на інцидент.

Аналіз шкідливого програмного забезпечення поділяється на три основні підходи [1]:

- Статичний аналіз досліджує код і структуру програми без її запуску, використовуючи методи аналізу сигнатур, хешів, рядків, метаданих і дизасемблювання. Це дозволяє оцінити потенційні загрози без ризику зараження системи.
- Динамічний аналіз передбачає виконання програми в ізольованому середовищі (наприклад, віртуальній машині), щоб простежити її поведінку, мережеву активність і зміни у файловій системі.
- Гібридний аналіз комбінує обидва методи для повнішого розуміння загрози. Наприклад, під час розслідування атаки REvil у 2021 році гібридний підхід допоміг виявити зашифровані команди в коді та відстежити комунікацію з серверами зловмисників у пісочниці, що прискорило ідентифікацію джерела атаки.

Важливим аспектом інтегрованого підходу є також можливість адаптації до нових типів загроз. Із появою складніших поліморфних вірусів, які постійно змінюють свій код, комбінація статичного аналізу для виявлення базових сигнатур і динамічного для відстеження поведінки стає незамінною.

Для реалізації цих методів застосовуються спеціалізовані інструменти: Wireshark (аналіз трафіку), Volatility (дослідження пам'яті), Autopsy і FTK Imager (дослідження файлової системи та відновлення файлів), Ghidra і dnSpy (зворотна інженерія). Одним із практичних прикладів є використання Volatility у розслідуванні банківських атак, де аналіз дампу пам'яті допоміг виявити залишки шкідливого коду, який було видалено з диска, що дозволило відтворити ланцюг подій кіберінциденту.

Таким чином, інтегрований підхід у цифровій криміналістиці є важливим напрямком для забезпечення ефективного розслідування кіберзлочинів. Використання поєднання різних методів аналізу дозволяє отримати комплексне розуміння інциденту, підвищує ефективність дослідження та мінімізує ризики втрати або компрометації цифрових доказів. Це сприяє швидшому виявленню атак, визначенню їхніх джерел та створенню надійних механізмів захисту від подібних загроз у майбутньому.

Список використаних джерел:

1. Malware Analysis Techniques. *E-SPIN Group*. URL: https://www.e-spincorp.com/malware-analysis-techniques/
2. Boardroom Cybersecurity Report 2024. *Secureworks*. URL: https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024
3. What Is Digital Forensics?. *Simplilearn*. URL: https://www.simplilearn.com/what-is-digital-forensics-article