INDEX COPERNICUS INTERNATIONAL

№68
MAY, 2026

ISSN 2710-3056

The issue of journal contains:

Proceedings of the XI Correspondence International Scientific and Practical Conference

GLOBALIZATION OF SCIENTIFIC KNOWLEDGE: INTERNATIONAL COOPERATION AND INTEGRATION OF SCIENCES

held on May 15th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

GRAIL OF SCIENCE
PERIODICAL SCIENTIFIC JOURNAL

ISSN 2710–3056

INTERNATIONAL SCIENTIFIC JOURNAL

GRAIL OF SCIENCE

№ 68 (May 2026)

with the proceedings of the:

XI Correspondence International Scientific and Practical Conference

GLOBALIZATION OF SCIENTIFIC KNOWLEDGE: INTERNATIONAL COOPERATION AND INTEGRATION OF SCIENCES

held on May 15th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

МІЖНАРОДНИЙ НАУКОВИЙ ЖУРНАЛ

ГРААЛЬ НАУКИ

№ 68 (травень, 2026)

за матеріалами:

XI Міжнародної науково-практичної конференції

GLOBALIZATION OF SCIENTIFIC KNOWLEDGE: INTERNATIONAL COOPERATION AND INTEGRATION OF SCIENCES

що проводилася 15.05.2026

ГО «Європейська наукова платформа» (Вінниця, Україна)
ТОВ «International Centre Corporative Management» (Відень, Австрія)

Вінниця – Відень, 2026

DOI 10.36074/grail-of-science.15.05.2026

ГРААЛЬ НАУКИ : міжнар. наук. журнал. – Вінниця : ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2026. – No 68. – 1378 с.

Видання розраховане на науковців, викладачів, аспірантів, студентів, усіх, хто прагне отримати ґрунтовні знання теоретичного і прикладного характеру.

Рекомендовано до видання Вченою Радою Наукової установи «Інститут науково-технічної інтеграції та співпраці». Протокол № 17 від 14.05.2026.

Верстальник: *Дудник Григорій (Україна).* ***Дизайнер:*** *Казьміна Надія (Україна).* ***Коректор:*** *Дудник Григорій (Україна).*

«Грааль науки» є офіційно зареєстрованим мультидисциплінарним науковим виданням з міжнародною сферою поширення, що підтримує політику відкритого доступу. **Ідентифікатор медіа R30-02704** (рішення № 430 від 22.02.2024 Національної Ради України з питань телебачення і радіомовлення).

Наказом МОН України № 582 від 24.04.2024 виданню «Грааль науки» присвоєно Категорію Б фахових видань України з питань економіки (051 «Економіка»).

«Грааль науки» індексується в міжнародних реферативних та наукометричних базах даних:
Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

Конференція зареєстрована УкрІНТЕІ (Посвідчення № 84 від 26.01.2026) та сертифікована Euro Science Certification Group (Сертифікат № 23287 від 11.03.2026).

За точність викладених фактів та правильність цитування відповідальність несе автор.

DOI 10.36074/grail-of-science.15.05.2026

GRAIL OF SCIENCE : inter. scientific journal. – Vinnytsia : NGO «European Scientific Platform»; SI «Institute of Scientific and Technical Integration and Cooperation», 2026. – No 68. – 1378 p.

The publication is intended for scientists, teachers, graduate students, students, all those who seek to obtain thorough knowledge of a theoretical and applied nature.

Recommended for publication by the Academic Council of the Institute of Scientific and Technical Integration and Cooperation. Protocol № 17 from May 14, 2026.

Responsible for e-layout: *Hryhorii Dudnyk (Ukraine).* ***Designer:*** *Nadiia Kazmina (Ukraine).* ***Proofreader:*** *Hryhorii Dudnyk (Ukraine).*

The journal «Grail of Science» is an officially registered in Ukraine multidisciplinary and internationally disseminated scientific edition that supports the policy of open access for scientific publications. **Media identifier R30-02704** (decision № 430 dated 22.02.2024 of the National Council of Ukraine on Television and Radio Broadcasting).

By order of the Ministry of Education and Culture of Ukraine № 582 of April 24, 2024, the journal «Grail of Science» was assigned Category B of specialized publications of Ukraine on economics (051 «Economics»).

The journal «Grail of Science» is indexed in international reference and scientometric databases:
Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

The conference is approved by UKRISTEI (Certificate № 84 dated January 26th, 2026) and certified by Euro Science Certification Group (Certificate № 23287 dated March 11th, 2026).

The author is responsible for the accuracy of the facts presented and the correctness of citations.

РОЗДІЛ IV.
ЦИФРОВА ЕКОНОМІКА, МАТЕМАТИЧНІ І ІНСТРУМЕНТАЛЬНІ МЕТОДИ ЕКОНОМІКИ (Категорія Б)

ЦИФРОВІ ТЕХНОЛОГІЇ ЯК ФАКТОР РОЗВИТКУ ІНТЕЛЕКТУАЛЬНОГО КАПІТАЛУ ПІДПРИЄМСТВА
Сімавін П.Ю. 471

ЕВОЛЮЦІЯ ТВОРЧОГО РУЙНУВАННЯ: ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА СТРУКТУРУ ЗАЙНЯТОСТІ В ГРУЗІЇ
Ванішвілі М., Lapachi A. 475

АВТОМАТИЗАЦІЯ РОЗРАХУНКУ ПОПИТУ, ПРОПОЗИЦІЇ ТА РИНКОВОЇ РІВНОВАГИ У СЕРЕДОВИЩІ MS EXCEL VBA
Ліснічук А.Є., Яворська А.В. 482

АДАПТИВНІ МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ ОПК УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ
Гусак А.Л. 489

АНАЛІЗ ФАКТОРІВ ЦІНОУТВОРЕННЯ НА УКРАЇНСЬКОМУ РИНКУ ЕЛЕКТРОМОБІЛІВ
Андрусик Є.В. 498

ВПЛИВ ДЕЗАГРЕГУВАННЯ МІЖГАЛУЗЕВОЇ МОДЕЛІ ЛЕОНТЬЄВА НА ЇЇ ЗУМОВЛЕНІСТЬ ТА ЧИСЛОВУ СТІЙКІСТЬ
Лупаренко О.В., Графов В.В. 505

ВПЛИВ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ НА ЕКОНОМІЧНУ ЕФЕКТИВНІСТЬ ЕНЕРГЕТИЧНИХ СИСТЕМ
Царева О.С. 516

ІДЕНТИФІКАЦІЯ ТА КЛАСИФІКАЦІЯ ФАКТОРІВ ВПЛИВУ НА РОЗВИТОК БРЕНДУ ПІДПРИЄМСТВА В УМОВАХ ЄВРОІНТЕГРАЦІЇ
Процайло І.Р. 521

ІНСТИТУЦІЙНА ПАСТКА ВИЖИВАННЯ В ТРАНЗИТИВНІЙ ЕКОНОМІЦІ: НЕЛІНІЙНЕ МОДЕЛЮВАННЯ ВПЛИВУ СОЦІАЛЬНОЇ ЗГУРТОВАНОСТІ
Слукін Г.І. 531

КОНЦЕПТУАЛІЗАЦІЯ ОПТИМІЗАЦІЇ КЛІЄНТСЬКИХ ВЗАЄМОВІДНОСИН В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ
Турчин В.В. 542

ЛЮДИНОЦЕНТРИЧНИЙ ПІДХІД ДО РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ БУХГАЛТЕРСЬКОГО ОБЛІКУ
Височан О.С., Ясінська А.І. 551

МЕТОДИКА ВИЯВЛЕННЯ ОЗНАК ФАЛЬСИФІКАЦІЇ ОБЛІКОВИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ (НА ПРИКЛАДІ СИСТЕМ ТИПУ 1С/BAS, SAP)
Гавриленко Н.В., Алєксєєва Г.М. 558

DOI 10.36074/grail-of-science.15.05.2026.059

МЕТОДИКА ВИЯВЛЕННЯ ОЗНАК ФАЛЬСИФІКАЦІЇ ОБЛІКОВИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ (НА ПРИКЛАДІ СИСТЕМ ТИПУ 1С/BAS, SAP)

Гавриленко Наталія Вікторівна
канд. екон. наук, доцент, доцент кафедри обліку та оподаткування
Первомайського навчально-наукового інституту
Національний університет кораблебудування імені адмірала Макарова, Україна
Алєксєєва Ганна Миколаївна
доцент кафедри комп'ютерних технологій та інформатики
Факультету фізико-математичної, комп'ютерної та технологічної освіти
Бердянський державний педагогічний університет, Україна

Анотація. *У статті розглянуто методичні підходи до ідентифікації маніпуляцій з обліковими даними в сучасних ERP-системах. Автором систематизовано ознаки фальсифікацій та запропоновано алгоритм їх виявлення через аналіз логів, журналів реєстрації та нетипових кореспонденцій рахунків.*

Ключові слова: *бухгалтерський облік, судово-бухгалтерська експертиза, фальсифікація даних, інформаційні системи, SAP, 1С/BAS, форензік, IT-аудит.*

Постановка проблеми. В умовах трансформації цифрової економіки, корпоративні інформаційні системи (КІС) перестали бути просто інструментами фіксації господарських операцій. Вони перетворилися на складні екосистеми, де фальсифікація облікових даних може відбуватися не лише на рівні первинної документації, а й через маніпуляції з алгоритмами обробки інформації. На відміну від традиційного паперового шахрайства, цифрова фальсифікація залишає специфічні «інформаційні відбитки», аналіз яких потребує поєднання знань з бухгалтерського обліку, криміналістики та системного адміністрування.

Аналіз останніх досліджень. Проблематика виявлення маніпуляцій у цифровому обліку ґрунтується на класичних роботах Д. Кресі, який сформував концептуальну модель «Трикутника шахрайства»[1], що сьогодні адаптується до ERP-середовищ. Вагомий внесок у розвиток методології судово-бухгалтерської експертизи в Україні внесли такі вчені, як І. Волкова[2] та Л. Гуцаленко[3], які досліджували інструменти внутрішнього аудиту та верифікації фінансових показників. Технологічні аспекти контролю в інтегрованих системах типу SAP та 1С аналізуються у працях О. Шипунова[4], який фокусується на автоматизації аудиторських процедур. Застосування математичних методів, зокрема закону

Бенфорда, для детекції аномалій у масивах даних досліджено у роботах західного фахівця Н. Хорунжак[5]. Водночас розробка уніфікованих алгоритмів детекції фальсифікацій саме через системні логи KIC потребує подальшого поглиблення, що і визначає мету цієї статті.

Мета роботи полягає в обґрунтуванні та розробці комплексної методики виявлення ознак маніпуляцій з обліковими даними в ERP-системах (SAP, 1С/BAS) шляхом інтеграції інструментів технічного IT-аудиту та аналітичних процедур форензіку. Дослідження спрямоване на створення алгоритму ідентифікації прихованих втручань у цифрові реєстри для забезпечення достовірності фінансової звітності та посилення системи внутрішнього контролю підприємства.

Виклад основного матеріалу. Одним із найбільш ефективних методів виявлення прихованих маніпуляцій є аналіз часових лагів між фізичним здійсненням операції та її відображенням у системі. В таблиці 1 наведено матрицю технічних маркерів фальсифікації.

Таблиця 1

Матриця технічних маркерів фальсифікації

Технічний маркер	Сутність аномалії	Спосіб верифікації в SAP	Спосіб верифікації в BAS
Темпоральний розрив	Невідповідність дати системної реєстрації (System Date) даті документа (Document Date).	Транзакція AUT10 (аналіз історії змін об'єктів).	Звіт «Журнал реєстрації» з фільтром за часом події.
Логічна суперечність	Проведення видатків за відсутності вхідних залишків (від'ємні залишки).	Перевірка таблиць MARD та MSEG на наявність ретроспективних проводок.	Аналіз регістра накопичення «Товари на складах» (контроль від'ємних залишків).
Користувацька колізія	Виконання взаємовиключних функцій одним логіном (SoD конфлікт).	Аналіз профілів ролей через SUIM та GRC Access Control.	Перевірка налаштувань RLS (Row Level Security) та прав доступу в Конфігураторі.

Джерело: *авторська розробка*

Теоретичний фундамент виявлення фальсифікацій в автоматизованих системах обліку (ERP-системах) базується на конвергенції класичної теорії бухгалтерського обліку та сучасних концепцій кібербезпеки. В основі дослідження лежить парадигма «цифрового сліду» (digital footprint), згідно з якою будь-яка навмисна маніпуляція даними в системах типу SAP або 1С/BAS неминуче створює аномалії в системних логах, метаданих або кореспондуючих реєстрах.

Ключовим теоретичним конструктом у даному контексті є модернізована модель «Трикутника шахрайства» (Fraud Triangle). У цифровому середовищі KIC її компоненти набувають специфічного змісту:

1. Можливість (Opportunity) визначається архітектурними недоліками системи - надлишковими правами доступу або відсутністю жорсткого розділення повноважень (SoD - Segregation of Duties).

2. Тиск (Pressure) та Виправдання (Rationalization) залишаються психологічними чинниками, проте їх реалізація переходить у площину технічних

транзакцій.

Важливим теоретичним аспектом є принцип цілісності та незмінності ретроспективних даних. В ідеально налаштованій системі (особливо в SAP з її суворою логікою періодів) зміна даних минулих періодів має бути технічно неможливою без створення сторнуючих записів. Отже, теорія виявлення фальсифікацій базується на ідентифікації спроб обходу цих системних обмежень через «технологічні лазівки» (наприклад, пряме редагування таблиць бази даних на рівні СУБД).

Методологія дослідження також спирається на теорію інформаційної ентропії. Фальсифіковані дані зазвичай мають нижчий рівень хаотичності, ніж реальні господарські операції. Це пояснюється людським фактором: зловмисники схильні використовувати «круглі» числа або повторювані патерни, що суперечить природному статистичному розподілу (закон Бенфорда). Таким чином, математичне обґрунтування методики полягає у виявленні статистично значущих відхилень цифрових масивів від очікуваного нормального розподілу.

Окреме місце в теорії займає концепція «безперервного аудиту» (Continuous Auditing). На відміну від традиційного підходу, де перевірка проводиться постфактум, методика виявлення ознак фальсифікації в ERP-системах передбачає впровадження превентивних алгоритмів, що працюють у режимі реального часу. Це трансформує роль облікової системи з пасивного сховища даних у активний інструмент детекції ризиків.

Для побудови ефективної методики виявлення фальсифікацій необхідно враховувати фундаментальні відмінності в архітектурі збереження даних та логування подій у досліджуваних системах. Хоча обидва типи систем спрямовані на автоматизацію обліку, механізми фіксації «цифрових слідів» у них суттєво різняться.

Система SAP (зокрема S/4HANA) базується на принципі суворої транзакційності та незмінності фінансових документів. Основним об'єктом аналізу для виявлення ознак фальсифікації є заголовки та позиції документів, що зберігаються у системних таблицях. Таблиця BKPF (Accounting Document Header): містить критичні метадані: USNAM (ім'я користувача), CPUDT (дата введення), CPUTM (час введення) та TCODE (код транзакції). Аномальна різниця між датою документа (BLDAT) та системною датою введення (CPUDT) є першим індикатором «backdating» (проведення документів заднім числом).

Таблиця BSEG (Accounting Document Segment): дозволяє виявити нетипові кореспонденції рахунків. Особлива увага приділяється типу документа (BLART). Наприклад, масова поява типу SA (G/L account document) у модулях, де мали б бути автоматичні проводки (MM або SD), свідчить про ручне втручання в обхід стандартних бізнес-процесів.

Журнали змін (Change Documents): SAP фіксує зміни в основних даних (Vendor/Customer Master Data) у таблицях CDHDR та CDPOS. Виявлення частих змін банківських реквізитів безпосередньо перед платежем є класичною ознакою зовнішнього або внутрішнього шахрайства.

Особливості пошуку аномалій у системах типу 1С/BAS наступні. На відміну від SAP, системи лінійки 1С/BAS мають більш гнучку архітектуру, що за відсутності жорстких адміністративних налаштувань підвищує ризики несанкціонованого

коригування даних. Журнал реєстрації (Event Log) є основним джерелом доказів. Він фіксує не лише створення об’єктів, а й їх модифікацію, проведення та скасування проведення. Ознакою фальсифікації тут є подія «Зміна» для документів минулих періодів або події від імені користувачів з правами «Повний доступ» у неробочий час.

Фальсифікація в 1С часто відбувається через ручне коригування регістрів (документ «Операція»). Оскільки бухгалтерська звітність у BAS часто будується на даних регістрів, а не лише бухгалтерських проводок, виникнення розбіжностей між ОСВ (оборотно-сальдовою відомістю) та звітами по регістрах (наприклад, «Відомість по товарах») є прямою ознакою приховування недостач або маніпуляцій з собівартістю.

Механізм версіонування об'єктів полягає в наступному: якщо в системі активована «Підсистема версіонування», аудитор має можливість порівняти різні стани одного документа. Видалення проміжних версій або їх різка зміна перед закриттям місяця є вагомим «червоним прапорцем».

Таблиця 2

Технічні об'єкти контролю для детекції фальсифікацій

Параметр аналізу	Об'єкт у SAP	Об'єкт у 1С/BAS
Реєстрація користувача	Поле USNAM (табл. BKPF)	Поле Користувач (Журнал реєстрації)
Історія змін реквізитів	Таблиці CDHDR / CDPOS	Версіонування об'єктів (довідник Версії об’єктів)
Ручні коригування	Тип документа SA, AB	Документ Операція (бухгалтерський облік)
Контроль видалення	Нумерація об'єктів (NRIV)	Аналіз подій Видалення у Журналі реєстрації

Ідентифікація технічних об’єктів контролю, систематизованих у Таблиці 2, є необхідною, проте недостатньою умовою для формування остаточного висновку про наявність фальсифікацій. Отримані дані з таблиць BKPF у SAP або Журналу реєстрації в 1С/BAS потребують подальшої інтерпретації крізь призму загальних налаштувань безпеки системи.

Виявлені аномалії в реєстрах можуть бути як результатом цілеспрямованого шахрайства, так і наслідком недосконалого адміністрування. Відтак, методика передбачає оцінку рівня довіри до облікових даних на основі аналізу конфігурації середовища інформаційної системи. Якщо технічні параметри системи дозволяють безперешкодне редагування журналів або використання надлишкових прав доступу, імовірність успішного приховування фальсифікації зростає експоненціально.

Для систематизації цих чинників та визначення ступеня вразливості облікових контурів розроблено матрицю рівнів довіри (Таблиця 3). Вона дозволяє аудитору або фахівцю з форензіку класифікувати виявлені технічні ознаки за ступенем їх критичності для достовірності фінансової звітності. Таким чином, перехід від простої фіксації «цифрових слідів» до оцінки системних ризиків дозволяє локалізувати найбільш вразливі ділянки обліку, де ймовірність маніпуляцій є найвищою.

Таблиця 3

Порівняння рівнів довіри до даних залежно від налаштувань системи

Рівень ризику	Ознаки в SAP	Ознаки в 1C/BAS
Високий	Наявність користувачів з профілем SAP_ALL у продуктивній системі	Відключений журнал реєстрації або доступ до бази через SQL-менеджер
Середній	Вимкнено логування таблиць змін (параметр rec/client)	Відсутність налаштованих прав «Тільки читання» для закритих періодів
Низький	Активовано Audit Logging та GRC модулі	Використання дати заборони редагування та версіонування

Зміст таблиці 3 розкриває зв'язок між технічними налаштуваннями системи та ступенем верифікованості облікових даних. Воно базується на оцінці «рівня залишкового ризику»: чим більше в системі залишається можливостей для неконтрольованого втручання, тим нижчою є доказова сила отриманих з неї звітів.

Тобто наведені в таблиці 3 дані дослідження обгрунтовують:

1. Критичність прав доступу: високий рівень ризику корелює з наявністю «суперкористувачів» (SAP_ALL в SAP або Повний доступ в 1С). Якщо адміністратор має право одночасно редагувати і операції, і лог-файли, технічне виявлення фальсифікації стає майже неможливим, оскільки зловмисник може видалити власні «цифрові сліди».

2. Цілісність логування: середній рівень ризику зазвичай пов'язаний із «вибірковим» контролем - коли система фіксує створення документів, але не відстежує зміну їхніх реквізитів або ручне коригування проводок. Це створює ілюзію безпеки, якою користуються для приховування маніпуляцій з датами (backdating).

3. Превентивні механізми: низький рівень ризику (висока довіра) досягається лише тоді, коли система технічно обмежує людський фактор. Використання жорстких періодів закриття (Posting Periods) та автоматизованих модулів GRC (Governance, Risk, and Compliance) перетворює ІС на саморегульоване середовище, де будь-яке відхилення від регламенту автоматично генерує «червоний прапорець» (Red Flag).

На основі проведеного аналізу технічних параметрів та ризиків, пропонується уніфікований алгоритм дій для внутрішніх аудиторів та форензік-фахівців. Він складається з п'яти послідовних етапів, що дозволяють перейти від масивів «сирих» даних до обґрунтованих висновків.

Етап 1. Оцінка середовища та вивантаження даних (Extraction). Першочерговим завданням є визначення рівня довіри до системи (згідно з даними, наведеними в таблиці 3). Після цього проводиться експорт даних. Для SAP - це вивантаження з таблиць BSEG/BKPF, для 1С/BAS - вивантаження Журналу реєстрації та Регістрів бухгалтерського обліку у форматі .xlsx або .csv для подальшої обробки.

Етап 2. Статистичне сканування (Data Profiling). Застосування автоматизованих тестів на предмет виявлення «круглих» сум, аномальних піків активності в неробочий час та перевірка масиву на відповідність закону Бенфорда. На цьому етапі відсікається основна маса коректних операцій та

виокремлюються потенційно ризикові транзакції.

Етап 3. Транзакційний крос-аналіз (Cross-Checking). Зіставлення даних з різних модулів. Наприклад, порівняння дати відвантаження товару зі складу (модуль MM/Склад) із датою визнання доходу (модуль FI/Бухгалтерія). Будь-який розрив у часі понад встановлений регламентом ліміт розглядається як ознака маніпуляції фінансовим результатом.

Етап 4. Верифікація «цифрових слідів» (Technical Audit). Для відібраних підозрілих операцій проводиться детальний перегляд історії змін. Перевіряється, чи не було спроб видалення логів або нетипових змін реквізитів контрагентів безпосередньо перед проведенням транзакції.

Етап 5. Формування доказової бази. Зіставлення системних даних із первинними документами (скан-копіями або паперовими оригіналами). Результатом є формування звіту про виявлені невідповідності.

Для узагальнення методичного підходу розроблено фінальну матрицю верифікації.

Таблиця 4

Матриця верифікації ознак фальсифікації за методологією контрольних точок

Контрольна точка	Метод детекції	Програмний індикатор (Trigger)
Цілісність періоду	Порівняння дат	CPUDT > BLDAT (SAP) або різниця між часом запису та часом документа > 24 год (BAS)
Авторизація	Аналіз SoD	Один UserID у транзакціях створення контрагента та створення платежу
Обґрунтованість	Аналіз коментарів	Наявність у полі «Призначення/Текст» слів: «коригування», «виправлення помилки», «згідно з розпорядженням»
Логічна повнота	Кількісний контроль	Невідповідність ваги товару в ТТН та обсягу в системі (аналіз через Excel-VLOOKUP)

Висновки. Використання специфічних інструментів SAP (системні таблиці) та 1С/BAS (журнали реєстрації та версіонування) у поєднанні зі статистичними методами аналізу забезпечує високу точність детекції навіть прихованих маніпуляцій. Впровадження запропонованого алгоритму на підприємствах сприятиме підвищенню прозорості облікових процесів та мінімізації ризиків корпоративного шахрайства.

Список використаних джерел:

[1] Sutherland, E. H. (1945). Is "white collar crime" crime? *American Sociological Review*, *10*(2), 132–139. washington.edu

[2] Hutsalenko, L. V. et al. (2011). *Sudovo-bukhhalterska ekspertyza* [Forensic accounting examination] (Manual). Tsentr uchbovoi literatury.

[3] Volkova, I. A. (2009). *Sudovo-bukhhalterska ekspertyza* [Forensic accounting examination] (Manual). Tsentr uchbovoi literatury.

[4] Shipunova, O. V. (2019). *Perspektyvy zastosuvannia ERP-system v Ukraini* [Prospects for the use of ERP systems in Ukraine] (Thesis). http://essuir.sumdu.edu.ua/handle/123456789/63172.

[5] Khorunzhak, N., & Koshy nets, M. (2026). Intehrovana systema obliku, kontroliu y analizu: strukturna kontseptualizatsiia ta lohika pobudovy [Integrated system of accounting, control and analysis: Structural conceptualization and logic of construction]. *Visnyk Ekonomiky*, (1), 148–156.

https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1939.
[6] Nestorenko, T., Ostenda, A. (2019). Public Internal Audit: International Scope. Journal of Modern Economic Research, 1(4), 33-43. Retrieved from https://lnk.ua/fw3qjPGWY /.
[7] Lemish K., Nestorenko T., Tokarenko O. Interaction of business and education in hospitality, restaurant, and catering business in Ukraine. Journal of Modern Economic Research. 2021. Vol. 3, № 4, 5-20. https://cutt.ly/nKeRkJh.
[8] Havrylenko, Yevgen, Cortez, Jose I., Kholodniak, Yuliia, Alieksieieva, Hanna, Garcia, Gregorio T. "Modelling of Surfaces of Engineering Products on the Basis of Array of Points." Tehnicki Vjesnik, vol. 27, no. 6, 2020, pp. 2034-2043. DOI: 10.17559/TV-20190720081227. ISSN: 13303651.
[9] Разнатовська О. М., О. А. Мурзіна, О. І. Потоцька, Г. М. Алексєєва Актуальність впровадження в освітній процес студентів-медиків інтерактивних методів навчання. Медична освіта. - 2018. - № 4. - С. 85-88. DOI https://doi.org/10.11603/me.2414-5998.2018.4.8726/.
[10] Алєксєєва Г.М, Бабич П.М. Використання платформи ARDUINO для професійної підготовки майбутніх інженерів-педагогів: [Електронний ресурс]. Фізико-математична освіта : науковий журнал. Вип. 4 (14) / Сумський державний педагогічний університет імені А.С. Макаренка, Фізико-математичний факультет редкол.: О.В. Семеніхіна (гол.ред.) [та ін.]. – Суми : [СумДПУ ім. А.С. Макаренка], 2018. – С. 12-17. DOI https://doi.org/10.31110/2413-1571-2018-018-4-002.
[11] Гавриленко, Н. В. (2026). Застосування штучного інтелекту в обліку та
[12] оптимізації бізнес-процесів. https://eir.nuos.edu.ua/handle/123456789/12631.
[13] Гавриленко, Н. В. (2024). Methodological features of researching objects of forensic accounting expertise in budgetary institutions. URI: https://eir.nuos.edu.ua/handle/123456789/9401.
[14] Гавриленко, Н. В. (2024). Розвиток документальних методів судово- бухгалтерської експертизи. URI: https://eir.nuos.edu.ua/handle/123456789/9615.

METHODOLOGY FOR DETECTING SIGNS OF ACCOUNTING DATA FALSIFICATION IN INFORMATION SYSTEMS (CASE STUDY OF 1C/BAS AND SAP SYSTEMS)

Nataliia Havrylenko
PhD in Economics, Associate Professor, Associate Professor of the Department of Accounting and Taxation of the Pervomaisk Educational and Scientific Institute
Admiral Makarov National University of Shipbuilding, Ukraine
ORCID ID: 0000-0002-2043-3917
Hanna Alieksieieva
Associate Professor of the Department of Computer Technologies and Informatics
Faculty of Physics, Mathematics, Computer and Technological Education
Berdiansk State Pedagogical University, Ukraine
ORCID ID: 0000-0003-3204-3139

Summary. *The article explores methodological approaches to identifying manipulations of accounting data within modern ERP systems. The author systematizes the indicators of data falsification and proposes a structured detection algorithm based on the analysis of system logs, event records, and atypical account correspondences. The study emphasizes the integration of IT auditing tools and forensic accounting techniques to ensure the integrity of financial reporting in complex information environments.*
Keywords: *accounting, forensic accounting examination, data falsification, information systems, SAP, 1C/BAS, forensics, IT audit.*

Дата публікації: 15.05.2026

Дата першого надходження статті до видання: 02.04.2026
Дата прийняття статті до друку після рецензування: 12.05.2026

