Наукова складова технічного забезпечення судової інженерно-технічної експертизи

Ігор Богданюк,
канд. юрид. наук, ст. дослідн., засл. юрист України, ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», м. Харків, Україна, ORCID: https://orcid.org/0000–0003–4782–9986, e-mail: bogdanyuk.hniise@gmail.com

Наукову складову технічного забезпечення судових інженерно-технічних експертиз запропоновано розглядати з позицій науково-технічного та науково-методичного забезпечення. Визначено поняття «науково-технічнт забезпечення» та окреслено складові наукового забезпечення експертної діяльності в галузі судової інженерно-технічної експертизи.

Ключові слова: технічне забезпечення; наукова складова; судова експертиза; інженерно-технічна експертиза.

Scientific component of technical support of forensic engineering and technical examination

Ihor Bohdaniuk

It is proposed to consider the scientific component of technical support of forensic engineering and technical examinations from the standpoint of scientific-technical support and scientific-methodological support. The scientific and technical support concept is defined and components of scientific support of forensic expert activities in the field of forensic engineering and technical examination are outlined.

Keywords: technical support, scientific component, forensic examination, forensic engineering and technical examination.

Зауважимо, що роль науки в сучасному світі постійно зростає та перетворюється уf безпосередню продуктивну силу, яка здатна розв'язати будь-які завдання в галузі соціального, економічного або культурного життя людей. Це з особливою гостротою виокремлює питання щодо призначення науки, мету й завдання її розвитку в конкретній практичній діяльності людини. Повною мірою це стосується й питань науково-технічного забезпечення судових інженерно-технічних експертиз. За всім цим стоїть специфічна за формою та змістом діяльність, яка зумовлює необхідність принципово іншого підходу до її організаційного, правового, наукового та технічного забезпечення.

На підставі аналізу дефініцій «науково-технічне забезпечення», що існує в науці [1, с. 184], на погляд окремих учених, науково-технічне забезпечення судово-експертної діяльності полягає в пошуку, виборі, пристосуванні, розробленні та використанні досягнень науково-технічного прогресу (загально-технічних, пристосованих і спеціально розроблених приладів, пристроїв, апаратури, обладнання, інструментів, програмних засобів, матеріалів, а також методів і прийомів їх застосування) з метою найбільш ефективного виконання експертних досліджень [2].

Основним завданням науково-технічного забезпечення судово-експертної діяльності слід визнати створення таких умов, за яких значно підвищується ефективність роботи судового експерта за допомогою сучасних технологічних науково-технічних засобів і методів. Наукову складову технічного забезпечення судових інженерно-технічних експертиз доцільно розглядати з позицій:

- науково-технічного забезпечення (пошук, вибір, пристосування та використання досягнень науково-технічного прогресу в процесі експертних досліджень);
- науково-методичного забезпечення (розроблення рекомендацій та експертних методик, створення необхідних умов для використання сприйняття та застосування цих матеріалів із урахуванням наявного устаткування та обладнання).

Розроблення наукових основ і положень, що визначають змістову сторону експертної діяльності є сферою науково-технічного забезпечення. Проблемам науково-технічного забезпечення практики розкриття, розслідування, попередження правопорушень і місцю в цих процесах судових експертиз свого часу було присвячено доволі багато ґрунтовних праць учених-криміналістів [3; 4]. Наприклад, Г. І. Грамович доводив, що науково-технічне забезпечення — це регламентована нормативними актами діяльність науково-дослідних, судово-експертних та інших установ, а також відповідних посадових осіб, на яких покладається обов'язок із розроблення та

реалізації комплексу взаємопов'язаних заходів із метою створення умов для ефективного застосування спеціальних знань і науково-технічних засобів у протидії правопорушенням [5].

Наукові дослідження в галузі технічного забезпечення експертних досліджень у процесі проведення судових інженерно-технічних експертиз можна об'єднати за видами у дві великі групи: наукові узагальнення та наукові розробки. Кожна із груп відповідає основним типам наукових досліджень — теоретичному та експериментальному, а також інформаційним формам, у яких наукові дослідження реалізуються в навчальних і методичних посібниках; наукових статтях, що містять теоретичні й практичні положення; експертних методиках і рекомендаціях; технічних удосконаленнях тощо. Важливим завданням залишається удосконалення наявних методичних рекомендацій для забезпечення потреб експертної діяльності в галузі судових інженерно-технічних експертиз.

Аналіз напрацювань науковців [1] дає змогу віднести до наукового забезпечення експертної діяльності в галузі судової інженерно-технічної експертизи:

- наукове тлумачення законодавчих актів із технічного забезпечення експертних досліджень і розроблення пропозицій щодо їхнього удосконалення;
- наукове розроблення проєктів підзаконних актів, пов'язаних із технічним забезпеченням судової експертизи (наприклад наказів, інструкцій, положень, настанов тощо);
- наукове узагальнення практики використання технічних засобів і розроблення пропозицій із її вдосконалення;
- розроблення з урахування потреб судової практики нових технічних засобів і методів експертного дослідження;
- наукову апробацію приладів і матеріалів, які виготовляють на підприємствах різних міністерств із метою визначення можливості їх використання експертами в процесі проведення інженерно-технічних експертиз;
- наукове розроблення прийомів, методів і методик виявлення, фіксації, вилучення й дослідження речових доказів;
- розроблення навчальних програм і методичної літератури з питань підготовки експертних кадрів у галузі судової інженерно-технічної експертизи;
- проведення судовими експертами практичних занять із питань судової інженерно-технічної експертизи зі слідчими, дізнавачами, експертами-криміналістами та курсантами для окреслення нових методів і засобів, які застосовуються під час проведення судових експертиз;
- вивчення й розповсюдження зарубіжного досвіду з використання нових засобів і методів під час проведення експертизи.

Зауважимо, що в судовій інженерно-технічній експертизі методи дослідження й технічні засоби запозичуються із природничих, технічних і багатьох інших наук, однак для проведення експертизи вони, як правило, трансформуються, набувають вигляду, який зумовлено своєрідністю завдань і специфічністю об'єктів експертизи. Тому запозичені методи дослідження та технічні засоби відрізняються якісно новими формами та процедурами їх реалізації — своєрідністю застосування підходів до дослідження й системою використання технічних засобів.

Наголосимо, що наявність високотехнологічного обладнання в експертних лабораторіях, автоматизованих робочих місць експертів, апаратних комплексів дає змогу ефективно виконувати завдання експертизи з мінімальними похибками та водночас зменшити експертні помилки. Це обумовлено тим, що за таких умов більшість процесів відбувається без участі людини — в автоматичному режимі. При цьому достовірність отриманих результатів значно вища, а строки проведення експертизи зазвичай менші.

Сучасні тенденції автоматизації, комп'ютеризації, інформатизації суспільного життя зумовлюють створення якісно нового напряму криміналістичної науки — «електронної криміналістики» [6]. Суттєвим залишається питання забезпечення доступу експерта до інформації про останні досягнення науки і техніки. Можна стверджувати, що поступово формується новий напрям матеріально-технічного забезпечення — інноваційне забезпечення судової інженерно-технічної експертизи.

Перелік джерел посилання

1. Павлишин Б. О. Наукова складова техніко-криміналістичного забезпечення досудового розслідування вбивств. *Підприємництво, господарство і право*. 2017. № 6. С. 183—187.

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;