**УДК 657.6**

***Куцик П. О.***
*kutsykpetro@gmail.com, ORCID ID: 0000-0001-5795-9704*
*Researcher ID: G-9204-2019*
*д.е.н., проф., ректор, професор кафедри обліку, контролю, аналізу та оподаткування, Львівський торговельно-економічний університет, м. Львів*

***Воронко Р. М.***
*rvoronko@ukr.net, ORCID ID: 0000-0003-3796-2556*
*Researcher ID: F-8536-2019*
*д.е.н., проф., завідувач кафедри обліку, контролю, аналізу та оподаткування, Львівський торговельно-економічний університет, м. Львів*

***Редченко К. І.***
*redchenko@ukr.net, ORCID ID: 0000-0001-8234-4074*
*Researcher ID: F-3039-2013*
*д.е.н., проф., професор кафедри обліку, контролю, аналізу та оподаткування, Львівський торговельно-економічний університет, м. Львів*

***Герасименко Т. О.***
*gtoa@meta.ua, ORCID ID: 0000-0002-4684-4773*
*Researcher ID: F-8903-2019*
*к.е.н., доц., професор кафедри обліку, контролю, аналізу та оподаткування, Львівський торговельно-економічний університет, м. Львів*

# РОЗВИТОК ВНУТРІШНЬОГО КОНТРОЛЮ В ТОРГІВЛІ: ВІД КЛАСИКИ ДО ЦИФРОВИХ РІШЕНЬ

***Анотація.*** *Стаття присвячена ґрунтовному дослідженню трансформації систем внутрішнього контролю в умовах цифровізації бізнес-процесів, із фокусом на сферу роздрібної торгівлі. У роботі аргументовано доводиться, що традиційні моделі контролю, такі як COSO та стандарти ІІА, виявляються недостатньо гнучкими й оперативними у реагуванні на виклики цифрової епохи, зокрема при обробці великих масивів транзакційних даних. Крім того, сучасні технології дають змогу перейти від фрагментарного контролю до безперервного моніторингу операцій у режимі реального часу. У відповідь на ці виклики автори пропонують концептуальну модель інтеграції потокової аналітики даних, алгоритмів виявлення аномалій і технологій роботизованої автоматизації процесів (RPA) для формування проактивної системи внутрішнього контролю, здатної забезпечити безперервний моніторинг і автоматизоване реагування в реальному часі. Окрему увагу приділено опису механізмів роботи потокової аналітики: від ідентифікації патернів до визначення порушень через статистичні методи, машинне навчання, нейронні мережі (включаючи автоенкодери та рекурентні архітектури) та алгоритми комплексної обробки подій (CEP). Обґрунтовано, що використання RPA суттєво підвищує продуктивність контролю, забезпечуючи автоматизацію типових задач – від збору доказів і звірки даних до блокування транзакцій і створення звітності. Запропонована авторами модель передбачає п'ятирівневу структуру: джерела даних, аналітичне ядро, диспетчеризація подій, реагування ботами та управлінський дашборд. Такий підхід дозволяє в режимі реального часу сканувати події, автоматично реагувати на типові ризики та залучати людину лише в складних або нетипових ситуаціях. Практичні приклади, наведені у статті, засвідчують, що інтеграція потокової аналітики та RPA може стати не лише інструментом виявлення шахрайства, а й дієвим засобом підтримки операційної ефективності в ритейлі. Отримані результати мають прикладне значення як для практиків внутрішнього аудиту, так і для розробників цифрових рішень у сфері контролю та аналітики.*

**Ключові слова:** внутрішній контроль, автоматизація, потокова аналітика даних, виявлення аномалій, роботизована автоматизація процесів (RPA), роздрібна торгівля.

***Kutsyk Petro***
*kutsykpetro@gmail.com, ORCID ID: 0000-0001-5795-9704*
*Researcher ID: G-9204-2019*
*Doctor of Economics, Rector, Professor of the Department of Accounting, Control, Analysis and Taxation, Lviv University of Trade and Economics, Lviv*

***Voronko Roman***
*rvoronko@ukr.net, ORCID ID: 0000-0003-3796-2556*
*Researcher ID: F-8536-2019*
*Doctor of Economics, Professor, Head of the Department of Accounting, Control, Analysis, and Taxation, Lviv University of Trade and Economics, Lviv*

***Redchenko Kostiantyn***
*redchenko@ukr.net, ORCID ID: 0000-0001-8234-4074*
*Researcher ID: F-3039-2013*
*Doctor of Economics, Professor, Professor of the Department of Accounting, Control, Analysis, and Taxation, Lviv University of Trade and Economics, Lviv*

***Gerasymenko Tamara***
*gtoa@meta.ua, ORCID ID: 0000-0002-4684-4773*
*Researcher ID: F-8903-2019*
*Ph.D, Associate Professor, Professor of the Department of Accounting, Control, Analysis and Taxation, Lviv University of Trade and Economics, Lviv*

# THE DEVELOPMENT OF INTERNAL CONTROL IN TRADE: FROM CLASSICAL APPROACHES TO DIGITAL SOLUTIONS

***Abstract.*** *The article is devoted to a thorough study of the transformation of internal control systems in the context of digitalization of business processes, with a focus on the retail sector. The article argues that traditional control models, such as COSO and IIA standards, are not flexible enough and are not efficient enough to respond to the challenges of the digital age, in particular when processing large amounts of transactional data. In addition, modern technologies make it possible to move from fragmented control to continuous monitoring of operations in real time. In response to these challenges, the authors propose a conceptual model for integrating data flow analytics, anomaly detection algorithms, and robotic process automation (RPA) technologies to form a proactive internal control system capable of providing continuous monitoring and automated response in real time. Special attention is paid to the description of the mechanisms of flow analytics: from pattern identification to violation detection using statistical methods, machine learning, neural networks (including autoencoders and recurrent architectures) and complex event processing (CEP) algorithms. It is substantiated that the use of RPA significantly increases control productivity, providing automation of typical tasks - from evidence collection and data reconciliation to transaction blocking and reporting. The model proposed by the authors provides a five-level structure: data sources, analytical core, event dispatching, bot response and management dashboard. This approach allows real-time scanning of events, automatic response to typical risks and involving a human only in complex or atypical situations. Practical examples given in the article demonstrate that the integration of flow analytics and RPA can become not only a tool for fraud detection, but also an effective means of supporting operational efficiency in retail. The results obtained have practical significance for both internal audit practitioners and developers of digital solutions in the field of control and analytics.*

**Keywords:** internal control, automation, streaming data analytics, anomaly detection, robotic process automation (RPA), retail trade.

**JEL Classification:** M21, M41, M42, F14, C81
**DOI: https://doi.org/10.32782/2522-1256-2025-45-05**

**Постановка проблеми.** Великі торговельні компанії, особливо мережеві ритейлери з широким асортиментом товарів та значним обсягом транзакцій, стикаються з численними викликами, пов'язаними з неефективністю традиційних систем внутрішнього контролю при роботі з величезними масивами даних. Аудиторські перевірки фінансової звітності, що проводяться періодично (зазвичай, щороку), також не встигають своєчасно виявляти порушення або шахрайство. Поряд з цим, сучасні технології дають змогу перейти від фрагментарного контролю до безперервного моніторингу операцій у режимі реального часу. Вони дозволяють перетворити внутрішній контроль на проактивний інструмент запобігання ризикам, що виглядає набагато привабливіше, ніж інструмент виявлення проблем, що вже сталися. Розуміння цієї можливості можна простежити через зростання інтересу до впровадження автоматизації та аналітики у системах внутрішнього контролю торговельних компаній. Автоматизовані рішення здатні підвищити ефективність і точність контролю, зменшити вплив людського фактору та прискорити виявлення проблемних ситуацій.

**Аналіз останніх досліджень і публікацій.** Протягом останніх десятиліть панівна ідеологія побудови внутрішнього контролю в комерційних організаціях базувалася на концептуальних основах, закладених COSO Integrated Framework та міжнародними стандартами Інституту внутрішніх аудиторів (IIA). Проте ці структури дедалі частіше демонструють недостатню гнучкість та низьку швидкість реагування в умовах роботи з великими обсягами даних, тобто в умовах, притаманних сучасному цифровому середовищу.

COSO Integrated Framework чітко структурує внутрішній контроль навколо п'яти взаємозв'язаних компонентів: контрольного середовища, оцінки ризиків, контрольних процедур, інформації та комунікації та моніторингу [1]. Разом з тим, ця структура страждає від закріпленої статичності принципів: так, COSO підкреслює, що принципи не змінюються із застосуванням технологій і не адаптує їх під швидкі зміни IT-ландшафту, що знижує актуальність окремих вимог для цифрових процесів [2]. Також COSO Integrated Framework визнає «вроджені обмеження» контролю через помилки, колізію, ймовірність обману, але не пропонує механізмів автоматизації цих аспектів, рівно як не пропонує адекватних інструментів чи засобів для роботи з великими даними у реальному часі [3].

Міжнародні професійні рамки внутрішнього аудиту (IPPF) включають: глобальні стандарти (Global Internal Audit Standards), тематичні вимоги (Topical Requirements) щодо окремих тем, таких як кібербезпека, глобальні настанови (Global Guidance), що містять рекомендації та кращі практики, а також GTAG® (Global Technology Audit Guides) – керівництва з оцінки IT-ризиків і контролів [4]. Недоліками цих стандартів у контексті сучасного бачення бізнес-процесів та використання інформаційних технологій є, по-перше, недостатня інтеграція з операційною діяльністю (стандарти IIA переважно розглядають IT-контроль як окрему дисципліну, а не як невід'ємну частину операційного контролю), а по-друге, високий рівень абстракції (поверхневі формулювання; надто загально викладені принципи, що залишає багато місця для інтерпретацій; відсутність конкретних інструментів або методів), а також брак гнучкості (стандарти оновлюються рідше, ніж змінюються технологічні тренди, тому внутрішні аудитори часто відстають від потреб бізнесу в автоматизованому контролі) [5, 6, 7].

Таким чином, незважаючи на вагомий внесок COSO та стандартів IIA у формування культури внутрішнього контролю, їхні традиційні інструменти дедалі більше вимагають доповнення новітніми технологіями задля забезпечення ефективності та оперативності контролю. До таких новітніх технологій належать аналітика потокових даних (Stream Analytics) і пов'язані з нею алгоритми виявлення аномалій, а також інструменти RPA (Robotic Process Automation), що можуть ефективно використовуватися для моніторингу транзакцій.

**Постановка завдання.** Стрімке зростання кількості транзакцій та асортименту товарів у тих торговельних компаніях, які активно освоюють торгівлю онлайн і розбудовують роздрібні мережі, вимагає вирішення проблем прозорості, достовірності та своєчасності внутрішнього контролю. Водночас традиційні методи (ручний аудит, періодичні перевірки) більше не здатні ефективно виявляти аномальні події або шахрайські операції в реальному часі. У зв'язку з цим зростає інтерес до більш сучасних інструментів, таких як аналітика потокових даних та роботизація

процесів для побудови динамічних і адаптивних систем внутрішнього контролю.

Метою цієї статті є дослідження концепції інтеграції потокової аналітики даних, алгоритмів виявлення аномалій та засобів RPA (роботизованої автоматизації процесів) у систему внутрішнього контролю торговельних компаній. Основний акцент зроблено на роздрібну торгівлю як галузь, що характеризується великим обсягом транзакцій і схильністю до операційних та шахрайських ризиків. Нами розроблено концептуальну модель такої інтеграції, проведено огляд типових алгоритмів виявлення аномалій та проаналізовано їх потенційні переваги для виявлення шахрайства, неефективності чи порушень стандартних процедур.

**Виклад основного матеріалу дослідження.** Внутрішній контроль у торговельних компаніях являє собою сукупність політик, процедур і заходів, запроваджених для забезпечення достовірності фінансової звітності, дотримання нормативних вимог, збереження активів та сприяння ефективності операцій. Для торговельних (особливо роздрібних) компаній найбільш актуальними ділянками внутрішнього контролю є контроль касових операцій, управління запасами, розмежування повноважень персоналу, моніторинг торгових знижок, акцій, повернень товару тощо. Традиційно внутрішній контроль здійснювався через регулярні аудити, вибіркові перевірки транзакцій і ручний аналіз звітів. Проте зі зростанням обсягів даних та швидкості операцій такий підхід вже є недостатнім – між вчиненням помилки чи шахрайської дії та її виявленням часто минає значний час. Це породжує потребу у нових технологічних рішеннях для безперервного контролю в реальному часі. Сучасні технології, зокрема аналітика великих даних та штучний інтелект, відкривають нові можливості для внутрішнього контролю. Так, безперервний моніторинг транзакцій у режимі реального часу стає реальністю завдяки поєднанню потокової (стримінгової) обробки даних та автоматизованих дій. Названі підходи належать до концепції безперервного аудиту (Continuous Auditing), коли контрольні процедури виконуються не періодично, а постійно, паралельно з бізнес-процесами. У внутрішньому аудиті вже зараз спостерігається поступовий перехід до проактивного нагляду: наприклад, впроваджуються інструменти аналізу даних, що дозволяють аудиторам переходити від реактивного контролю до прогнозування ризиків і виявлення аномалій у режимі онлайн.

Потокова аналітика даних – це технологія обробки даних, що надходять безперервним потоком, для отримання аналітичної інформації та виявлення значущих подій у режимі реального часу. На відміну від традиційної пакетної обробки, де дані накопичуються й аналізуються постфактум, потокова аналітика працює з «живими» стрімами подій (транзакцій, кліків, показників датчиків тощо). Спеціалізовані платформи потокової аналітики (наприклад, Apache Kafka Streams, Apache Flink, Azure Stream Analytics тощо) забезпечують моніторинг та аналіз потоків подій у реальному часі і можуть генерувати оповіщення або дії, коли виявляються визначені патерни, тобто повторювані структури, послідовності, які можна ідентифікувати, вивчити, описати і застосувати повторно в різних ситуаціях.

Таким чином, потокова аналітика дозволяє негайно реагувати на аномальні чи важливі події, не чекаючи завершення дня або місяця для підбиття підсумків. У контексті внутрішнього контролю потокова аналітика дає змогу відстежувати потік операцій (продажів, оплат, переміщення товарів) і виявляти відхилення від норми майже миттєво. Наприклад, якщо протягом години в магазині відбулася нетипово велика кількість скасувань чеків або повернень товару, система потокової аналітики може одразу позначити таку ситуацію як аномалію та ініціювати перевірку, оскільки це може свідчити про зловживання касира або про технічний збій. Аномалією у даних називають патерн або окремий випадок, що суттєво відхиляється від очікуваного (нормального) поведінкового патерну для даної системи.

Іншими словами, аномальні транзакції – це такі, що не відповідають визначенню норми, яке формується на основі історичних даних або очікуваної поведінки процесу. Завдання виявлення аномалій (Anomaly Detection) полягає у тому, щоб знайти в потоці даних такі нетипові об’єкти або події. Якщо характеристики чергової транзакції не вписуються в діапазон нормальних значень чи взаємозв’язків, дану транзакцію слід розглядати як потенційно аномальну та підозрілу.

Важливо підкреслити, що аномалія не завжди означає шахрайство або помилку –

це лише індикатор, що подія потребує уваги. У торговельних компаніях до аномалій можуть належати: підозріло великі знижки, нестандартні комбінації товарів у чеку, транзакції в нетиповий час, раптові піки або спади продажів окремих товарів, незвичні маршрути руху товарів на складі тощо.

Алгоритми виявлення аномалій у потокових даних можна умовно поділити на кілька груп, основні з яких розглянуті в [8, 9].

1. ***Методи порогових значень.*** Найпростіший підхід, коли для певних показників встановлюються граничні значення (пороги), перевищення або падіння нижче яких сигналізує про аномалію. Наприклад, поріг максимальної знижки 50%: якщо касир надає знижку вище 50%, це фіксується як порушення. Недолік жорстких порогів – вони не враховують динаміку і контекст. Тому зазвичай застосовуються адаптивні пороги, які автоматично коригуються залежно від часу доби, активності користувачів тощо. Адаптивний пороговий моніторинг більш гнучкий: наприклад, система може збільшити поріг допустимих повернень товару у період сезонних розпродаж, коли зростає загальний потік покупок.

2. ***Статистичні методи.*** Ці методи моделюють розподіл нормальних даних і шукають відхилення від статистичних закономірностей. Використовуються показники розсіювання (стандартне відхилення, квартилі), коридори значень, контрольні карти Шухарта та інші інструменти математичної статистики. Статистичні методи більш гнучкі, ніж фіксовані пороги, оскільки враховують ймовірнісний характер появи аномалій. Наприклад, метод контрольних карт встановлює динамічні границі на основі середнього значення і розсіювання процесу: якщо показник виходить за 3σ межі, це сигнал аномалії. Важливо правильно обрати модель розподілу, щоб метод ефективно працював; інакше можливі хибні спрацьовування або пропуски.

3. ***Методи на основі машинного навчання (інтелектуального аналізу даних).*** Цей напрям є найперспективнішим, адже алгоритми машинного навчання (ML) здатні виявляти складні та неочевидні патерни аномальної активності. Серед них можна виділити підгрупи:

*Кластеризація та відстань*: алгоритми, що групують дані і визначають аномалії як точки, віддалені від усіх кластерів (наприклад, метод найближчих сусідів, локальний фактор віддаленості LOF, мікрокластери в потоках даних).

*Класифікація*: алгоритми, що навчаються розпізнавати «норму» й «аномалію» на основі мічених даних. Зокрема, метод однокласової SVM будує гіперплощину, що відділяє всі нормальні дані від простору можливих аномалій. При появі нового об'єкта, якщо він лежить по інший бік гіперплощини, він розцінюється як аномалія. Перевагою є гнучкість під різні розподіли, але вибір ядра SVM суттєво впливає на результат.

*Деревоподібні методи*: популярний алгоритм Isolation Forest (ліс ізоляцій) та його похідні. Isolation Forest випадковим чином розбиває дані, будуючи багато дерев розподілу; аномальні точки ізолюються (відокремлюються) за меншу кількість розбиттів, ніж нормальні. Цей метод не потребує попереднього масштабування даних і добре працює на високовимірних даних. Для потоків даних розроблено спрощені та прискорені варіанти, такі як Streaming Half-Space Trees (HS-Trees) – надшвидкий однокласовий детектор аномалій, який постійно оновлюється новими даними.

*Глибоке навчання*: нейромережеві моделі (автоенкодери, рекурентні нейромережі, нейронні детектори послідовностей) набули поширення для складних задач. Автоенкодер може навчитися реконструювати нормальні приклади і погано реконструюватиме аномальні – за різницею (помилкою реконструкції) можна сигналізувати про аномалію. Рекурентні нейромережі (LSTM) застосовують для аномалій у часових рядах, прогнозуючи наступне значення і виявляючи значні відхилення від прогнозу. Перевага глибокого навчання – здатність враховувати складні нелінійності та взаємозв'язки; недолік – потреба у великих обчислювальних ресурсах і даних для навчання.

*Комплексні правила та CEP*: окремо варто згадати методи комплексного виявлення подій (Complex Event Processing), які налаштовують логічні правила в потоці подій (наприклад, «якщо протягом 1 хвилини сталося більше 5 трансакцій на суму > X з однієї карти – сигналізувати про можливе шахрайство»). CEP часто використовується разом із машинним навчанням, комбінуючи прості правила з інтелектуальними моделями.

Важливо зазначити, що виявлення аномалій у режимі реального часу стикається

з низкою викликів: обмежені ресурси (процесор, пам'ять) для аналізу безперервного потоку; необхідність обробляти дані за один прохід; поступова зміна поведінки системи (концептуальний дрейф), що вимагає адаптивних алгоритмів. Тому на практиці часто поєднують офлайн-моделі з періодичним перенавчанням та онлайн-алгоритми з швидким оновленням [8]. Наприклад, модель може будуватися на основі історичних даних для досягнення високої точності, а потім коригуватися на ходу новими даними для врахування актуальних змін у процесах.

Тепер розглянемо сутність та застосування роботизованої автоматизації процесів (RPA). Це підхід, в якому спеціальне програмне забезпечення (так звані «програмні роботи» або боти) імітує дії людини в інформаційних системах для виконання рутинних, чітко регламентованих задач. RPA-системи працюють на рівні графічного інтерфейсу користувача (GUI), повторюючи послідовність кліків, введення даних та інших операцій так, як це зробив би працівник вручну. Фактично програмний робот бере на себе операції, які раніше вимагали участі людини, що дозволяє суттєво пришвидшити процеси і знизити кількість помилок. Сучасні платформи RPA (UiPath, Blue Prism, Automation Anywhere тощо) дедалі частіше оснащуються вбудованим штучним інтелектом та машинним навчанням – такий симбіоз називають інтелектуальною автоматизацією (Intelligent Automation) або RPA наступного покоління. Вона дозволяє ботам не лише виконувати запрограмовані дії, але й «навчатися» на даних, приймати прості рішення та працювати з неструктурованою інформацією.

У сфері бухгалтерського обліку та внутрішнього контролю RPA вже зарекомендувала себе як ефективний інструмент для автоматизації масових рутинних завдань. Одним із основних застосувань програмних роботів є обробка великих обсягів фінансових даних, підготовка звітності та виконання повторюваних процедур, що забирають багато часу. Наприклад, бот може щоденно збирати дані з кількох облікових систем і формувати зведений управлінський звіт замість того, щоб кілька бухгалтерів вручну зіставляли цифри в Excel. Інший приклад – звірка рахунків і транзакцій: RPA-бот швидко порівнює тисячі записів між системою замовлень і оплат, знаходить невідповідності та готує список транзакцій, що потребують уваги контролера. Таким чином, RPA усуває «вузькі місця» у бізнес-процесах, підвищує продуктивність персоналу та мінімізує людський фактор.

Дослідження [12] показало, що провідні компанії у сфері торгівлі та ритейлу вже застосовують RPA у найрізноманітніших процесах – від планування попиту і пропозиції до обробки замовлень, звірки даних, управлінської звітності та аналітики продажів. Зокрема, роботи широко використовуються для фінансового контролю: перевірки повноти документів, контролю кредиторської та дебіторської заборгованості, моніторингу відповідності операцій встановленим правилам. RPA-боти швидкі, точні та ніколи не втомлюються; вони технологічно нейтральні, тож можуть працювати поверх різних, у тому числі застарілих, IT-систем без їхньої модернізації. Це особливо важливо для великих роздрібних мереж, де інформаційне середовище часто гетерогенне (кілька різних облікових систем у регіональних підрозділах, старі POS-термінали тощо). Боти здатні зв'язати та зістикувати такі розрізнені системи, виконуючи роль «клею» між ними: наприклад, зчитувати дані з екрану однієї програми і вводити їх в іншу систему по заданому шаблону.

Внутрішній контроль виграє від застосування RPA на кількох рівнях. По-перше, автоматизація гарантує, що контрольні процедури виконуються послідовно та однаково кожного разу, без пропусків і помилок, притаманних людському фактору. По-друге, RPA дозволяє перейти до безперервного контролю. Якщо раніше співробітник вибірково перевіряв документи раз на місяць, то тепер бот може щоденно або щогодини перевіряти всі транзакції на відповідність правилам і одразу повідомляти про виняткові ситуації. Як свідчить досвід аудиту, RPA-технології дають змогу моніторити транзакції у режимі реального часу і відразу виявляти аномалії, на відміну від періодичних вибіркових перевірок [11].

По-третє, використання роботів розширює охоплення контролем: ресурси внутрішнього аудиту завжди обмежені, а автоматизація дозволяє «робити більше з меншими витратами», збільшуючи кількість перевірених операцій і напрямків без пропорційного збільшення штату [13].

Слід також зважати на ризики і виклики впровадження RPA, такі як початкові інвестиції, технічна складність інтеграції ботів

у застарілі системи, питання кібербезпеки та контролю доступу ботів до чутливих даних. Успішне застосування RPA вимагає чіткого планування, залучення як IT, так і фахівців із внутрішнього аудиту, а також розробки нових політик контролю, які враховують присутність «цифрових працівників» у процесах. Проте світовий досвід демонструє, що ці перепони подоланні, і вигоди від автоматизації значно переважають. Для обґрунтування таких переваг ми пропонуємо розроблену нами концептуальну модель інтеграції потокової аналітики і RPA у внутрішньому контролі.

Ця модель описує, як саме потокова аналітика даних може бути інтегрована з роботизованою автоматизацією процесів для створення проактивної системи внутрішнього контролю в торговельній компанії. Модель охоплює декілька взаємопов'язаних рівнів: (1) джерела даних та подій; (2) шар стримінгової обробки і виявлення аномалій; (3) компонент управління подіями та черга завдань; (4) роботизовані процедури реагування; (5) інтерфейс контролю та ухвалення рішень.

***Рівень 1: джерела даних.*** На цьому рівні знаходяться всі системи та сенсори, з яких надходять події для аналізу. Для роздрібної мережі такими джерелами є: транзакції з POS-терміналів (чеки продажу, повернення, скасування), дані систем лояльності (активація купонів, нові учасники програми), операції складського обліку (надходження та відпуск товарів, переміщення між складами), фінансові операції (оплати постачальникам, інкасація тощо), журнали роботи касових апаратів і відеоспостереження, а також зовнішні дані (курси валют, погода, які можуть впливати на продажі). Усі ці різнорідні потоки в режимі реального часу спрямовуються до системи потокової аналітики. Технічно це реалізується через шину даних або стримінгову платформу – наприклад, Kafka збирає повідомлення про кожну транзакцію і ставить у чергу на обробку.

***Рівень 2: потокова аналітика і виявлення аномалій.*** Це ключова частина системи – програмний модуль або набір модулів, що в режимі реального часу аналізують вхідні події за заданими алгоритмами. Тут відбувається застосування описаних вище методів виявлення аномалій. Система підтримує кілька паралельних аналітичних правил та моделей:

*Прості правила виявлення подій (CEP)*: наприклад, відстеження підозрілих серій операцій («N транзакцій із однієї картки за M секунд»).

*Статистичний моніторинг ключових метрик*: моніторинг середньої та дисперсії сум чеків, кількості повернень за годину, швидкості сканування товарів касиром тощо. Якщо метрика виходить за динамічні довірчі інтервали, генерується сигнал.

*ML-моделі для аномалій*: наприклад, класифікатор, який оцінює ймовірність того, що дана транзакція є шахрайською, на основі десятків факторів (час, ID касира, склад кошика, використані купони, історія покупця тощо); або автоенкодер, що аналізує час закриття зміни у магазині і виявляє нестандартні патерни.

*Моделі прогнозування*: наприклад, модель прогнозує, скільки продажів і на яку суму має бути в магазині станом на 12:00 дня на основі ранкової динаміки і порівнянь із аналогічними днями; якщо фактичні продажі сильно відстають чи перевищують прогноз, це може свідчити про проблему (збій системи продажів або аномальний наплив покупців відповідно).

Усі ці компоненти аналізу працюють постійно та формують стрім контрольних подій – повідомлень про виявлені аномалії або тригерні ситуації. Важливо, що система знижує кількість хибних тривог шляхом кореляції подій: наприклад, якщо велика кількість повернень супроводжується одночасним падінням електроживлення в магазині (від датчиків «інтернету речей»), то ці аномалії можуть бути поєднані в один інцидент (наприклад, «збій електрики») замість декількох інцидентів («підозрілі повернення»).

***Рівень 3: управління подіями та черга завдань.*** Тут здійснюється обробка результатів, що надходять із аналітичного модуля. Спеціальний компонент (диспетчер подій) вирішує, як реагувати на кожен тип аномалії. Для гнучкості використано підхід через чергу завдань: кожна зафіксована аномалія перетворюється на завдання з певним пріоритетом і типом. Наприклад, «перевірити дії касира № 3 (10 підозрілих скасувань чеків за годину)» або «розібратися з розбіжністю даних складського обліку між складами А і Б». Завдання ставляться у чергу та направляються на виконання або роботам, або людям – залежно від категорії. На цьому рівні також визначається, чи треба запускати RPA-скрипт, чи спершу спрямувати проблему до менеджера. Напри-

клад, подія «виявлено транзакцію з можливо викраденої кредитної картки» може автоматично ініціювати RPA-дію щодо блокування цієї транзакції і маркування облікового запису клієнта, а паралельно – завдання для співробітника служби безпеки перевірити деталі. Натомість подія «перевищено ліміт знижок касиром» може одразу спрямувати RPA-бота на збір логів по роботі цього касира за зміну та відправку звіту менеджеру магазина для розслідування.

***Рівень 4: роботизовані процедури реагування (RPA).*** На цьому рівні використовуються конкретні RPA-боти, налаштовані виконувати ті чи інші дії внутрішнього контролю. Вони підключені до систем управління чергою: як тільки з'являється нове завдання, що відповідає їхній компетенції, запускається відповідний бот. Кожен бот – це програмний сценарій, який може увійти до необхідних IT-систем (ERP, CRM, банківська система, електронна пошта тощо) і виконати серію дій. Типові приклади RPA-реакцій у внутрішньому контролі торговельної компанії:

*Збір доказів і документів.* Якщо аналітика сигналізує про аномалію, бот може автоматично зібрати всі пов'язані документи і дані: наприклад, знайти та витягти копії товарних чеків, накладних, відео з камери спостереження за відповідний час і помістити їх у окрему папку для перевірки.

*Виправлення помилок.* У разі виявлення розбіжності в даних (наприклад, система обліку показує, що відпущено товар на суму 10'000 грн, а оплата в касі пройшла лише на 9'900 грн), RPA-скрипт може самостійно запустити процедуру сторнування/документування недостачі, оформити службову накладну чи створити резерв на суму різниці, тобто виконати регламентну процедуру, передбачену політиками компанії.

*Блокування та сповіщення.* Бот може оперативно заблокувати користувача або транзакцію до з'ясування обставин. Наприклад, при підозрі на шахрайство з боку співробітника – деактивувати його доступ до систем, доки інцидент не перевірять. Одночасно бот надішле повідомлення відповідальним особам (через e-mail чи повідомлення в корпоративному месенджері) з описом ситуації.

*Перехресний контроль.* Програмний робот може сам виконувати роль контролера: скажімо, щодня о 9:00 ранку бот звіряє залишки товарів між системою складського обліку і POS-системою магазинів. Якщо знайдено невідповідності, бот формує акт розбіжностей. Таким чином, контроль здійснюється щоденно й автоматично, тоді як раніше це робилося раз на місяць вручну.

Використання RPA на даному рівні суттєво розширює можливості реагування. По-перше, реакція стає швидкою (фактично, в реальному часі), оскільки бот починає діяти відразу при надходженні завдання, не чекаючи, поки людина побачить проблему. По-друге, дії виконуються за попередньо затвердженим сценарієм, що гарантує дотримання внутрішніх процедур. По-третє, роботи можуть працювати масштабовано: якщо, припустимо, одночасно виникло 50 аномалій у різних магазинах, система може паралельно зробити 50 запусків бота, аби всі випадки були оброблені без затримки (людині-контролеру таке завдання буде не під силу). Технічно інтеграція реалізується через API або спеціалізовані адаптери. Зокрема, сучасні платформи інтеграції (Oracle Integration Cloud, Microsoft Power Automate) надають вбудовані конектори до RPA-систем.

***Рівень 5: інтерфейс контролю і прийняття рішень.*** Хоча значну частину рутинної роботи беруть на себе штучний інтелект і роботи, остаточні управлінські рішення все одно залишаються за відповідальними особами. Тому модель передбачає зручний інтерфейс (панель моніторингу, дашборд), де відображаються всі виявлені аномалії, статус їхнього опрацювання роботами і потрібні дії від людини. Менеджери чи внутрішній аудитор можуть бачити, які інциденти вже автоматично виправлені, а які потребують їхнього втручання. Система також дозволяє підтверджувати або відхиляти запропоновані автоматикою дії. Наприклад, бот підготував акт списання товару – відповідальна особа переглядає його і електронним підписом затверджує або повертає на доопрацювання. Таким чином забезпечується принцип, що автоматизація допомагає, але не усуває контроль з боку людини: критичні рішення проходять перевірку, а рутинні операції виконуються алгоритмами.

Що стосується взаємодії компонентів моделі, то у нормальному режимі система працює циклічно: джерела генерують події – аналітика їх перевіряє і при виявленні відхилень створює сигнал – диспетчер подій при-

значає завдання – RPA-бот виконує необхідні кроки – результат фіксується і відображається для контролерів. Якщо автоматизованих дій достатньо, інцидент закривається; якщо ні, – він передається на ручний розгляд. Усе це здатне відбуватися в масштабі секунд або хвилин. Модель можна порівняти з імунною системою організму: вона постійно «сканує» операційну діяльність компанії, автоматично нейтралізує типові загрози (порушення) і сигналізує про більш складні проблеми, щоб «лікар» (менеджер чи внутрішній аудитор) втрутився. Запропонована модель має гнучку архітектуру і легко може масштабуватися. Проте для малого бізнесу деякі рівні можуть бути спрощені (наприклад, без використання складних ML-моделей, а лише за правилами і RPA-скриптами для типових задач). Для великої торговельної мережі, навпаки, можна розгорнути повноцінний центр управління даними та контролю, що оброблятиме тисячі подій щосекунди.

**Висновки і перспективи подальших досліджень у даному напрямі.** Компанії роздрібної торгівлі та інші торговельні компанії, які оперують великими обсягами даних, можуть суттєво посилити свій внутрішній контроль шляхом впровадження потокової аналітики даних, алгоритмів виявлення аномалій та роботизованої автоматизації процесів (RPA). Проведене дослідження підтверджує, що така інтеграція переводить контрольні функції на якісно новий рівень – рівень безперервного, проактивного моніторингу з можливістю миттєвої реакції на відхилення. Розроблена нами концептуальна модель демонструє, як елементи системи (джерела даних, аналітичні модулі, диспетчер подій, RPA-боти, інтерфейс) взаємодіють задля автоматичного виявлення й усунення порушень у режимі реального часу. Огляд алгоритмів виявлення аномалій показав, що існує широкий спектр методів (від простих порогів до сучасних нейромереж), придатних для аналізу потокових транзакцій. Грамотне поєднання цих методів дозволяє вловити як тривіальні, так і нестандартні аномалії. RPA довела свою ефективність у виконанні рутинних контрольних операцій без помилок і втоми, особливо у таких задачах як звірка даних, перевірка повноти інформації, дотримання послідовності процедур. Синергія аналітики та RPA проявляється у тому, що система не лише сигналізує про проблему, а й одразу робить перші кроки для її вирішення (збирає документи, виправляє дані, повідомляє відповідальних тощо). Практичні кейси, зокрема досвід мережі магазинів «Фора», підтверджують реальність та результативність таких рішень [10].

Отримані результати можуть слугувати методичною основою для подальших досліджень та розробок у галузі цифрового внутрішнього контролю та аудиту. Перспективними вбачаються дослідження ефективності конкретних алгоритмів виявлення аномалій на реальних наборах даних торговельних компаній, а також питання кібербезпеки в умовах масового використання RPA та елементів штучного інтелекту.

## ЛІТЕРАТУРА

1. Leland A. Fundamentals of the COSO Framework: Building Blocks for Integrated Internal Controls. *Audit Board.* 2024, June 20. URL: https://auditboard.com/blog/coso-framework-fundamentals

2. PwC. Re-inventing Internal Controls in the Digital Age. 2019, April. 34 p. URL: https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904.pdf

3. Bone J. Why COSO's Internal Control FrameworkCan'tGiveYouConfidence.*ResearchGate*. 2022, January. URL: https://www.researchgate.net/publication/358247648_Why_COSO's_Internal_Control_Framework_Can't_Give_You_Confidence DOI: https://doi.org/10.13140/RG.2.2.29562.57280

4. Global Internal Audit Standards. Published January 9, 2024. 120 p. URL: https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf

5. Internal Audit's Digital Transformation Imperative: Advances Amid Crisis. Analysing the Impact of 2020 on Internal Audit Functions' Implementation of Technology. *Internal Audit Foundation and Audit Board.* 2021. 16 p. URL: https://www.theiia.org/globalassets/documents/content/research/foundation/2021-1581-fnd--ias-dig-transf-imperative-report_auditboard_fnl.pdf

6. Chambers R., O'Reilly T. The New IIA Standards Are Raising the Bar for CAEs on Technology Strategies. *Audit Board*. August 1, 2024. URL: https://auditboard.com/blog/the-new-iia-standards-are-raising-the-bar-for-caes-on-technology-strategies/

7. Guttenplan A., Connor Y. The impact of the new Global Internal Audit Standards. *Cohn Reznick*. 04/25/2024. URL: https://www.cohnreznick.com/insights/impact-of-new-global-internal-audit-standards

8. Lu T., Wang L., Zhao X. Review of Anomaly Detection Algorithms for Data Streams. *Applied Sciences.* 2023. № 13 (10). P. 6353. DOI: https://doi.org/10.3390/app13106353

9. Tan S. C., Ting K. M., Liu T. F. Fast Anomaly Detection for Streaming Data. *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence*. 2025. P. 1511–1516. URL: https://www.jcai.org/Proceedings/11/Papers/254.pdf

10. Світельський І. Реальні витрати ручної обробки документів у бізнесі в Україні: аналіз та рішення. *Innora*. 12 May 2025. URL: https://www.innora.com.ua/blog/realni-vitrati-ruchnoyi-obrobki-dokumentiv-u-biznesi-v-ukrayini-analiz-ta-rishennya_1

11. Kush Tapas. The Rise of Robotic Process Automation (RPA) in Auditing. *LinkedIn Pulse*. 2025, April 2. URL: https://www.linkedin.com/pulse/rise-robotic-process-automation-rpa-auditing-ca-kush-tapas-qkpnf

12. Childs K., Abel T. Accelerating RPA Maturity: 3 Ways Consumer Products and Retail Companies Can Step Up Their Game. *Protiviti*. July 19, 2019. URL: https://blog.protiviti.com/2019/07/19/accelerating-rpa-maturity-3-ways-consumer-products-and-retail-companies-can-step-up-their-game/

13. Robotic process automation: A primer for internal audit professionals. *PwC*. 2017. 4 p. URL: https://www.pwc.com/us/en/risk-assurance/publications/assets/pwc-robotics-process-automation-a-primer-for-internal-audit-professionals-october-2017.pdf

## REFERENCES

1. Leland A. Fundamentals of the COSO Framework: Building Blocks for Integrated Internal Controls. *Audit Board*. 2024, June 20, available at: https://auditboard.com/blog/coso-framework-fundamentals

2. PwC. Re-inventing Internal Controls in the Digital Age. 2019, April. 34 p., available at: https://www.pwc.com/sg/en/publications/assets/reinventing-internal-controls-in-the-digital-age-201904.pdf

3. Bone J. Why COSO's Internal Control Framework Can't Give You Confidence. *ResearchGate*. 2022, January., available at: https://www.researchgate.net/publication/358247648_Why_COSO's_Internal_Control_Framework_Can't_Give_You_Confidence. DOI: https://doi.org/10.13140/RG.2.2.29562.57280

4. Global Internal Audit Standards. Published January 9, 2024. 120 p., available at: https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf

5. Internal Audit's Digital Transformation Imperative: Advances Amid Crisis. Analysing the Impact of 2020 on Internal Audit Functions' Implementation of Technology. *Internal Audit Foundation and Audit Board*. 2021. 16 p., available at: https://www.theiia.org/globalassets/documents/content/research/foundation/2021-1581-fnd--ias-dig-transf-imperative-report_auditboard_fnl.pdf

6. Chambers R. and O'Reilly T. The New IIA Standards Are Raising the Bar for CAEs on Technology Strategies. *Audit Board*. August 1, 2024, available at: https://auditboard.com/blog/the-new-iia-standards-are-raising-the-bar-for-caes-on-technology-strategies/

7. Guttenplan A. and Connor Y. The impact of the new Global Internal Audit Standards. *Cohn Reznick*. 04/25/2024, available at: https://www.cohnreznick.com/insights/impact-of-new-global-internal-audit-standards

8. Lu T., Wang L. and Zhao X. (2023). Review of Anomaly Detection Algorithms for Data Streams. *Applied Sciences*, № 13 (10), p. 6353. DOI: https://doi.org/10.3390/app13106353

9. Tan, S. C. Ting, K. M. and Liu, T. F. (2025). Fast Anomaly Detection for Streaming Data. *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence*, p. 1511–1516, available at: https://www.jcai.org/Proceedings/11/Papers/254.pdf

10. Svitelskyi I. Realni vytraty ruchnoi obrobky dokumentiv u biznesi v Ukraini: analiz ta rishennia. *Innora*. 12 May 2025, available at: https://www.innora.com.ua/blog/realni-vitrati-ruchnoyi-obrobki-dokumentiv-u-biznesi-v-ukrayini-analiz-ta-rishennya_1

11. Kush Tapas. The Rise of Robotic Process Automation(RPA)inAuditing.*LinkedInPulse*.2025, April 2, available at: https://www.linkedin.com/pulse/rise-robotic-process-automation-rpa-auditing-ca-kush-tapas-qkpnf

12. Childs K. and Abel T. Accelerating RPA Maturity: 3 Ways Consumer Products and Retail Companies Can Step Up Their Game. *Protiviti*. July 19, 2019, available at: https://blog.protiviti.com/2019/07/19/accelerating-rpa-maturity-3-ways-consumer-products-and-retail-companies-can-step-up-their-game/

13. Robotic process automation: A primer for internal audit professionals. PwC. 2017. 4 p., available at: https://www.pwc.com/us/en/risk-assurance/publications/assets/pwc-robotics-process-automation-a-primer-for-internal-audit-professionals-october-2017.pdf

*Стаття надійшла до редакції*
*14 квітня 2025 р.*