

DOI: 10.15276/ETR.02.2026.3

DOI: 10.5281/zenodo.20348951

UDC: 657.6:658.15:004.65:343.98

JEL: M42, C55, O17

Received: 2025-11-20, Revised: 2026-01-13, Accepted: 2026-02-03, Published: 2026-03-11

## ІНТЕГРАЦІЯ ФОРЕНЗІК-МЕТОДІВ ТА DATA ANALYTICS У СИСТЕМУ ВНУТРІШНЬОГО АУДИТУ ЯК МЕХАНІЗМ ПРОТИДІІ ШАХРАЙСТВУ

### INTEGRATION OF FORENSIC METHODS AND DATA ANALYTICS INTO THE INTERNAL AUDIT SYSTEM AS A MECHANISM FOR FRAUD PREVENTION

Alla A. Balan, PhD in Economics, Associate Professor  
Odesa Polytechnic National University, Odesa, Ukraine  
ORCID: 0000-0002-2017-8813  
Email: a.a.balan@op.edu.ua

Diana V. Bondaruk  
Odesa Polytechnic National University, Odesa, Ukraine  
ORCID: 0009-0001-7833-4815  
Email: 10253158@stud.op.edu.ua

*Балан А.А., Бондарук Д.В. Інтеграція форензик-методів та Data Analytics у систему внутрішнього аудиту як механізм протидії шахрайству. Науково-методична стаття.*

У статті досліджено інтеграцію форензик-методів та інструментів Data Analytics у систему внутрішнього аудиту як ефективного механізму протидії шахрайству. Підкреслюється, що шахрайство залишається однією з головних загроз для фінансової стійкості, репутації та операційної ефективності організацій. Розглянуто роль внутрішнього аудиту у запобіганні, виявленні та документуванні шахрайських дій, а також необхідність адаптації сучасних технологій та аналітичних методів для підвищення оперативності та точності аудитів. Проаналізовано ключові фактори виникнення шахрайства на основі моделі «Трикутник шахрайства», показано практичні підходи до оцінки ризиків та запровадження превентивних заходів. Висвітлено стратегічну значущість комплексної трансформації внутрішнього аудиту за напрямками кадри, процеси та технології, що забезпечує перехід від реактивного контролю до проактивного моніторингу та захисту фінансових ресурсів організації.

*Ключові слова:* форензик-аудит, Data Analytics, внутрішній аудит, шахрайство, фінансові ризики, внутрішній контроль

*Balan A.A., Bondaruk D.V. Integration of Forensic Methods and Data Analytics into the Internal Audit System as a Mechanism for Fraud Prevention. Scientific and methodical article.*

The article examines the integration of forensic methods and Data Analytics tools into the internal audit system as an effective mechanism for countering fraud. It is emphasized that fraud remains one of the main threats to the financial stability, reputation, and operational efficiency of organizations. The role of internal audit in preventing, detecting, and documenting fraudulent activities is discussed, as well as the necessity of adapting modern technologies and analytical methods to increase the speed and accuracy of audits. Key factors in the occurrence of fraud are analyzed based on the «Fraud Triangle» model, and practical approaches to risk assessment and the implementation of preventive measures are demonstrated. The strategic significance of the comprehensive transformation of internal audit across the dimensions of personnel, processes, and technologies is highlighted, ensuring the transition from reactive control to proactive monitoring and protection of the organization's financial resources.

*Keywords:* forensic audit, Data Analytics, internal audit, fraud, financial risks, internal control

У сучасних умовах шахрайство є однією з найбільш руйнівних загроз для фінансової стійкості, репутації та загальної операційної ефективності будь-якої організації. Необхідність у надійних механізмах контролю та моніторингу стає критичною, особливо з огляду на те, що шахрайство може проявлятися у фальсифікації фінансових документів, привласненні активів чи застосуванні корупційних схем. З огляду на це, внутрішній аудит, як превентивний механізм щодо виникнення шахрайства набуває стратегічного значення.

Сучасний розвиток інформаційних технологій та масове накопичення великих даних відкривають нові можливості для підвищення ефективності внутрішнього аудиту. Інтеграція форензик-методів із сучасними інструментами Data Analytics дозволяє не лише виявляти факти шахрайства на ранніх стадіях, але й прогнозувати потенційні ризики та реагувати на них превентивно. Такий підхід поєднує класичні аудиторські процедури з аналізом великих обсягів інформації, алгоритмічним пошуком аномалій та автоматизованою перевіркою транзакцій, що значно підвищує оперативність і точність аудитів.

Більш того, застосування форензик-методів у поєднанні з Data Analytics сприяє формуванню більш прозорого та структурованого процесу внутрішнього контролю, де кожна операція може бути відстежена, а потенційні зловживання – виявлені з мінімальними витратами часу та ресурсів. Це дозволяє організаціям не лише реагувати на шахрайські дії, а й створювати проактивну систему управління ризиками, що стає важливим стратегічним інструментом забезпечення фінансової безпеки та стабільності бізнес-процесів.

## Аналіз останніх публікацій по проблемі

Питання розвитку внутрішнього аудиту та його ролі у виявленні та запобіганні шахрайству є актуальним і активно досліджується як вітчизняними, так і зарубіжними науковцями та практиками. Серед вітчизняних авторів особливу увагу цьому приділяють А.А. Аренс, Дж.К. Лоббек, В.В. Скобар, О.А. Петрик, А.М. Поддєрьогін та С.В. Свірко, які розглядають методологічні аспекти внутрішнього контролю, оцінку ризиків шахрайства та оптимізацію процедур аудиту.

Зарубіжні науковці, такі як Дж.Т. Веллс та Т.Д. Кохран, зосереджуються на розвитку форензич-аудиту, включаючи технології аналізу великих даних, використання цифрових слідів для виявлення аномалій та інтеграцію інформаційних систем у процес контролю. Вони підкреслюють важливість поєднання традиційних аудиторських методів з сучасними аналітичними інструментами для підвищення ефективності виявлення шахрайських схем.

## Виділення невирішених раніше частин загальної проблеми

Проте, незважаючи на численні дослідження, комплексне вивчення інтеграції методів форензич-аудиту та Data Analytics у систему внутрішнього аудиту для оперативного виявлення шахрайства та мінімізації фінансових ризиків на підприємствах залишається недостатньо висвітленим у науковій літературі. Динамічний розвиток технологій та постійна еволюція шахрайських схем формують необхідність для постійного оновлення методологій та вдосконалення практичних інструментів внутрішнього аудиту.

## Формулювання цілей дослідження (постановка завдання)

Метою статті є обґрунтування теоретичних і методичних засад інтеграції форензич-методів та інструментів Data Analytics у систему

внутрішнього аудиту як дієвого механізму протидії шахрайству, визначення напрямів їх практичного застосування для підвищення ефективності аудиторського контролю, оперативності виявлення порушень та формування проактивної системи внутрішнього моніторингу фінансових ризиків.

## Матеріали та методи

Інформаційною базою роботи слугували законодавчі акти України, Міжнародні стандарти внутрішнього аудиту, дані Опендатабот (2023-2024 рр.) та концепція COSO. У роботі використано методи теоретичного узагальнення, статистичного аналізу, моделювання (при побудові логіки Data Governance) та системний підхід для розробки алгоритму оцінки ризиків.

## Виклад основних результатів та їх обґрунтування

Шахрайство у фінансовій звітності визнається як незаконні дії, що включають обман, приховування або зловживання довірою з метою отримання фінансової вигоди чи інших переваг. Воно може проявлятися у фальсифікації фінансових документів, привласненні активів, маніпуляціях зі звітністю або застосуванні корупційних схем. Такі дії часто супроводжуються порушеннями внутрішніх процедур і стандартів, що вимагає від внутрішнього аудиту постійного моніторингу та аналізу фінансових потоків і операцій. Наявність ефективної системи внутрішнього аудиту дозволяє організації своєчасно виявляти ознаки шахрайства, реагувати на них і запобігати масштабним негативним наслідкам [1].

Так, за даними офіційних джерел, у 2024 році було відкрито 64 978 кримінальних проваджень за статтею 190 Кримінального кодексу України («Шахрайство»). Це на 21% менше, ніж у 2023 році, коли було зафіксовано рекордні 82 609 справ, проте рівень шахрайства все ще значно перевищує показники до початку повномасштабної війни (рис. 1) [2].

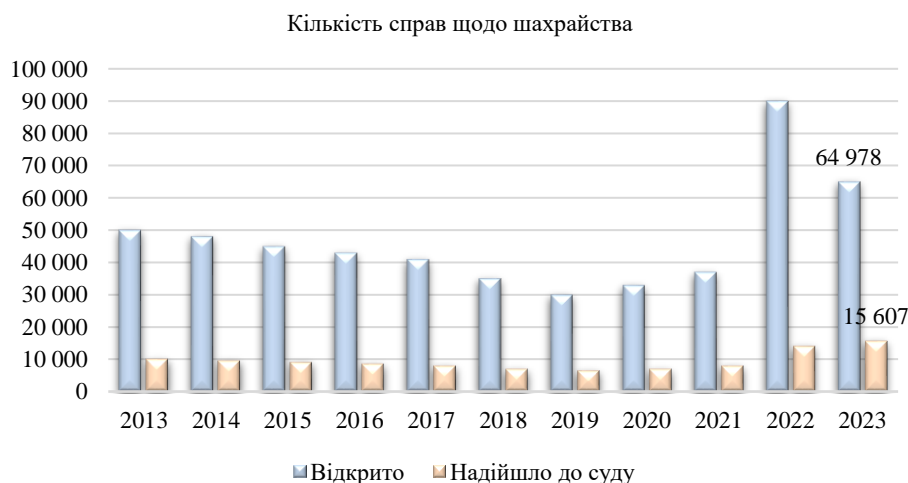


Рисунок 1. Кількість справ за статтею «Шахрайство» (2023-2024)  
Джерело: складено авторами за матеріалами [2]

Варто зазначити, що протягом 2023 року справ про шахрайство поменшало у 2,4 рази. Якщо у першому кварталі, в середньому, відкривали близько 8 тисяч таких проваджень на місяць, то в останньому – лише 3,3 тисячі [2].

Розкривати подібні справи стали також краще: у 2024 році до суду дійшло 15 607 справ. Це становить 24% від загальної кількості відкритих справ у 2024 році. До порівняння, у 2022 і 2023 роках цей показник становив лише 18% [2].

Модель «Трикутник шахрайства», розроблена Дональдом Кресі, дозволяє розуміти три основні фактори, що сприяють виникненню шахрайства: тиск, можливість і раціоналізація (рис. 2).

Фінансові труднощі, високі вимоги до результатів або особисті проблеми створюють тиск на працівників, що може провокувати шахрайські дії. Недоліки у внутрішньому контролі, відсутність нагляду або слабка корпоративна культура формують можливості для шахрайства, а працівники часто раціоналізують свої дії, виправдовуючи їх незначністю або необхідністю для досягнення особистих цілей. Внутрішній аудит повинен зосереджуватися на виявленні та усуненні цих факторів через посилення внутрішнього контролю, підвищення етичних стандартів і забезпечення прозорості в діяльності організації.

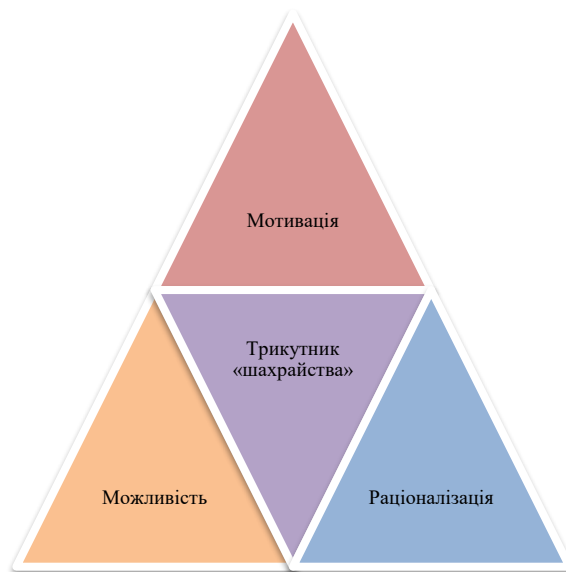


Рисунок 2. Трикутник «шахрайства»  
Джерело: складено авторами за матеріалами [1]

Для виникнення шахрайства необхідне одночасне поєднання трьох умов: мотивації, раціоналізації та можливості. Мотивація зазвичай пов'язана з особистим тиском або фінансовими проблемами працівника. Раціоналізація проявляється у виправданні власних дій, коли особисті інтереси ставляться вище інтересів організації. Можливість виникає через слабкий внутрішній контроль та недосконалі процедури, що відкриває шлях для шахрайських дій. Внутрішній аудит може ефективно зменшити ризик шахрайства, обмежуючи можливості його вчинення через посилення контролю, навчання персоналу, анонімні гарячі лінії та підвищення етичної культури організації [1].

Внутрішній аудит відіграє важливу роль у запобіганні помилок і шахрайства на підприємстві, оскільки його основна мета полягає у забезпеченні достовірності фінансової звітності та захисті ресурсів компанії, що, у свою чергу, зміцнює довіру зацікавлених сторін. Аудитори здійснюють систематизований і послідовний аналіз діяльності підприємства для виявлення аномалій, оцінки ризиків і впровадження ефективних процедур

контролю, що дозволяє мінімізувати можливість неправомірних дій з боку працівників.

Одним із ключових методів є аналітичні процедури, що дозволяють виявляти потенційні шахрайські операції. Під час аналізу фінансових трендів та коефіцієнтів внутрішній аудитор звертає увагу на «червоні прапорці» – показники або операції, які суттєво відхиляються від очікуваних норм і можуть свідчити про маніпуляції з обліком. Крім того, аудитори порівнюють дані підприємства з галузевими стандартами та показниками аналогічних компаній, що дозволяє своєчасно виявляти потенційні шахрайські дії [3].

Сучасні технології значно підвищують ефективність аудиту. Використання спеціалізованого програмного забезпечення дозволяє автоматично виявляти дублікати транзакцій, аналізувати виняткові операції та оцінювати первинні документи, що допомагає оперативному виявленню маніпуляцій з обліковими записами, неправильну оцінку активів чи незаконне заволодіння майном.

Оцінка ризиків і суттєвості відхилень є ще одним важливим елементом роботи аудитора. Суттєві відхилення – це ті, що можуть впливати на

економічні рішення користувачів фінансової звітності. Аудитор оцінює ефективність внутрішньої системи контролю та планує обсяг тестування, визначаючи ризики за окремими рахунками та операціями. У разі підозри на шахрайство або істотні помилки аудиторі проводять додаткові процедури, щоб з'ясувати, чи відхилення є наслідком навмисних дій або випадкових помилок, і повідомляють керівництво про підтвержені порушення [3].

Крім перевірки фінансових даних, внутрішній аудит сприяє запобіганню шахрайства через формування ефективної системи контролю. Працівники повинні чітко знати свої обов'язки, а корпоративна культура підтримувати прозорість і принцип невідворотності покарання за порушення.

У цьому сенсі аудит – це не лише перевірка бухгалтерії, а комплекс послуг, спрямованих на підвищення ефективності управління та мінімізацію ризиків шахрайства.

У сучасних умовах шахрайство є однією з головних загроз фінансовій стійкості та ефективності управління підприємством. Для його своєчасного виявлення та запобігання застосовується системний підхід до оцінки ризиків, що враховує особливості управлінського персоналу, працівників, контрагентів, структуру підприємства та вплив макроекономічних факторів. Поетапний алгоритм оцінки дозволяє аудиторам систематично визначати потенційні загрози та впроваджувати превентивні заходи, детально описані в табл. 1.

Таблиця 1. Основні групи ризиків шахрайства та алгоритм їх оцінки на підприємстві

Етап / Група ризику	Опис факторів та ознак	Приклад
R1 – Управлінський персонал та власники	Конфлікти інтересів, надмірний тиск на персонал, залежність фінансових результатів від бонусів та ключових показників ефективності, родинні зв'язки, ефективність внутрішнього аудиту	Пропорційна залежність бонусів керівників від фінансових результатів може стимулювати маніпуляції з прибутком
R2 – Працівники різних підрозділів	Неналежний доступ до інформаційних систем, високий рівень плинності кадрів, економічно необгрунтовані фінансові операції, невідповідність посадових обов'язків професійному рівню	Фактори, що підвищують ймовірність шахрайства
R3 – Контрагенти	Економічна обгрунтованість договорів, наявність ризикових банківських установ, сумнівних інвесторів та третіх сторін	Договори на невигідних умовах або з економічно необгрунтованими цінами
R4 – Інституційні особливості та стан діяльності підприємства	Складна організаційна структура, часті зміни форми власності, відсутність ефективного внутрішнього аудиту, вразливість бізнес-моделі, судові позови та штрафи, складні фінансові механізми	Ознаки підвищеного ризику шахрайства
R5 – Макро- та глобальні фактори	Економічна нестабільність, гіперінфляція, банкрутства банків, підвищене податкове навантаження, корупція, технологічні зміни, природні катаклізми, соціально-демографічні зміни	Підвищують загрозу шахрайства на підприємстві
Загальний рівень ризику (R)	Комплексний аналіз R1-R5, встановлення превентивних заходів для мінімізації негативного впливу	Дозволяє аудиторам обрати відповідні процедури, підвищити ефективність внутрішнього контролю та фінансову прозорість

*Джерело: складено авторами за матеріалами [4]*

Державні та місцеві бюджети є привабливим джерелом для отримання злочинних доходів через великі обсяги фінансування діяльності державних установ та суб'єктів, що фінансуються за рахунок бюджету. Виявляються випадки закупівель товарів, робіт та послуг у підприємств з сумнівною репутацією або без виробничих потужностей, складських приміщень та кваліфікованого персоналу, що призводить до завищення витрат і створює можливості для розкрадання коштів.

Фінансові розслідування показують схеми, коли державні установи перераховують кошти підприємствам-посередникам, які надалі переводять їх фізичним особам-підприємцям або на власні рахунки для зняття готівки, купівлі валютних цінностей чи погашення кредитів. Такі операції охоплюють значну частину бюджетних надходжень і підвищують ризик нецільового використання коштів [5].

Також використовуються ризикові підприємства, які отримують кошти від місцевих організацій, житлово-комунальних підприємств та органів самоврядування, перераховують їх на власні карткові рахунки або виводять через ланцюги фіктивних угод, що унеможливує контроль за призначенням платежів. Нерідко такі підприємства створюються спеціально перед тендерами, не маючи технічної бази або персоналу для виконання договірних зобов'язань [5].

В окремих випадках державні установи чи органи самоврядування перераховують кошти на користь компаній-нерезидентів у межах міжнародних проектів або агентських договорів, частина яких надалі переводиться у готівку або розподіляється між пов'язаними групами фізичних та юридичних осіб. Ці операції демонструють механізм нелегального заволодіння бюджетними

ресурсами через фіктивні угоди та непрозорі фінансові канали [5].

Інтеграція форензик-методів у регулярну практику внутрішнього аудиту є важливим кроком для ефективного запобігання та виявлення шахрайських дій у компанії. Форензик-аудит передбачає систематичне дослідження фінансової інформації, документів та електронних даних з метою виявлення, аналізу та документування можливих фінансових злочинів, неправомірних дій або порушень бізнес-процесів. До основних методів належать комплексна перевірка благонадійності контрагентів, аналіз бухгалтерських та первинних документів, внутрішніх розслідувань фактів шахрайства, Data Analytics для обробки великих масивів даних та перевірка дотримання антикорупційних і законодавчих норм [6].

Практичне впровадження таких методів вимагає не лише адаптації процедур внутрішнього аудиту, але й систематичного навчання персоналу та внутрішніх аудиторів. Регулярні тренінги з виявлення нових схем шахрайства, кібератак,

маніпуляцій з фінансовими ресурсами та порушень внутрішніх регламентів дозволяють підвищити обізнаність співробітників та зменшити ризики недобросовісних дій. Форензик-аудитори мають у своїй роботі поєднувати фінансовий, юридичний та організаційний аналіз, що забезпечує всебічну перевірку бізнес-процесів і трансакцій та дозволяє оперативно реагувати на виявлені порушення.

Для підвищення ефективності виявлення аномалій, своєчасного реагування на фінансові ризики та протидії шахрайству пропонується інтеграція методів форензик-аудиту та Data Analytics у систему внутрішнього контролю.

Рамкова логіка інтеграції Data Governance у внутрішній аудит і форензик-аналітику передбачає опрацювання та інтеграцію п'яти ключових компонентів: управління даними, збір та інтеграцію даних, аналітику аномалій, прогнозу аналітику та форензик-методи (рис. 3).

Критичний аналіз цих компонентів та їх розвиток дозволяють сформувати єдину систему контролю проти шахрайства (табл. 2).

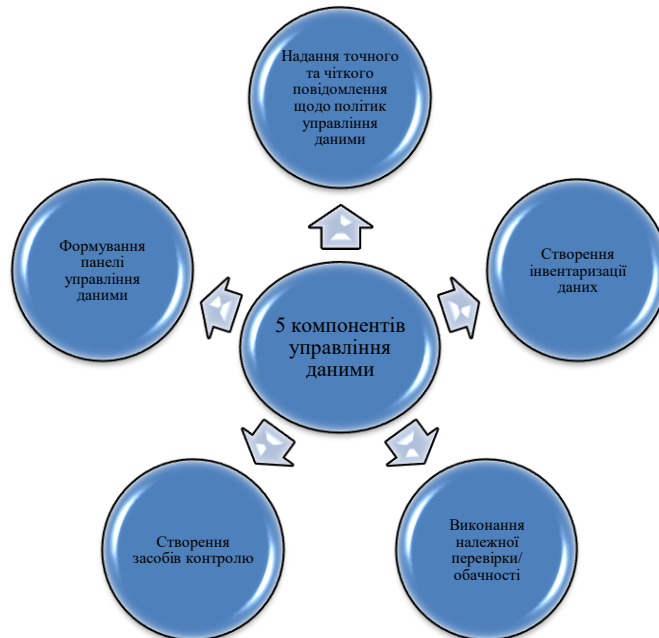


Рисунок 3. Рамкова логіка інтеграції Data Governance у внутрішній аудит та форензик-аналітику

Джерело: складено авторами за матеріалами [7]

Таблиця 2. Єдина система контролю проти шахрайства

Компонент інтеграції	Інструменти інтеграції	Етапи впровадження	Очікуваний ефект
1	2	3	4
Управління даними: Data Governance	Словники даних, стандарти якості, політики доступу, метадані, лінія походження даних (data lineage)	1. Аналіз джерел даних; 2. Встановлення стандартів; 3. Реєстр джерел	Зменшення хибних спрацьовувань, підвищення довіри до аналітики
Збір та інтеграція даних	Інтеграція даних із різних джерел, що включає об'єднання транзакційних даних з ERP-систем, банківських виписок, журналів подій, систем закупівель і HR-систем для проведення комплексного аналітичного контролю	1. Підключення джерел; 2. Налаштування потоків даних; 3. Анонімізація/маскування	Можливість кореляції подій, раннє виявлення схем шахрайства

## Продовження таблиці 2

1	2	3	4
Аналітика аномалій	Статистичні контрольні карти, алгоритми виявлення аномалій	1. Формування базових правил; 2. Навчання моделей; 3. Поріг спрацювань	Виявлення нетипових платежів, дивних змін залишків, підозрілих контрагентів
Прогнозна аналітика	Прогнозні моделі і алгоритми	1. Визначити цільові ризикові події; 2. Сформувати історично-аналітичну базу даних для формування критеріїв ідентифікації аномалій і ризиків шахрайства; 3. Навчити аналітичну модель на історичних даних і перевірити її ефективність у виявленні аномалій та ризиків шахрайства	Прогноз ймовірності шахрайства, пріоритезація інцидентів
Форензик-методи та розслідування	Ланцюговий аналіз транзакцій, рекреація подій, судово-економічні процедури, збереження доказів	1. Підготовка процедури збору доказів, налаштування обліково-аналітичної системи під потреби моделі Data Analytics; 2. Обговорення процесів інтеграції і їх результатів із аудитором; 3. Навчання моделі Data Analytics	Надійне документування інцидентів, підвищення успішності притягнення до відповідальності
Моніторинг	Аналіз системи ризиків	1. Визначення подій для моніторингу; 2. Налаштування точок контролю; 3. Інтеграція з процесами реагування на інциденти	Миттєве виявлення та блокування підозрілих операцій
Кейс-менеджмент та робочі процеси	Система керування інцидентами, ролі та ескалації, шаблони розслідувань	1. Впровадити систему трекінгу; 2. Регламент ескалації; 3. SLA на реакцію	Узгоджене, швидке реагування, контроль компетенцій
Юридична та комплаєнс-сумісність	Правова оцінка збору/обробки даних, комунікація із зацікавленими аудиторами, контрольними службами, безпековими органами: служба фінмоніторингу, правоохоронці, зовнішні аудитори, ДАСУ, РПУ тощо	1. Аудит прав доступу; 2. Політика збереження даних; 3. Шаблони запитів до зацікавлених суб'єктів	Захищеність доказів, законність реагування
Навчання та організаційна трансформація	Форензик-тренінги, Data Literacy, сценарні вправи (tabletop exercises)	1. Оцінка навичок; 2. Програма навчання; 3. Регулярні вправи	Підвищення якості розслідувань, швидкість реакції, зниження внутрішнього шахрайства
Інфраструктура і безпека	Захист середовища аналітики, контроль доступу, резервування, журналювання	1. Оцінка ІТ-ландшафту; 2. Впровадження безпечних середовищ; 3. Аудит доступів	Запобігання витоку даних, збереження цілісності аналітики

Джерело: складено авторами за матеріалами [7]

Надані рекомендації дозволяють розширити традиційний підхід до Data Governance, поєднуючи правові та організаційно-функціональні механізми з діяльністю конкретних суб'єктів контролю. Запропонований підхід орієнтований на документування доказів, комплаєнс-захист, участь державних контролюючих органів (ДАСУ, СБУ, НБУ, правоохоронні органи) та розвиток аналітичної культури персоналу.

Для забезпечення цілісності системи контролю та відповідності міжнародним стандартам внутрішнього контролю інтеграція форензик-

аудиту та Data Analytics узгоджується з компонентами моделі COSO (табл. 3).

Інтеграція форензик-аудиту та Data Analytics не підміняє класичні компоненти COSO, а цифрово трансформує їх, створюючи високоєфективне, проактивне та доказове контрольне середовище. Застосування інтегрованого підходу дозволяє автоматизувати ідентифікацію ризиків, оцінювати ймовірність шахрайства, забезпечувати документування доказів та комплаєнс-захист, залучати державні контролюючі органи та підвищувати аналітичну культуру персоналу. Це

створює умови для постійного моніторингу ризикових операцій і контролю ефективності запроваджених механізмів, що сприяє своєчасному реагуванню на інциденти та зниженню внутрішнього шахрайства.

Не менш важливою складовою інтеграції є належна звітність про ризики та виявлені факти. Компанії повинні формувати чіткі вимоги щодо

фіксації всіх підозрілих операцій, їх оцінки та подання керівництву у вигляді зрозумілих аналітичних звітів. Така звітність забезпечує прозорість діяльності, допомагає в прийнятті управлінських рішень і сприяє підвищенню довіри до фінансової звітності та системи внутрішнього контролю компанії.

Таблиця 3. Узгодження інтеграції форензик-аудиту та Data Analytics у СВК

Компоненти COSO	Відповідні компоненти інтеграції	Змістовне узгодження
1. Контрольне середовище	Навчання та організаційна трансформація, управління контрольним середовищем, юридична та комплаєнс-сумісність	Розвиває етичну культуру за рахунок формування нульової толерантності до шахрайства, забезпечує умови щодо дотримання законності розслідувань, змінює характеристики середовища: доступність, швидкість реагування на запити
2. Оцінка ризиків	Аналітика аномалій, прогнозна аналітика, управління даними	Data Analytics автоматизує ідентифікацію ризиків та оцінює ймовірність шахрайства через аналіз транзакцій, історичних даних, моделей поведінки контрагентів
3. Контрольні заходи	Збір та інтеграція даних; форензик-методи та розслідування, інфраструктура і безпека	Реалізують механізми запобігання та виявлення аномалій: від автоматизованих контролів до процедур збереження доказів і технічного захисту даних.
4. Інформація та комунікації	Управління даними, юридична та комплаєнс-сумісність	Забезпечують обмін достовірними даними між аудиторами, фінансовими службами, безпековими підрозділами, правоохоронними органами, встановлюють регламент звітності та комунікацій
5. Моніторинг	Моніторинг ризиків, управління процесами моніторингу, прогнозна аналітика	Data-driven моніторинг забезпечує постійне спостереження за ризиковими операціями, контроль результатів аналітичних моделей, оцінку ефективності запроваджених контролів

*Джерело: власна розробка авторів*

Інтеграція форензик-методів та інструментів Data Analytics є критично важливим кроком, який підвищує превентивну та детективну спроможність внутрішнього аудиту, трансформуючи його з реактивної функції на проактивний механізм протидії шахрайству. Для досягнення цієї мети необхідна комплексна трансформація у трьох ключових сферах: кадрів, процесів та технологій.

Насамперед, необхідно забезпечити, щоб внутрішні аудитори мали відповідні знання та навички для проведення форензик-розслідувань. Слід запровадити обов'язкове, регулярне навчання з основ форензик-бухгалтерії, методів збору та збереження електронних доказів, а також основ правового регулювання розслідувань. Для забезпечення комплексної експертизи при розслідуваннях доцільно формувати мультидисциплінарні аудиторські команди, які включатимуть фахівців із фінансів, Data Science/Analytics та юридичних питань. Також критично важливим є створення спеціалізованої функції або залучення IT-аудиторів для перевірки доступу, логів та захисту інформаційних систем, оскільки електронні докази є наріжним каменем форензик-аудиту. Крім того, аудитори повинні розвивати «м'які» навички, зокрема, опанувати методи проведення інтерв'ювання та ефективного документування висновків, щоб забезпечити їхню доказову силу.

Трансформація методології починається з розробки протоколу реагування на шахрайство,

який має чітко описувати кроки внутрішнього аудиту після виявлення «червоних прапорців» за допомогою DA-інструментів, включаючи порядок ізоляції даних, збереження доказів і звітування керівництву. Оцінка ризиків має стати Data-Driven, тобто слід регулярно оновлювати таблицю ризиків шахрайства на основі результатів Data Analytics, використовуючи ці інструменти для кількісної оцінки ризиків у високоризикових сферах, як-от закупівлі чи дебіторська заборгованість. Ключовим елементом сучасної методології є впровадження постійного моніторингу, що забезпечує перехід від періодичних аудитів до автоматизованого відстеження ключових транзакцій і «червоних прапорців» у режимі реального часу. Нарешті, форензик-процедури мають бути включені як стандартна частина аудиторських програм для високоризикових областей, зокрема, для аудиту витрат на представницькі потреби або взаємодії з ризиковими контрагентами.

Для ефективного інтеграції необхідно забезпечити внутрішній аудит відповідним технологічним арсеналом. Це вимагає впровадження спеціалізованого програмного забезпечення для Data Analytics, що дозволить аудиторам ефективно опрацьовувати великі масиви даних. Крім того, слід використовувати спеціалізовані технології для форензик-аналізу, зокрема, програмне забезпечення для електронного пошуку доказів та аналізу неструктурованих даних, як-от електронна пошта та повідомлення. Важливим кроком є

автоматизація «червоних прапорців» шляхом налаштування алгоритмів у DA-інструментах, які автоматично генеруватимуть попередження про підозрілі транзакції, наприклад, про подвійні платежі, розділення великих закупівель (сплітинг), або про операції, проведені у неробочий час. І, зрештою, для збереження доказової сили результатів форензич-аналізу, необхідно забезпечити незмінність даних шляхом впровадження процесів створення криміналістичної копії первинних даних перед початком розслідування.

Узагальнюючи, інтеграція форензич-методів та інструментів Data Analytics є критичною стратегічною трансформацією внутрішнього аудиту. Вона необхідна для протидії шахрайству, що постійно еволюціонує, та переходу від реактивної функції до проактивного механізму моніторингу.

Ключовий успіх полягає у усуненні можливості для зловживань (згідно з «Трикутником шахрайства») завдяки глибині форензич-розслідувань та широті охоплення DA-інструментів.

Для реалізації цієї мети потрібна комплексна трансформація за трьома напрямками: кадри, процеси та технології. Ця системна інтеграція дозволяє аудиту не лише ефективно документувати фінансові злочини, але й суттєво мінімізувати ризики їхнього виникнення, зміцнюючи загальну фінансову прозорість.

#### **Висновки та перспективи подальших досліджень**

Інтеграція форензич-методів та інструментів Data Analytics у систему внутрішнього аудиту є стратегічно важливим кроком для підвищення ефективності запобігання, виявлення та документування шахрайства в організаціях. Сучасні умови, що характеризуються складністю бізнес-процесів, великим обсягом даних та постійною еволюцією шахрайських схем, роблять традиційні методи внутрішнього аудиту недостатньо ефективними. У цьому контексті поєднання класичних аудиторських процедур із цифровими інструментами та аналітичними технологіями дозволяє організаціям переходити від реактивного контролю до проактивного моніторингу фінансових ризиків.

Форензич-аудит у поєднанні з Data Analytics забезпечує комплексний підхід до виявлення

шахрайських дій, включаючи аналіз фінансових і первинних документів, обробку великих масивів даних, автоматизоване відстеження аномалій і «червоних прапорців». Це не лише підвищує точність та швидкість виявлення порушень, а й формує прозору і структуровану систему внутрішнього контролю, яка дозволяє обмежити можливості для зловживань у відповідності до моделі «Трикутник шахрайства».

Особливо важливим є комплексний розвиток трьох ключових компонентів внутрішнього аудиту: кадрів, процесів та технологій. Підготовка фахівців із компетенціями у сфері форензич-аудиту, Data Analytics та правового регулювання забезпечує всебічний аналіз та перевірку бізнес-процесів. Вдосконалені процеси, що передбачають протоколи реагування на підозрілі транзакції, регулярний Data-Driven аналіз ризиків та постійний моніторинг, забезпечують своєчасне реагування на загрози. Технологічна трансформація, включаючи використання спеціалізованого програмного забезпечення для аналізу великих даних, електронного пошуку доказів та автоматизації сигналів «червоних прапорців», сприяє підвищенню ефективності внутрішнього контролю та мінімізації людського фактору.

Інтеграція форензич-методів і Data Analytics не лише дозволяє виявляти і документувати шахрайство, а й створює проактивну систему управління ризиками, яка зміцнює фінансову стійкість організацій, підвищує прозорість діяльності та довіру зацікавлених сторін. Таким чином, ця інтеграція виступає ключовим механізмом трансформації внутрішнього аудиту, забезпечуючи перехід від традиційного реагування на порушення до стратегічного запобігання фінансовим злочинам та ефективного захисту ресурсів підприємства.

Загалом, комплексне впровадження форензич-методів і Data Analytics створює синергетичний ефект: поєднання глибокого аналізу транзакцій та сучасних аналітичних технологій дозволяє організаціям не лише виявляти шахрайство на ранніх стадіях, а й запобігати його виникненню, підвищуючи загальний рівень фінансової безпеки та управлінської ефективності.

#### **Abstract**

Fraud remains one of the greatest threats to financial stability, organizational reputation, and operational effectiveness. Financial misconduct, document falsification, asset misappropriation, and corruption schemes require the implementation of effective control mechanisms. Internal audit plays a key role in the timely detection and prevention of fraud, ensuring the reliability of financial reporting and the transparency of business processes.

The integration of forensic methods with Data Analytics enhances audit effectiveness by enabling the detection of anomalies, risk prediction, and automated transaction verification. This approach creates a transparent, structured, and proactive internal control system, where every operation is monitored and opportunities for misconduct are minimized.

Special attention is given to the comprehensive transformation of three key aspects: the development of personnel with competencies in forensic auditing and Data Analytics; the improvement of processes with clear response protocols and continuous data-driven risk analysis; and technological transformation through the implementation of software for big data processing and automation of “red flag” signals.

The integration of forensic methods and Data Analytics establishes a proactive risk management system, strengthens financial security, enhances transparency and stakeholder trust, and transforms internal audit from a reactive function into a strategic mechanism for fraud prevention.

## References:

1. Ministry of Finance of Ukraine. (n.d.). Methodological guidelines on internal audit in the public sector of Ukraine. [https://www.mof.gov.ua/storage/files/МВ\\_новий\\_формат\\_Вступ\\_+\\_розділи\\_1-8.pdf](https://www.mof.gov.ua/storage/files/МВ_новий_формат_Вступ_+_розділи_1-8.pdf)
2. Opendatobot. (2024). Fraud cases decreased by 21% over the year. <https://opendatobot.ua/analytics/fraud-2024-12>
3. Mykhalchyshyna, L.H., & Kalashnyk, V.V. (2012). Internal audit in preventing errors and fraud at the enterprise. Collection of Scientific Works of VNAU. Series: Economic Sciences, 2(64), 99-105. <https://socrates.vsau.org/repository/getfile.php/6192.pdf>
4. Stetsiuk, O., & Chubai, V. (2023). Fraud detection at the enterprise: Algorithm of actions and indicators of high fraud risk. *Economy and Society*, (48). <https://doi.org/10.32782/2524-0072/2023-48-83>
5. State Financial Monitoring Service of Ukraine. (2019). Typological study: Laundering of proceeds from misappropriation of funds and property of state enterprises and other entities financed from state and local budgets (p. 82). [https://fiu.gov.ua/assets/userfiles/books/book\\_topology2020UA.pdf](https://fiu.gov.ua/assets/userfiles/books/book_topology2020UA.pdf)
6. Nesterenko, O. (2024). Forensic audit as an effective tool for combating internal corporate fraud in wartime. *Acta Academiae Beregsasiensis. Economics*, (5), 392-405. <https://doi.org/10.58423/2786-6742/2024-5-392-405>
7. Fortinet. (n.d.). What is data governance? Definition, framework, and best practices. <https://www.fortinet.com/resources/cyberglossary/data-governance>

### **Посилання на статтю:**

*Балан А.А. Інтеграція форензик-методів та Data Analytics у систему внутрішнього аудиту як механізм протидії шахрайству / А.А. Балан, Д.В. Бондарук // Економіка: реалії часу. Науковий журнал. – 2026. – № 2 (84). – С. 23-31. – Режим доступу: <https://etr.economics.net.ua/files/archive/2026/No2/23.pdf>. DOI: 10.15276/ETR.02.2026.3. DOI: 10.5281/zenodo.20348951.*

### **Reference a Journal Article:**

*Balan A.A. Integration of Forensic Methods and Data Analytics into the Internal Audit System as a Mechanism for Fraud Prevention / A.A. Balan, D.V. Bondaruk // Economics: time realities. Scientific journal. – 2026. – № 2 (84). – P. 23-31. – Retrieved from: <https://etr.economics.net.ua/files/archive/2026/No2/23.pdf>. DOI: 10.15276/ETR.02.2026.3. DOI: 10.5281/zenodo.20348951.*



This is an open access journal and all published articles are licensed under the terms of the Creative Commons Attribution License (CC BY 4.0)

© 2026 The Author(s). Published by Odessa Polytechnic National University