УДК 657.6:343.98:336.22 **DOI**: https://doi.org/10.31521/modecon.V53(2025)-24

Лугова О. І., кандидат економічних наук, доцент, доцент кафедри обліку та оподаткування, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID: 0000-0003-4432-0295
e-mail: lugova@mnau.edu.ua

Політікіна І. В., здобувач вищої освіти обліково-фінансового факультету, Миколаївський національний аграрний університет, м. Миколаїв, Україна

ORCID: 0009-0002-7144-0882
e-mail: innapolitikina965@gmail.com

Внутрішній контроль і технологічні інструменти протидії шахрайству в обліку та оподаткуванні

Анотація. *У статті досліджено проблему професійного шахрайства - умисних дій, вчинених працівниками проти роботодавців. Дослідження базується на аналізі даних міжнародного звіту ACFE, який охоплює понад 2 тисячі кейсів із 138 країн світу. Визначено найпоширеніші форми шахрайства, серед яких домінує незаконне привласнення активів, а також охарактеризовано умови, за яких зростає ризик вчинення таких дій. Детально розглянуто типові поведінкові ознаки зловмисників, роль посадового статусу та схильність до змови. Окрему увагу приділено механізмам виявлення шахрайства - від повідомлень інформаторів до автоматизованого моніторингу, а також сучасним технологіям, які використовуються для протидії шахрайству: аналітика даних, машинне навчання, блокчейн та біометрія. Результати дослідження мають прикладну цінність і можуть бути використані для формування політики внутрішнього контролю, оцінки ризиків шахрайства, підготовки антикорупційних заходів, навчання працівників та впровадження інновацій у сфері комплаєнсу.*

Ключові слова*: професійне шахрайство; внутрішній контроль; облік; оподаткування; фінансові збитки; поведінкові індикатори.*

Luhova Olha, Candidate of Economic Sciences, Associate Professor of the Department of Accounting and Taxation, Mykolaiv National Agrarian University, Mykolaiv, Ukraine

Politikina Inna, student of the Accounting and Finance Faculty, Mykolaiv National Agrarian University, Mykolaiv, Ukraine

Internal Control and Technological Tools to Combat Accounting and Tax Fraud

Abstract. Introduction. *Occupational fraud remains one of the most widespread and damaging threats to organizations across industries and countries. According to estimates by the Association of Certified Fraud Examiners (ACFE), organizations lose around 5% of their annual revenues due to fraudulent activities, which amounts to trillions of dollars globally. High-profile scandals such as Enron, WorldCom and Wirecard illustrate the devastating consequences of fraud, which go far beyond financial losses and include reputational damage, legal repercussions, and declining stakeholder trust. The increasing complexity of financial operations, digitalization, and globalization have created new opportunities for fraudulent schemes, making the study of occupational fraud highly relevant.*

Purpose*. The aim of the research is to provide a comprehensive assessment of the current state of occupational fraud, identify its most common forms and risk factors, and define effective approaches, tools, and technologies for its detection and prevention.*

Results*. The study, based on ACFE's Occupational Fraud 2024 Report to the Nations, confirms that occupational fraud schemes fall into three major categories: asset misappropriation, corruption and financial statement fraud. Fraudsters frequently combine two or more schemes, particularly asset misappropriation and corruption. Collusion among multiple perpetrators and fraud committed by executives lead to faster and more severe financial damage. The most common concealment methods remain falsification or alteration of documents, while fraud detection primarily relies on tips, followed by internal audit and managerial review. Proactive detection mechanisms reduce both the duration of fraud schemes and their financial impact. The analysis highlights the role of internal control weaknesses - such as lack of oversight, override of controls, or unethical "tone at the top" - as key enablers of fraud. Advanced technologies, including big data analytics, artificial intelligence, machine learning, blockchain, and biometric tools, are increasingly adopted by organizations to enhance monitoring, anomaly detection, and preventive measures.*

Conclusions*. The findings emphasize that occupational fraud represents a systemic challenge that cannot be addressed by financial controls alone. An effective anti-fraud strategy requires an integrated approach that combines modern technological solutions with ethical leadership, corporate culture of integrity, strong governance, and continuous staff awareness. Such a*

[1]**Стаття надійшла до редакції**: 06.10.2025
Received: 6 October 2025

holistic framework reduces both the likelihood and the impact of fraud, strengthening organizational resilience in the face of evolving threats.

***Keywords**: professional fraud; internal control; accounting; taxation; financial losses; behavioural indicators.*

***JEL Classification:** H 26, K42; M 40.*

Постановка проблеми. Шахрайство у сфері бухгалтерського обліку та оподаткування є значною проблемою, яка впливає на бізнес, уряд та приватних осіб. За оцінками Асоціації сертифікованих експертів з питань шахрайства (ACFE), організації втрачають близько 5% річного доходу від шахрайства, що в глобальному масштабі становить трильйони доларів. Наслідки бухгалтерського шахрайства є глибокими і виходять за межі фінансових втрат, включаючи втрату репутації, юридичні наслідки та зниження довіри зацікавлених сторін [1]. Гучні корпоративні скандали, пов'язані з компаніями Enron, WorldCom, Wirecard, висвітлюють серйозні наслідки шахрайської діяльності та підкреслюють гостру потребу в ефективних механізмах виявлення шахрайства [2].

Зростання складності фінансових операцій, поширення цифрових технологій, глобалізація бізнесу створюють нові можливості для реалізації шахрайських схем. Саме тому дослідження стану, форм прояву, детекторів і засобів протидії професійному шахрайству є актуальним як у науковому, так і в прикладному вимірах.

Аналіз останніх досліджень та публікацій. Дослідження базується на аналізі даних міжнародного звіту ACFE «Occupational Fraud 2024: A Report to the Nations» [3], який охоплює понад 2 тисячі кейсів із 138 країн світу за даними приватних, державних, урядових і неприбуткових організацій у 22 різних галузях, що забезпечує глобальний і широкий діапазон та включає як статистичну, так і структурну характеристику проявів шахрайства.

Формулювання цілей дослідження. Метою дослідження є всебічна оцінка сучасного стану професійного шахрайства та визначення ефективних напрямів його виявлення й протидії.

Виклад основного матеріалу дослідження. Схеми професійного шахрайства поділяються на три основні категорії: незаконне привласнення активів, корупція та шахрайство з фінансовою звітністю. Найпоширенішим видом професійного шахрайства є привласнення активів (89% випадків) із найнижчим середнім збитком - 120 тис. дол. США. Майже половина випадків (48%) стосувалася корупції із середнім збитком 200 тис дол США. Найрідше траплялося шахрайство з фінансовою звітністю (5%), проте воно завдавало найбільших збитків - у середньому 766 тис дол США [3].

Хоча професійне шахрайство можна розділити на три окремі категорії, зловмисники не завжди обмежують свої схеми лише однією категорією. У 38% випадків було використано два або більше видів професійного шахрайства, при цьому найчастіше відбувається перетин між незаконним привласненням активів і корупцією (35% випадків) і тільки 1% випадків стосувався лише шахрайства з фінансовою звітністю (табл. 1).

Таблиця 1 **Частота поєднання видів шахрайства у професійній діяльності**

Види професійного шахрайства	Частка, %
Тільки незаконне привласнення активів	51
Незаконне привласнення активів та корупція	35
Тільки корупція	10
Корупція, привласнення активів та шахрайство з фінансовою звітністю	2
Незаконне привласнення активів та шахрайство з фінансовою звітністю	1
Тільки шахрайство з фінансовою звітністю	1
Корупція та шахрайство з фінансовою звітністю	<1

Джерело: складено авторами на основі даних [3]

Схеми незаконного привласнення активів можуть набувати різних форм, що часто залежить від доступу або можливостей, які має злочинець в організації-жертві (табл. 2).

Таблиця 2 **Схеми незаконного привласнення активів**

Категорія	Кількість випадків	Відсоток усіх випадків, %	Середні втрати, дол
Безготівковий розрахунок	426	22	66 000
Виставлення рахунків	424	22	100 000
Відшкодування витрат	248	13	50 000
Підробка чеків та платежів	217	11	155 000
Готівка в касі	205	11	50 000
Скімінг	200	10	43 000
Крадіжка готівки	192	10	50 000
Нарахування заробітної плати	190	10	50 000
Реєстрація виплат	52	3	50 000

Джерело: складено авторами на основі даних [3]

У таксономії «Дерева шахрайства» схеми незаконного привласнення активів поділено на дев'ять окремих підсхем залежно від способу вчинення злочину. Розуміння того, яка з цих підсхем становить найбільший ризик для організації, може допомогти в оцінці ризиків і мінімізації втрат від шахрайства.

Певні типи схем ускладнюються набагато швидше, ніж інші, причому найбільшу швидкість мають схеми шахрайства з фінансовою звітністю та корупційні схеми. Аналогічно, випадки, пов'язані зі змовою між 2 або більше злочинцями, та випадки, скоєні особами на вищих щаблях влади, також мають більшу швидкість і швидше завдають фінансової шкоди жертвам (табл. 3).

Таблиця 3 **Фінансові наслідки шахрайства за категоріями правопорушників**

Категорія правопорушників	Середні втрати, дол	Середня тривалість, місяці	Втрати на місяць, дол
Один злочинець	75 000	12	6 300
Двоє злочинців	135 000	12	11 300
Троє або більше злочинців	329 000	14	23 500
Працівник	60 000	8	7 500
Менеджер	184 000	18	10 200
Власник / керівник	500 000	24	20 800

Джерело: складено авторами на основі даних [3]

Після того, як шахраї реалізують свої схеми, вони, як правило, вживають заходів для приховування злочинів. Розуміння методів, які використовують шахраї для приховування злочинів, може допомогти організаціям покращити зусилля із запобігання та виявлення шахрайства (табл. 4).

Таблиця 4 **Методи приховування професійного шахрайства**

Схеми професійного шахрайства	Частка, %
Створення підроблених фізичних документів	41
Змінено фізичні документи	37
Створення підроблених електронних документів або файлів	31
Змінено електронні документи або файли	28
Знищення або приховування фізичних документів	23
Створення підроблених операцій в системі бухгалтерського обліку	19
Видалення або приховування електронних документів або файлів	19
Змінені операції в системі бухгалтерського обліку	16
Видалені або пропущені операції в системі бухгалтерського обліку	13
Відсутність способу приховування	11
Інше	10
Створення підроблених журнальних записів	9
Примусова або змінена звірка рахунків	9
Примусово виконані або змінені залишки рахунків в системі обліку	8
Змінені журнальні записи	7
Видалено або пропущено журнальні записи	6

Джерело: складено авторами на основі даних [3]

У 11% випадків не було застосовано жодного методу приховування. З 89% випадків, які включали певне проактивне приховування, найпоширенішими методами були створення фальшивих фізичних документів (41% випадків) або зміна фізичних документів (37% випадків). Ці результати свідчать, що навіть попри те, що багато транзакцій перейшли в цифровий формат, речові докази все ще залишаються важливою частиною запобігання, виявлення та розслідування шахрайства.

З появою криптовалют у фінансовому ландшафті та їх дедалі ширшим використанням організації та фахівці з протидії шахрайству повинні усвідомлювати, як ці активи можуть впливати на ризики професійного шахрайства. Лише 4% випадків у дослідженні «Occupational Fraud 2024: A Report to the Nations» були пов'язані з криптовалютою; майже в половині з них (47%) зловмисник конвертував викрадені активи в криптовалюту, а третина (33%) - з хабарами або «відкатами» співучасникам у криптовалюті.

Розуміння методів, за допомогою яких найчастіше виявляють професійне шахрайство, має вирішальне значення для ефективного виявлення та переривання схем, зменшуючи таким чином їхній вплив і тривалість (табл. 5).

Таблиця 5 **Методи первинного виявлення професійного шахрайства**

Методи виявлення шахрайства	Частка, %	Хто повідомляє про шахрайство	Частка, %
Повідомлення про шахрайство	43	Працівники	52
Внутрішній аудит	14	Клієнти	21
Управлінська перевірка	13		
Перевірка документів	6	Аноніми	15
Звірка рахунків	5		
Випадково	5	Постачальники	11
Зовнішній аудит	3		
Автоматизований моніторинг транзакцій / даних	3	Інші	7
Нагляд / моніторинг	2	Акціонери/власники	1
Інше	2		
Повідомлення правоохоронних органів	2	Конкуренти	1
Зізнання	1		

Джерело: складено авторами на основі даних [3]

Найпоширенішим способом виявлення шахрайства були повідомлення, причому 43% випадків було розкрито завдяки інформації, отриманій від викривачів. Це більш ніж утричі перевищує будь-який інший механізм виявлення. Іншими поширеними методами виявлення були внутрішній аудит (14%) та управлінська перевірка (13 відсотків). Разом ці три методи виявлення становлять 70% випадків. Більше половини всіх повідомлень (52%) надійшли від працівників організації. На зовнішні джерела, такі як клієнти, постачальники та конкуренти, припадає приблизно третина всіх повідомлень.

Цей висновок підкреслює важливість забезпечення та механізми звітування як внутрішніх, так і зовнішніх сторін. Організації, які мають гарячі лінії, майже вдвічі частіше виявляють шахрайство за допомогою повідомлень, ніж організації без гарячих ліній, що ілюструє вирішальну роль, яку відіграють гарячі лінії в комплексній програмі виявлення шахрайства.

Деякі методи виявлення шахрайства є більш ефективними, ніж інші, для швидкого викриття шахрайства та обмеження розміру збитків (табл. 6).

Таблиця 6 **Зв'язок між методом виявлення шахрайства, його тривалістю та завданими збитками**

Методи виявлення шахрайства	Тривалість, місяці	Середні втрати, дол
Повідомлення правоохоронних органів	24	675 000
Зізнання	21	121 000
Зовнішній аудит	18	227 000
Випадково	18	110 000
Управлінська перевірка	14	125 000
Повідомлення про шахрайство	12	155 000
Експертиза документів	12	133 000
Внутрішній аудит	12	100 000
Звірка рахунків	9	118 000
Автоматизований моніторинг транзакцій / даних	6	83 000
Спостереження / моніторинг	6	65 000

Джерело: складено авторами на основі даних [3]

Більшість пасивно виявлених схем (повідомлення поліції, випадковість або зізнання шахрая) тривали довше і були пов'язані з вищими середніми збитками порівняно з усіма іншими методами виявлення.

Схеми, виявлені активним методом (вивчення документів або спостереження / моніторинг), мали меншу тривалість і нижчу середню суму збитків, ніж ті, що були виявлені пасивним методом.

Методи виявлення, які потенційно можуть бути як пасивними, так і активними (повідомлення про шахрайство та зовнішній аудит), як правило, перебувають посередині за середньою тривалістю та збитками.

Проактивні зусилля з виявлення шахрайства є важливими для захисту від ризику шахрайства. Загалом, активні методи виявлення пов'язані з набагато швидшим, ніж пасивні, а це означає, що організації можуть значно зменшити вплив шахрайства, впроваджуючи внутрішній контроль і політики, які активно виявляють шахрайство, такі як ретельна з боку керівництва, звірка рахунків і спостереження / моніторинг. Організації, які не займаються активним виявленням шахрайства, можуть зіткнутися зі схемами, які триватимуть набагато довше і коштуватимуть набагато дорожче.

Як зазначено в Посібнику з управління ризиками шахрайства COSO/ACFE [4], добре розроблена та ефективно впроваджена система контролю за протидією шахрайству є одним з основоположних принципів цілісної програми управління ризиками шахрайства. Однак наявність будь-якого конкретного засобу контролю або їх комбінації не гарантує повного запобігання шахрайству (табл. 7).

Таблиця 7 **Засоби протидії шахрайству на момент його вчинення**

Засоби протидії шахрайству	Частка, %
Кодекс корпоративної етики	85
Зовнішній аудит фінансової звітності	84
Відділ внутрішнього аудиту	80
Засвідчення фінансової звітності керівництвом	77
Управлінська перевірка	72
Зовнішній аудит системи внутрішнього контролю за фінансовою звітністю	72
Гаряча лінія	71
Незалежний аудиторський комітет	68
Тренінги з протидії шахрайству для працівників	63
Тренінги з протидії шахрайству для менеджерів/керівників	62
Політика протидії шахрайству	60
Програми підтримки працівників	59
Спеціальний відділ, функція або команда з питань протидії шахрайству	50
Офіційні оцінки ризиків шахрайства	48
Моніторинг / аналіз даних на основі упереджувального підходу	45
Неочікувані аудиторські перевірки	42
Ротація посад / обов'язкова відпустка	23
Заохочення для викривачів	14

Джерело: складено авторами на основі даних [3]

В організаціях-жертвах на момент вчинення шахрайства було впроваджено багато засобів контролю для його протидії. Найбільш поширеними засобами протидії шахрайству були кодекс корпоративної етики (85%), зовнішній аудит фінансової звітності (84%) та відділи внутрішнього аудиту (80 відсотків).

Розуміння факторів, що призвели до виникнення шахрайства, може допомогти організаціям посилити свою програму для захисту від майбутніх випадків професійного шахрайства (табл. 8).

Таблиця 8 **Основні недоліки внутрішнього контролю, які сприяють професійному шахрайству**

Основні недоліки внутрішнього контролю	Частка, %
Відсутність внутрішнього контролю	32
Скасування існуючого внутрішнього контролю	19
Відсутність аналізу з боку керівництва	18
Відсутність компетентного персоналу на наглядових посадах	9
Порушення етичних норм на рівні топменеджменту	8
Відсутність незалежних перевірок/аудитів	5
Інше	4
Відсутність навчання працівників щодо протидії шахрайству	3
Відсутність чіткого розподілу обов'язків	1
Відсутність механізму звітності	1

Джерело: складено авторами на основі даних [3]

Найбільш поширеним фактором, який спричинив шахрайство, був брак внутрішнього контролю (32%), за яким слідує обхід існуючого внутрішнього контролю (19 відсотків). У сукупності це означає, що більше половини випадків сталися через недостатню систему внутрішнього контролю.

Традиційні методи виявлення шахрайства в бухгалтерському обліку значною мірою спираються на ручні процеси, аудит та системи, засновані на правилах [5]. Ці методи, хоча і є фундаментальними, мають ряд обмежень, які роблять їх менш ефективними в сучасному ландшафті складних фінансових операцій та витончених схем шахрайства.

Для запобігання та виявлення шахрайства організації впроваджують різні внутрішні засоби контролю доступу, такі як розподіл обов'язків, вимоги до авторизації та звірки. Хоча внутрішній контроль має важливе значення для створення надійної системи запобігання шахрайству, він не є стовідсотково надійним. Працівники, які вступають у змову, можуть обійти ці засоби контролю, а самі засоби контролю іноді можуть бути занадто жорсткими, що призводить до операційної неефективності [6].

Штучний інтелект (далі – ШІ) став трансформаційною технологією з потенціалом для революції у виявленні шахрайства в бухгалтерському обліку [7]. ШІ охоплює низку технологій, включаючи машинне навчання (ML), обробку природної мови (NLP) та інтелектуальний аналіз даних, які дозволяють системам навчатися на основі даних, виявляти закономірності та приймати рішення з мінімальним втручанням людини. Алгоритми ML можуть аналізувати величезні обсяги фінансових даних для виявлення закономірностей і аномалій, які можуть свідчити про шахрайство [8, 9].

У сучасному стрімкому цифровому світі шахрайство викликає все більше занепокоєння як у бізнесу, так і у приватних осіб. Експерти із запобігання шахрайству постійно шукають нові способи випередити шахраїв, які використовують все більш витончені методи. На щастя, технології пропонують безліч інструментів і методів, які допомагають виявляти та запобігати шахрайським діям.

Технології відіграють вирішальну роль у допомозі фахівцям у виявленні та запобіганні шахрайству. З появою передових алгоритмів, машинного навчання та аналізу даних стало легше виявляти підозрілі дії та шаблони, які можуть свідчити про шахрайську поведінку.

З появою нових класів технологій, які підтримують розслідування, виявлення та запобігання шахрайству, багато організацій оцінюють потенційні переваги, які ці технології можуть надати їхнім програмам боротьби з шахрайством (табл. 9).

Таблиця 9 **Новітні технології, які використовують підприємства для боротьби з шахрайством**

Новітні технології	Використовують, %	Не використо-вують, очікують протягом 1–2 років, %	Не використо-вують, очікують більш ніж через 2 роки, %	Не передбачається використання, %
Фізична біометрія	40	17	12	31
Аналіз на основі технологій комп'ютерного зору	20	22	26	32
Робототехніка	20	21	20	39
Поведінкова біометрія	20	19	19	42
Блокчейн / технологія розподіленого реєстру	11	16	20	53
Візуальна / доповнена реальність	7	14	17	62

Джерело: складено авторами на основі даних [10]

Новою технологією, яку наразі застосовує більшість організацій, є фізична біометрія, яка використовується для ідентифікації осіб на основі фізичних атрибутів, таких як відбитки пальців, риси обличчя або голосу; 40% респондентів зазначили, що їхня організація наразі використовує фізичну біометрію, а ще 17% очікують, що ця технологія буде впроваджена в найближчому майбутньому.

Хоча сьогодні фізична біометрія використовується вдвічі частіше, ніж аналіз комп'ютерного зору (20%), робототехніка (20%) та поведінкова біометрія (20%), всі чотири технології або використовуються зараз, або очікується, що вони будуть використовуватися в майбутньому більш ніж у 50% організацій-респондентів [10].

Існує багато інструментів запобігання шахрайству, кожен з яких має свої сильні та слабкі сторони. Важливо обирати інструменти, які відповідають потребам організації та її профілю ризику. Наприклад, фінансова установа може отримати вигоду від розширеного моніторингу транзакцій на основі ШІ, в той час як компанія, що займається електронною комерцією, може віддати перевагу біометричній автентифікації для входу в систему клієнтів.

Запобігання шахрайству – це безперервний процес, який потребує постійного моніторингу та

вдосконалення. Технології розвиваються, як і тактика, яку використовують шахраї. Регулярне оновлення та вдосконалення стратегій і технологій запобігання шахрайству гарантує, що вони залишатимуться ефективними у боротьбі з новими загрозами.

Висновки та перспективи подальших досліджень. Професійне шахрайство є поширеним і небезпечним явищем, яке завдає суттєвих збитків як малим, так і великим організаціям у різних сферах діяльності. Його характерною рисою є навмисне зловживання посадовими повноваженнями або довірою роботодавця з метою особистого збагачення. Найбільш поширеними видами шахрайства є незаконне привласнення активів, шахрайство з фінансовою звітністю та корупційні схеми. При цьому саме фінансове шахрайство спричиняє найбільші збитки, хоча за частотою найчастіше фіксується саме привласнення активів. Фактори, що сприяють вчиненню шахрайства, включають не лише відсутність або слабкість системи внутрішнього контролю, але й недоліки корпоративної етики, занижений рівень нагляду з боку вищого керівництва, а також так званий «поганий тон згори» - приклад неетичної поведінки, що задається менеджментом. Важливу роль відіграють також поведінкові чинники: серед найпоширеніших «червоних прапорців» – спосіб життя, що не відповідає доходам, фінансові труднощі, надмірна прихильність до постачальників або клієнтів тощо.

Сучасні технології протидії шахрайству демонструють суттєвий потенціал у його виявленні, моніторингу та запобіганні фінансовим правопорушенням. Зокрема, використання аналітики великих даних, машинного навчання, штучного інтелекту, блокчейн-технологій, систем розпізнавання аномалій у транзакціях, а також біометричних засобів підвищує точність і швидкість реагування на загрози. Цифрові інструменти дозволяють не лише виявляти шахрайство, а й прогнозувати ризики його виникнення.

Таким чином, результати дослідження свідчать про необхідність комплексного підходу до боротьби з професійним шахрайством, що включає не лише технологічні засоби, а й етичне лідерство, послідовну політику внутрішнього контролю, розбудову культури доброчесності та постійне підвищення обізнаності персоналу. Такий підхід дозволяє мінімізувати як ймовірність шахрайства, так і його наслідки для підприємств.

Література:

1. Campa D., Quagli A., Ramassa P. The roles and interplay of enforcers and auditors in the context of accounting fraud: a review of the accounting literature. *Journal of Accounting Literature*. 2023. Vol. 47 No. 5. P. 151-183. URL: https://doi.org/10.1108/JAL-07-2023-0134.
2. Mutschmann M., Hasso T., Pelster M. Dark triad managerial personality and financial reporting manipulation. *Journal of Business Ethics*. 2021. P. 1-26. URL: https://ideas.repec.org/a/kap/jbuset/v181y2022i3d10.1007_s10551-021-04959-1.html.
3. Occupational Fraud 2024: A Report to the Nations. URL: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf.
4. Fraud Risk Management Guide. URL: https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide.
5. Shahana T., Lavanya V., Bhat A.R. State of the art in financial statement fraud detection: A systematic review. *Technological Forecasting and Social Change*, 2023. 192. P. 122527. URL: https://ideas.repec.org/a/eee/tefoso/v192y2023ics0040162523002123.html.
6. Lartey P.Y., Akolgo I.G., Jaladi S.R., Ayeduvor S., Afriyie S.O. Recent advances in internal control: Soft control overcoming the limits of hard control. *Frontiers in Management and Business.* 2023. 4(1). P. 289-302. URL: https://www.syncsci.com/journal/FMB/article/view/FMB.2023.01.004.
7. Hasan A.R. Artificial Intelligence (AI) in accounting & auditing: A Literature review. *Open Journal of Business and Management*. 2021. 10 (1). P. 440-465. URL: https://www.scirp.org/journal/paperinformation?paperid=115007.
8. Ashtiani M.N., Raahemi B. Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. *Ieee Access*. 2021. 10. P. 72504-72525. URL: https://www.researchgate.net/publication/363364663_Intelligent_Fraud_Detection_in_Financial_Statements_Using_Machine_Learning_and_Data_Mining_A_Systematic_Literature_Review.
9. Lakhan A., Mohammed M.A., Ibrahim D.A., Kadry S., Abdulkareem K.H. ITS based on deep graph convolutional fraud detection network blockchain-enabled fogcloud. *IEEE Transactions on Intelligent Transportation Systems*. 2022. URL: https://www.researchgate.net/publication/358650154_ITS_Based_on_Deep_Graph_Convolutional_Fraud_Detection_Network_Blockchain-Enabled_Fog-Cloud .
10. 2024 Anti-fraud technology benchmarking report. URL: https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/third-party-whitepapers/en/acfe-anti-fraud-technology-benchmark-report-113778.pdf?utm_source=linkedin&utm_medium=social-cpc&utm_campaign=public-sector-us-fsi-gen-americas&utm_content=pt-US_lead-gen-form.

References:

1. Campa, D., Quagli, A., & Ramassa, P. (2023). The roles and interplay of enforcers and auditors in the context of accounting fraud: a review of the accounting literature. *Journal of Accounting Literature*. Vol. 47 No. 5, 151-183. https://doi.org/10.1108/JAL-07-2023-0134.
2. Mutschmann, M., Hasso, T., & Pelster, M. (2021). Dark triad managerial personality and financial reporting manipulation.

Journal of Business Ethics, 1-26. URL: https://ideas.repec.org/a/kap/jbuset/v181y2022i3d10.1007_s10551-021-04959-1.html.

3. Occupational Fraud 2024: A Report to the Nations. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf.
4. Fraud Risk Management Guide. URL: https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide.
5. Shahana, T., Lavanya, V., & Bhat, A.R. (2023). State of the art in financial statement fraud detection: A systematic review. *Technological Forecasting and Social Change*, 192, 122527. https://ideas.repec.org/a/eee/tefoso/v192y2023ics0040162523002123.html.
6. Lartey, P.Y., Akolgo, I.G., Jaladi, S.R., Ayeduvor, S., & Afriyie, S.O. (2023). Recent advances in internal control: Soft control overcoming the limits of hard control. *Frontiers in Management and Business*, 4(1), 289-302. https://www.syncsci.com/journal/FMB/article/view/FMB.2023.01.004.
7. Hasan, A.R. (2021). Artificial Intelligence (AI) in accounting & auditing: A Literature review. *Open Journal of Business and Management*, 10(1), 440-465. https://www.scirp.org/journal/paperinformation?paperid=115007.
8. Ashtiani, M.N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. *Ieee Access*, 10, 72504-72525. https://www.researchgate.net/publication/363364663_Intelligent_Fraud_Detection_in_Financial_Statements_Using_Machine_Learning_and_Data_Mining_A_Systematic_Literature_Review.
9. Lakhan, A., Mohammed, M.A., Ibrahim, D.A., Kadry, S., & Abdulkareem, K.H. (2022). ITS based on deep graph convolutional fraud detection network blockchain-enabled fogcloud. *IEEE Transactions on Intelligent Transportation Systems*. https://www.researchgate.net/publication/358650154_ITS_Based_on_Deep_Graph_Convolutional_Fraud_Detection_Network_Blockchain-Enabled_Fog-Cloud .
10. 2024 Anti-fraud technology benchmarking report. https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/third-party-whitepapers/en/acfe-anti-fraud-technology-benchmark-report-113778.pdf?utm_source=linkedin&utm_medium=social-cpc&utm_campaign=public-sector-us-fsi-gen-americas&utm_content=pt-US_lead-gen-form.