

ОПТИМІЗАЦІЯ ФОРЕНЗІК-ДІАГНОСТИКИ ТА АУДИТУ ДІЯЛЬНОСТІ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

©2024 ПАЦКАНЬ Ю. В., НАЗАРОВА К. О.

УДК 657.633:343.357
JEL: G17; G39; M42; O16

Пацкань Ю. В., Назарова К. О. Оптимізація форензик-діагностики та аудиту діяльності суб'єкта господарювання

Метою статті є розробка теоретико-методичних засад і практичних рекомендацій для вдосконалення процесу форензик-діагностики та аудиту діяльності суб'єкта господарювання, що передбачає створення інструментів для виявлення, запобігання та мінімізації фінансових ризиків і шахрайства, а також підвищення рівня прозорості та економічної безпеки підприємства. У статті охарактеризовано науковий міжнародний і вітчизняний доробок учених, досвід практичної діяльності аудиторських фірм, а також проаналізовано ключові аспекти оптимізації форензик-діагностики та аудиту діяльності суб'єкта господарювання. Визначено оптимальний підхід, що являє собою комбінування автоматизованих інструментів із роботою професійних експертів форензик-діагностики та забезпечує максимальну ефективність і точність. Автоматизація забезпечує масштабованість, а форензик-діагностика дозволяє враховувати індивідуальні особливості кейсів, що досягається завдяки зменшенню ризиків через коригування помилок експертами форензик-діагностики або упередження алгоритмів. Комбінований підхід дозволяє отримати баланс між ефективністю технологій та аналітичними здібностями людини. Важливим етапом оптимізації форензик-діагностики, який досліджено у статті, є поліпшення методів аналізу, які зосереджені на інтеграції передових алгоритмів, автоматизації процесів, обробці великих даних і підвищенні візуалізації. Ці інновації забезпечують точний, швидкий і комплексний підхід до виявлення шахрайства, що є важливим для сучасного бізнесу та транспарентності результатів форензик-діагностики та аудиту. Їхнє впровадження дозволяє мінімізувати ризики, скоротити витрати та підвищити ефективність внутрішнього контролю. Запропонована модернізація методів аналізу сприятиме зниженню витрат на ручну обробку, підвищуючи продуктивність форензик-команд. Завдяки прогнозуванню ризиків шахрайських дій у процесі застосування модернізованих методів аналізу компанії зможуть зменшити витрати, пов'язані з шахрайством. Кроком в оптимізації форензик-діагностики є ризик-орієнтований підхід у форензик-діагностиці, що передбачає ідентифікацію, оцінку та пріоритизацію ризиків для оптимізації процесів виявлення шахрайства, кримінальних дій чи порушень. Даний підхід дозволяє зосередитися на найбільш критичних ділянках, де ймовірність помилок або втрат є найвищою, і забезпечує більш ефективний розподіл ресурсів. Оптимізація ризик-орієнтованого підходу у форензик-діагностиці й аудиті дозволяє не лише виявляти поточні ризики, а й прогнозувати можливі загрози, зменшуючи кількості інцидентів через проактивний підхід та готовність до потенційних викликів і загроз. Інтеграція форензик-діагностики з іншими бізнес-процесами дозволить компаніям краще контролювати свої операції, знижувати ризики шахрайства та відповідати нормативним вимогам.

Ключові слова: фінансові ризики, оптимізація, модернізація, інноваційні технології, форензик-діагностика, аудит, шахрайство.

Рис.: 4. **Табл.:** 2. **Бібл.:** 27.

Пацкань Юлія Вадимівна – аспірантка кафедри фінансового аналізу та аудиту, Державний торговельно-економічний університет (вул. Кіото, 19, Київ, 02156, Україна)

E-mail: a_sidrorov@ukr.net

Назарова Каріна Олександрівна – доктор економічних наук, професор, завідувачка кафедри фінансового аналізу та аудиту, Державний торговельно-економічний університет (вул. Кіото, 19, Київ, 02156, Україна)

E-mail: k.nazarova@knu.edu.ua

ORCID: <https://orcid.org/0000-0002-5019-9244>

Researcher ID: <https://www.webofscience.com/wos/author/record/N-3427-2016>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57216845110>

UDC 657.633:343.357
JEL: G17; G39; M42; O16

Patskan Yu. V., Nazarova K. O. Optimizing the Forensic Diagnostics and Audit of Activities of Economic Entity

The article is aimed at developing theoretical and methodological foundations and practical recommendations for improving the process of forensic diagnostics and audit of the activities of an economic entity, which provides for the creation of tools for detection, prevention and minimization of financial risks and fraud, as well as increasing the level of transparency and economic security of the enterprise. The article characterizes the scientific international and domestic achievements of scholars, the experience of practical activities of audit firms, as well as analyzes the key aspects of optimizing the forensic diagnostics and audit of the activities of an economic entity. The optimal approach is defined, which is a combination of automated tools with the work of professional forensic diagnostics experts and ensures maximum efficiency and accuracy. Automation provides scalability, and forensic diagnostics allows you to take into account the individual characteristics of cases, which is achieved by reducing risks due to the correction of errors by forensic diagnostics experts or algorithm bias. The combined approach allows you to obtain a balance between the efficiency of technology and the analytical abilities of an individual. An important stage in the optimization of forensic diagnostics, which is explored in the article, is the improvement of analysis methods that focus on the integration of advanced algorithms, process automation, big data processing and visualization improvement. These innovations provide an accurate, fast, and comprehensive approach to fraud detection, which is essential for modern business and the transparency of forensic diagnostics and audit results. Their implementation allows for minimizing risks, reducing costs and increasing the efficiency of internal control. The proposed modernization of analysis methods will help reduce the cost of manual processing, increasing the productivity of forensic teams. By predicting the risks of fraudulent actions in the process of applying modernized analysis methods, companies will be able to reduce losses associated with fraud. A next step in the optimization of forensic diagnostics is a risk-based approach in forensic diag-

nostics, which involves the identification, assessment and prioritization of risks to optimize the processes of detecting fraud, criminal actions or violations. This approach allows you to focus on the most critical areas, where the probability of errors or losses is highest, and provides a more efficient allocation of resources. Optimization of the risk-based approach in forensic diagnostics and audit allows not only to identify current risks, but also to predict possible threats, reducing the number of incidents through a proactive approach and preparedness for potential challenges and threats. Integrating forensic diagnostics with other business processes will allow companies to better control their operations, reduce fraud risks, and comply with regulatory requirements.

Keywords: financial risks, optimization, modernization, innovative technologies, forensic diagnostics, audit, fraud.

Fig.: 4. **Tabl.:** 2. **Bibl.:** 27.

Patskan Yuliia V. – Postgraduate Student of the Department of Financial Analysis and Audit, State University of Trade and Economics (19 Kioto Str., Kyiv, 02156, Ukraine)

E-mail: a_sidorov@ukr.net

Nazarova Karina O. – D. Sc. (Economics), Professor, Head of the Department of Financial Analysis and Audit, State University of Trade and Economics (19 Kioto Str., Kyiv, 02156, Ukraine)

E-mail: k.nazarova@knu.edu.ua

ORCID: <https://orcid.org/0000-0002-5019-9244>

Researcher ID: <https://www.webofscience.com/wos/author/record/N-3427-2016>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57216845110>

Оптимізація форензик-діагностики та аудиту є важливим кроком для будь-якого суб'єкта господарювання в умовах невідомості економічних процесів та глобальної нестабільності, що допомагає не тільки захистити бізнес від шахрайства, а й підвищує ефективність роботи компанії загалом.

Оптимізація форензик-діагностики для суб'єкта господарювання символізує вдосконалення процесів і методів виявлення, аналізу та попередження шахрайства, фінансових зловживань або інших порушень у діяльності. Мета оптимізації – зробити процес більш ефективним, швидким, економічним і адаптованим до змін у внутрішньому середовищі компанії та на ринку.

Оптимізація форензик-діагностики та аудиту є важливим інструментом для забезпечення економічної стабільності, прозорості та боротьби з шахрайством. В Україні це питання має особливу актуальність через високий рівень ризиків і потребу у швидкій адаптації до міжнародних стандартів. У світовій практиці такі заходи підвищують ефективність бізнесу та довіру до нього, що є ключовим фактором сталого розвитку.

Теоретичну та практичну бази для дослідження оптимізації форензик-діагностики й аудиту суб'єкта господарювання висвітлено в працях як іноземних, так і вітчизняних науковців, а саме: J. T. Wells [1], M. J. Comer [2], M. T. Biegelman [3], Т. Гайдучок [4], М. В. Дубініна, С. В. Сирцева, Т. Ю. Янковська [5], М. Хеленюк [6] та ін.

Попри наявність значної кількості досліджень та теорій щодо оптимізації форензик-діагностики й аудиту для суб'єктів господарювання, існує багато недосліджених аспектів, які цілком обґрунтовані, такі як адаптація міжнародного досвіду до національних умов, розробка стандартів та регламентів, використання сучасних технологій, розуміння мотивації та поведінкових моделей осіб, схильних до

фінансових злочинів, які можуть сприяти розробці превентивних заходів та оптимізації процесу розслідування.

Мета статті – розробка теоретико-методичних засад і практичних рекомендацій для вдосконалення процесу форензик-діагностики й аудиту діяльності суб'єкта господарювання, що передбачає створення інструментів для виявлення, запобігання та мінімізації фінансових ризиків і шахрайства, а також підвищення рівня прозорості та економічної безпеки підприємства.

У сучасному бізнес-середовищі збільшуються ризики фінансових злочинів, зловживань і шахрайських дій, що негативно впливають на діяльність суб'єкта господарювання. Форензик-діагностика й аудит є ключовими інструментами для своєчасного виявлення та протидії цим ризикам. Питання впровадження інноваційних технологій для проведення форензик-діагностики й аудиту залишаються актуальними та нагальними, дослідження та впровадження яких сприятиме підвищенню ефективності економічних розслідувань.

Упровадження сучасних технологій для збору, аналізу та перевірки даних без необхідності ручної роботи є важливим фактором в ефективній роботі форензик-діагностики й аудиту. Автоматизація цих процесів дозволить підвищити ефективність, точність і швидкість виявлення аномалій, зменшуючи людський фактор і ризик помилок. Інноваційні технології дозволяють зробити процес форензик-діагностики й аудиту швидшим, точнішим і прозорішим, сприяють підвищенню ефективності економічних розслідувань, мінімізують ризики шахрайства та фінансових порушень, а також забезпечують вищий рівень економічної безпеки суб'єкта господарювання (рис. 1). Автоматизація форензик-діагностики й аудиту має великий потенціал для підвищення ефективності та точності аналізу.



Рис. 1. Переваги автоматизації форензик-діагностики й аудиту суб'єкта господарювання

Джерело: авторська розробка.

Оптимальним підходом, на нашу думку, є комбінування автоматизованих інструментів із роботою професійних експертів форензик-діагностики, що забезпечує максимальну ефективність і точність. Автоматизація бере на себе рутинні та виснажливі завдання, залишаючи експертам форензик-діагностики час для аналізу критично важливих аспектів. Автоматизовані системи проводять первинну обробку, виділяючи потенційні аномалії, підозрілі транзакції або невідповідності. Експерти форензик-діагностики приймають остаточні рішення, враховуючи як дані, отримані з автоматизації, так і свою інтуїцію та досвід. Автоматизація забезпечує масштабованість, а форензик-діагностика дозволяє враховувати індивідуальні особливості кейсів, що досягається завдяки зменшенню ризиків через коригування помилок експертами форензик-діагностики або упередження алгоритмів. Комбінований підхід дозволяє отримати баланс між ефективністю технологій та аналітичними здібностями людини. Цей метод забезпечує точність, масштабованість і адаптивність, які є необхідними для вирішення сучасних викликів у форензик-діагностиці й аудиті, що сприятиме забезпеченню довгострокової стабільності та надійності процесів суб'єкта господарювання.

Важливим етапом оптимізації форензик-діагностики є поліпшення методів аналізу, які зосереджені на інтеграції передових алгоритмів, авто-

матизації процесів, обробці великих даних і підвищенні візуалізації. Ці інновації забезпечують точний, швидкий і комплексний підхід до виявлення шахрайства, що є важливим для сучасного бізнесу та транспарентності результатів форензик-діагностики й аудиту. Їхнє впровадження дозволяє мінімізувати ризики, скоротити витрати та підвищити ефективність внутрішнього контролю (табл. 1).

Інтеграція інноваційних технологій, таких як AI, Big Data та аналітика ризиків, забезпечить більш точне виявлення загроз і підвищить ефективність форензик-діагностики й аудиту суб'єкта господарювання шляхом зосередження на найважливіших даних, які потребують негайної перевірки, здійснюючи ідентифікацію сфер, де можливі найбільші втрати, шахрайство у фінансових операціях тощо.

Упровадження AI, яке здатне будувати прогностичні моделі на основі історичних даних, дозволить не лише виявляти шахрайство, яке вже відбулося, а й прогнозувати майбутні ризики та шахрайські схеми. Наприклад, аналіз транзакцій у кредитній сфері дозволяє передбачити ризик шахрайства клієнта ще до його виникнення. Big Data дозволить об'єднувати дані з різних джерел (ERP-систем, CRM, банківські транзакції, соціальні мережі тощо) в єдину базу для аналізу, що сприятиме комплексному баченню ситуації, забезпеченню

Оптимізація методів аналізу форензик-діагностики й аудиту

Напрямок	Обґрунтування	Рекомендації щодо модернізації	Запровадження у форензик-діагностиці
1	2	3	4
Штучний інтелект і машинне навчання (AI/ML)	Алгоритми AI можуть знаходити аномалії та складні нелінійні залежності, які недоступні для традиційних методів. Методи машинного навчання демонструють високу ефективність у виявленні аномалій	– Використання Isolation Forest для автоматичного виявлення аномалій; – налаштування моделей для класифікації типів шахрайства; – прогнозування зон ризиків шахрайства	– Автоматизація виявлення шахрайства в банківських транзакціях; – розпізнавання аномалій у поведінкових паттернах співробітників; – пошук нових схем шахрайства
Big Data (великі дані)	Інструменти, такі як Hadoop і Spark, дозволяють аналізувати мільйони записів за секунди, що необхідно для обробки складних і великих обсягів інформації	– Централізація даних із різних джерел; – потокова обробка даних для миттєвого реагування на підозрілі дії	– Аналіз великих обсягів транзакцій для пошуку фінансових махінацій; – виявлення кіберзагроз у корпоративній мережі; – обробка лог-файлів
Мультифакторний аналіз	Аналіз інформації з різних джерел, таких як бази даних, поведінкові патерни та соціальні мережі, дозволяє отримувати більш точні результати	– Побудова графів зв'язків; – кореляція між фінансовими операціями, IT-доступом і внутрішнім листуванням; – мультиджерельний аналіз	– Виявлення складних схем змови між співробітниками; – поєднання фінансових і поведінкових даних для аналізу шахрайських дій; – побудова соціальних графів
Автоматизація обробки цифрових доказів	Автоматизація забезпечує швидкість і точність аналізу даних із цифрових носіїв, зменшуючи вплив людського фактора	– Автоматизована обробка зображень дисків і логів; – інтеграція платформ для аналізу мереж, електронної пошти та файлів	– Аналіз мережевого трафіку для виявлення порушень; – автоматична обробка даних із пристроїв підозрюваних; – обробка великих наборів метаданих
Блокчейн-технології	Блокчейн забезпечує незмінність записів і прозорість транзакцій, що ідеально підходить для створення захищених журналів	– Захищеність цифрових доказів; – використання смарт-контрактів; – прозоре збереження результатів аудиту	– Збереження ланцюгів цифрових доказів для судових процесів; – відстеження змін у фінансових документах; – верифікація автентичності транзакцій
Когнітивний аналіз	Когнітивні системи дозволяють аналізувати природну мову й ідентифікувати приховані взаємозв'язки у великих текстових масивах	– Аналіз текстів через NLP; – контекстуальний аналіз для розуміння ситуацій; – ідентифікація прихованих зв'язків	– Виявлення шахрайських дій через аналіз електронного листування; – аналіз звітів для виявлення розбіжностей; – розуміння складних мотивів дій співробітників
Стандарти та протоколи	Використання стандартів ISO/IEC 27037 гарантує правильне поводження з цифровими доказами, забезпечуючи їх прийняття в судах	– Стандартизована процедура збору, обробки та зберігання цифрових доказів; – юридична відповідність міжнародним нормам	– Використання стандартів для оформлення цифрових доказів; – створення документації для судових процесів; – захист конфіденційних даних

1	2	3	4
Підготовка кадрів	Постійна освіта та навчання співробітників дозволяють адаптуватися до швидкозмінних технологій і методів аналізу	– Використання симуляцій для тренування команд; – розробка навчальних програм; – тренінги з нових інструментів	– Навчання персоналу роботи з інструментами форензик-діагностики; – підвищення кваліфікації у виявленні кіберзагроз; – імітація інцидентів для поліпшення реакції

Джерело: складено авторами на основі [7–27].

більш точної діагностики та значному вдосконаленню процесів економічних розслідувань і управління ризиками.

На схемі потоку запропоновані основні пріоритети для модернізації методів аналізу форензик-діагностики в умовах нестабільної економіки, яка організована за ключовими напрямками, що логічно взаємопов'язані та ілюструють послідовність і взаємодію між етапами процесу (рис. 2). Пріоритети суб'єкта господарювання повинні бути спрямовані на оптимізацію витрат, підвищення точності, забезпечення безпеки та створення адаптивної, масштабованої системи. Впровадження сучасних технологій в систему, таких як AI, Big Data та хмарні обчислення, дозволять ефективно реагувати на виклики сучасних ринкових умов і потреб бізнес середовища. Завдяки Big Data та AI суб'єкти господарювання зможуть створювати системи, які працюватимуть у режимі реального часу, постійно відстежуючи транзакції, операції або документообіг, що дозволить виявляти шахрайські дії миттєво, а не після закінчення операційного циклу.

Запропонована модернізація методів аналізу сприятиме зниженню витрат на ручну обробку, підвищуючи продуктивність форензик-команд. Завдяки прогнозуванню ризиків оцінки шахрайських дій у процесі застосування модернізованих методів аналізу компанії зможуть зменшити втрати, пов'язані з шахрайством. Шахрайські схеми швидко змінюються, але моделі машинного навчання та штучного інтелекту автоматично підлаштовуються до нових ризиків, підвищують ефективність виявлення складних схем шахрайства, забезпечують обробку великих обсягів даних і гарантують дотримання стандартів обробки цифрових доказів, що дозволяє форензик-діагностиці залишатися актуальною та ефективною за будь-яких умов процесу.

Наступним кроком в оптимізації форензик-діагностики є ризик-орієнтований підхід, що передбачає ідентифікацію, оцінку та пріоритизацію ризиків для оптимізації процесів виявлення шах-

райства, кримінальних дій чи порушень. Даний підхід дозволяє зосередитися на найбільш критичних ділянках, де ймовірність помилок або втрат є найвищою, і забезпечує більш ефективний розподіл ресурсів.

Управління ризиками, як основа ефективності діяльності суб'єкта господарювання, свідчить, що концентрація зусиль відбувається на ділянках із найбільшим потенційним впливом, таким як високий ризик шахрайства, що дозволяє досягати більшого ефекту за менших витрат. У форензик-діагностиці фокус зосереджується на ідентифікації зон високого ризику, таких як певні типи злочинів, локації чи методи вчинення правопорушень. Розробка спеціалізованих методик для аналізу найбільш ризикованих сценаріїв, що використовуються в ризик-орієнтованих моделях, дозволяє зменшити кількість хибнопозитивних результатів у криміналістичному аналізі.

Криміналістичний аналіз є невід'ємною складовою форензик-діагностики, спрямованої на виявлення, розслідування та запобігання економічним злочинам і шахрайству в діяльності суб'єкта господарювання. Використання криміналістичних методів дозволяє глибше дослідити фінансові документи, виявити приховані схеми зловживань та забезпечити доказову базу для судових процесів. Форензик-діагностика відрізняється від традиційного аудиту, інспектування та економічної експертизи своєю спрямованістю на розслідування конкретних інцидентів та збору доказів. Проведення порівняльного аналізу дозволяє визначити унікальні риси форензик-діагностики та її практичне застосування.

Криміналістичний аналіз у форензик-діагностиці й аудиті має значні переваги, зокрема забезпечує глибокий аналіз, підвищує прозорість та зменшує ризики шахрайства. Проте він вимагає значних ресурсів і спеціалізованих знань. Незважаючи на це, його використання дає компанії стратегічні та фінансові переваги, включно з довгостроковим зниженням витрат і підвищенням довіри до бізнесу.



Рис. 2. Схема потоку процесу модернізації методів аналізу форензік-діагностики

Джерело: авторська розробка.

Оптимізацію ризик-орієнтованого підходу у форензік-діагностиці й аудиті пропонуємо базувати на системному підході до ідентифікації, оцінки, управління, моніторингу та вдосконалення методів роботи з ризиками, що дозволить досягти високої ефективності, знизити втрати від шахрайства та підвищити адаптивність у мінливих умовах (рис. 3).

У запропонованій потенціалізації ризик-орієнтованого підходу у форензік-діагностиці передбачається чіткий алгоритм дій для підвищення точності, ефективності й адаптивності процесів виявлення ризиків шахрайства. Кожен етап потенціалізації спрямований на усунення недоліків, покращення якості аналізу та ефективне використання ресурсів у процесі форензік-діагностики й аудиту. Ризик-орієнтований підхід передбачає структуровану та послідовну роботу форензік-діагностики з ризиками шахрайства, забезпечуючи при цьому цілісне управління ризиками та легкість інтеграції з іншими бізнес-процесами та системами моніторингу. Ефективне управління ризиками зменшує ймовірність репутаційних втрат через інциденти шахрайства або витік даних, підтримує довіру з боку клієнтів, партнерів і регуляторів, а також поліпшує імідж компанії як відповідального та надійного суб'єкта господарювання.

Таким чином, оптимізація ризик-орієнтованого підходу у форензік-діагностиці й аудиті до-

зволяє не лише виявляти поточні ризики, а й прогнозувати можливі загрози, зменшуючи кількість інцидентів шляхом проактивного підходу та готовності до потенційних викликів і загроз. Систематизація ризик-орієнтованого підходу сприяє кращій координації між підрозділами компанії, що зумовлює забезпечення більш ефективної командної роботи та узгодженості дій між відділами безпеки, аналітики й управління. Цей підхід є ключовим для компаній, які прагнуть досягти високого рівня безпеки та довіри.

Оцінка ефективності впровадження ризик-орієнтованого підходу у форензік-діагностиці є багатогранним процесом, що включає в себе аналіз точності, фінансових показників, операційної ефективності, адаптивності, а також організаційних змін. Використовуючи ці метрики, можна зрозуміти, чи досягнуто бажаних результатів і в яких аспектах є потреба в подальшому вдосконаленні. Оцінка впровадження ризик-орієнтованого підходу залежить від багатьох метрик, але пріоритетними є ті, які дозволяють забезпечити максимальну точність, ефективність та мінімізацію втрат. Ключові метрики, які слід вважати найважливішими:

1. Метрики точності та виявлення ризиків.

1.1. Точність (*Precision*) – визначає, скільки з усіх виявлених ризикових випадків були правиль-



Рис. 3. Потенціалізація ризик-орієнтованого підходу у форензик-діагностиці й аудіті

Джерело: авторська розробка.

ними; зменшує витрати на додаткову перевірку хибно-позитивних результатів; мінімізує витрати часу та ресурсів на перевірку помилкових спрацювань.

1.2. Повнота (*Recall*) – показує, скільки реальних ризиків система змогла виявити; особливо критична для виявлення шахрайства чи серйозних загроз; максимізує захоплення реальних ризиків.

1.3. *F1-Score* – гармонійний баланс між точністю (*Precision*) і повнотою (*Recall*); особливо корисна, якщо є дисбаланс у даних (наприклад, шахрайство є рідкісним явищем); забезпечує збалансований підхід між мінімізацією помилок і виявленням всіх ризиків.

2. Метрики фінансової ефективності.

2.1. *Зниження фінансових витрат* – прямо пов'язана з основною метою впровадження – мінімізацією витрат від шахрайства, кіберзагроз або ін-

ших ризиків; дозволяє оцінити економічний ефект впровадження, порівняти втрати до і після впровадження.

2.2. *ROI (Return on Investment)* – відображає фінансову вигоду від впровадження ризик-орієнтованого підходу порівняно з витратами; служить візуалізацією вигідності інвестицій у нові системи.

2.3. *Скорочення операційних витрат* – автоматизація процесів і зменшення ручної роботи дозволяє скоротити витрати на персонал і перевірки; оцінює зменшення витрат на рутинні операції.

3. Метрики швидкості та операційної ефективності.

3.1. *Швидкість реагування* – дає змогу оцінити, наскільки швидко система реагує на підозрілі активності чи аномалії; зменшення часу реагування дозволяє мінімізувати втрати.

3.2. *Інтеграція з процесами* – впровадження має працювати разом із наявними системами CRM, ERP чи кібербезпеки; забезпечення безшовної роботи системи без перешкод у процесах.

4. Метрики адаптивності та масштабованості.

4.1. *Адаптивність до нових ризиків* – здатність системи розпізнавати нові типи шахрайства чи загроз забезпечує її довгострокову актуальність; проводить оцінку швидкості оновлення моделі на основі нових даних.

4.2. *Масштабованість* – система має ефективно працювати при зростанні обсягів даних чи збільшенні кількості транзакцій; підтримка стабільності при значному навантаженні.

5. Метрики продуктивності персоналу.

5.1. *Успішність навчання персоналу* – забезпечує ефективну роботу з новими інструментами; рівень засвоєння нових методів і підходів.

5.2. *Поліпшення співпраці між підрозділами* – ризик-орієнтований підхід вимагає інтеграції між різними департаментами; надає оцінку взаємодії та обміну інформацією між підрозділами.

Перелічені маркери забезпечать чітке розуміння ефективності впровадженої системи ризик-орієнтованого підходу у форензик-діагностику, що дозволять визначити успішні аспекти та сфери для вдосконалення, зокрема точність, швидкість, масштабованість і фінансову вигоду.

Важомим при дослідженні оптимізації форензик-діагностики стало отримання ефективних результатів при інтеграції форензик-діагностики в рамках основних бізнес-процесів. Інтеграція форензик-діагностики з іншими бізнес-процесами допомагає суб'єктам господарювання підвищити ефективність управління ризиками, забезпечити відповідність нормативним вимогам і поліпшити внутрішній контроль. Інтеграція форензик-діагностики передбачає впровадження методів та інструментів для виявлення аномалій, шахрайства або ризиків у рамках основних бізнес-процесів, що дозволить компаніям ідентифікувати проблеми на ранньому етапі та оперативно реагувати на них (табл. 2). Більшість рішень форензик-діагностики, заснованих на AI, є «чорними ящиками», що ускладнює розуміння, яким методом були отримані результати. Ризик упередженості інтеграції форензик-діагностики полягає в тому, що моделі програмувалися на упереджених даних і, як наслідок, можуть генерувати некоректні висновки.

Інтеграція нових технологій може створювати додаткові точки доступу для зловмисників, які можуть маніпулювати даними, що аналізуються форензик-діагностикою й аудитом, або здійснювати атаки на інфраструктуру.

Інтеграція форензик-діагностики й аудиту супроводжується значними викликами, проте правильний підхід до планування, вибору інструментів, забезпечення відповідності нормативам, упровадження засобів кібербезпеки та навчання персоналу допоможе мінімізувати ризики та реалізувати потенціал інтеграції форензик-діагностики для поліпшення бізнес-процесів.

Отже, інтеграція форензик-діагностики з іншими бізнес-процесами дозволить компаніям краще контролювати свої операції, знижувати ризики шахрайства та відповідати нормативним вимогам. Цей стратегічний підхід підвищує ефективність і забезпечує конкурентні переваги суб'єкта господарювання. Мета інтеграції форензик-діагностики з іншими бізнес-процесами – зробити форензик-діагностику невід'ємною частиною бізнесу, а не лише «реакцією на проблему».

Таким чином, завдяки оптимізації форензик-діагностики суб'єкта господарювання підвищується ефективність управління ресурсами шляхом автоматизації процесів, які зменшують витрати часу та людських ресурсів, а також завдяки аналітичним інструментам, що оптимізують витрати на аудит і розслідування форензик-діагностики. Виявлення шахрайства на ранніх етапах дозволяє мінімізувати збитки та посилити ефективність внутрішнього контролю, який сприятиме запобіганню неправомірного використання активів.

Зміцнення системи внутрішнього контролю шляхом упровадження інструментів моніторингу дозволяє своєчасно реагувати на ризики. Зниження ризику шахрайства сприяє підвищенню стабільності та зростанню конкурентоспроможності суб'єкта господарювання, що веде до прозорості бізнес-процесів, підвищує репутацію компанії та посилює довіру інвесторів і партнерів. Системний підхід до внутрішнього контролю демонструє надійність управління. Ефективний внутрішній контроль дозволяє суб'єктам господарювання залишатися економічно привабливими, мінімізувати ризики та швидше реагувати на зовнішні виклики.

Оптимізація форензик-діагностики допомагає суб'єктам господарювання не лише запобігати збиткам, але й створювати більш стабільні та прозорі умови для ведення бізнесу, що, своєю чергою, формує умови для транспарентності результатів проведених досліджень.

Транспарентність результатів форензик-діагностики й аудиту діяльності суб'єкта господарювання може суттєво вплинути на ефективність його діяльності та є ознакою відкритості, чіткості та зрозумілості висновків, отриманих у процесі дослідження, для всіх зацікавлених сторін. Висока

Інтеграція форензик-діагностики з бізнес-процесами суб'єкта господарювання

Сфера	Завдання	Інструменти	Переваги	Виклики
Фінансові процеси	<ul style="list-style-type: none"> – Автоматичний аналіз транзакцій; – виявлення фальсифікації звітності; – перевірка платежів для уникнення дублювань 	<ul style="list-style-type: none"> – ACL Analytics; – IDEA; – Power BI 	<ul style="list-style-type: none"> – Прозорість транзакцій; – зменшення витрат на аудит; – відповідність нормативам 	<ul style="list-style-type: none"> – Складність інтеграції з ERP; – потреба у великих обсягах якісних даних; – високі витрати на впровадження
Управління кадрами	<ul style="list-style-type: none"> – Аналіз поведінкових даних працівників; – виявлення конфліктів інтересів; – перевірка надійності нових співробітників 	<ul style="list-style-type: none"> – Workday; – SAP Success Factors; – форензик-застосунки 	<ul style="list-style-type: none"> – Підвищення надійності кадрів; – зменшення конфліктів інтересів; – поліпшення управління персоналом 	<ul style="list-style-type: none"> – Опір співробітників до змін; – складність навчання персоналу; – забезпечення конфіденційності даних
Ланцюги постачання	<ul style="list-style-type: none"> – Перевірка відповідності контрактів; – аналіз ризиків постачальників; – моніторинг витрат для уникнення переплат 	<ul style="list-style-type: none"> – Coupa; – Ariba; – аналітика ризиків 	<ul style="list-style-type: none"> – Зниження ризиків шахрайства; – ефективний контроль витрат; – поліпшення відносин із постачальниками 	<ul style="list-style-type: none"> – Невідповідність контрактів; – можливість шахрайства серед постачальників; – недостатній моніторинг ризиків
Операційна діяльність	<ul style="list-style-type: none"> – Аналіз продуктивності операцій; – виявлення недоліків у процесах; – запобігання витоку ресурсів 	<ul style="list-style-type: none"> – Tableau; – Qlik Sense; – операційна аналітика 	<ul style="list-style-type: none"> – Зменшення операційних втрат; – підвищення продуктивності; – прогнозування ризиків у реальному часі 	<ul style="list-style-type: none"> – Технічні збої у процесах; – високі вимоги до ресурсів; – потреба в регулярному оновленні моделей

Джерело: складено авторами.

якість фінансової та операційної прозорості сприяє залученню нових партнерів. Відкритість і прозорість результатів забезпечують довіру з боку інвесторів, кредиторів, партнерів і регуляторів, що в кінцевому підсумку позитивно відображається на фінансовій і ринковій позиції суб'єкта господарювання, що є ключовим аспектом якості й ефективності проведення процедури форензик-діагностики й аудиту (рис. 4).

Відкритість результатів діяльності суб'єкта господарювання підвищує довіру інвесторів, кредиторів і бізнес-партнерів, що спрощує доступ до капіталу, зменшує витрати на позики та сприяє залученню стратегічних партнерів, а прозорість бізнес-процесів створює відчуття справедливості та підвищує лояльність працівників. Транспарентність результатів діяльності сприяє виявленню й усуненню можливих корупційних схем, шахрайства чи інших зловживань, що можуть знижувати ефективність діяльності компанії.

Результати форензик-діагностики можуть виявити слабкі місця в бізнес-процесах, які за рішенням управлінського персоналу підлягають по-

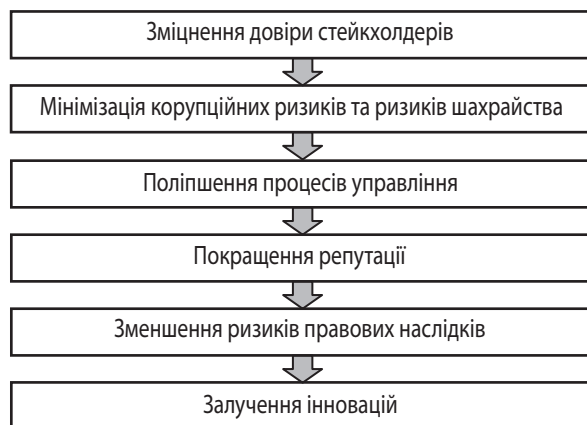


Рис. 4. Вплив транспарентності результатів форензик-діагностики та аудиту на ефективність діяльності суб'єкта господарювання

Джерело: авторська розробка.

ліпшенню та вдосконаленню. Прозорість дозволяє керівникам швидше приймати обґрунтовані рішення, засновані на даних, а не на припущеннях. Транспарентність результатів діяльності суб'єкта господарювання у виявлених недоліках сприяє впровадженню нових технологій або підходів

для їхнього усунення, що в перспективі покращує ефективність діяльності. Проте є і певні недоліки: надмірна відкритість може призвести до розголошення вразливих аспектів діяльності, які можуть бути використані конкурентами, а також публікація негативних результатів може спровокувати короткострокові репутаційні втрати.

Таким чином, оптимальний рівень транспарентності у форензик-діагностиці й аудиту забезпечує баланс між довірою стейкхолдерів, зменшенням ризиків та збереженням конкурентних переваг, що дозволяє суб'єкту господарювання підвищити ефективність управління та довгострокову стабільність.

Важливо зазначити, що в сучасному бізнес-середовищі транспарентність результатів форензик-діагностики й аудиту діяльності суб'єкта господарювання сприяє відповідності екологічним, соціальним і управлінським стандартам, які враховуються при оцінці компаній, а також позитивна репутація підвищує конкурентоспроможність компанії, що збільшує дохід і, відповідно, її ринкову вартість. При цьому інвестори отримують чітке розуміння ризиків, що дозволяє їм точніше оцінювати бізнес, а зниження ризиків зазвичай приводить до збільшення вартості компанії (зменшується дисконт за ризик при оцінці).

Отже, транспарентні результати форензик-діагностики й аудиту свідчать про надійність і відкритість бізнесу, що підвищує інвестиційну привабливість та сприяє зростанню довіри інвесторів на фондових ринках, що, своєю чергою, приводить до зростання ринкової капіталізації компанії. Прозорість знижує ризик регуляторних штрафів, втрати контрактів або репутаційних втрат через корупцію чи шахрайство. Виявлення й усунення таких явищ у процесах завдяки форензик-діагностиці й аудиту сприяє підвищенню рентабельності, що позитивно впливає на фінансові результати і вартість суб'єкта господарювання, забезпечує стабільність грошових потоків, що позитивно впливає на оцінку бізнесу загалом.

ВИСНОВКИ

Узагальнюючи проведені дослідження, слід зазначити, що запровадження оптимізованої форензик-діагностики й аудиту в діяльність суб'єкта господарювання сприятиме транспарентності результатів завдяки своєчасному усуненню слабких місць у системі внутрішнього контролю, де можуть виникати шахрайські схеми або корупційні дії, що сприятиме зниженню ймовірності фінансових втрат, судових позовів і репутаційних ризиків. Запровадження оптимізованої форензик-діагности-

ки й аудиту допомагає виявляти неефективність в операційній діяльності, а саме: у логістиці, закупівлях або фінансовому управлінні, що зумовить економію ресурсів і підвищить продуктивність компанії. Інтеграція технологій штучного інтелекту, машинного навчання та блокчейну у форензик-діагностику й аудит дозволить забезпечити високий рівень точності аналізу та захисту даних, що позитивно вплине на інноваційність компанії, її конкурентоспроможність і знизить ймовірність технічних помилок. Упровадження оптимізованих форензик-діагностики й аудиту стане стратегічним кроком, що забезпечить прозорість і стабільність у діяльності суб'єкта господарювання. ■

БІБЛІОГРАФІЯ

1. Wells J. T. *Fraud examination: investigative and audit procedures*. New York : Quorum Books, 1992. 369 p.
2. Comer M. J. *Investigating Corporate Fraud*. Routledge, 2003. 264 p.
3. Biegelman M. T. *Building a World-Class Compliance Program: Best Practices and Strategies for Success*. Wiley, 2008. 320 p.
4. Гайдучок Т. Форензик-контроль: захист фінансових активів та виявлення шахрайства. *Фінансово-економічні, соціальні та правові аспекти розвитку регіонів: загрози та виклики* : матеріали Міжнародної науково-практичної конференції (м. Чернівці, 24 травня 2024 р.). Чернівці : Технодрук, 2024. С. 101–105.
5. Дубініна М. В., Сирцева С. В., Янковська Т. Ю. Форензик як метод розслідування внутрішньокорпоративних випадків шахрайства. *Інфраструктура ринку*. 2019. Вип. 38. С. 377–383. DOI: <https://doi.org/10.32843/infrastruct38-59>
6. Хеленюк М. Форензик: європейський досвід vs українські реалії. *Юридична Газета online*. 2021. № 8. URL: <https://jur-gazeta.com/publications/practice/korporativne-pravo-ma/forenzik-evropeyskiy-dosvid-vs-ukrayinski-realiyi.html>
7. Штучний інтелект у виявленні шахрайства та підвищенні безпеки. URL: <https://www.probesto.com/ua>
8. Використання машинного навчання для виявлення шахрайства в електронній комерції. URL: <https://peerdh.com/uk/blogs/programming-insights/leveraging-machine-learning-for-fraud-detection-in-e-commerce-transactions>
9. Що таке Machine Learning? *denovo*. 17.05.2024. URL: <https://denovo.ua/resources/what-is-machine-learning>
10. Що таке глибоке навчання? Все, що вам потрібно знати. *cybercalm*. 15.04.2024. URL: <https://cybercalm.org/novyny/shho-take-deep-learning/>
11. Впровадження алгоритмів виявлення аномалій для визначення шахрайських витрат. URL: <https://peerdh.com/uk/blogs/programming-insights/>

- implementing-anomaly-detection-algorithms-for-identifying-fraudulent-expenses
12. Рубитель О. Значення моделі шахрайства для аудитора, або мінуси висококваліфікованих людей. *LIGA.net*. 23.10.2024. URL: <https://blog.liga.net/user/orubitel/article/54563>
 13. Li K., Yang T., Zhou M. et al. SEFraud: Graph-based Self-Explainable Fraud Detection via Interpretative Mask Learning. *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 24 August 2024. P. 5329–5338. DOI: <https://doi.org/10.1145/3637528.3671534>
 14. Семеренська В. В. Дослідження методів виявлення аномалій за допомогою відеоаналітики на основі штучного інтелекту у комплексних системах безпеки : пояснювальна записка. Харків, 2023. 66 с. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/9107dae1-edcf-46a9-a780-818cf2973aea/content>
 15. Ezugwu A. E., Ikotun A. M., Oyelade O. O. et al. A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects. *Engineering Applications of Artificial Intelligence*. 2022. Vol. 110. Art. 104743. DOI: <https://doi.org/10.1016/j.engappai.2022.104743>
 16. Alghanmi N., Alotaibi R., Buhari S. M. HLMCC: A Hybrid Learning Anomaly Detection Model for Unlabeled Data in Internet of Things. *IEEE Access*. 2019. Vol. 7. P. 179492–179504. DOI: <https://doi.org/10.1109/access.2019.2959739>
 17. Ahmed N., Barczak A. L. C., Susnjak T. et al. A comprehensive performance analysis of Apache Hadoop and Apache Spark for large scale data sets using HiBench. *Journal of Big Data*. 2020. Vol. 7. Art. 110. DOI: <https://link.springer.com/article/10.1186/s40537-020-00388-5>
 18. Venkatraman S., Fahd K., Kaspi S., Venkatraman R. SQL Versus NoSQL Movement with Big Data Analytics. *International Journal of Information Technology and Computer Science*. 2016. Vol. 8. No. 12. P. 59–66. DOI: <https://doi.org/10.5815/ijitcs.2016.12.07>
 19. Habeeb R. A. A., Nasaruddin F., Gani A. et al. Real-time big data processing for anomaly detection: A Survey. *International Journal of Information Management*. 2019. Vol. 45. P. 289–307. DOI: <https://doi.org/10.1016/j.ijinfomgt.2018.08.006>
 20. Gottwalt F., Chang E., Dillon T. CorrCorr: A feature selection method for multivariate correlation network anomaly detection techniques. *Computers & Security*. 2019. Vol. 83. P. 234–245. DOI: <https://doi.org/10.1016/j.cose.2019.02.008>
 21. Maciqg P. S., Kryszkiewicz M., Bembenik R. et al. Unsupervised Anomaly Detection in Stream Data with Online Evolving Spiking Neural Networks. *Neural Networks*. 2021. Vol. 139. P. 118–139. DOI: <https://doi.org/10.1016/j.neunet.2021.02.017>
 22. Prajapati J., Choudhary N. A Systematic Review on Anomaly Detection. *International Journal of Advanced Research in Science, Communication and Technology*. 2023. Vol. 3. Iss. 2. P. 75–82. DOI: <https://doi.org/10.48175/ijarsct-8664>
 23. Лихошерст В. Р. Алгоритм класифікації та класкового аналізу DenStream для вирішення задач з забезпечення інформаційної безпеки : дипломна робота. Київ, 2021. 80 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/902fdf1b-040a-4242-9e36-6113980516ef/content>
 24. Fosić I., Žagar D., Grgić K., Križanović V. Anomaly detection in NetFlow network traffic using supervised machine learning algorithms. *Journal of Industrial Information Integration*. 2023. Vol. 33. DOI: <https://doi.org/10.1016/j.jii.2023.100466>
 25. Zhang Ch., Yang Sh., Mao L, Ning H. Anomaly detection and defense techniques in federated learning: a comprehensive review. *Artificial Intelligence Review*. 2024. Vol. 57. Art. 150. DOI: <https://doi.org/10.1007/s10462-024-10796-1>
 26. Badr W. Uncovering Anomalies with Variational Autoencoders (VAE): A Deep Dive into the World of Unsupervised Learning. *Medium*. 17.01.2023. URL: <https://towardsdatascience.com/uncovering-anomalies-with-variational-autoencoders-vae-a-deep-dive-into-the-world-of-1b2bce47e2e9>
 27. Pedregosa F., Varoquaux C., Gramfort A. et al. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*. 2011. Vol. 12. P. 2825–2830. URL: <https://www.jmlr.org/papers/volume12/pedregosa11a/pedregosa11a.pdf>

REFERENCES

- Ahmed, N. et al. "A comprehensive performance analysis of Apache Hadoop and Apache Spark for large scale data sets using HiBench". *Journal of Big Data*, art. 110, vol. 7 (2020). DOI: <https://link.springer.com/article/10.1186/s40537-020-00388-5>
- Alghanmi, N., Alotaibi, R., and Buhari, S. M. "HLMCC: A Hybrid Learning Anomaly Detection Model for Unlabeled Data in Internet of Things". *IEEE Access*, vol. 7 (2019): 179492-179504. DOI: <https://doi.org/10.1109/access.2019.2959739>
- Badr, W. "Uncovering Anomalies with Variational Autoencoders (VAE): A Deep Dive into the World of Unsupervised Learning". *Medium*. January 17, 2023. <https://towardsdatascience.com/uncovering-anomalies-with-variational-autoencoders-vae-a-deep-dive-into-the-world-of-1b2bce47e2e9>
- Biegelman, M. T. *Building a World-Class Compliance Program: Best Practices and Strategies for Success*. Wiley, 2008.
- Comer, M. J. *Investigating Corporate Fraud*. Routledge, 2003.
- Dubinina, M. V., Syrtseva, S. V., and Yankovska, T. Yu. "Forenzik yak metod rozsliduvannia vnutrishno-

- korporatyvnykh vypadkiv shakhraistva" [Forensic as a Method of Investigation of Internal Corporate Cases of Fraud]. *Infrastruktura rynku*, no. 38 (2019): 377-383.
DOI: <https://doi.org/10.32843/infrastruct38-59>
- Ezugwu, A. E. et al. "A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects". *Engineering Applications of Artificial Intelligence*, art. 104743, vol. 110 (2022).
DOI: <https://doi.org/10.1016/j.engappai.2022.104743>
- Fosic, I. et al. "Anomaly detection in NetFlow network traffic using supervised machine learning algorithms". *Journal of Industrial Information Integration*, vol. 33 (2023).
DOI: <https://doi.org/10.1016/j.jii.2023.100466>
- Gottwalt, F., Chang, E., and Dillon, T. "CorrCorr: A feature selection method for multivariate correlation network anomaly detection techniques". *Computers & Security*, vol. 83 (2019): 234-245.
DOI: <https://doi.org/10.1016/j.cose.2019.02.008>
- Habeeb, R. A. A. et al. "Real-time big data processing for anomaly detection: A Survey". *International Journal of Information Management*, vol. 45 (2019): 289-307.
DOI: <https://doi.org/10.1016/j.ijinfomgt.2018.08.006>
- Haiduchok, T. "Forenzik-kontrol: zakhyst finansovykh aktyviv ta vyavleniia shakhraistva" [Forensic Control: Protection of Financial Assets and Fraud Detection]. *Finansovo-ekonomichni, sotsialni ta pravovi aspekty rozvytku rehioniv: zahrozy ta vyklyky*. Chervnivsi: Tekhnodruk, 2024. 101-105.
- Kheleniuk, M. "Forenzik: yevropeyskyi dosvid vs. ukraïnski realii" [Forensics: European Experience vs. Ukrainian Realities]. *Yurydychna Hazeta online*. 2021. <https://jur-gazeta.com/publications/practice/korporativne-pravo-ma/forenzik-evropeyskiy-dosvid-vs-ukrayinski-realiyi.html>
- Li, K. et al. "SEFraud: Graph-based Self-Explainable Fraud Detection via Interpretative Mask Learning". *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. 2024. 5329-5338.
DOI: <https://doi.org/10.1145/3637528.3671534>
- Lykshosherst, V. R. "Alhorytm klasyfikatsii ta klasterneho analizu DenStream dlia vyrishennia zadach z zabezpechennia informatsiinoi bezpeky : diplomna robota" [Algorithm of Classification and Cluster Analysis of DenStream for Solving Information Security Problems: thesis]. Kyiv, 2021. <https://ela.kpi.ua/server/api/core/bitstreams/902fdf1b-040a-4242-9e36-6113980516ef/content>
- Maciqg, P. S. et al. "Unsupervised Anomaly Detection in Stream Data with Online Evolving Spiking Neural Networks". *Neural Networks*, vol. 139 (2021): 118-139.
DOI: <https://doi.org/10.1016/j.neunet.2021.02.017>
- Pedregosa, F. et al. "Scikit-learn: Machine learning in Python". *Journal of Machine Learning Research*, vol. 12 (2011): 2825-2830. <https://www.jmlr.org/papers/volume12/pedregosa11a/pedregosa11a.pdf>
- Prajapati, J., and Choudhary, N. "A Systematic Review on Anomaly Detection". *International Journal of Advanced Research in Science, Communication and Technology*, vol. 3, no. 2 (2023): 75-82.
DOI: <https://doi.org/10.48175/ijarsct-8664>
- Rubytel, O. "Znachennia modeli shakhraistva dlia audytora, abo minusy vysokokvalifikovanykh liudei" [The Importance of the Fraud Model for the Auditor, or the Disadvantages of Highly Qualified People]. *LIGA.net*. October 23, 2024. <https://blog.liga.net/user/orubitel/article/54563>
- "Shcho take hlyboke navchannia? Vse, shcho vam potribno znaty" [What Is Deep Learning? Everything You Need to Know]. *cybercalm*. April 15, 2024. <https://cybercalm.org/novyny/shho-take-deep-learning/>
- "Shcho take Machine Learning?" [What Is Machine Learning?]. *denovo*. May 17, 2024. <https://denovo.ua/resources/what-is-machine-learning>
- "Shtuchnyi intelekt u vyavleniia shakhraistva ta pidvyschenni bezpeky" [Artificial Intelligence in Fraud Detection and Increased Security]. <https://www.probesto.com/ua>
- Semerenska, V. V. "Doslidzhennia metodiv vyavleniia anomalii za dopomohoiu videoanalitiki na osnovi shtuchnoho intelektu u kompleksnykh systemakh bezpeky : poiasniuvalna zapyska" [Study of Anomaly Detection Methods Using Video Analytics Based on Artificial Intelligence in Complex Security Systems: explanatory note]. Kharkiv, 2023. <https://openarchive.nure.ua/server/api/core/bitstreams/9107dae1-edcf-46a9-a780-818cf2973aea/content>
- "Vprovadzhennia alhorytmiv vyavleniia anomalii dlia vyznachennia shakhraiskykh vytrat" [Implementation of Anomaly Detection Algorithms to Determine Fraudulent Expenses]. <https://peerdh.com/uk/blogs/programming-insights/implementing-anomaly-detection-algorithms-for-identifying-fraudulent-expenses>
- "Vykorystannia mashynnoho navchannia dlia vyavleniia shakhraistva v elektronni komertsii" [Using Machine Learning to Detect Fraud in E-commerce]. <https://peerdh.com/uk/blogs/programming-insights/leveraging-machine-learning-for-fraud-detection-in-e-commerce-transactions>
- Venkatraman, S. et al. "SQL Versus NoSQL Movement with Big Data Analytics". *International Journal of Information Technology and Computer Science*, vol. 8, no. 12 (2016): 59-66.
DOI: <https://doi.org/10.5815/ijitcs.2016.12.07>
- Wells, J. T. *Fraud examination: investigative and audit procedures*. New York: Quorum Books, 1992.
- Zhang, Ch. et al. "Anomaly detection and defense techniques in federated learning: a comprehensive review". *Artificial Intelligence Review*, art. 150, vol. 57 (2024).
DOI: <https://doi.org/10.1007/s10462-024-10796-1>