УДК 657.633:343.357
DOI: 10.60022/2(4)-3S

Пацкань Юлія Вадимівна
здобувач третього (освітньо-наукового) рівня вищої освіти кафедри фінансового аналізу та аудиту
Державний торговельно-економічний університет, Україна
Patskan Yulia
PhD Student
State University of Trade and Economics, Ukraine
ORCID: 0009-0008-6940-4907

Назарова Каріна Олександрівна
доктор економічних наук, професор, завідувач кафедри фінансового аналізу та аудиту
Державний торговельно-економічний університет, Україна
Nazarova Karina
Doctor of Economics, Professor, Head of the Department of Financial Analysis and Audit
State University of Trade and Economics, Ukraine
ORCID: 0000-0002-5019-9244

ДИДЖИТАЛІЗАЦІЯ ЯК ФАКТОР ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФОРЕНЗІК-ДІАГНОСТИКИ ТА АУДИТУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Анотація. *У статті досліджено вплив ключових фаторів на підвищення ефективності форензік-діагностики та аудиту суб'єктів господарювання. Розглянуто переваги використання цифрових технологій, зокрема штучного інтелекту, аналітичних платформ та автоматизованих систем контролю у процесі виявлення ознак шахрайства. Обґрунтовано, що цифровізація дозволяє значно прискорити аналітичні процедури, знизити ймовірність людських помилок та підвищити якість виявлення ризиків. Запропоновано інтеграційний підхід до впровадження IT-рішень у систему аудиту та форензік-діагностику.*

Ключові слова: *форензік-діагностика, аудит, цифрові технології, штучний інтелект, шахрайство, контроль, диджиталізація, цифровізація.*

DIGITALIZATION AS A FACTOR FOR INCREASING THE EFFICIENCY OF FORENSIC DIAGNOSTICS AND AUDIT OF BUSINESS ENTITIES

Abstract. *The article explores the role of digitalization as a key factor in increasing the effectiveness of forensic diagnostics and audit processes in business entities. In the context of growing digital transformation and the rapid integration of information technologies into economic activities, the need for adaptive and technologically advanced approaches to fraud detection, risk management, and internal control has significantly intensified. The study emphasizes that traditional audit methods are becoming less effective in identifying complex and hidden fraud schemes, which often involve digital manipulation, unauthorized transactions, and behavior-based anomalies.*

Digital technologies-such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), and big data analytics-offer a new paradigm for forensic auditing. Their application enables real-time analysis of large volumes of structured and unstructured data, which facilitates the early identification of suspicious patterns, enhances the transparency of business operations, and allows for the automation of routine audit tasks. In particular, AI-driven anomaly detection systems can identify atypical transactions and generate behavioral risk profiles, which are used to strengthen preventive mechanisms in internal control systems.

The article also analyzes the integration of forensic diagnostics with enterprise digital ecosystems, including ERP, CRM, POS, and HRM systems. Such integration enables the formation of a unified analytical environment that allows auditors and forensic analysts to quickly respond to changes in operational and financial indicators. It is argued that digitalization not only improves the speed and quality of fraud detection but also contributes to the development of a risk-oriented audit model.

As a result of the research, a conceptual framework for implementing digital forensic diagnostics in the

audit of business entities was developed. This framework includes key technological components, stages of implementation, and criteria for evaluating the effectiveness of digital tools in audit procedures. Furthermore, the study highlights the importance of ethical and regulatory considerations in applying digital technologies to forensic audit, particularly with respect to data privacy and algorithm transparency.

In conclusion, digitalization is not only a tool but a strategic imperative for enhancing forensic audit efficiency. The integration of advanced IT solutions into the audit environment enables more accurate risk assessments, reduces the burden on human resources, and increases stakeholder confidence in financial reporting and corporate governance. The article proposes practical recommendations for businesses seeking to strengthen their forensic capabilities in the era of digital transformation.

Keywords: *forensic diagnostics, audit, digital technologies, artificial intelligence, fraud, control, digitalization.*

Постановка проблеми. Сучасні умови функціонування суб'єктів господарювання характеризуються високим рівнем невизначеності, зростанням кіберзагроз, ускладненням бізнес-процесів та масштабністю фінансових операцій. Водночас поширення шахрайства, корпоративних зловживань і маніпуляцій фінансовою інформацією створює додаткові виклики для забезпечення прозорості та достовірності облікових даних. Традиційні підходи до аудиту та внутрішнього контролю часто не здатні своєчасно реагувати на приховані або автоматизовані форми порушень, що формує потребу у вдосконаленні методологій і технологічних інструментів.

В умовах цифрової трансформації бізнесу виникає нагальна необхідність у використанні цифрових рішень – таких як аналітика великих даних, штучний інтелект, автоматизовані модулі моніторингу, ERP та CRM-системи – у процесах форензік-діагностики та аудиту. Цифровізація дозволяє не лише обробляти великі масиви інформації в режимі реального часу, а й формувати поведінкові профілі ризику, оперативно виявляти нетипові транзакції та формалізувати процедури оцінки доказів.

Однак, попри наявність сучасних ІТ-рішень, вітчизняні компанії часто стикаються з труднощами у впровадженні цифрових технологій у системи аудиту та форензік-діагностику через брак стандартизованих підходів, методичних рекомендацій і практичних моделей застосування. Таким чином, актуальним є наукове обґрунтування цифровізації як чинника підвищення ефективності форензік-діагностики та аудиту, розробка відповідних моделей та інструментів, а також оцінка результатів їх впровадження в діяльність суб'єктів господарювання. Це дозволить сформувати дієву систему превентивного контролю та забезпечити підвищення довіри до фінансової звітності та корпоративного управління.

Аналіз останніх досліджень і публікацій. Упродовж останніх років проблематика форензік-діагностики та її поєднання з цифровими технологіями в аудиті активно досліджується як вітчизняними, так і зарубіжними науковцями. Провідні автори, такі як W.S. Albrecht [1] та J.T. Wells [2], акцентують увагу на важливості використання аналітики даних та поведінкових моделей у боротьбі з шахрайством, а також підкреслюють роль цифрових слідів у виявленні зловживань.

Серед вітчизняних дослідників заслуговують на увагу праці А. Семенець [3], Г. Соломіна [4], Ю. Шевчук [5], які розглядають форензік не лише як етап постаудиторського реагування, а як інтегральний інструмент ризик-орієнтованого управління. Вони пропонують використовувати підходи форензік-аналізу ще на етапі планування та тестування внутрішнього контролю.

Окрему нішу в науковому дискурсі займають дослідження Дубініна М.В., С.В. Сирцева, Т.Ю. Янковська [6], С. М. Тютченко [7], які розглядають форензік у контексті виявлення економічних злочинів, фіктивного банкрутства та маніпуляцій із фінансовою звітністю. Автори наголошують на потребі адаптації світових методик до реалій українського корпоративного середовища.

Попри зростання уваги до теми, досі недостатньо висвітлено питання про впровадження цифрових інструментів у форензік-аудит саме в межах інтеграції з інформаційними системами підприємств, такими як ERP, CRM, POS тощо. Також бракує моделей, які б дозволяли оцінювати ефективність цифрових підходів у контексті синергії внутрішнього та зовнішнього аудиту.

Отже, існує потреба в узагальненні наявного наукового доробку та розробці практично орієнтованих підходів до цифровізації форензік-діагностики як інструменту мінімізації ризиків шахрайства в суб'єктах господарювання.

Метою статті є наукове обґрунтування цифровізації як ключового чинника підвищення ефективності форензік-діагностики та аудиту суб'єктів господарювання, а також розробка практичних

рекомендацій щодо впровадження цифрових інструментів для виявлення, попередження та мінімізації ризиків шахрайства і корупційних дій.

У межах досягнення цієї мети передбачено: аналіз сучасних технологічних підходів, оцінка можливостей їх інтеграції з внутрішніми та зовнішніми аудиторськими процедурами, формування моделі цифрової форензік-діагностики, орієнтованої на підвищення прозорості, достовірності звітності та стійкості бізнесу до зловживань.

Виклад основного матеріалу. В умовах цифрової трансформації економіки, коли обсяги даних стрімко зростають, а бізнес-процеси набувають все більшої складності, традиційні методи аудиту та виявлення шахрайства стають недостатніми для ефективного контролю та превенції фінансових порушень. Водночас суб'єкти господарювання стикаються з новими типами ризиків – від кібершахрайства до внутрішніх маніпуляцій, які все складніше виявити без залучення сучасних цифрових технологій.

Форензік-діагностика як інструмент виявлення фінансових зловживань, за умови інтеграції з цифровими аналітичними платформами, штучним інтелектом (ШІ), великими даними та автоматизованими системами внутрішнього контролю, набуває нової якості. Поєднання даних із ERP-, CRM-, POS- та HRM-систем дозволяє формувати поведінкові профілі співробітників, виявляти нетипові транзакції та визначати потенційні джерела ризиків у реальному часі.

У цьому контексті важливо не лише впровадити ІТ-рішення, а й забезпечити ефективну організаційно-інформаційну модель аудиту, яка охоплює як зовнішній, так і внутрішній контроль. Синергетичний підхід дозволяє узгодити завдання форензік-діагностики між аудиторськими функціями, підвищуючи об'єктивність, оперативність та достовірність висновків.

Застосування складних цифрових інструментів зі сторони шахраїв, а також необхідність в обробці великих баз даних (технології Big Data) потребують нових автоматизованих підходів в частині аналізу поведінкових ризиків. Так за даними компанії Oberig It, шахраї використовують різні механізми, щоб обійти традиційні схеми захисту, що унеможливлює виявлення шахрайських дій. В зв'язку з цим, компанія Gartner пропонує п'ятишарову систему онлайн-виявлення, яка включає здійснення моніторингу кінцевих точок, а також використання великих даних для виявлення шахрайських схем [8]. Також за даними Ощадбанку, регулятори фінансового ринку досліджують перспективи впровадження моделей на базі штучного інтелекту для протидії шахрайським діям та відмиванню коштів, що обґрунтовує важливість у впровадженні сучасних підходів у сфері ризик-менеджменту та цифрових технологій з метою підвищення безпеки фінансових операцій [9].

Саме впровадження алгоритмів (механізмів) штучного інтелекту в поведінковій аналітиці, забезпечить підвищення автоматизації виявлення ризикових подій, дозволяючи швидко адаптуватися до нових шахрайських схем зменшуючи вплив людського фактору та суб'єктивних помилок в транзакціях.

Основна відмінність в частині використання методів та підходів штучного інтелекту під час застосування процедур аудиту та форензік-діагностики полягає в цілях та завданнях.

Так, під час аудиту доцільно застосовувати такі методи штучного інтелекту як: наглядове навчання, часові ряди, NLP і баєсові моделі, які дозволять поглибити автоматизацію аудиторської перевірки, забезпечити прогнозування ризиків та здійснити аналіз ефективності бізнес-процесів. Зважаючи на те, що процедури аудиту направлені на перевірку відповідності господарських операцій та звітності міжнародним стандартам, а також виявлення потенційних, можливих ризиків, що можуть призвести до погіршення фінансового стану підприємства та результатів його діяльності, використання методів штучного інтелекту під час аудиторської перевірки має забезпечити поглиблений аналіз в частині, зокрема, виявлення та класифікації легітимних чи ризикових транзакцій, автоматизації процедур перевірки, а також прогнозування фінансових показників на базі алгоритмів машинного та глибинного навчання та статистичних моделей.

В свою чергу, форензік-діагностика спрямована на виявлення та розслідування випадків шахрайства, встановлення прихованих схем зловживань, аналізі нетипових операцій та формуванні доказової бази, що сприяє передбаченню використання більш складних та деталізованих підходів, таких як глибинне навчання, методи виявлення аномалій для встановлення причин та закономірностей, що можуть свідчити про наявність шахрайських дій.

На рис. 1 наведена інформація, яка обґрунтовує важливість в запровадженні нових, сучасних методів під час форензік-діагностики та аудиту бізнес-процесів, що потребує:

- підвищення складності шахрайських схем;
- забезпечення зниження людського фактору під час аудиту та форензік-діагностики;

- необхідності проведення аналізу та досліджень великих даних в реальному часі;
- відсутності адаптивності традиційних методів до нових типів шахрайства.

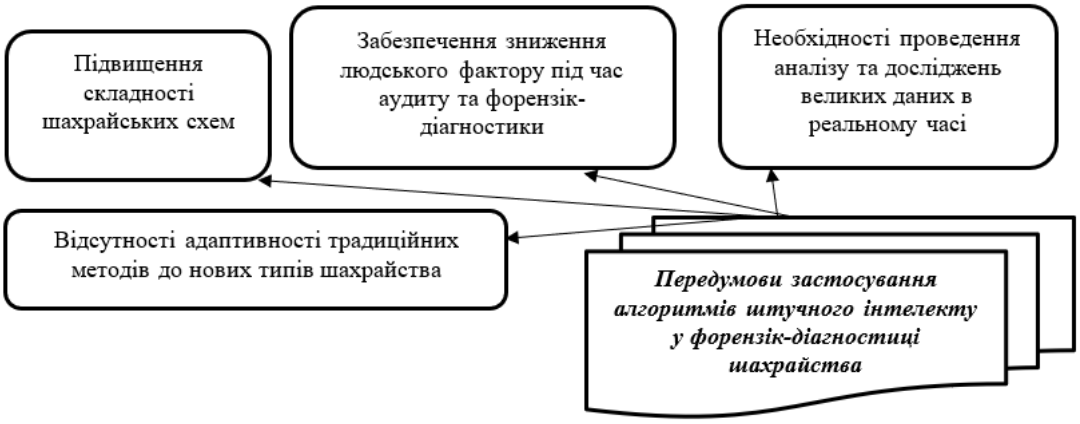

Рис. 1. Фактори модернізації методів форензік-діагностики у корпоративному аудиті
Джерело: сформовано авторами

Варто зазначити, що традиційні методи форензік-діагностики та аудиту поступаються сучасним методам з використанням ШІ в частині оперативного аналізу великих масивів інформації в реальному часі. За допомогою алгоритмів ШІ, великі обсяги інформації можуть бути швидко та ефективно опрацьовані в результаті чого забезпечується здійснення аудиту, а також оперативно виявляються факти порушень та шахрайства.

На сьогоднішній день, ускладнення шахрайських схем, вимагає запровадження нових, сучасних методів діагностики з використанням ШІ, які дозволять встановлювати поведінкові патерни (тобто повторювані або нетипові операції), що пов'язані з нехарактерними діями зі сторони працівників суб'єктів господарювання.

На рис. 2 узагальнені проблеми та напрями їх вирішення в умовах використання методів аналізу транзакцій з використанням ШІ на основі «поведінкових ризиків» в умовах здійснення форензік-діагностики та аудиту діяльності суб'єктів господарювання.

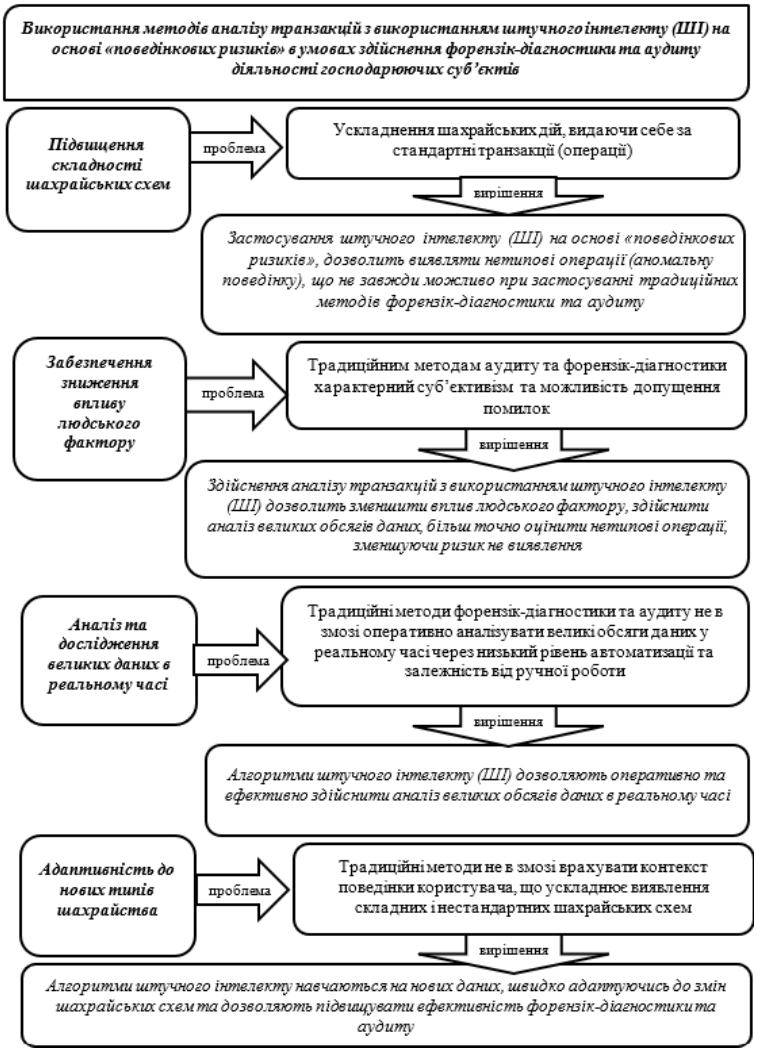

Рис. 2. Причини та наслідки впровадження ШІ в умовах здійснення форензік-діагностики та аудиту діяльності суб'єктів господарювання
Джерело: сформовано авторами

Перевагами у використанні методів на базі алгоритмів ШІ є також зниження впливу суб'єктивних факторів під час здійснення аудиту та форензік-діагностики, що виключає ризик упередженості, людських помилок та забезпечує більш об'єктивний і точний аналіз даних.

Вищенаведена інформація обґрунтовує необхідність в удосконаленні традиційних методів та процедур аудиту та форензік-діагностики зважаючи на збільшення складності шахрайських схем, динамічності фінансових операцій та необхідності виявлення нетипових операцій (дій) в реальному часі з метою підвищення безпеки бізнес-процесів.

Попри актуальність вищенаведеного питання, а саме впровадження сучасних методів в умовах виявлення фактів шахрайства та зловживань, а також значну увагу з боку як вітчизняних, так і зарубіжних науковців, питання виявлення шахрайства у фінансово-економічних системах крізь призму поведінкових ризиків залишається недостатньо опрацьованим. Це зумовлює потребу у впровадженні нових підходів до поведінкової аналітики та інтеграції сучасних інструментів форензік-діагностики із застосуванням ШІ.

Зважаючи на це, ми пропонуємо новий підхід до аналізу транзакцій з використанням «поведінкових ризиків». Дана методологія аналізу є не дослідженою та передбачає врахування під час застосування процедур форензік-діагностики та аудиту не лише ретроспективних фінансових даних, а й поведінкових *патернів* співробітників та контрагентів підприємства з метою підвищення ефективності виявлення шахрайства та зловживань.

Процес побудови поведінкових профілів, передбачає розслідування конкретних ризиків та

випадків шахрайства, зосереджуючи увагу на потенційних ризиках маніпуляцій та зловживань.

Запропонована модель аналізу транзакцій з використанням «поведінкових ризиків» (рис. 3), передбачає інтеграцію поведінкових даних та складних алгоритмів аналізу під час застосування форензік-діагностики та аудиту, та дозволяє покращити автоматизацію процесів виявлення ризиків та шахрайських дій посилюючи точність економічних розслідувань.

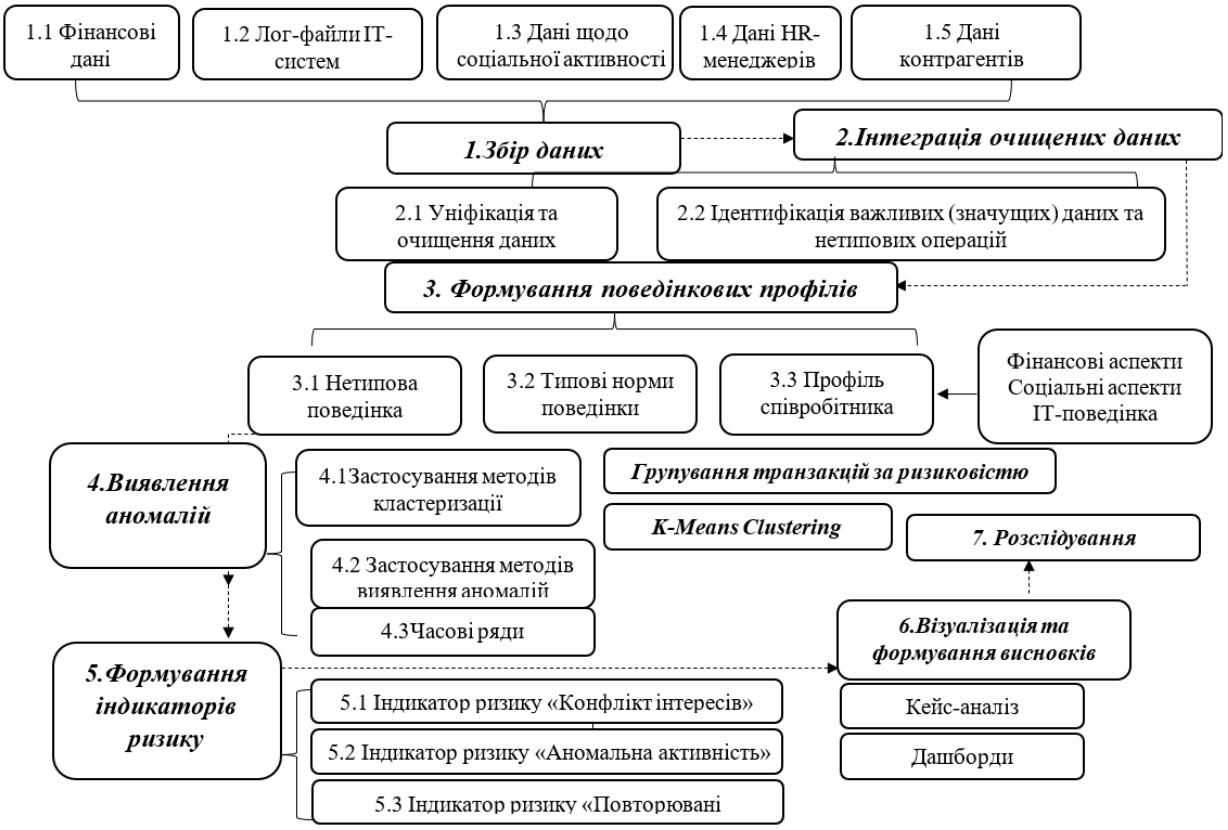

Рис. 3. Модель поведінкового аналізу транзакцій у форензік-діагностиці: інтеграція ризик-орієнтованого підходу в аудиті суб'єктів господарювання
Джерело: сформовано авторами

Так, на початковому етапі запропонованої моделі аналізу транзакцій з використанням «поведінкових ризиків», необхідно зібрати дані з усіх доступних джерел, які дозволять визначити ризикові дії (операції) співробітників (контрагентів) компанії. Наприклад, з метою виявлення поведінкових ризиків співробітників підприємства, що можуть свідчити про можливі шахрайські дії, такі як: несанкціонований доступ до коштів компанії, та (або) запровадження шахрайських схем в частині розрахунків з контрагентами, доцільно зібрати інформацію з наступних джерел:

- системи управління доступом, сервери;
- бази даних системи управління (ERP-системи, CRM-системи);
- бухгалтерські системи, фінансові звіти;
- контракти, платіжні документи, розрахунки;
- електронна пошта співробітників;
- платформи для корпоративних комунікацій;
- дані HR-системи (зокрема, PeopleSoft, SAP SuccessFactors).

Інформація щодо платіжних транзакцій співробітників компанії, а саме розрахунки з контрагентами, виплати коштів підрядникам та постачальникам, які можна отримати з внутрішніх фінансових систем компанії (SAP, Oracle) дозволяють ідентифікувати індикатори шахрайства.

Дані, що містяться в контрактах (специфікаціях), а також облікові записи про великі та нетипові платежі одному і тому ж контрагенту, допоможуть виявити несанкціоновані фінансові операції. Лог-файли та документи до корпоративних систем, дозволяють ідентифікувати неавторизовані входи або несанкціонований доступ до конфіденційної інформації. Інтегровані корпоративні системи такі як (ERP та CRM-системи) дозволяють виявити нетипові зміни у фінансових документах та бухгалтерських

звітах та можуть свідчити про наявність маніпуляцій із фінансами.

Дані про співробітників, які наведені в системах кадрового обліку (HR-системах), дозволяють оцінити час роботи та перевантаження співробітників компанії з метою визначення факторів, що можуть сприяти порушенням, пов'язаним із перевищенням посадових повноважень чи неефективною організацією праці. Вивчення корпоративної пошти по відповідному співробітнику дозволяє оцінити сумнівні запити на оплату рахунків, а також здійснення платежів без належної їх перевірки чи погодження.

Наведені вище джерела отримання всієї необхідної для аналізу інформації є важливими елементами форензік-діагностики бізнес-процесів, які дозволяють сформувати їх комплексну модель, виявити проблемні зони та підвищити ефективність внутрішніх розслідувань (рис. 4).

Рис. 4. Інтеграція та очищення даних під час аналізу транзакцій з використанням поведінкових ризиків

Джерело: сформовано авторами

Наступним етапом аналізу є інтеграція та очищення зібраних даних з метою виявлення потенційних загроз шахрайства, що включає в себе: приведення транзакцій в хронологічний вигляд із зазначенням ID-співробітників, суми понесених витрат, контрагента (отримувача) платежу; структурування лог-файлів з метою відстеження активності співробітників в частині входів до ERP та CRM-систем, очищення відібраних даних та ідентифікації значущих подій для подальшого аналізу. На даному етапі, важливо виявити помилкові та нетипові операції, зокрема при подвійній реєстрації відповідної транзакції, доцільно видалити дублікати та уніфікувати дані.

Також, доцільно відстежувати доступ співробітників до систем компанії, що дозволить оцінити ефективність співробітників в реальному часі. За допомогою лог-файлів, аудитор може ідентифікувати аномальну, не типову поведінку співробітника компанії, який міг здійснити вхід в корпоративну систему компанії, зокрема через незахищені канали доступу, що може свідчити про потенційну загрозу шахрайства.

З метою деталізації та більш повного розкриття інформації про види аномальних дій співробітників, які могли б свідчити про наявність поведінкових ризиків, дану інформацію узагальнено та відображено на рис. 5.

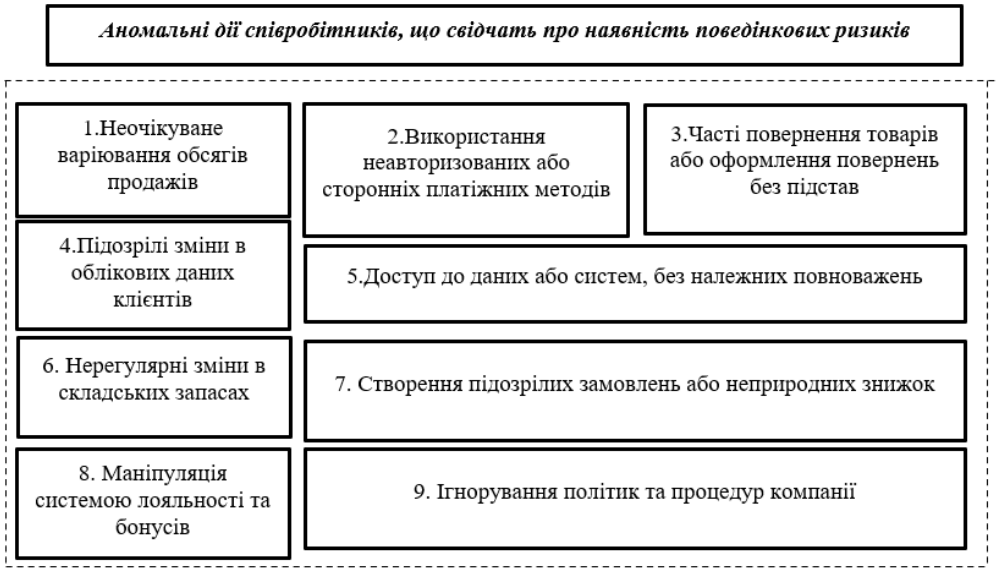

Рис. 5. Ключові індикатори поведінкових ризиків співробітників компанії
Джерело: розроблено авторами

З метою підвищення ефективності форензік-діагностики у системі внутрішнього контролю доцільним є впровадження згрупованого переліку аномальних (нетипових) дій співробітників, як представлено в табл. 1.

Таблиця 1

Ідентифікація та наслідки аномальних транзакцій (причинно-наслідковий зв'язок)

Аномальні (нетипові) дії співробітників	Поведінкові ризики	Можливі наслідки для компанії
Незвична зміна обсягів продажів	Підозріла кількість продажів без пояснень.	Махінації з продажами, шахрайські операції, втрати товарів.
Використання неавторизованих платіжних методів	Використання карток або платіжних систем, не санкціонованих компанією.	Шахрайські операції, втрати коштів, підроблені платіжні дані.
Часті повернення товарів або оформлення повернень без підстав	Незвична кількість повернень, що не відповідає типу операцій.	Шахрайство через повернення товарів, зловживання політикою повернення.
Підозрілі зміни в облікових даних клієнтів	Часті зміни контактної інформації без попередження клієнта	Витік особистих даних, зловживання клієнтською інформацією.
Доступ до даних або систем, не пов'язаний з посадовими обов'язками	Неправомірний доступ до конфіденційної інформації.	Розкриття даних, викрадення інформації, шахрайство з обліковими записами.
Нерегулярні зміни в складських запасах	Зміни в інвентаризації без належного обґрунтування або документації.	Крадіжка товарів, маніпулювання обліком запасів, фінансові збитки.
Створення підозрілих замовлень або неприродних знижок	Надмірне використання знижок або створення замовлень на товар для себе.	Шахрайство з товарними знижками, втрати через неправильне застосування знижок.
Часті спроби маніпулювати системою лояльності або бонусами	Неавторизоване нарахування бонусів або маніпулювання програмами лояльності.	Зловживання бонусними програмами, фінансові збитки, порушення корпоративних політик.
Ігнорування політик та процедур компанії	Ігнорування встановлених процедур без належного контролю.	Збільшення ризику внутрішніх порушень, зниження безпеки, витік інформації.

Джерело: складено авторами

Цей перелік дозволяє ідентифікувати потенційно ризиковану поведінку, що може свідчити про наявність поведінкових ризиків, пов'язаних із шахрайськими або деструктивними діями.

Застосування такої ідентифікації як елемента методології форензік-діагностики дає змогу:

- своєчасно реагувати на нетипові бізнес-процеси;

- здійснювати превентивне втручання для мінімізації втрат;
- забезпечувати надійність, безпеку і стійкість функціонування компанії;
- систематизувати фактори внутрішніх загроз і оцінити їх критичність.

Таким чином, запропонований підхід сприяє розширенню аналітичного інструментарію форензік-діагностики, посиленню комплаєнс-контролю та формуванню ефективного механізму управління поведінковими ризиками.

Використання запропонованої моделі аналізу транзакцій з використанням поведінкових ризиків та ШІ, дозволить автоматизувати виявлення аномальних (нетипових) дій співробітників компанії, забезпечуючи здійснення аналізу звичних патернів поведінки співробітників порівнюючи їх з відхиленнями, що можуть виникати в реальному часі.

За результатами досліджень сучасних методів форензік-діагностики та аудиту, пропонується застосування методу K-Means із використанням алгоритмів ШІ. Впровадження алгоритму кластеризації K-Means передбачає здійснення групування транзакцій таким чином, щоб операції з подібними кластерами опинились у спільних кластерах. Так, в результаті кластеризації виділяються кілька груп транзакцій, що є типовими, а також виділяється аномальний (нетиповий) кластер, що значно відрізняється від типового шаблону поведінки (наприклад, перерахунок значних грошових сум на користь контрагентів у нічний час, використання нових платіжних засобів, тощо).

Поглиблений аналіз нетипових кластерів, дозволить встановити тих співробітників, які зокрема за допомогою підроблених документів можуть здійснювати незаконні операції, що вимагає подальших досліджень та запровадження контрольних заходів.

Досліджуючи переваги та недоліки застосування запропонованого методу кластеризації K-Means у форензік-діагностиці, встановлено, що з використанням даного методу та ШІ, забезпечується посилення автоматизації аналізу великих обсягів інформації, в результаті чого виявляються ризикові операції. Також, даний метод забезпечує виявлення прихованих патернів поведінки, які б мали залишитись непоміченими під час застосування традиційних методів аудиту та форензік-діагностики.

За належної підготовки даних, оптимальному налаштуванні параметрів та інтерпретації результатів, даний метод залишається потужним інструментом в аналізі великих обсягів інформації під час здійснення форензік-діагностики та аудиту діяльності суб'єктів господарювання.

Висновки. Результати проведеного дослідження засвідчують, що цифровізація є ключовим фактором підвищення ефективності форензік-діагностики та аудиту суб'єктів господарювання. Застосування сучасних технологічних рішень, зокрема поведінкових індикаторів ризиків, дозволяє аудиторам і аналітикам не лише ідентифікувати потенційно шахрайські транзакції, але й формувати превентивну модель виявлення фінансових зловживань.

Запропонований у межах дослідження механізм інтеграції та очищення мультиджерельних даних дозволяє значно підвищити точність аналізу, забезпечуючи релевантність вхідної інформації для подальшого аналізу транзакцій. Це, в свою чергу, забезпечує основу для побудови більш гнучкої та адаптивної моделі контролю в реальному часі.

Окрему увагу приділено впровадженню методу кластеризації K-Means, який у поєднанні з алгоритмами штучного інтелекту продемонстрував високу ефективність у групуванні транзакцій за ризик-профілями та виділенні нетипової поведінки користувачів або структурних одиниць. Такий підхід дозволяє формувати поведінкові профілі ризику, що можуть бути інтегровані у систему внутрішнього аудиту та оперативно оновлюватися відповідно до змін у середовищі.

Таким чином, поєднання цифрових технологій, поведінкової аналітики та кластерного аналізу створює нову якість форензік-діагностики, орієнтовану на своєчасне виявлення ризиків, мінімізацію людського фактора та підвищення прозорості фінансової звітності. Запропоновані підходи можуть бути впроваджені як частина комплексної цифрової моделі аудиту, що базується на інтеграції внутрішнього та зовнішнього контролю.

Література

1. Albrecht, W.S. *Fraud Examination*, Cengage Learning. 2019. 675p. (Дата звернення: 16.04.2025).
2. Wells, J.T. *Forensic Accounting and Fraud Examination*, John Wiley & Sons Inc. 2010. 560 p. (Дата звернення: 18.04.2025).
3. Семенець А. *Форензік аудит як ефективний засіб антикризового управління торговельною діяльністю*. Бізнес-Інформ. 2019. № 4. С. 280–287. URL: https://doi.org/10.32983/2222-4459-2019-4-280-287 (Дата звернення: 18.04.2025).

4. Соломіна Г. *Форензік – інструмент фінансового розслідування діяльності підприємства*. Науковий вісник Мукачівського державного університету. 2018. № 2. С. 144–149. (Дата звернення: 18.04.2025).

5. Шевчук Ю. *Форензік: як вчасно виявити шахрайство в бізнесі.* FEMIDA.UA: Юридичний журнал. 2018. № 3(13). С. 33–36. (Дата звернення: 18.04.2025).

6. Дубініна М.В., Сирцева С.В., Янковська Т.Ю. *Форензік як метод розслідування внутрішньокорпоративних випадків шахрайства.* URL: http://www.market-infr.od.ua/journals/2019/38_2019_ukr/61.pdf. (Дата звернення: 01.05.2025).

7. Тютченко С. М. *Функції форензіку як інструменту упередження корпоративного шахрайства та підвищення економічної безпеки підприємств*. URL: http://www.economy.nayka.com.ua/pdf/5_2021/101.pdf. (Дата звернення: 01.05.2025).

8. Масове шахрайство у сфері мобільного банкінгу демонструє потребу банків у безпеці додатків, модернізованої автентифікації та аналітики ризиків. Oberig it Distribution jf Innovations. 2021. URL: https://oberig-it.com/statti/masove-shakhraistvo-u-sferi-mobilnogo-bankningu/. (Дата звернення: 01.05.2025).

9. Штучний інтелект в українському банківському секторі: можливість чи необхідність? Офіційний сайт Ощадбанк. 2025р. URL: https://www.oschadbank.ua/news/stucnij-intelekt-v-ukrainskomu-bankivskomu-sektori-mozlivist-ci-neobhidnist. (Дата звернення: 01.05.2025).

References

1. Albrecht, W.S. *Fraud Examination*, Cengage Learning. 2019. 675p. (Accessed: 16.04.2025).

2. Wells, J.T. *Forensic Accounting and Fraud Examination*, John Wiley & Sons Inc. 2010. 560 p. (Accessed: 18.04.2025).

3. Semenets A. *Forensic audit as an effective means of anti-crisis management of commercial activities*. Business-Inform. 2019. No. 4. P. 280–287. URL: https://doi.org/10.32983/2222-4459-2019-4-280-287 (Accessed: 18.04.2025).

4. Solomina G. *Forensic – a tool for financial investigation of the activities of the enterprise*. Scientific Bulletin of Mukachevo State University. 2018. No. 2. P. 144–149. (Accessed: 18.04.2025).

5. Shevchuk Yu. *Forensic: how to detect fraud in business in time*. FEMIDA.UA: Legal Journal. 2018. No. 3(13). P. 33–36. (Accessed: 18.04.2025).

6. Dubinina M.V., Syrtseva S.V., Yankovska T.Yu. *Forensic as a method of investigating intra-corporate fraud cases*. URL: http://www.market-infr.od.ua/journals/2019/38_2019_ukr/61.pdf. (Accessed: 01.05.2025).

7. Tyutchenko S. M. *Functions of forensics as a tool for preventing corporate fraud and increasing the economic security of enterprises*. URL: http://www.economy.nayka.com.ua/pdf/5_2021/101.pdf. (Accessed: 01.05.2025).

8. Mass fraud in the field of mobile banking demonstrates the need for banks in application security, modernized authentication and risk analytics. Oberig it Distribution jf Innovations. 2021. URL: https://oberig-it.com/statti/masove-shakhraistvo-u-sferi-mobilnogo-bankningu/. (Accessed: 01.05.2025).

9. Artificial intelligence in the Ukrainian banking sector: an opportunity or a necessity? Official website of Oschadbank. 2025. URL: https://www.oschadbank.ua/news/stucnij-intelekt-v-ukrainskomu-bankivskomu-sektori-mozlivist-ci-neobhidnist. (Accessed: 01.05.2025).