DOI: https://doi.org/10.33994/kndise.2020.65.22
УДК 343.98

Лариса Володимирівна Борисова
кандидат юридичних наук, доцент,
доцент кафедри організації та технічного забезпечення
аварійно-рятувальних робіт

ORCID 0000-0001-6554-1949
E-mail: larisa.borysova@gmail.com

Національний університет цивільного захисту України

Петро Дмитрович Біленчук
кандидат юридичних наук, доцент, професор кафедри кримінального
права та процесу юридичного факультету

ORCID ID 0000-0002-9599-0347
E-mail: aur.consalt@gmail.com;

Національний авіаційний університет

Микола Іванович Малій
директор

E-mail: aur.consalt@gmail.com

Правнича компанія ТОВ «АЮР-КОНСАЛТИНГ»

Валентина Степанівна Виноградова
молодший науковий співробітник
відділу нормативно-методичної діяльності та стандартизації
лабораторії організації наукової, методичної діяльності
та міжнародного співробітництва

E-mail: nauka@kndise.gov.ua

ЕКСПЕРТИЗА ЯК ЗАСІБ УСТАНОВЛЕННЯ ФАКТІВ І ОБСТАВИН ВЧИНЕННЯ ТРАНСНАЦІОНАЛЬНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Розглядаються проблемні питання, пов'язані із збиранням та дослідженням доказової інформації під час експертизи комп'ютерної техніки і програмних продуктів, визначаються обставини, що підлягають обов'язковому встановленню і доказуванню за даним видом злочинів.

Ключові слова: *транснаціональні комп'ютерні злочини, експертиза, ідентифікаційні та не ідентифікаційні ознаки.*

О. Ф. Коні у статті «Суд – наука – мистецтво» відмічав, що «судова практика дуже часто примушує звертатися до спеціальних досліджень, зосереджуючи на них тягар справи, або звертатися за допомогою до обізнаних людей, тобто експертів, у різних спеціальних галузях знань, мистецтв і ремесел»[1, с.34-38].

Б. М. Шавер ще у 1938 році зробив правильний висновок, що для забезпечення високого рівня розслідування необхідно «пристосувати дані природознавчих і технічних наук до завдань розслідування. Разом із тим пристосувати до завдань розслідування дані, що отримані в результаті вивчення діяльності злочинця, тим самим розробити систему прийомів і методів виявлення й дослідження доказів» [2, с.68]. У 1949 році А. І. Вінберг уперше порушив питання про введення в кримінальний процес поряд з експертом такої особи, як спеціаліст, функції якої мають бути відмінними від функцій експерта [3, с. 21-25, с. 131-133; 4, с. 31-32].

У кримінально-процесуальній діяльності спеціальні знання використовуються у двох формах – при залученні спеціалістів під час окремих слідчих чи судових дій та в межах проведення експертизи. Проведення судової експертизи регламентується Законом України «Про судову експертизу», Кримінально-процесуальним кодексом України, Цивільно-процесуальним кодексом України, Інструкцією про організацію провадження судових експертиз у науково-дослідних судово-експертних установах Міністерства юстиції України від 08.10.1998 № 53/5, Положенням про експертну службу МВС України від 20.06.2000 № 988.

Судова експертиза – це слідча дія з організації тактики застосування спеціальних знань експерта для дослідження за дорученням слідчого і суду речових доказів та інших матеріалів справи з метою одержання доказової інформації [5, с. 399]. У ході досудового слідства використовують дванадцять класів судових експертиз. З середини 90-х років започатковано новий вид судових експертиз, який у 1996 році було запропоновано називати комп'ютерно-технічною експертизою і включити його в клас інженерно-технічних експертиз, оскільки своїм народженням обчислювальна техніка зобов'язана саме інженерно-технічним наукам [6, 160].

Основними завданнями експертизи комп'ютерної техніки і програмних продуктів у відповідності з Науково-методичними рекомендаціями з питань підготовки та призначення судових експертиз, затверджених наказом Міністерства юстиції України від 08.10.1998 № 53/5 є:

– становлення технічного стану комп'ютерної техніки;

– виявлення інформації, що міститься на комп'ютерних носіях та визначення її цільового призначення;

– встановлення відповідності програмних продуктів певним параметрам;

– встановлення авторства програмного продукту;

– встановлення вартості програмного продукту;

– встановлення вартості комп'ютерної техніки.

Використання висновку експерта потребує від слідчого перш за все оцінки його як рівноправного доказу в системі збирання доказів за справою.

Готуючись до проведення комп'ютерно-технічної експертизи слідчий повинен визначити обставини, що підлягають обов'язковому встановленню і доказуванню за даним видом злочинів, формулювання і «бажано, щоб кінцева редакція питань складалася за участю самого експерта після попереднього ознайомлення його з обставинами справи і зібраними матеріалами» [7, с. 217]. Пропонується ставити такі питання:

– Яка модель комп'ютера надана на дослідження, її технічні характеристики, параметри периферійних пристроїв?

– Чи є неполадки в окремих пристроях, носіях інформації і чи можливо виявити їх тестовими програмами?

– Які технічні пристрої використовуються для захисту інформації та які їхні характеристики?

– Чи зазнавали засоби захисту інформації програмної модифікації або фізичного впливу?

При експертизі даних і програмного забезпечення мережі з'ясовуються такі питання:

– Який тип і версія операційної системи, що використовується в комп'ютері, ліцензійні чи «піратські» копії?

– Для яких прикладних задач застосовуються дані програмні продукти?

– Які програмні засоби захисту використовуються (ідентифікаційні коди, паролі, ідентифікація клавіатурного почерку, програми захисту, розмежування доступу та ін.)?

– Чи змінювався зміст файлів, яких саме і в чому це виражалося?

– Чи були збої в роботі окремих програм і в чому вони проявлялися?

– Як технічно здійснене з'єднання комп'ютерів у мережу, чи є вихід у глобальну комп'ютерну мережу?

– Який розмір і вид завданих збитків (слід враховувати не тільки розкрадання коштів, програм, послуг, інформації, а також моральний зиск, наприклад, у разі не проходження банківських платежів)?

Значну допомогу в дослідженні апаратних і програмних засобів комп'ютерної техніки може надати вирішення наступних завдань:

– відновлення витертих файлів і записів у базах даних, уточнення часу знищення, внесення змін, копіювання й модифікації комп'ютерної інформації;

– визначення часу введення в комп'ютер певних файлів, записів у бази даних;

– подолання рубежів захисту, підбирання паролів, розшифрування закодованих файлів, іншої інформації;

– визначення технічного стану і справності засобів обчислювальної техніки;

– виявлення каналів витоку інформації з локальних і глобальних мереж.

Наприклад, О. Р. Россинська вважає, що ціллю комп'ютерно-технічної експертизи є: вивчення конструктивних особливостей і стану комп'ютера, його периферійних пристроїв, магнітних носіїв, комп'ютерних мереж, а також причин виникнення збоїв у роботі; вивчення інформації, що зберігається в комп'ютері та магнітних носіях; рішення питань ідентифікаційного характеру [8, с. 76].

В. О. Голубєв пропонує виділяти наступні види комп'ютерно-технічних експертиз:

– технічна експертиза комп'ютерів і периферійних пристроїв (технічних особливостей комп'ютера, його периферійних пристроїв, технічних параметрів комп'ютерних мереж, а також причин збоїв у роботі комп'ютерного обладнання);

– технічна експертиза обладнання захисту комп'ютерної інформації (пристрої захисту інформації);

– експертиза машинних даних і програмного забезпечення ЕОМ (інформації, що зберігається в комп'ютері та на магнітних носіях, у тому числі, вивчення програмних методів захисту комп'ютерної інформації) [9, с. 143-144].

В. О. Усов дотримується думки, що видова класифікація комп'ютерно-технічної експертизи така:

– апаратно-комп'ютерна експертиза – проведення діагностичного дослідження технічних (апаратних) засобів комп'ютерної техніки, визначення функціональних можливостей фактичного і початкового стану, технологій виготовлення, експлуатаційних режимів;

– програмно-комп'ютерна експертиза функціонального призначення, характеристик і реалізації вимог, алгоритму і структурних особливостей користувальницького стану представленого на дослідження системного, прикладного і авторського програмного забезпечення комп'ютерної системи як видових об'єктів експертизи;

– інформаційно-комп'ютерна експертиза для отримання доказової інформації шляхом вирішення більшості діагностичних й ідентифікаційних питань, що пов'язані з комп'ютерною інформацією;

– комп'ютерно-мережева експертиза ґрунтується на функціональному призначенні комп'ютерних засобів, які реалізують будь-яку мережеву інформаційну технологію [10].

За характером розв'язуваних завдань експертизи поділяються на ідентифікаційні й неідентифікаційні (діагностичні та ситуаційні). Ідентифікаційне дослідження спрямоване на встановлення тотожності об'єкта, діагностичне – вирішує завдання встановлення часу події, механізму дій; ситуаційна експертиза використовує різноманітні спеціальні знання, що дають можливість досліджувати всю матеріальну обстановку місця події в комплексі та вирішувати такі питання, як встановлення способу вчинення злочину, спосіб дії осіб, які перебували на місці злочину тощо.

Слідчий не в змозі відстежувати всі технологічні зміни в сфері інформаційних технологій і для дослідження слідів комп'ютерних злочинів особливу увагу належить приділяти використанню можливостей експертизи комп'ютерних систем і машинних носіїв. Пропонуємо за допомогою комп'ютерно-технічної експертизи вирішувати такі завдання.

Ідентифікаційні:

– діагностика системних процесів і поведінки системи;

– ідентифікація системи;

– системний аналіз обставин місця події;

– реконструкція обставин місця події методами математичного аналізу і комп'ютерного моделювання;

– діагностика ролі та функціонального призначення окремих елементів комп'ютерної системи, системи інтелектуального злому;

– ідентифікація автора комп'ютерного тексту.

Неідентифікаційні:

– визначення структури й функцій телекомунікаційних систем і засобів електронної пошти;

– визначення елементів системи та її мереж;

– реконструкція й прогнозування поведінки системи;

– визначення надійності та стійкості комп'ютерних систем;

– віднесення інформації до категорії програмного забезпечення;

– віднесення конкретних програм до шкідливих;

– визначення семантики і граматики спірних текстів;

– діагностика і класифікація принтерів, факсів, копіювальної техніки за текстом, який виготовлено з їхнім застосуванням.

Сліди комп'ютерного злочину можуть бути вилучені спеціалістом або експертом при проведенні експертного дослідження комп'ютерних систем, їхніх мереж і периферійного обладнання.

Для проведення антивірусного тестування та аудиту мережі експерт повинен отримати права адміністратора (кореневого користувача або root), тобто мати повний контроль над роботою системи, доступ до всіх файлів і виключне право запускати певні програми.

У висновку висвітлюються факти фіксації інформаційних слідів-відображень про дії шкідливих програм:

– зміна розмірів файлів, що виконуються;

– зменшення об'ємів вільної оперативної пам'яті;

– поява кластерів магнітних носіїв, які позначені як не використовувані;

– зміна приймача інформації, призначеного системою;

– поява невідомих файлів;

– стирання окремої інформації на диску або його форматування;

– заміна перших чи останніх байтів блоку записів;

– заміна окремих символів.

Після закінчення аудиту експертом робиться оцінка зовнішніх файлових слідів (атрибутів файлів, їхніх розмірів, типу, імені, розширення, часу створення і/або модифікації). Дослідження інформаційних слідів-відображень – пошук вилучених файлів, частин файлів, які були спеціально вилучені (приведені в непридатність) до початку огляду чи випадково в процесі огляду, треба проводити в лабораторних умовах.

Для криміналістичного дослідження операційних систем експертом проводиться перевірка системного журналу, журналу захисту і журналу додатків із застосуванням документів, які регламентують правила архівації журналів реєстрації. Доказом правильності роботи комп'ютерної системи є підтримка протоколу операційної системи, яка реєструє всі етапи роботи системи, а також реєстрація всіх повідомлень про системні збої чи подібних інцидентів за допомогою системного журналу.

Більшість зловмисників намагається сховати сліди своєї присутності (у тому числі й в системному журналі). Варто звертати увагу:

– на невеликі або незрозумілі журнали;

– журнали із «дивними» мітками;
– реєстрацію користувачів з невірними правами доступу;
– записи про перезавантаження та перезапуск служб;
– відсутність системних журналів;
– su-записи чи реєстрація з дивних місць.

Для дослідження цілісності системи особливо доречною є увага на журнал захисту, в якому вміщується заголовок і номер версії, що знаходяться на початку кожного файлу журналу (події можуть бути відсортовані по елементам заголовків і категоріям).

Криміналістичне дослідження систем управління базами даних передбачає:

– аудит операторів – відстеження операторів особливого типу для одного або декількох користувачів;

– аудит привілей – відстеження дій, що пов'язані з певними привілеями в системі для одного або декількох користувачів;

– аудит об'єктів – відстеження конкретних операторів особливої схеми об'єктів для всіх користувачів бази даних.

У своєму висновку експерт висвітлює результати аудитів, до висновку додаються звіти, що були генеровані відповідним програмним забезпеченням, копії на машинних носіях, які отримані при проведенні фізичної фіксації.

Криміналістичному дослідженню документів, виконаних з використанням засобів комп'ютерної техніки, підлягають:

– програмне забезпечення принтера (знакогенератор, мова керування принтером);

– елементи виконавчого механізму принтера.

Варто звертати увагу на відстань між відбитками голок друкуючої головки принтера, розмір і форму відбитків, відносну інтенсивність забарвлення відбитків.

Поряд із основними завданнями при проведенні експертизи можливе вирішення питань допоміжного характеру, а саме:

– оцінка вартості комп'ютерної техніки, периферійних пристроїв, магнітних носіїв, програмних продуктів, перевірка контрактів на постачання;

– визначення рівня професійної підготовки окремих осіб у галузі програмування і роботи із засобами комп'ютерної техніки.

Наприклад, з точки зору використання прихованого моніторингу комп'ютерних систем є ідентифікація користувача за допомогою клавіатурного почерку. Клавіатурний почерк – це набір динамічних характеристик роботи на клавіатурі, а саме швидкість набору символів, звичка використовувати основну чи допоміжну частину клавіатури, особливості «подвійних» або «потрійних» натискань на клавіші, улюблені прийоми управління комп'ютером. Сучасна ідентифікація клавіатурного почерку полягає у виборі відповідного еталону зі списку збережених у пам'яті комп'ютера еталонів, на основі оцінки подібності до цього еталона параметрів почерку одного з користувачів, які мають право на роботу з цим комп'ютером. Класичний статистичний підхід до ідентифікації користувача за допомогою клавіатурного почерку (набору ключових слів) виявив ряд

особливостей: залежність почерку від буквених сполучень у слові, існування зв'язків між набором окремих символів, наявності «затримань» під час введення символів, залежність швидкості введення слів від їхнього змісту, відносний час натиску різних клавіш, а також важливою характеристикою біометричної ідентифікації є довжина парольної фрази. Практика показує, що довжина парольної фрази повинна легко запам'ятовуватися і складатися від 21 до 42 натискань на клавіші. Таким чином, особливості клавіатурного почерку виявляються двома методами: набором ключової фрази і набором «вільного» тексту.

Як показує практика:

– основні види комп'ютерно-технічних експертиз застосовуються комплексно і, найчастіше, послідовно;

– встановлення причетності тієї чи іншої особи до здійснення злочину можливо при вирішенні ідентифікаційних задач і, відповідно, питання ідентифікаційного характеру представляються більш важливими для слідства і суду. Ці аспекти знайшли відображення в новітніх наукових дослідженнях в галузі кібербезпеки критичної інфраструктури, кіберзахисту та кібероборони [11;12;13].

Перелік посилань

1. *Кони А. Ф.* Собрание сочинений: в 8 т. / под общ. ред. В. Г. Базанова и др. Москва: Юрид. лит., 1967. Т. 4. 543 с., С. 34-38.

2. *Шавер Б. М.* Предмет и метод советской криминалистики.*Социалистическая законность.* 1938. № 6. С. 56-82.

3. *Винберг А. И.* Криминалистическая экспертиза в советском уголовном процессе. Москва: Госюриздат, 1956. 220 с.

4. *Винберг А. И.* Специалист в процессе предварительного расследования. *Социалистическая законность*. Москва, 1961. № 9. С. 31-32

5. *Салтевський М. В.* Криміналістика: навч.-довід. посіб. Київ: НВТ "Правник", 1996. 159 с.

6. *Панов М. І., Шепітько В. Ю., Коновалова В. О. та ін.* Настільна книга слідчого: наук.-практ. вид. для слідчих і дізнавачів. Київ: Видав. Дім „Ін Юре", 2003. 715 с.

7. *Криминалистика*: в 2-х кн.: учеб. пособ. для слушателей правовых вузов,

References

1. *Koni, A. F.* (1967). Collected Works: In 8 Vols. Bazanova, V.G. et al. (Eds.) M.: Yurid. lit. Vol. 4. 543 p., P. 34-38. (In Russian).

2. *Shaver, B. M.* (1938). The subject and method of Soviet forensics. *Socialist Legality*. No. 6. P. 56-82. (In Russian).

3. *Vinberg, A. I.* (1956). Forensic expertise in the Soviet criminal trial. M.: Gosiurizdat, 220 p. (In Russian).

4. *Vinberg, A. I.* (1961). Specialist in the process of preliminary investigation. *Socialist legality*. Moscow. No. 9. P. 31-32 (In Russian).

5. *Saltevskyi, M. V.* (1996). Criminalistics: educational texbook. Kyiv: NVT "Pravnyk", 159 p. (In Ukrainian).

6. *Panov, M. I., Shepitko, V. Yu., Konovalova, V. O.* et al (2003). Handbook of an investigator: a scientific and practical publication for investigators. K.: Publishing House "In Yure". 715 p. (In Ukrainian).

7. *Vishinskii, A. Ia.* (Ed.) (1935). Forensics: In 2 books: textbook for students of law

НИИ угол. политики при прокуроре СССР, Верховном Суде СССР И НКЮ РСФСР / под ред. А. Я. Вышинского. Москва: Сов. Законодательство. 1935. Кн. 1: Техника и тактика расследования преступлений. 251 с.

8. *Россинская Е. Р., Усов А. И.* Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. – 416с.

9. *Голубєв В. О.* Розслідування комп'ютерних злочинів: моногр. / Гуман. ун-т „Запоріжський ін-т держ. та муніципал. упр." Запоріжжя: Гум ун-т „ЗІДМУ", 2003. 296 с.

10. *Усов В. А.* Компьютерно-техническая экспертиза и её видовое деление. *Crime-research.org*. *URL*: http://www.crime-research.ru/articles/Rossinskay/

11. *Біленчук П. Д., Кобилянський О. Л.*, *Малій М.І.,* та ін. Е-суспільство: цифрове майбутнє України: моногр. 2-ге вид. переробл. Київ: УкрДГРІ, 2019. 292 с.

12. *Біленчук П. Д.*, *Близнюк М. М., Кобилянський О. Л. , Малій М. І., Пілюков Ю. О., Соболєв О. В.* Електронна цивілізація: інноваційне майбутнє України: моногр. Київ: УкрДГРІ, 2019. 284 с.

13. *Біленчук П. Д., Береський Я. О., Кобилянський О. Л., Малій М. І. Перелигіна Р. В.* Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: моногр. Київ: УкрДГРІ, 2019. 416 с

schools, research institutes of criminal politics under the USSR prosecutor, the Supreme Court of the USSR and the NKIU of the RSFSR. Moscow: Sov. Zakonodatelstvo. Book. 1: Technique and tactics of crime investigation. 251 p. (In Russian).

8. *Rossinskaia, E. R., Usov, A. I.* (2001). Forensic computer-technical examination. Moscow: Pravo i zakon. 416 p. (In Russian).

9. *Golubiev, V. O.* (2003). Computer Crime Investigation. Classic Private University "Zaporizhzhia state and municipal institute". Zaporizhzhia: ZIDMU. 296 p (In Ukrainian).

10. *Usov, V. A.* Computer-technical expertise and its species division. Crime-research.org. Retrieved from http://www.crime-research.ru/articles /Rossinskay/ (In Russian).

11. *Bilenchuk, P. D. Kobylyanskyi, O. L., Malii, M. I. et al*. (2019). E-society: Ukraine's digital future. Kyiv: UkrDHRI. 292 p. (In Ukrainian).

12. *Bilenchuk, P. D., Blyzniuk, M. M., Kobylyanskyi O. L., Malii M. I., Piliukov Yu. O., Soboliev O. V.* (2019). Electronic Civilization: Ukraine's innovative future. Kyiv: UkrDHRI, 228 p. (In Ukrainian).

13. *Bilenchuk, P. D., Bereskyi, Ya. O., Kobylianskyi, O. L., Malii, M. I., Perelyhina, R. V.* (2019). Convergence of the solar knowledge society: creative education and civilizational development. Kyiv: UkrDHRI. 416 p. (In Ukrainian).

ЭКСПЕРТИЗА КАК СРЕДСТВО УСТАНОВЛЕНИЯ ФАКТОВ И ОБСТОЯТЕЛЬСТВ СОВЕРШЕНИЯ ТРАНСНАЦИОНАЛЬНЫХ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Л. В. Борисова
П. Д. Биленчук
Н. И. Малий
В. С. Виноградова

Отмечается, что следователи не в состоянии отслеживать все технологические изменения в сфере информационных технологий и для

исследования следов данного вида преступлений особое внимание уделяется использованию экспертизы компьютерных систем и машинных носителей (приказ Министерства юстиции Украины от 08.10.98 г. № 53/5).

Во время проведения экспертизы целесообразно решать такие задачи:

– *идентификационные* – диагностика системных процессов и поведения системы; идентификация системы; многофакторный анализ и реконструкция обстоятельств места события (методами математического анализа и компьютерного моделирования); диагностика функционального назначения отдельных элементов компьютерной системы, системы интеллектуального взлома; идентификация автора компьютерного текста (представляются более важными для следствия и суда);

– *не идентификационные* – определение структуры и функций телекоммуникационных сетей и средств электронной почты; реконструкция и прогнозирование поведения системы; определение надежности и стойкости компьютерных систем; отнесение информации к категории программного обеспечения; отнесение конкретных программ к вредным; определение семантики и грамматики спорных текстов; диагностика и классификация принтеров, факсов, копировальной техники по тексту, который изготовлено с них применением.

Целесообразно в выводе эксперта, отображать факты фиксации информационных следов-отображений о действиях вредных программ и поиск изъятых файлов, частей файлов, которые были специально изъяты к началу обзора или случайно в процессе обзора. Результаты проверки журналов регистрации, защиты и приложений с применением документов, которые регламентируют правила архивации журналов регистрации; результаты аудита (операторов, привилегий, объектов).

К выводу необходимо присоединять отчеты, которые были генерированы соответствующим программным обеспечением, копии на машинных носителях, которые получены при проведении физической фиксации. В случае использования компьютерного документа как доказательства, нужно указать: средства сбора и обработки информации; тип использованой системы; средства контроля, которые встроены в систему для гарантированного выявления и исправления ошибок, определение уровня профессиональной подготовки отдельных лиц в области программирования и работы со средствами компьютерной техники.

Ключевые слова: транснациональные компьютерные преступления экспертиза, идентификационные и не идентификационные признаки.

EXAMINATION AS A MEANS OF ESTABLISHING THE FACTS AND CIRCUMSTANCES OF COMMISSION OF TRANSNATIONAL COMPUTER CRIMES

L. Borysova
P. Bilenchuk
M. Malii
V. Vynohradova

The article is noted that investigators are not able to track all technological changes in the field of information technology and to study the traces of this type of crime, special attention is paid to the use of examination of computer systems and computer media (order of the Ministry of Justice of Ukraine dated 08.10.98, No. 53/5).

During the examination, it is advisable to solve the following problems:

– identification, that is the diagnosis of system processes and system behavior; system identification; multivariate analysis and reconstruction of the circumstances of the event place (by methods of mathematical analysis and computer simulation); diagnostics of the functional purpose of individual elements of a computer system, an intelligent hacking system; identification of the author of the computer text (they seem more important for the investigation and the court);

– non-identification, that is determination of the structure and functions of telecommunication networks and e-mail facilities; reconstruction and prediction of system behavior; determination of the reliability and resilience of computer systems; classifying information as software; classifying specific programs as harmful; definition of semantics and grammar of controversial texts; diagnostics and classification of printers, faxes, copy machines according to the text that was made from them.

It is advisable in the expert's conclusion to display the facts of fixing information traces about the actions of malicious programs and search for seized files, parts of files that were specially removed at the beginning of the review or accidentally during the review; results of verification of system, protection, and application logs using documents that govern the rules for archiving logs; audit results (operators, privileges, objects).

To the conclusion, it is necessary to attach reports that were generated by the corresponding software, copies on machine media that were obtained during physical fixation. In the case of using a computer document as evidence, there is a need to specify: the means of collecting and processing information; type of system used; control tools that are built into the system for guaranteed detection and correction of errors, determining the level of professional training of individuals in the field of programming and working with computer equipment.

Key words: transnational computer crimes, examination, identification and non-identification features.

DOI: https://doi.org/10.33994/kndise.2020.65.23
УДК 343.14

Олег Вячеславович Баулін
кандидат юридичних наук, доцент,
старший викладач відділу підготовки прокурорів з процесуального керівництва та криміналістичного забезпечення досудового розслідування

E-mail: baulin_ov@ukr.net

Національна академія прокуратури України

ОСОБЛИВОСТІ ДОКАЗУВАННЯ НЕНАЛЕЖНОГО ВИКОНАННЯ ПРОФЕСІЙНИХ ОБОВ'ЯЗКІВ МЕДИЧНИМ ПРАЦІВНИКОМ

В статті розглядається доказування неналежного виконання професійних обов'язків медичним працівником. На підставі аналізу положень