УДК 004.056

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЖУРНАЛУ ПОДІЙ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS В ІНТЕРЕСАХ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Павленко В.С., Агасов С.М.
e-mail: vladyslav.pavlenko3@nure.ua, salman.agasov@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
ім. В.В. Поповського
м. Харків, Україна

The study presents the results of the analysis of the possibility of using the operating system event log for digital forensics. The structure and configuration of the event log are described. The requirements for the specifics of configuring and using the event log for digital forensics are described, namely: setting a specific event log configuration, setting a record retention policy, enabling advanced auditing for specific events, backing up and archiving the log, controlling access to the log, and others.

Журнали подій (Event Logs) операційної системи (ОС) Windows започатковано з версії Windows 3.1. В останніх версіях ОС Windows 10 та Windows 11 служба логування є критично важливою для діагностики функціонування операційної системи. Журнал подій ОС Windows є важливим джерелом інформації для цифрової криміналістики, оскільки він дозволяє **виявити сліди діяльності користувачів, встановити факт інциденту або кіберзлочинної поведінки в системі, відновити часову лінію подій та зібрати цифрові докази для розслідування**.

Особливістю використання журналу подій ОС Windows в інтересах цифрової криміналістики є з однієї сторони нескладна можливість перегляду журналу експертом різними інструментами, як то eventvwr.exe (інтегрований у Windows), LogParser.exe (Парсер від Microsoft), Event Log Explorer та інші. З іншої сторони це велика кількість даних, які генеруються в журналі. Тому розробка методів цифрової криміналістичної експертизи журналу подій ОС Windows є актуальним завданням.

Журнал подій ОС Windows містить наступні стандартні журнали, а також спеціальні журнали.

Application (додатки). Містить події, зареєстровані програмами. Наприклад, програма бази даних може записати помилку файлу.

Security (безпека). Містить такі події, як дійсні та недійсні спроби входу, а також події, пов’язані з використанням ресурсів, наприклад створення, відкриття або видалення файлів чи інших об’єктів.

System (система). Містить події, зареєстровані компонентами системи, як-от збій завантаження драйвера або іншого системного компонента під час запуску.

CustomLog (Користувацький журнал). Містить події, зареєстровані програмами, які створюють спеціальний журнал.

Конфігурація журналу подій. **Джерело подій (Event source).** Кожен запис містить інформацію про програму, службу або компонент системи, який її створив. **Ідентифікатор події (Event ID).** Кожна подія має унікальний **ідентифікатор події,** який допомагає визначити тип події та її причину. **Часові міткі (Timestamp).** Кожен запис містить точний **час виникнення події,** що дозволяє створювати хронологію дій у системі та інші. Перегляд журналу подій можливий з використанням фільтру, наприклад по ідентифікатору події.

Використання журналу подій для цифрової криміналістики потребує певних наступних налаштувань журналу та організації процесів, а саме:

- встановлення конфігурації журналу подій, яка має забезпечити максимальне збереження подій, деталізацію записів та неможливість їх втрати;
- встановлення політики збереження записів, при яких події не перезаписуються автоматично, а очищення записів можливо тільки адміністратором;
- увімкнення розширеного аудиту по подіям аутентифікації, керування обліковими записами, доступу до файлів, реєстру, мережних ресурсів, використання привілеїв, зміни політик;
- копіювання журналу на окремий сервер для його зберігання;
- використання точної синхронізації часу для побудови правильної тайм-лінії інциденту або злочину та правильної кореляції інформації про події, отриманої з різних систем;
- контроль доступу до журналу лише адміністратору та експерту-криміналісту;
- архівування журналу для збереження історії подій;
- створення банку подій з детальним їх описом, які можуть надати експерту-криміналісту максимальну інформацію про інциденти або злочини (далеко не усі події інформативні для криміналістики).

Таким чином використання журналу подій ОС Windows для цифрової криміналістики дає можливість проведення якісного розслідування інцидентів або злочинів. Але журнал подій створювався для адміністраторів системи, і для його використання експертом-криміналістом мають бути виконанні певні налаштування журналу подій та організація процесу роботи з журналом подій.

Список використаних джерел:

1.EVENTLOGRECORD structure (winnt.h). Microsoft. URL: http://msdn.microsoft.com/en-us/library/windows/desktop/ aa363646%28v =vs.85%29.aspx. (дата звернення: 12.03.2026).