ІНТЕГРУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА СУДОВО-ЕКОНОМІЧНОЇ ЕКСПЕРТИЗИ

INTEGRATION OF INFORMATION TECHNOLOGIES AND FORENSIC ECONOMIC EXPERTISE

Зростання економічних злочинів у сучасному бізнес-ландшафті вимагає модернізації методів судово-економічної експертизи, яка ретельно розглядає нові умови, створені середовищем інформаційних технологій (ІТ). Метою статті є поглиблення теоретичних та методичних аспектів судово-економічної експертизи в частині їх інтегрування до умов діджиталізованого середовища. Спираючись на низку наукових джерел, це дослідження окреслює ключові області, які потребують модифікації методик та процедур. Проаналізовано інструментарій цифрової криміналістики у розслідуванні фактів економічних злочинів з урахуванням цифрових форматів фінансових операцій і транзакцій. Згруповано критично важливі проблеми ІТ-об'єктів та виявлено їх взаємозв'язок з судово-експертними дослідженнями економічних злочинів з урахуванням впливу ІТ на бізнес-операції. Обґрунтовано доцільність стандартизації судово-економічних процедур цифрових баз даних, що забезпечить можливість випереджати нові загрози та гарантувати цілісність цифрових доказів на основі галузевих стандартів.

Ключові слова: *судово-економічна експертиза, методика, стандартизація, процедури, цифрові докази, цифрова інформація.*

The growth of economic crimes in the modern business environment necessitates the modernization of forensic economic examination methods in the context of the use of information technology (IT). The current issues related to the utilization of digital evidence in criminal proceedings, as presented by forensic experts, are explored. Solutions obtained through methods of theoretical analysis, synthesis, and specialized cognitive methods are proposed. The article aims to deepen the theoretical and methodological aspects of forensic economic examination in the context of integration into a digitized environment. Drawing from various scientific sources, this study identifies key areas of forensic science that require modification of techniques and procedures. The tools of digital forensics in the investigation of economic crimes are analyzed, taking into account digital formats of financial transactions. Critical IT-related problems are grouped into several categories: data breaches and cybersecurity, digital forensics and electronic evidence, blockchain and cryptocurrencies, digital accounting and financial systems, regulatory compliance and the admissibility of digital evidence in court, social engineering, phishing attacks, insider threats, and inappropriate employee behavior. The relationship between these issues and forensic research is revealed, considering the influence of information technology. Solutions have been proposed to modernize the procedures of forensic economic examination for each object of examination. The feasibility of standardizing forensic and economic procedures of digital databases is substantiated, providing the opportunity to stay ahead of new threats and guarantee the integrity of digital evidence based on industry standards. The experience of standardizing forensic procedures in the United States, European Union countries, and Australia may be useful in reforming Ukrainian legislation and developing guidelines for the use of digital evidence. It was found that the rapid change in information technologies for identifying, seizing, recording, and researching digital information poses certain difficulties for forensic economic experts in Ukraine. It is recommended to improve the efficiency of using digital evidence in legal proceedings by developing guidelines for working with it and enhancing the qualifications of forensic experts.

Key words: *forensic economic examination, methodology, standardization, procedures, digital evidence, digital information.*

УДК 343.98

DOI: https://doi.org/10.32782/dees.9-17

Іванков В.М.[1]
к.е.н.,
Науково-дослідна судово-експертна установа

Ivankov Volodymyr
Forensic Research Institution

Постановка проблеми. Необхідність трансформації судово-економічної експертизи обґрунтовується безпрецедентною інтеграцією інформаційних технологій (ІТ) у бізнес-операції в поєднанні зі сплеском злочинної діяльності та шахрайства з використанням цифрових засобів. Зростання обсягів цифрових транзакцій у сучасному бізнес-ландшафті вимагає відповідної еволюції стратегій судової експертизи для ретельного вивчення електронних записів, відстеження фінансових потоків і виявлення аномалій у заплутаній сфері цифрових фінансів. Зростаюча складність кіберзагроз змушує експертів-криміналістів використовувати передові методології та інструменти, щоб розширити їхні можливості для виявлення та протидії складним шахрайським схемам, які здійснюються через цифрові канали. Поява криптовалют і технології блокчейн створює нові виклики, оскільки ці технології забезпечують анонімність і децентралізацію, спонукаючи судових експертів розвивати навички аналізу транзакцій блокчейну та розуміння динаміки криптовалют. Швидкий розвиток технологій вимагає оновлень навичок судового економічного експерта і використовувати новітні технології для збору цифрових доказів під час виконання завдань судової експертизи. Визначення правового поняття «цифровий доказ» Цивільним процесуальним кодексом України (стаття 100) недостатньо регламентує потреби експертизи у роботі з цифровими і електронними доказами. Крім того, множина їх проявів в діяльності бізнес-середовища настільки широка, що потребує суттєвої модифікації інструментів судово-економічної експертизи.

[1] ORCID https://orcid.org/ 0000-0001-5513-4290

Аналіз останніх досліджень і публікацій. Інтеграція інформаційних технологій у бізнес-операції змінила динаміку економічної діяльності, водночас створивши нові можливості для фінансових зловживань [1, с. 44; 2, с. 92]. У світлі цього судово-економічна експертиза економічних злочинів вимушена розвиватися, щоб охоплювати складності, пов'язані з ІТ-середовищем, створюючи інформаційні системи та модифікуючи методики проведення судових експертиз [3, с. 273; 4, с. 14]. Дослідження, спрямовані на розробку передових методів аналізу цифрових транзакцій, виявлення аномалій в електронних записах і відстеження фінансових потоків у цифрових бухгалтерських і фінансових системах, виконані зарубіжними дослідниками [5, 6], визначають вектор, за яким зосередились вітчизняні науковці, адаптуючи світовий досвід до реалій законодавчих вимог судово-економічних експертиз [7, с. 140]. Інтеграція новітніх методів прогнозної аналітики в судово-економічну експертизу шляхом застосування інформаційних систем дозволяє підвищити ефективність та точність розслідувань економічних злочинів з використанням цифрових засобів. Крім того, дослідники вивчають правові та етичні аспекти, пов'язані з конфіденційністю даних, прийнятністю цифрових доказів і встановленням стандартизованих практик для забезпечення надійності криміналістичних методологій. Незважаючи на їх значний внесок у міждисциплінарну галузь судово-економічної експертизи, необхідним є подальше поглиблення напрямків використання знань різних сфер, пов'язаних з інтеграцією інформаційних технологій у фінансові системи.

Формулювання цілей статті (постановка завдання). Цілями статті є поглиблення теоретичних та методичних засад судово-економічної експертизи, спрямованих на розвиток інструментарію використання ІТ, цифрової криміналістики для ефективного вирішення завдання судово-економічної експертизи встановлення доказової бази досудового та судового розслідування економічних злочинів.

Виклад основного матеріалу дослідження. У цьому дослідженні нами було проаналізовані наукові джерела та практику здійснення судово-економічних експертиз в умовах формування даних з використанням ІТ, які було узагальнено у вигляді проблем з окресленими питаннями їх вирішення (табл. 1).

Порушення зберігання даних, їх втрата і кібербезпека в умовах ери тотального використання ІТ та автоматизованих систем зберігання інформації, становлять чи не найбільш значні ризики для цілісності фінансової інформації. Судова експертиза повинна включати ретельний аналіз протоколів безпеки даних, механізмів шифрування та стратегій реагування на інциденти, щоб виявити потенційні вразливості та оцінити ступінь компрометації даних, які будуть використовуватись

Таблиця 1

Проблематика об'єктів ІТ середовища для судово-економічної експертизи

№	Проблеми ІТ середовища для судово-економічної експертизи	Об'єкти, на які спрямовані рішення судово-економічної експертизи
1.	Порушення збереженості даних і кібербезпека	Кібергігієна Кібербезпека
2.	Цифрова криміналістика та електронні докази	Ідентифікація та збір електронних доказів Аналіз цифрових артефактів Шифрування та конфіденційність даних Хмарні обчислення Антикриміналістичні методи Оперативна криміналістика Аналіз хронології даних Хешування та цілісність даних Алгоритми виявлення відхилень в цифровій криміналістиці
3.	Блокчейн і криптовалюти	Псевдоанонімність та складність відстеження Смарт-контракти та юридикція Психологія криптозлочинців та використання анонімності
4.	Цифрові бухгалтерські та фінансові системи	Складність програмного забезпечення та систем Обсяг і швидкість зміни даних Взаємозв'язаність систем та проблеми інтеграції
5.	Відповідність нормативним вимогам і прийнятність цифрових доказів у суді	Правова база, що розвивається Ланцюг постачання та автентифікація Стандартизація судово-економічних процедур
6.	Соціальна інженерія та фішингові атаки	Соціальна інженерія Наслідки фішингових атак
7.	Інсайдерські погрози та неналежна поведінка співробітників	Інсайдерська інформація Професійна етика співробітників

Джерело: авторська розробка

в судовому процесі в якості доказів. Але основні обсяги роботи судового експерта пов'язані з дослідженням діджиталізованої інформації у вигляді електронних та цифрових доказів [7, с. 129–132]. Це є однією з проблем ІТ для судово-економічної експертизи, яка відображена в таблиці.

Оскільки транзакції все більше здійснюються через різноманітні цифрові платформи, судово-економічні експерти повинні орієнтуватися в сфері цифрової криміналістики. Завдання полягає в тому, щоб ефективно використовувати специфічну електронну інформацію для виявлення шахрайських дій, відстеження фінансових операцій і створення доказового сліду, необхідного для судового розгляду. Ця сфера представляє унікальні виклики, які вимагають складних методологій та інструментів, інтегрованих до цифрових форматів даних.

Ідентифікація та збір електронних доказів є основними кроками в процесі судово-економічної експертизи. Це передбачає розпізнавання відповідних цифрових артефактів, таких як електронні листи, документи, журнали транзакцій і метадані. Судово-економічні експерти повинні забезпечити збереження цифрових доказів для підтримки їх цілісності для аналізу та представлення в суді [7; 8].

Щоб вирішити цю проблему, зарубіжні експерти-криміналісти використовують передові інструменти та методи криміналістики, зокрема пристрої для блокування запису, щоб запобігти зміні цифрових доказів під час збирання. Крім того, використання спеціалізованих програмних інструментів для виділення даних і аналізу на основі сигнатур допомагає відновити видалені або приховані файли, сприяючи більш повному розумінню справи.

Аналіз цифрових артефактів є наступним етапом дослідження доказів для реконструкції подій, встановлення часових рамок і виявлення моделей, що вказують на економічні злочини. Аналіз може охоплювати вивчення метаданих файлів, вивчення шаблонів зв'язку та відстеження фінансових операцій через цифрові канали [9].

Шифрування та конфіденційність даних створює високі ризики у роботі судового експерта, адже ці технології шифрування можуть перешкоджати вилученню та аналізу даних. Розробка і використання методів дешифрування, підтримка постійного прогресу у вивченні криптографічних досліджень зумовлює рішення подолання цієї проблеми [9].

Використання хмарних обчислень для виконання економічних транзакцій та зберігання даних, часто децентралізованих між хмарними службами, ускладнює відстеження та збір відповідних цифрових доказів. Рішенням для судового експерта є розробка інструментів і методів хмарної криміналістичної експертизи, які можуть переміщатися та аналізувати дані, що зберігаються в різноманітних хмарних середовищах.

Злочинці чи шахраї можуть використовувати антикриміналістичні методи, щоб стерти або змінити цифрові докази, перешкоджаючи розслідуванню або ж створюючи перешкоди на шляху пошуку доказів економічних злочинів. Судово-економічна експертиза спрямовує власні дослідження способів і інструментів для виявлення та протидії цим методам [5].

Проведення криміналістичного аналізу інформаційних систем в режимі реального часу дозволяє дослідникам перевіряти ймовірність дестабілізації даних та оперативно оцінювати їх наслідки, що дозволяє встановлювати ступінь достовірності даних в системі. Побудова хронологічної шкали цифрових подій допомагає слідчим реконструювати послідовність дій та ідентифікувати потенційні ознаки економічних злочинів внаслідок втручання у відображення фактів з метою їх зміни чи знищення.

Судово-економічні експерти зарубіжжя використовують методи криптографічного хешування для забезпечення цілісності цифрових доказів під час збору та аналізу фактів та їх використання в якості доказів в суді [9].

Широке поширення серед аудиторів та судових бухгалтерів набула інтеграція алгоритмів машинного навчання для автоматичного виявлення шаблонів і аномалій у великих базах даних. Результати аналізу аномалій допомагають ідентифікувати потенційні відхилення, які надалі досліджуються більш детально на предмет виявлення шахрайства або зумисного злочинного діяння [10].

Розвиток технології блокчейн і криптовалют створює нові проблеми у виявленні та розслідуванні економічних злочинів та шахрайства. Експерти-криміналісти повинні володіти розумінням цих технологій, щоб розкривати складні фінансові операції та відстежувати незаконну діяльність на децентралізованих платформах. Проблема блокчейну та криптовалют в судовій експертизі економічних злочинів пов'язана перш за все з питанням псевдо-анонімності, зважаючи на складність відстеження власників таких операцій. Вирішенням для судової експертизи можуть бути розробка та вдосконалення технологій аналізу таких транзакцій, використання кластеризації адрес для ідентифікації користувачів.

Технологія блокчейну надає високий рівень децентралізації, ускладнюючи визначення конкретних власників та виконавців транзакцій. Анонімність криптовалют, зокрема, ускладнює відстеження фінансових операцій. Тому розробка алгоритмів аналізу транзакцій, які дозволяють встановлювати зв'язки між адресами гаманців та реальними особами стає одним із інтегрованих інструментів аналітики в судовій експертизі.

Власне навіть наявність такої форми угоди в цій сфері, як смарт-контракти створюють юридичні колізії, оскільки їх функціонування базується на коді, а не на традиційних юридичних документах. Вирішенням питання може бути лише розробка стандартів та юридичних механізмів для інтерпретації та визнання смарт-контрактів у судових процесах, тобто визнання легітимності цифрових доказів [7].

Про нову для вітчизняної судової експертизи проблему психології криптозлочинців та її рішення писали в своїх роботах зарубіжні вчені [8]. Криптозлочинці можуть використовувати психологічні аспекти та технічні засоби для уникнення судового переслідування, тому вивчення цього аспекту та розробка технологічних засобів для виявлення та протидії є одним із актуальних напрямків подальшого розвитку судової експертизи.

В цілому, шляхи вирішення проблем для судової експертизи економічних злочинів в сфері блокчейн-технологій та крипто валюти потребують створення спеціалізованих аналітичних інструментів для обробки та аналізу блокчейн-даних з урахуванням їх особливостей вдосконалення методів кластеризації та їх більш широкого використання технік кластеризації адрес для виявлення груп користувачів (власників) та встановлення зв'язків між їхніми транзакціями.

Близько півстоліття тому почали створюватись програмні цифрові бухгалтерські та фінансові продукти для автоматизації операцій та зберігання даних. Цифрові бухгалтерські та фінансові системи стали основою сучасного бізнесу, пропонуючи ефективність і зручність. Однак із цифровізацією зросла вразливість до економічних злочинів. Судово-економічна експертиза зосередилась на ретельному вивченні цих систем, включаючи бухгалтерське програмне забезпечення, фінансові бази даних та електронні записи транзакцій, щоб виявити порушення, маніпуляції або несанкціонований доступ. Нами ідентифіковано наступні проблемні аспекти, пов’язані з автоматизацією бухгалтерських і фінансових операцій, які потребують реагування від судово-економічної експертизи під час дослідження даних: складність програмного забезпечення та систем, обсяг і швидкість зміни даних, взаємозв'язаність систем та проблеми інтеграції (табл. 1).

Складний характер сучасного програмного забезпечення для бухгалтерського обліку та інтегрованих фінансових систем може ускладнити судовим експертам виявлення шахрайських дій. Рішення цієї проблеми полягатиме у впровадженні передових інструментів судової експертизи, які можуть комплексно аналізувати складне програмне забезпечення та системи для виявлення аномалій і порушень.

Наступний виклик пов'язаний з величезним обсягом і швидким потоком фінансових даних у цифрових системах, які на сьогодні перевищують можливості традиційних процесів дослідження судової експертизи. Рішення питання знаходиться в площині використання аналітики даних і алгоритмів машинного навчання для ефективної обробки великих обсягів даних, що дозволяє своєчасно виявляти підозрілі шаблони чи аномальні операції. Судово-економічні експерти стикаються з тим, що підприємства часто використовують низку взаємопов’язаних систем, що створює проблеми інтеграції даних [3, с. 274]. Вирішенням спів ставності інформації може стати розробка комплексної стратегії криміналістичної експертизи, яка враховує взаємозв’язок різних систем і використовує інструменти, здатні обробляти інтегровані набори даних [4, с. 18].

Крім того, постійними інструментами судово-економічної експертизи, які б забезпечували здатність ефективно виконувати завдання слідства мають стати управлінські рішення щодо запровадження систем постійного моніторингу. Вони регулярно перевіряють фінансові операції та діяльність, щоб швидко виявляти порушення та реагувати на них. Вивчення інтеграції технології блокчейн у фінансові системи для підвищення прозорості та створення констант, а також використання штучного інтелекту та алгоритмів машинного навчання для розробки складних систем виявлення шахрайства, здатних навчатися та адаптуватися до нових тактик шахрайства є перспективними напрямками використаня ІТ для судової експертизи. При цьому підтримка високого рівня обізнаності судово-економічних експертів про потенційні шахрайські дії можлива, коли відбувається інвестування в програми навчання працівників та заохочення культури етичних практик [11, с. 5].

Серед проблем, які впливають не лише на діяльність, а й на визнання результатів роботи судово-економічного експерта виділена проблема відповідності нормативним вимогам і прийнятності цифрових доказів. Правовий ландшафт, який регулює економічні злочини, тісно пов’язаний із цифровою сферою. Експерти-криміналісти повинні бути в курсі нормативно-правової бази, що розвивається і мати впевненість, що цифрові докази, які вони збирають, відповідають правовим стандартам допустимості. Це передбачає розуміння правил доказів, протоколів ланцюжка зберігання та допустимості цифрових доказів у судових процесах [7].

Проблема з дотриманням нормативних вимог і прийнятністю цифрових доказів, виокремлена нами, зумовлена швидким розвитком інформаційних технологій, які випереджають розвиток законодавчої бази, створюючи невизначеність

щодо прийнятності цифрових доказів [7]. Активна участь у законодавчих процесах, сприяння діалогу між юридичними та судово-експертними спільнотами допоможе забезпечити відповідність правових норм технологічним досягненням.

Болючим питанням автентичності цифрових доказів стає технологія встановлення та підтримка ланцюга зберігання судовими експертами цифрових доказів. Перевірка їх походження та цілісності може бути складною через нематеріальну природу цифрових даних. Використання судовими економічними експертами самих лише методів криптографічного хешування, цифрових підписів і методів безпечного зберігання для забезпечення цілісності та автентичності цифрових доказів у всьому ланцюжку зберігання недостатньо. В цьому процесі потрібно створити правову основу для прийняття таких доказів у суді. Такою основою може виступити стандартизація судово-економічних процедур. Наявність методик в сфері судово-економічної експертизи не покриває прогалини відсутності стандартизованих судових процедур для роботи з цифровими доказами, що призводить до неузгодженості в практиці, викликаючи сумніви щодо надійності доказів [9].

Стандартизація криміналістичних процедур у цифрових розслідуваннях має вирішальне значення для забезпечення узгодженості, надійності та прийнятності цифрових доказів у судовому процесі. Різними країнами уже визнана необхідність стандартизованих практик. Так, Наукова робоча група з цифрових доказів (SWGDE) в Сполучених Штатах зосередилась на розробці стандартів і вказівок для цифрових і мультимедійних доказів. SWGDE надає рекомендації щодо судово-експертних процедур, методологій і найкращих практик, охоплюючи широкий спектр тем, таких як цифрові зображення, аналіз і звітність [9].

Регулятор судової експертизи у Сполученому Королівстві відіграє вирішальну роль у встановленні стандартів судової практики, включно з цифровою криміналістикою. Регулятор видає кодекси практики та проводить оцінювання, щоб забезпечити дотримання встановлених стандартів, сприяючи послідовності та якості цифрових судових розслідувань [12]. Європейська ініціатива зі стандартизації цифрової криміналістики (DFSI) стала результатом співпраці європейських країн для встановлення стандартизованих практик у цифровій криміналістиці. Ініціатива спрямована на гармонізацію процедур, методологій і стандартів звітності для підвищення сумісності цифрових доказів через кордони. Австралійський стандарт Нової Зеландії (AS/NZS 4885:2018) описує принципи та процеси криміналістичного аналізу пристроїв і цифрових доказів. Він забезпечує стандартизовану структуру для збору, аналізу та інтерпретації цифрових доказів, забезпечуючи послідовний підхід до всіх судових розслідувань [13]. Різні країни, визнаючи важливість стандартизації процедур судової бухгалтерії у сфері цифрових розслідувань, забезпечують належне нормативне середовище для такої діяльності.

Серед проблемних зон досліджень судовою експертизою ІТ даних зарубіжними вченими виділяються фактори впливу **с**оціальної інженерії та фішингових атак [6; 9]. Людський фактор залишається значною вразливістю в ІТ-середовищі, а соціальна інженерія та фішингові атаки є поширеними методами вчинення економічних злочинів. У вітчизняній практиці такі факти ще не набули поширення, однак судова експертиза повинна оцінювати програми навчання працівників, аналізувати канали зв'язку та досліджувати випадки соціальної інженерії, щоб визначити ступінь їхнього впливу на фінансову безпеку. Проблеми інсайдерських погроз, характерні для країн з розвинутими ринковими механізмами регулювання економіки, та питання неналежної поведінки співробітників компаній також можуть значно вплинути на обставини скоєння економічних злочинів. Судова експертиза повинна ретельно перевіряти журнали доступу, аналітику поведінки користувачів і системи керування привілейованим доступом, щоб виявити та зменшити ризик внутрішніх злочинів. Тому у світлі інтеграції інформаційних технологій у бізнес-ландшафт судова експертиза економічних злочинів повинна мати багатовимірний підхід. Вивчаючи системи цифрового обліку, усуваючи вразливості соціальної інженерії та забезпечуючи відповідність нормативним вимогам, судові експерти можуть забезпечити всебічний аналіз, який враховує тонкощі ІТ-середовища.

Така інтеграція технологічних міркувань у процес судово-економічної експертизи має першочергове значення для ефективної боротьби з економічними злочинами та підтримки цілісності фінансових систем у цифрову епоху.

Висновки. Підсумовуючи, слід зазначити, що судова експертиза економічних злочинів має розвиватися разом із динамікою змін ІТ-середовища. Зростання економічних злочинів з використанням ІТ бізнес-процесів потребує інтеграції методик та інструментів судово-економічної експертизи. Рішення проблем, пов'язаних із шифруванням, хмарними обчисленнями та антикриміналістичними методами, потребують постійних досліджень, технологічного прогресу та співпраці між експертами-криміналістами, ІТ-фахівцями та фахівцями з права. Застосовуючи інноваційні методології та використовуючи технологічні розробки, судові слідчі можуть розширити свої можливості для ефективної боротьби з економічними злочинами в епоху цифрових технологій.

Використовуючи знання з кібербезпеки, цифрової криміналістики, технології блокчейн і виявлення

внутрішніх загроз, експерти-криміналісти можуть розширити свою здатність виявляти, розслідувати та запобігати економічним злочинам у сучасному бізнес-ландшафті. Дослідження дозволило виявити в кожній із окреслених сфер проблематику та рішення щодо впровадження передових технологій у діяльність судового експерта.

Постійні дослідження та співпраця між експертами-криміналістами, розробниками програмного забезпечення та фінансовими фахівцями мають важливе значення для того, щоб випереджати нові загрози та гарантувати цілісність цифрових доказів на основі галузевих стандартів для цифрових судово-економічних процедур.

Різні країни визнали важливість стандартизації процедур судової бухгалтерії у сфері цифрових розслідувань. Такі ініціативи, як SWGDE у Сполучених Штатах, Forensic Science Regulator у Великобританії, Європейський DFSI, Австралійський AS/NZS 4885 і Японський JICFE є прикладом глобальних зусиль із встановлення узгоджених практик. Ці стандарти сприяють надійності та допустимості цифрових доказів, сприяючи прозорості та якості судово-економічних експертиз.

По суті, описана в дослідженні трансформація методів судово-економічної експертизи є не просто відповіддю на технологічний розвиток бізнес-середовища, а багатогранним імперативом адаптації, узгодженням методології розслідування зі складністю цифрового ландшафту та зміцненням стійкості підходів судово-економічних експертиз проти мінливого спектру економічних злочинів в епоху цифрових технологій і надалі.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Фісуненко, Н. (2023). Цифрові трансформації в Україні: євроінтеграційні процеси та сучасні вимоги світу. *Цифрова економіка та економічна безпека*, (8 (08), 43–48. DOI: https://doi.org/10.32782/dees.8-8

2. Ночвіна І.О. Цифровізація економіки: можливості та основні загрози. *Зб. наук. праць ХНПУ імені Г.С. Сковороди «Економіка»*. 2021. Вип. 19. С. 90–97.

3. Філіпенко Н.Є. Інформаційні системи в судово-експертній діяльності. *Теорія та практика судової експертизи і криміналістики*. 2018. Том 18 (2018). С. 271–281. DOI: https://doi.org/10.32353/khrife.2018.31

4. Журавель В.А. Автоматизовані інформаційні системи як засіб забезпечення ефективності досудового розслідування. *Теорія та практика судової експертизи і криміналістики.* 2015. Випуск 15. С. 13–21

5. Huber, W.D. and DiGabriele, J.A. (2014). Research in forensic accounting – what matters?, *Journal of Theoretical Accounting Research,* Vol. 10. No. 1.

6. Barrett, N. (2005), "Computer forensics as a corporate governance tool", IQ Magazine – Records Management Association of Australia, Vol. 21 No. 2.

7. Авдєєва, Г., Живуцька-Козловська, Е. (2023). Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). С. 126–143. DOI: 10.32353/khrife.1.2023.07

8. Upward, F. (2000), "Modelling the continuum as paradigm shift in recordkeeping and archiving processes and beyond – a personal reflection", *Records Management Journal*, Vol. 10. No. 3, pp. 115–139.

9. Scientific Working Group on Digital Evidence (SWGDE). (2018). Digital and Multimedia Evidence Terminology. SWGDE Best Practices for Digital and Multimedia Evidence. URL: https://www.swgde.org/documents/published-complete-listing (дата звернення: 10.12.2023).

10. Marrington, A. (2015). Machine Learning in Computer Forensics: A Case Study in the Use of a Random Forest Classifier for Identifying Digital Image Source. *Digital Investigation*, 13, 93–103.

11. Цифрові компетенції як умова формування якості людського капіталу (2019): аналіт. зап. / [В.С. Куйбіда, О.М. Петроє, Л.І. Федулова, Г.О. Андрощук]. Київ: НАДУ. 28 с.

12. Forensic Science Regulator's Code of Practice 2023. URL: https://www.cps.gov.uk/legal-guidance/forensic-science-regulator-act-2021-and-forensic-science-regulators-code-practice (дата звернення: 10.12.2023).

13. Standards Australia. (2018). AS/NZS 4885:2018, Forensic Analysis – General Procedures for the Examination of Digital Evidence. URL: file:///C:/Users/Irina/Downloads/Australia%20and%20New%20Zealand%20Guidelines%20for%20Digital%20Imaging%20Processes%202013%20(1).pdf (дата звернення: 10.12.2023).

REFERENCES:

1. Fisunenko, N. (2023). Tsyfrovi transformatsii v ukraini: yevrointehratsiini protsesy ta suchasni vymohy svitu [Digital transformations in Ukraine: European integration processes and modern requirements of the world]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, (8 (08), 43–48. DOI: https://doi.org/10.32782/dees.8-8 [in Ukrainian]

2. Nochvina I.O. (2021). Tsyfrovizatsiia ekonomiky: mozhlyvosti ta osnovni zahrozy [Digitalization of the economy: opportunities and main threats]. *Zb. nauk. prats KhNPU imeni H.S. Skovorody «Ekonomika»*, 19, 90–97 [in Ukrainian]

3. Filipenko N. Ye. (2018). Informatsiini systemy v sudovo-ekspertnii diialnosti [Information systems in forensic expert activity]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vol. 18, 271–281 DOI: https://doi.org/10.32353/khrife.2018.31 [in Ukrainian]

4. Zhuravel V.A. (2015). Avtomatyzovani informatsiini systemy yak zasib zabezpechennia efektyvnosti dosudovoho rozsliduvannia [Automated information systems as a means of ensuring the effectiveness of pre-trial investigation]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*. Vol 15, 13–21 [in Ukrainian]

5. Huber, W.D. and DiGabriele, J.A. (2014). Research in forensic accounting – what matters?, *Journal of Theoretical Accounting Research,* Vol. 10. No. 1.

6. Barrett, N. (2005), "Computer forensics as a corporate governance tool", IQ Magazine – Records Management Association of Australia, Vol. 21 No. 2.

7. Avdieieva, H., Zhyvutska-Kozlovska, E. (2023). Problemy vykorystannia tsyfrovykh dokaziv u kryminalnomu sudochynstvi Ukrainy ta SShA. [Problems of using digital evidence in criminal justice in Ukraine and the USA.] *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*, 1 (30), 126–143. DOI: 10.32353/khrife.1.2023.07. [in Ukrainian]

8. Upward, F. (2000), "Modelling the continuum as paradigm shift in recordkeeping and archiving processes and beyond – a personal reflection", *Records Management Journal*, Vol. 10. No. 3, pp. 115–39.

9. Scientific Working Group on Digital Evidence (SWGDE). (2018). Digital and Multimedia Evidence Terminology. SWGDE Best Practices for Digital and Multimedia Evidence. Available at: https://www.swgde.org/documents/published-complete-listing (accessed December 10, 2023).

10. Marrington, A. (2015). Machine Learning in Computer Forensics: A Case Study in the Use of a Random Forest Classifier for Identifying Digital Image Source. *Digital Investigation*, 13, 93–103.

11. Tsyfrovi kompetentsii yak umova formuvannia yakosti liudskoho kapitalu (2019) [Digital competences as a condition for the formation of the quality of human capital]: analyst. zap / [V.S. Kuybida, O.M. Petroye, L.I. Fedulova, G.O. Androschuk]. Kyiv: NADU. 28 p. [in Ukrainian]

12. Forensic Science Regulator's Code of Practice 2023. Available at: https://www.cps.gov.uk/legal-guidance/forensic-science-regulator-act-2021-and-forensic-science-regulators-code-practice (accessed December 10, 2023).

13. Standards Australia. (2018). AS/NZS 4885:2018, Forensic Analysis – General Procedures for the Examination of Digital Evidence. Available at: file:///C:/Users/Irina/Downloads/Australia%20and%20New%20Zealand%20Guidelines%20for%20Digital%20Imaging%20Processes%202013%20(1).pdf (accessed December 10, 2023).