УДК 347.94
DOI https://doi.org/10.32782/2524-0374/2023-1/157

ЗАСТОСУВАННЯ КОМП'ЮТЕРНОЇ ФОРЕНЗИКИ У ДОСЛІДЖЕННІ ЕЛЕКТРОННИХ ДОКАЗІВ У ГОСПОДАРСЬКОМУ СУДОЧИНСТВІ УКРАЇНИ

APPLICATION OF COMPUTER FORENSICS IN THE RESEARCH OF ELECTRONIC EVIDENCE IN ECONOMIC JURISDICTION OF UKRAINE

Матвєєв П.С., доктор юридичних наук, професор,
професор кафедри приватного права
факультету права та міжнародних відносин
Київський університет імені Бориса Грінченка
ORCID 0000-0001-7087-115X

В сучасному світі насиченість електронних інформаційних даних та складних технічних процесів може супроводжуватись утворенням (шифруванням) вказаної інформації, відтак встановлення автентичності та цілісності електронних доказів є важливою складовою під час здійснення правосуддя.

У статті розглянуто особливості комп'ютерної форензики як засобу дослідження поданих суду електронних доказів. Комп'ютерна експертиза дозволяє встановити автентичність електронних доказів шляхом виявлення будь-яких змін, редагування або підробки даних, що можуть вплинути на їх достовірність.

Також комп'ютерна експертиза може бути використана для відновлення втраченої, видаленої або пошкодженої інформації, дозволяє виявляти сліди втручання в інформацію, що розглядається як електронні докази. Це може полягати у виявленні шкідливих програм, встановленні доступу до нелегального контенту, виявленні кібератак або виявленні електронних слідів у справах, пов'язаних зі злочинами, які відбуваються в онлайн-середовищі.

Комп'ютерна форензика є напрямом дослідження об'єктивності обставин, завдяки застосуванню методів і технологій у сфері інформатики та кібербезпеки для збору, аналізу та інтерпретації електронних доказів, а її застосування обґрунтовується чинними нормами господарського процесуального права.

Встановлено, що комп'ютерна експертиза може використовуватись в аналізі метаданих, що містяться в електронних доказах – час, дату, місцезнаходження та інші відомості, які можуть бути важливими для справедливого та ефективного здійснення судового розгляду.

Також в даній статті встановлено, що електронні докази - це інформація, яка знаходиться в електронній формі або електронних записах, і може бути використана для підтвердження фактів, пов'язаних з електронними комунікаціями, транзакціями та збереженням даних.

Крім того, з'ясовано, що електронні докази можуть містити інформацію про злочини, підробку, зловживання, кібератаки, шахрайство та інші злочинні діяння, доведення яких є надзвичайно важливим під час здійснення судочинства.

Ключові слова: електронні докази, господарське судочинство, електронна експертиза, форензики, господарські правовідносини, судовий спір.

In today's world, the saturation of electronic information data and complex technical processes can be accompanied by the formation (encryption) of the specified information, therefore establishing the authenticity and integrity of electronic evidence is an important component in the administration of justice.

The article examines the features of computer forensics as a means of researching electronic evidence submitted to the court. Computer forensics allows you to establish the authenticity of electronic evidence by detecting any changes, editing or falsification of data that may affect its authenticity.

Computer forensics can be used to recover lost, deleted, or damaged information, and can reveal traces of tampering with information considered as electronic evidence. This can be to detect malware, establish access to illegal content, detect cyber attacks or detect electronic traces in cases related to crimes that occur in the online environment.

Computer forensics is a direction of investigating the objectivity of circumstances, thanks to the application of methods and technologies in the field of informatics and cyber security for the collection, analysis and interpretation of electronic evidence, and its application is justified by the current norms of economic procedural law.

It has been established that computer forensics can be used in the analysis of metadata contained in electronic evidence - time, date, location and other information that may be important for a fair and efficient trial.

This article also states that electronic evidence is information that is in electronic form or electronic records and can be used to prove facts related to electronic communications, transactions, and data storage.

In addition, it has been found that electronic evidence can contain information about crimes, forgery, abuse, cyber-attacks, fraud and other criminal acts, the proof of which is extremely important in the course of legal proceedings.

Key words: electronic evidence, economic litigation, electronic expertise, forensics, economic legal relations, litigation.

Постановка проблеми. Різноманітність видів електронних доказів, які можуть бути використані в господарському судочинстві для доведення аргументів сторін є досить великою. Господарський процесуальний кодекс України (далі за текстом – ГПК України) надаючи визначення поняття електронних доказів у статті 96, наводить певний (не вичерпний) перелік, якими є, зокрема електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі.

Дослідження електронних доказів у господарському судочинстві - це діяльність суду, яка відіграє ключову роль для правильного вирішення спору, відтак встановлення належності та достовірності поданих електронних доказів є обов'язком суду при вирішенні судового спору.

У випадку виникнення в суду чи сторін у справі сумнівів у добросовісному здійсненні учасниками справи їхніх процесуальних прав або виконанні обов'язків щодо поданих електронних доказів, суд може призначити експертне дослідження таких доказів.

Комп'ютерна експертиза дозволяє перевірити автентичність електронних доказів, таких як електронні листи, фотографії, відео та звукозаписи, документи тощо. Експерт з комп'ютерної форензики аналізує метадані, цифровий слід, артефакти обробки, які дозволяють встановити чи були дані оброблені, змінені або ж втрачені.

Стан дослідження проблеми. В контексті кримінального права, технічних та комп'ютерних наук проводились дослідження питань сутності, цілей та методики форензики такими вченими як: Г. В. Соломіна, С. О. Твердун, С. М. Тютченко, О. Г. Рябчук, Т. Ю. Климко, О. О. Мель-

ник, S. Mojsoska, N. Dujovski та іншими, які вносять вагомий вклад у розвиток методів і технологій комп'ютерної форензики. Проте, дослідження питання використання форензики як елемента системи в господарських відносинах вченими майже не проводились, що обумовлює нашу увагу до комп'ютерної форензики під час дослідженні електронних доказів в господарському судочинстві.

Метою дослідження є з'ясування особливостей комп'ютерної форензики як засобу визначення достовірності електронних доказів у господарському судочинстві України.

Викладення основного матеріалу. Приписами частини 1 та 2 статті 73 ГПК України встановлено, що доказами є будь-які дані, на підставі яких суд встановлює наявність або відсутність обставин (фактів), що обґрунтовують вимоги і заперечення учасників справи, та інших обставин, які мають значення для вирішення справи. Ці дані встановлюються такими засобами: письмовими, речовими і електронними доказами; висновками експертів та показаннями свідків.

Електронні документи, електронні листи, файли, бази даних та інші цифрові матеріали, які містять інформацію про фінансові операції, контракти, спілкування з контрагентами, фінансові звіти тощо, можуть подаватися учасниками господарського спору в якості електронних доказів.

Як зазначалося вище, дослідження електронних доказів у господарському судочинстві - це діяльність суду, яка відіграє ключову роль для правильного вирішення спору. Встановлення належності та достовірності поданих електронних доказів є обов'язком суду при вирішенні судового спору. У випадку виникнення в суду чи сторін у справі сумнівів у добросовісному здійсненні учасниками справи їхніх процесуальних прав або виконанні обов'язків щодо поданих електронних доказів, суд може призначити експертне дослідження таких доказів.

Варто зауважити, що Кримінальним кодексом України передбачено відповідальність за введення в оману суду або іншого уповноваженого органу. Так, згідно з частиною 1 статті 384 Кримінального кодексу України завідомо неправдиве показання свідка, потерпілого, завідомо неправдивий висновок експерта, спеціаліста, складені для надання або надані органу, що здійснює досудове розслідування, виконавче провадження, суду, Вищій раді правосуддя, тимчасовій слідчій чи спеціальній тимчасовій слідчій комісії Верховної Ради України, подання завідомо недостовірних або підроблених доказів, завідомо неправдивий звіт оцінювача про оцінку майна, а також завідомо не правильний переклад, зроблений перекладачем у таких самих випадках, караються виправними роботами на строк до двох років або арештом на строк до шести місяців, або обмеженням волі на строк до двох років.

Експертиза електронних доказів (англ. digital forensics) є процесом аналізу та інтерпретації електронних даних з метою виявлення та дослідження автентичності електронних доказів, а також відновлення у цифрових пристроях даних, пов'язаних з кіберзлочинністю. Вона використовує методи, техніки та інструменти для виявлення, підтвердження та дослідження доказів, що знаходяться на електронних пристроях, таких як комп'ютери, мобільні телефони, цифрові носії та ін.

Термін forensic з англійської перекладається як «судовий», а у США forensic є синонімом criminalistics (криміналістики) – науки про закономірності злочинної діяльності та її відображення в джерелах інформації, які слугують основою для розроблення засобів і методів збирання, дослідження, оцінки і використання доказів із метою розкриття, розслідування, судового розгляду та запобігання злочинам [1, с. 78].

В Україні комп'ютерна форензика, зокрема, використовується для розслідування комп'ютерних злочинів, зокрема таких як крадіжка конфіденційної інформації, порушення авторських прав, кібератаки та інші правопорушення, пов'язані з використанням комп'ютерних технології.

На думку Г.В. Соломіної, форензік – це ефективний інструмент, спрямований на дослідження всіх потоків інформації всередині підприємства, а також взаємодії із зовнішніми сторонами, такими як клієнти, постачальники, якими регулюють органи, інвестори, та іншими зацікавленими особами. На основі даних зв'язків і оцінюються можливості виникнення шахрайства [2].

На думку С.С. Чернявського, О.Є. Користіна, В.А. Некрасова, форензік є послугою з виявлення та зменшення ризиків виникнення шахрайства, незаконних дій та неетичної поведінки у сфері господарської діяльності [3].

Вище згадані вчені розглядають форензик як окреме поняття, яке має практичне відображення у вигляді послуги або інструменту.

Т.Ю. Климко, О.О. Мельник ототожнюють поняття «форензік» із розслідуванням. Зазначається, що форензік є резервним елементом внутрішнього аудиту, який використовується за потреби [4].

А.О. Семенець пропонує поняття «форензікаудит», під яким слід розуміти процес вивчення звітності та господарських операцій компанії з метою розроблення заходів із реагування, управління та запобігання шахрайству на підставі експертного судження про наявність відповідних фактів [5].

Особливу увагу при визначенні характерних особливостей експертизи електронних доказів слід звернути на наведені нижче судові рішення.

Так, з рішення Господарського суду Львівської області від 15.03.2021 у справі № 914/2860/20 вбачається, що «Рівненським науково-дослідним експертно-криміналістичним центром МВС України, проведено комп'ютерно-технічне дослідження електронних файлів завантажених ТОВ «НВП Шляхбуд» з мережі Інтернет за Веб-адресою: https://prozorro.gov.ua/tender/UA-2Q 19-09- 19-002534-Ь. Висновком експертного дослідження № 1.4-71/20 від 17.07.2020 стверджується наступне: «Встановлені властивості та метадані наданих на дослідження файлів не свідчать про спільний доступ до мережі Інтернет. Використання учасниками спільного комп'ютерного обладнання експертом також не виявлено». Вказане свідчить про те, що Відділенням не було доведено факту використання спільного доступу до мережі Інтернет та спільного комп'ютерного обладнання» [6].

Також досліджуючи в Єдиному державному реєстрі судових рішень постанову Центрального апеляційного господарського суду від 25.01.2023 у справі №904/9795/16 вбачається, що суди приймають до уваги комп'ютерно-технічні дослідження. Так, у вказаній постанові зазначено: «Із висновку експертного дослідження від 28.09.2015р. №2КТ, проведеного ТОВ «Лабораторія комп'ютерної криміналістики» на запит приватного нотаріуса Бовбалан Н.Р. щодо проведення комп'ютерно-технічного дослідження вбачається, що на ноутбук приватного нотаріуса Бовбалан Н.Р. було встановлене шкідливе програмне забезпечення LiteManager, основними функціями якого є віддалене управління комп'ютером та передача файлів на сервер в мережі Інтернет. З використанням цього програмного забезпечення було викрадено файли електронних ключів доступу до Державного реєстру та встановлено програму Punto Switehtr, за допомогою якої було викрадено пароль доступу. В період часу з 17.08.2015р. по 07.09.2015р. від імені приватного нотаріуса Бовбалан Н.Р. з використанням викрадених облікових даних було здійснено реєстрацію заяв. Матеріали даної справи свідчать, що державна реєстрація припинення обтяження (арештів) спірного нерухомого майна була здійснена в Державному реєстрі речових прав на нерухоме майно 07.09.2015р. за межами робочого часу (після 18:00 год.), через раніше встановлене на комп'ютері при-

ватного нотаріуса Бовбалан Н.Р. шкідливе програмне забезпечення. Наведені обставини свідчать про те, що відсутність в Державному реєстрі речових прав на нерухоме майно записів про арешти спірного нерухомого майна відбулась внаслідок неправомірних дій.» [7].

Північний апеляційний господарський суд в постанові від 06.02.2020 у справі №910/6398/16 зазначив, що «згідно відповідей на питання судової експертизи щодо монтажу наданого позивачем файлу CaptureMovie013_converted.avi, експертами, зокрема, зроблено висновки про відсутність ознак, характерних для електронного монтажу відео зображення, спотворення відео зображення, електронного монтажу запису звуку, цифрової обробки звуку ані в момент запису, ані після нього, а також переривання у записі відеофонограми. Тобто, вказані висновки свідчать про оригінальність наданого позивачем файлу з фіксацією, а також відсутність в ньому будь-яких змін та монтажу, що в свою чергу, підтверджує факт порушення відповідачем майнових авторських прав позивача.» [8].

Аналіз судової практики на предмет наявності призначення господарськими судами компютерно-технічних експертиз електронних доказів та, відповідно, їх дослідження дозволяє виділити певні особливості таких експертиз.

Мабуть однією із важливих та специфічних є те, що проведення експертизи електронних доказів є складним завданням, оскільки електронні докази можуть бути розміщені на різних електронних пристроях, такі як комп'ютери, смартфони, сервери, зовнішні носії і т.п. Кожен з цих пристроїв може мати власні особливості, операційні системи, формати файлів і методи збереження даних. Експертам потрібно мати глибокі знання про ці пристрої та їх технічні складові, а також володіти вмінями в роботі зі спеціалізованим програмним забезпеченням для дослідження вказаних електронних доказів.

Не менш важливу роль відіграє збереження електронних доказів відповідно до спеціальних процедур та стандартів, оскільки ці дані можуть бути дуже вразливими і піддаватися змінам або втраті. Відтак, експертам необхідно забезпечити правильне збереження доказів та забезпечити їх цілісність, щоб вони залишалися незмінними протягом усього процесу проведення експертизи та судового розгляду.

Також, як слідує із наведених судових рішень, достовірність проведення експертного дослідження комп'ютерної форензики має передбачати дотримання чітко визначеної етапності:

1-й етап: Постановка завдання. Експерт повинен визначити мету та обсяг дослідження відповідно до поставлених судом запитань.

2-й етап: Аналіз даних. Експерт проводить детальний аналіз зібраних даних з використанням різних методів та інструментів, включаючи спеціалізоване комп'ютерне програмне забезпечення. Цей аналіз може включати пошук підозрілих або видалених файлів, відновлення видалених даних, аналіз мережевої активності, виявлення шифрованої інформації та інше.

3-й етап: Інтерпретація результатів. Експерт аналізує зібрані дані, встановлює зв'язки і формує висновки.

4-й етап: Підготовка звіту (висновку). Експерт надає письмовий звіт (висновок), в якому висвітлюються всі важливі факти, методологія дослідження, знайдені докази та інтерпретація результатів. Звіт повинен бути чітким, об'єктивним і підтверджуватися достовірними доказами.

Також комп'ютерні форензичні експерти можуть пояснити технічні деталі, процеси аналізу та інтерпретації доказів, а також встановлювати достовірність та чи недостовірність електронних доказів.

Вищезазначене доводить, що застосування комп'ютерної форензики в господарському судочинстві України є важливим інструментом для розгляду господарських справ.

В сучасному світі комп'ютерна форензика стає все більш важливою, оскільки електронні злочини стають все поширенішими. Комп'ютерна форензика дозволяє відновлювати втрачені, видалені або пошкоджені дані з електронних пристроїв, що дозволяє визначити обставини для об'єктивного вирішення спору та встановлення істини у спірних правовідносинах.

Висновки. 1. Електронні докази - це інформація, яка знаходиться в електронній формі або електронних записах, і може бути використана для підтвердження фактів, пов'язаних з електронними комунікаціями, транзакціями та збереженням даних;

2. Електронні докази можуть містити інформацію про злочини, підробку, зловживання, кібератаки, шахрайство та інші злочинні діяння, доведення яких є надзвичайно важливим під час здійснення судочинства;

3. Комп'ютерна форензика є напрямом дослідження об'єктивності обставин, завдяки застосуванню методів і технологій у сфері інформатики та кібербезпеки для збору, аналізу та інтерпретації електронних доказів, а її застосування обґрунтовується чинними нормами господарського процесуального права.

ЛІТЕРАТУРА

1. Рябчук О.Г., Твердун С.О. Форензік як інструмент протидії економічним злочинам та фінансовому шахрайству на підприємстві. *Науковий* вісник Ужгородського національного університету. 2021. №40. С. 77-83.

2. Соломіна Г.В. Форензік – інструмент фінансового розслідування діяльності підприємства. *Науковий* вісник Мукачівського державного університету. 2018. № 2. С. 144–149.

3. Фінансові розслідування у сфері протидії легалізації злочинних доходів в Україні: методичні рекомендації / С.С. Чернявський, О.Є. Користін, В.А. Некрасов та ін. Київ : Нац. акад. внутр. справ, 2017. 164 с.

4. Климко Т.Ю., Мельник О.О. Удосконалення роботи внутрішнього аудиту для запобігання фродів на підприємстві. *Науковий* вісник Міжнародного гуманітарного університету. Серія «Економіка і менеджмент». 2015. Вип. 13. С. 251–254.

5. Семенець А.О. Форензік аудит як ефективний засіб антикризового управління торговельною діяльністю. Бізнес Інформ. 2019. № 4(495). С. 280–287.

6. Рішення Господарського суду Львівської області від 15.03.2021 у справі №914/2860/20. Єдиний державний реєстр судових рішень. Офіційний вебпортал. URL: https://reyestr.court.gov.ua/ Review/95743549.

7. Постанова Центрального апеляційного господарського суду від 25.01.2023 у справі №904/9795/16. Єдиний державний реєстр судових рішень. Офіційний веб портал. URL: https://reyestr.court.gov.ua/ Review/108681654.

8. Постанова Північного апеляційного господарського суду від 06.02.2020 у справі №910/6398/16. Єдиний державний реєстр судових рішень. Офіційний вебпортал. URL: https://reyestr.court.gov.ua/ Review/87651786