2. Леонов Б. Д., Надіжко М. М. Науково-технічне забезпечення судово-експертної діяльності: сучасний стан та перспективи. *Юридичний вісник*. 2020. № 2 (55). С. 184—190.
3. Гончаренко В. Г. Науково-технічні засоби в роботі слідчого. Київ, 1972. 108 с.
4. Лисиченко В. К. Использование данных естественных и технических наук в следственной и судебной практике. Киев, 1979. 88 с.
5. Грамович Г. И. Проблемы теории и практики эффективного применения специальных знаний и научно-технических средств в раскрытии и расследовании преступлений : автореф. дис … докт. юрид. наук. — Киев, 1989. 43 с.
6. Біленчук П. Д., Колонюк В. П., Ярмолюк А. А. Криміналістика третього тисячоліття: освіта, наука, практика. *Теория и практика судебной экспертизы*. 2015. Вип. 60. С. 109.

Журнали подій операційних систем *Linux* в комп'ютерно-технічній експертизі

Юрій Божко,
Сумський НДЕКЦ МВС України, м. Суми, Україна, e-mail: yuriybozhko93job@gmail.com

У роботі розглянуто дослідження журналів операційних систем Linux, наведено перелік журналів, що існують у більшості дистрибутивів ОС Linux, та роз'яснено інформацію з деяких основних журналів.

Ключові слова: журнали подій; операційні системи; Linux; Ubuntu; Arch Linux; Red Hat.

Linux operating systems event logs in computer forensics

Yurii Bozhko

This paper outlines research on logs of Linux operating systems, provides a list of logs existing in most Linux OS distributions, and explains information from some main logs.

Keywords: event logs; operating systems; Linux; Ubuntu; Arch Linux; Red Hat.

Журнали операційних систем є важливою складовою комп'ютерно-технічної експертизи, що містять інформацію про те, як операційна система взаємодіє з різними програмами та апаратними засобами, які процеси відбуваються в системі, як вона зберігає та обробляє дані, які помилки та проблеми виникають у системі та як їх можна вирішити.

У комп'ютерно-технічній експертизі журнали операційних систем можна використати для відновлення подій, що сталися на комп'ютері. Наприклад, якщо комп'ютер було використано для злочинної діяльності, експерт може проаналізувати журнали операційної системи для визначення, які програми та файлові дії та коли було виконано та які дані було збережено на комп'ютері.

Журнали операційної системи також допомагають виявити технічні проблеми, які можуть бути пов'язаними з помилками в роботі операційної системи, вірусами або шкідливим програмним забезпеченням.

Наприклад, операційні системи сімейства *Linux* мають кілька базових журналів, які містить більшість дистрибутивів та які зберігають інформацію про різні системні події. До них належать:

- *syslog* — журнал системних подій;
- *kernel.log* — журнал подій, що стосуються ядра системи;
- *auth.log* — журнал авторизації та аутентифікації;
- *daemon.log* — журнал подій, пов'язаних із системними службами та «демонами»;
- *messages* — журнал повідомлень про стан системи та різні інформаційні повідомлення.

До нетипових журналів, що містять не всі дистрибутиви, належать:

- *apache access log* — журнал доступу до вебсервера *Apache* з інформацією про запити до вебсайту, що обробляє сервер;
- *apache error log* — журнал вебсервера *Apache* з інформацією про помилки, що сталися під час оброблення запитів до вебсайту;
- *MySQL log* — журнал запитів і відповідей бази даних *MySQL*;
- *cron log* — журнал виконання розкладів *cron* з інформацією про заплановані завдання та їх виконання;

- *SSH log* — журнал доступу до *SSH*-сервера з інформацією про спроби входу до системи через *SSH*-протокол.

Ці списки можуть змінюватися, оскільки кожен дистрибутив ОС *Linux* може мати власний набір журналів, які можуть різнитися залежно від конфігурації системи та встановлених компонентів.

Журнал *syslog* зберігає інформацію про системні події, що сталися в ОС *Linux* (зокрема, події мережі; запуск або завершення служб; проблеми зі стартом системи; помилки, пов'язані з драйверами пристроїв тощо).

Наприклад, розберемо деякі рядки з журналу *syslog*.

```
Feb 25 09:43:22 server sshd[1234]:
Failed password for root from 192.0.2.1
port 1234 ssh2
```

У цьому рядку ми бачимо дату та час події (25 лютого 09:43:22), назву сервера (*server*) та «демона», який обробляв запит (*sshd[1234]*), повідомлення про те, що авторизація користувача *root* на сервері не вдалася (*Failed password for root*), та інформацію про *IP*-адресу та порт, з яких було виконано запит (*192.0.2.1 port 1234 ssh2*).

```
Feb 26 10:20:10 server kernel:
[  20.123456] ata1: link is slow to
respond, please be patient (ready=0)
```

У цьому рядку ми бачимо дату та час події (26 лютого 10:20:10), назву сервера (*server*) та «демона», який обробляв запит (*kernel*), повідомлення про те, що диск на контролері *ATA* не відповідає на запити, тому потрібно зачекати (*ata1: link is slow to respond, please be patient (ready=0)*). У квадратних дужках зазначено час від моменту запуску системи, що допомагає визначити часові межі помилки.

У журналі *kernel.log* зберігається інформація про події, пов'язані з ядром операційної системи *Linux* (зокрема, повідомлення про помилки в роботі драйверів пристроїв; статистика використання ресурсів системи; повідомлення про завантаження ядра; інформація про процеси, що виконуються в системі, та ін.).

Розберемо кілька рядків з журналу *kernel.log*.

```
Feb 25 09:43:22 server kernel:
[  20.123456] ata1: link is slow to
respond, please be patient (ready=0)
```

У цьому записі журналу ми бачимо дату та час події (25 лютого 09:43:22), назву сервера (*server*) та журналу (*kernel*), повідомлення про те, що диск на контролері *ATA* не відповідає на запити, тому потрібно зачекати (*ata1: link is slow to respond, please be patient (ready=0)*). У квадратних дужках зазначено час із моменту запуску системи, що допомагає визначити часові координати помилки.

```
Feb 26 10:20:10 server kernel:
[  21.123456] eth0: link up (1000Mbps/
Full duplex)
```

У цьому записі ми бачимо дату та час події (26 лютого 10:20:10), назву сервера (*server*) та журналу (*kernel*), повідомлення про те, що мережевий інтерфейс *eth0* було успішно підключено до мережі зі швидкістю 1000 *Mbps* та повнодуплексним режимом (*eth0: link up (1000Mbps/Full duplex)*).

Журнал *auth.log* містить інформацію про події, пов'язані з авторизацією в операційній системі (зокрема, повідомлення про спроби входу до системи, інформація про вхідні та вихідні з'єднання, повідомлення про помилки аутентифікації та ін.).

Наводимо кілька рядків з журналу *auth.log*.

```
Feb 25 09:43:22 server sshd[1234]:
Failed password for user john from
192.168.0.1 port 1234 ssh2
```

У цьому рядку ми бачимо дату та час події (25 лютого 09:43:22), назву сервера (*server*) та журналу (*auth.log*), повідомлення про невдалу спробу авторизації користувача *john* (*Failed password for user john*) за допомогою *SSH*-з'єднання з *IP*-адресою 192.168.0.1 та портом 1234.

У журналі *daemon.log* зберігається інформація про системні «демони», які запускаються на операційній системі *Linux*. Це можуть бути повідомлення про старт, зупинки та помилки «демонів», що відповідають за роботу різноманітних сервісів і програм на системі.

Розглянемо кілька рядків з журналу *daemon.log*.

```
Feb 25 09:12:34 server systemd[1]:
Starting LSB: Apache2 web server...
```

У цьому рядку ми бачимо дату та час події (25 лютого 09:12:34), назву сервера (*server*) та журналу (*daemon.log*), повідомлення про ініціалізацію системного «демона» *Apache2 web server* за допомогою *LSB*.

```
Feb 26 10:00:01 server CRON[1234]:
(root) CMD ( /usr/local/bin/backup.sh )
```

У цьому рядку ми бачимо дату та час події (26 лютого 10:00:01), назву сервера (*server*) та журналу (*daemon.log*), повідомлення про те, що запустився *cron*-демон (*CRON*) і виконується команда */usr/local/bin/backup.sh* для користувача *root*.

Записи журналів можуть допомогти виявити проблеми в системі, такі як помилки в програмах,

проблеми з обладнанням та безпекою. Більше того, журнали є важливим інструментом для аналізування діяльності користувачів у системі та виявлення несанкціонованого доступу.

Журнали є важливим джерелом інформації для комп'ютерно-технічної експертизи, які дають змогу відновлювати хронологію подій системи та відстежувати активність користувачів, що є важливим для збирання даних у комп'ютерно-технічній експертизі.

Перелік джерел посилання

1. The Linux Kernel documentation / The Linux Kernel Archives. URL: https://www.kernel.org/doc/html/latest/ (дата звернення: 02.02.2023).
2. The Linux Documentation Project. URL: http://tldp.org/ (дата звернення: 02.02.2023).
3. Linux.com. URL: https://www.linux.com/ (дата звернення: 02.02.2023).
4. Linux Logging Basics / SolarWinds. URL: https://www.loggly.com/ultimate-guide/linux-logging-basics/ (дата звернення: 02.02.2023).
5. Viewing and monitoring log files / Ubuntu. URL: https://ubuntu.com/tutorials/viewing-and-monitoring-log-files#1-overview, https://ubuntu.com/tutorials/viewing-and-monitoring-log-files#2-log-files-locations, https://ubuntu.com/tutorials/viewing-and-monitoring-log-files#3-viewing-logs-using-gnome-system-log-viewer (дата звернення: 02.02.2023)
6. systemd/Journal / Arch Linux Wiki. URL: https://wiki.archlinux.org/title/Systemd/Journal (дата звернення: 02.02.2023).
7. Red Hat Training. Chapter 23. Viewing and Managing Log Files / Red Hat Customers Portal. URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-viewing_and_managing_log_files (дата звернення: 02.02.2023).

Судово-балістичне дослідження окремих моделей військової вогнепальної зброї спеціального призначення

Володимир Бондар,
канд. юрид. наук, доцент, Луганський ННІ ім. Е. О. Дідоренка Донецького державного університету внутрішніх справ, м. Івано-Франківськ, Україна, ORCID: https://orcid.org/0000-0003-1552-4555, e-mail: bondarlivd@gmail.com

Запропоновано оцінити ефективність та обґрунтованість викладених теоретичних положень шляхом їх експериментальної апробації на практиці експертами-балістами.

Ключові слова: вогнепальна зброя спеціального призначення; експерт-баліст; науково-методичне забезпечення.

Forensic-ballistic research of individual models of special-purpose military firearms

Volodymyr Bondar

This paper proposes to evaluate the effectiveness and validity of the stated theoretical provisions by means of their experimental approbation in practice by ballistics experts.

Keywords: special-purpose firearms; ballistics expert; scientific and methodological support.

Важливою складовою сил російського агресора у війні проти України є сили спеціальних операцій зс рф, на озброєнні яких є військова вогнепальна зброя спеціальної призначеності. У питаннях протидії органів правопорядку та судово-експертних установ України злочинам, скоєним військослужбовцями рф із застосуванням такої зброї важлива роль належить оптимізації науково-методичного забезпечення виявлення, розкриття та розслідування даних злочинів, пошуку нових засобів та методів судово-балістичного дослідження вогнепальної зброї, боєприпасів та слідів їх застосування. Специфіка конструктивних рішень, що застосовуються для розробки військової зброї спеціального призначення актуалізує проблему розв'язання класифікаційних та діагностичних завдань, як то:

- діагностика фактів застосування військової вогнепальної зброї (боєприпасу) спеціального призначення за слідами на стріляних кулях, гільзах, а також перешкодах та визначення моделі такої зброї;
- дослідження окремих зразків вогнепальної зброї на предмет визначення їх цільового призначення.