УДК 682.12

О. П. Войтович

Д. В. Саковський

Дослідження вимог до засобу збирання цифрових доказів

Вінницький національний технічний університет.

Анотація

Робота присвячена огляду та аналізу вимог до засобу збирання даних, які використовуються підчас реагування на кіберінциденти і є складовою частиною управління інцидентами інформаційною безпеки. Розглядаються методи та процеси, пов'язані з етапом збору цифрових доказів, а також визначаються важливі аспекти цього етапу.

Ключові слова: *Цифрові докази, збирання цифрових доказів, інциденти інформаційної безпеки, методи збирання цифрових доказів.*

Abstract

The paper is devoted to the review and analysis of the requirements for data collection tools used in cyber incident response and as an integral part of information security incident management. The methods and processes associated with the digital evidence collection stage are considered, and important aspects of this stage are identified.

Keywords*: Digital evidence, data collection module, collection process, collection methods, cyber evidence.*

Вступ

У сучасному світі з ростом використання цифрових технологій та збільшенням кількості цифрових пристроїв, збір цифрових доказів стає надзвичайно важливим етапом в системі управління інцидентами інформаційної безпеки. Цей етап дозволяє збирати інформацію з різних цифрових пристроїв і мереж для подальшого аналізу та, за потреби, використання в судових та дослідницьких процедурах. Актуальність роботи полягає в необхідності ефективного збору цифрових доказів для виявлення та розслідування кіберінцидентів, а також у підтримці правопорядку та захисті від кіберзагроз.

Результати дослідження

У процесі дослідження вимог до засобу збирання цифрових доказів, проаналізовані ключові аспекти, важливі для ефективного збору цифрових доказів згідно зі стандартом ISO 27035 [1].

Одним з таких аспектів є методологія, яка включає в себе процеси і методи, за допомогою яких здійснюється збір цифрових доказів. Важливо враховувати не лише технічні аспекти цього процесу, але й його відповідність вимогам правових норм та стандартів.

Згідно з ISO/IEC 27037 [2] пристрої та функції, що використовуються у зборі цифрових доказів, можуть бути різноманітними, включаючи цифрові носії інформації, мобільні пристрої, камери, комп'ютери та мережеві пристрої. Важливо мати на увазі, що список таких пристроїв є орієнтовним і не вичерпним, оскільки можуть існувати пристрої у різних формах та комбінаціях, а також нові технології можуть привести до появи нових пристроїв для збору цифрових доказів (рис.1).

Рисунок 1 - Пристрої

Вивчення вимог до засобу для збирання даних є важливим кроком у підготовці до роботи з цифровими доказами, а розуміння методології та криміналістичної готовності допомагає забезпечити ефективність та надійність цього процесу.

Правильно обрані методи збору та обробки цифрових доказів забезпечують надійність та автентичність отриманих даних. Використання відповідних методів, таких як

- створення образів цифрових носіїв[3];
- використання хеш-функцій для перевірки цілісності даних,

є важливими кроками у зборі та збереженні цифрових доказів.

Для забезпечення ефективності та надійності процесу збору цифрових доказів необхідно мати відповідну кваліфікацію та компетенцію у персоналу. Це стосується як Digital Evidence First Responders (DEFR), так і Digital Evidence Specialists (DES), які відповідають за проведення цього процесу та аналіз отриманих даних[4].

Важливою складовою засобу збору даних у вигляді цифрових доказів є розгляд різних типів цифрових пристроїв та функцій, які можуть використовуватися в різних обставинах. Врахування різноманітності пристроїв дозволяє розробляти адаптивні стратегії збору доказів.

Одним з ключових аспектів є: важливість зберігання цифрових доказів в безпечному середовищі - evidence preservation facility[5]. Це забезпечує збереження цілісності та конфіденційності доказів, що є критичним для забезпечення їх придатності та використання у судовому процесі.

Збір цифрових доказів має бути проведений у відповідності зі стандартами та рекомендаціями, такими як ISO/IEC 27037. Це дозволяє забезпечити їхню прийнятність та надійність у судовому процесі та інших важливих діях. Розгляд вимог до засобу збору даних показує важливість ретельного документування процесу збору цифрових доказів. Це включає в себе крім іншого:

- реєстрацію усіх кроків, виконаних під час збору доказів,
- зберігання інформації про джерела та методи збору.

Висновок

Загалом, в збиранні цифрових доказів важливо дотримуватись правильної методології та компетентного персоналу для ефективного та надійного збору цифрових доказів. Дотримання встановлених процедур та стандартів забезпечує необхідну довіру до отриманих доказів та підвищує їхню вагомість у судовому процесі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ISO/IEC 27035: Information technology. Information security incident management. Part 1: Principles and process [Електронний ресурс] https://www.iso.org/standard/78973.html
2. ISO/IEC 27037: Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence [Електронний ресурс] https://www.iso.org/standard/44381.html
3. Årnes, A. (Ed.). (2017). Digital forensics. John Wiley & Sons. [Електронний ресурс] https://books.google.com.ua/books?id=xqNaDwAAQBAJ&dq=digital+forensics+&lr=&hl=uk&source=gbs_navlinks_s
4. Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press. [Електронний ресурс] https://books.google.com.ua/books?id=xNjsDprqtUYC&dq=digital+forensics&lr=&hl=uk&source=gbs_navlinks_s
5. Interpol Digital forensics [Електронний ресурс] https://www.interpol.int/How-we-work/Innovation/Digital-forensics

Саковський Дмитро Володимирович – студент групи БКС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Войтович Олеся Петрівна - канд. техн. наук, доцент кафедри інформаційних технологій, Вінницький національний технічний університет

Sakovskyi Dmytro Volodymyrovych - student of group BCS-20b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Voitovych Olesia Petrivna - Candidate of Technical Sciences, Associate Professor of the Department of Information Technologies, Vinnytsia national technical university