Кафедра аудиту
ФФО ЗУНУ

ЗНУ
60 РОКІВ

ЦИФРОВІ ТЕХНОЛОГІЇ В АУДИТІ

За загальною редакцією
професора Валентини Панасюк

2026

УДК: 657.6:004
П 14

Затверджено
Вченою радою Західноукраїнського національного університету (протокол № 5 від 9 січня 2026 р.)

Рецензенти:
Ю. І. Клюс *– д.е.н., професор, завідувач кафедри обліку і оподаткування, Східноукраїнський національний університет імені Володимира Даля;*
Т. В. Шталь *– д.е.н., професор, проректор з наукової роботи та міжнародного співробітництва, Харківський національний економічний університет імені Семена Кузнеця;*
А. В. Шлапак *– д.е.н., доцент, проректор з науково-педагогічної роботи та інноваційного розвитку, Київський столичний університет імені Бориса Грінченка.*

Цифрові технології в аудиті: е-підручник / за ред. д.е.н., проф. Панасюк В. М. Тернопіль: ЗУНУ, 2026. 753 с.

ISBN 978-966-654-810-1

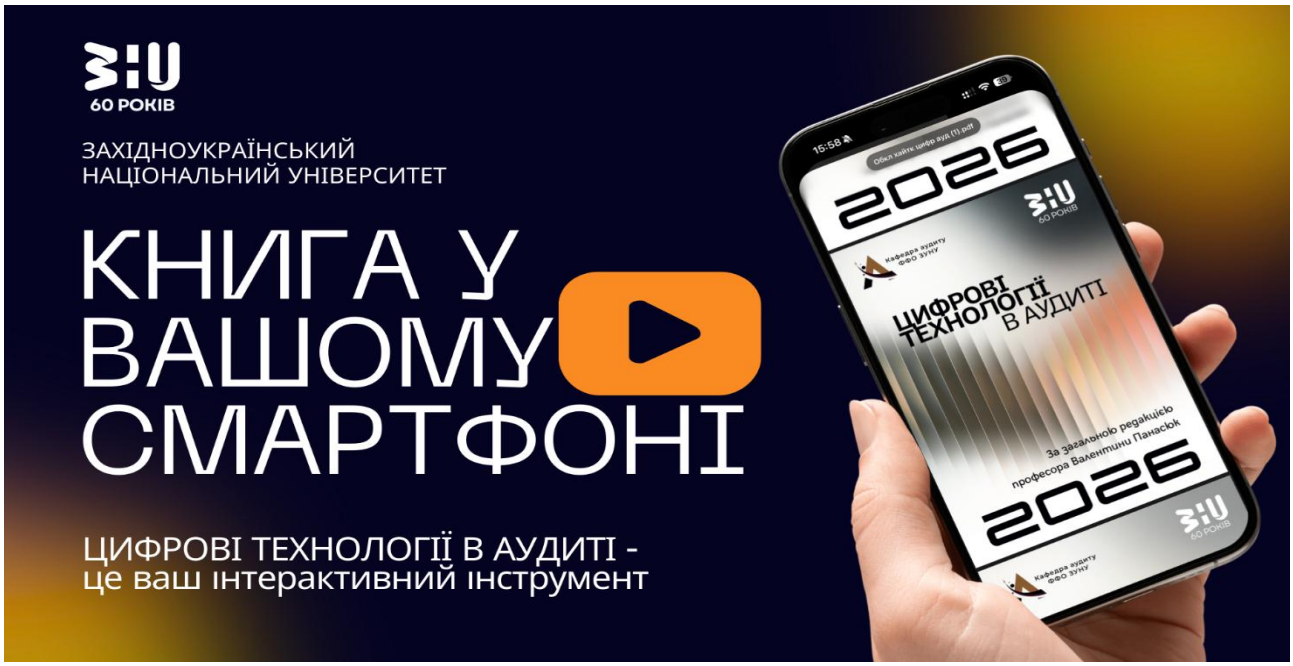
Е-підручник розкриває теоретичні й прикладні засади цифровізації обліку та аудиту і демонструє, як сучасні технології змінюють аудиторські цілі, методи й інструменти в умовах зростання ІТ-ризиків і вимог до фінансової безпеки бізнесу. У виданні системно розкрито цифрову трансформацію бізнес-процесів, моделювання та оптимізацію процесів в обліку й аудиті, нормативно-правове забезпечення цифрового аудиту та організацію аудиторського процесу з урахуванням е-документообігу, хмарних сервісів і онлайн-платформ.

Окрему увагу приділено інформаційним системам підприємства як об’єкту аудиту (ERP, CRM, бухгалтерські системи), внутрішньому контролю в ІТ-середовищі та застосуванню цифрових інструментів аудитора (CAATs, Excel, Google Sheets, спеціалізоване ПЗ). Е-підручник охоплює технології виявлення шахрайства й підозрілих операцій, питання інформаційної та кібербезпеки фінансових даних, роль аудитора в інвестиційному консалтингу, інклюзивний аудит, а також інтеграцію ШІ в аудиторські процедури з урахуванням ризиків та етичних аспектів. Він містить кейси з використанням цифрових даних і відкритих реєстрів для оцінки контрагентів, оптимізації процесів та організації цифрового аудиту; матеріал доповнено питаннями для самоперевірки й тестами підсумкового контролю та глосарієм.

Е-підручник буде корисним для студентів економічних спеціальностей, викладачів, аудиторів, бухгалтерів, фахівців з внутрішнього контролю та фінансової безпеки, фінансових менеджерів і всіх, хто працює або планує працювати в середовищі цифрового аудиту та управління ризиками.

ISBN 978-966-654-810-1

Авторський колектив: *Десятнюк Оксана Миронівна* – доктор економічних наук, професор кафедри фінансів ім. С. І. Юрія, заслужений працівник освіти України (розд. 9, др. арк. – 5,1); *Панасюк Валентина Миколаївна* – доктор економічних наук, професор, завідувач кафедри аудиту, заслужений працівник освіти України (розд. 3, розд. 6, розд. 12, розд. 14, розд. 15, др. арк. – 19,8); *Бродовська Оксана Григорівна* – доктор економічних наук, президент ТОВ «Фінансова компанія «Магнат»», заслужений працівник освіти України (розд. 13, др. арк. – 1,5); *Сохацька Олена Миколаївна* – доктор економічних наук, професор кафедри міжнародних економічних відносин, заслужений економіст України (розд. 11, др. арк. – 2,8); *Буяк Леся Михайлівна* – доктор економічних наук, професор, завідувач кафедри економічної кібернетики та інформатики (розд. 1, розд. 2, др. арк. – 3,0); *Птащенко Олена Валеріївна* – доктор економічних наук, професор кафедри економічної кібернетики та інформатики (розд. 5, розд. 8, др. арк. – 3,8); *Жуковська Аліна Юріївна* – доктор економічних наук, професор кафедри аудиту (розд. 13, др. арк. – 2,0); *Бобрівець Віталій Володимирович* – PhD, доцент кафедри аудиту, голова правління ПрАТ «Тернопільміськгаз» (розд. 4, др. арк. – 1,5); *Коваль Оксана Євгеніївна* – кандидат педагогічних наук, доцент кафедри економічної кібернетики та інформатики, директор Навчально-наукового центру комунікацій (розд. 7, др. арк. – 1,5); *Кулик Роман Романович* – кандидат економічних наук, доцент кафедри аудиту (розд. 11, др. арк. – 1,5); *Черешнюк Оксана Михайлівна* – кандидат економічних наук, доцент кафедри аудиту (розд. 3, розд. 6, др. арк. – 4,5); *Шестерняк Марія Михайлівна* – кандидат економічних наук, доцент кафедри аудиту (розд. 7, др. арк. – 1,5); *Сохацький Олександр Юрійович* – PhD, доцент кафедри міжнародних економічних відносин (розд. 10, др. арк. – 2,3); *Семененко Юрій Сергійович* – PhD, старший викладач кафедри економічної кібернетики та інформатики (розд. 2, др. арк. – 1,5); *Сушко Дмитро Сергійович* – кандидат економічних наук, доцент, аудитор, судовий експерт, керуючий партнер компанії MGI PSP Audit (розд. 4, розд. 5, др. арк. – 1,5); *Шухманн Вадим Александерович* – головний аудитор ТОВ «ФК «Абсолют Фінанс»», аспірант кафедри економічної кібернетики та інформатики (розд. 1, розд. 10, др. арк. – 5,0); *Осійчук Ірина Сергіївна* – головний аудитор ТОВ «Фінансова компанія «Магнат»» (розд. 8, др. арк. – 1,0).



Відео-презентація підручника: https://youtu.be/s9S4--S437A

Комп'ютерна верстка: Вадим Шухманн
Оцифрування матеріалу та дизайн: Вадим Шухманн

КАФЕДРА АУДИТУ ЗУНУ, ТЕРНОПІЛЬ

2026

ЗНУ 60 РОКІВ

Шановна університетська спільното!

Прийміть щирі вітання з нагоди 60-річчя Західноукраїнського національного університету. Це визначна дата, що символізує не лише поважний вік закладу, а й багаторічну працю кількох поколінь викладачів, науковців, студентів і випускників, які спільно формували інтелектуальний потенціал університету та його авторитет в освітньому й науковому просторі України.

Упродовж десятиліть університет утверджує високі стандарти освіти й науки, розвиває дослідницьку культуру, підтримує академічні традиції та готує професійні кадри для різних сфер економіки й суспільного життя. ЗУНУ послідовно поєднує фундаментальність підготовки з практичною орієнтацією. Університет відкритий до міжнародної співпраці та водночас зберігає відповідальність перед громадою і державою. Він упроваджує сучасні освітні підходи та підтримує класичні університетські цінності. Важливо, що університет не лише реагує на зміни, а й бере активну участь у трансформаційних процесах, підтримує ініціативи, спрямовані на інновації, цифровізацію та підвищення якості освітніх програм.

Символічно, що ювілей університету підсилюють нові науково-освітні здобутки, зокрема вихід у світ підручника «Цифрові технології в аудиті». Це видання відображає актуальний запит практики й освіти на сучасні підходи до аудиту в цифровому середовищі. Видання покликане сприяти формуванню компетентностей, необхідних для професійної діяльності в умовах технологічних змін, а також зміцнювати зв'язок між університетською підготовкою і реальними потребами ринку.

Переконані, що саме такі освітні й наукові результати, які мають практичну цінність, методологічну вивіреність і орієнтацію на майбутнє, посилюють позиції університету, підвищують його конкурентоспроможність і формують стійку довіру до університетської школи. Нехай кожне нове покоління студентів отримує не лише знання, а й культуру відповідальності, професійної етики та прагнення до розвитку.

Бажаємо Західноукраїнському національному університету подальшого поступу й процвітання, успішної реалізації стратегічних ініціатив, зміцнення наукових шкіл, розширення партнерств і міжнародних проєктів, натхнення на нові ідеї та впевненої реалізації амбітних планів. Нехай попереду буде ще багато вагомих досягнень, яскравих подій, перемог і суспільного визнання, а авторитет ЗУНУ в Україні та світі лише зростає.

З повагою, авторський колектив підручника «Цифрові технології в аудиті»

ЗМІСТ

«Технологія сама по собі нічого не змінює. Її змінюють люди, які вміють нею користуватися.»

Білл Ґейтс

Передмова

У сучасному соціально-економічному просторі цифровізація стала не лише технологічним трендом, а новою нормою організації діяльності підприємств, фінансових установ і державних інституцій. Бізнес-процеси дедалі частіше реалізуються через інформаційні системи, документообіг переходить в електронну форму, зростає роль платформ, хмарних сервісів і дистанційних каналів взаємодії, а дані перетворюються на ключовий ресурс управління. Водночас підвищується складність господарських операцій, прискорюється їх виконання, а також зростає залежність результатів діяльності від якості IT-середовища, належності прав доступу, коректності налаштувань систем і безперервності цифрових сервісів.

За таких умов аудит не може залишатися виключно паперовою перевіркою документів і вибіркових процедур. Сучасний аудитор дедалі частіше працює з цифровими слідами операцій, електронними доказами, журналами подій, даними з ERP, CRM та бухгалтерських систем, онлайн-реєстрами, інтеграціями сервісів і аналітичними інструментами. Це змінює підхід до оцінювання ризиків, планування перевірки та формування висновків. У центрі уваги опиняються IT-контролі, надійність даних, логіка бізнес-процесів, цілісність інформаційних потоків і захищеність фінансової інформації. Разом із новими можливостями цифрове середовище приносить і нові загрози. До них належать помилки налаштувань і викривлення даних, кіберінциденти, шахрайські схеми, маніпуляції з транзакціями, а також підміна або фрагментація доказів в електронному документообігу.

Підручник «Цифрові технології в аудиті» має на меті сформувати у читача цілісне бачення аудиту в цифровому середовищі та надати систематизований інструментарій для практичного застосування цифрових рішень у професійній

діяльності. У навчальному виданні узагальнено підходи до цифрової трансформації бізнес-процесів і показано, як зміни в організації даних та інформаційних системах впливають на облік, аудит і фінансову безпеку. Значну увагу приділено методологічним основам процесного підходу, зокрема моделюванню, аналізу та оптимізації бізнес-процесів. Це дає змогу краще розуміти, де виникають ризики, як формується доказова база та які контролі реально працюють у цифровому контурі підприємства.

Окремий акцент зроблено на нормативно-правових аспектах цифрового аудиту та практичних питаннях електронних документів, електронного підпису й електронного документообігу. Саме ці елементи визначають юридичну значущість доказів, порядок їх отримання і збереження, а також можливість відтворення результатів перевірки. У підручнику також розглянуто організаційні особливості цифрового аудиту, підходи до планування з урахуванням ІТ-ризиків і ризиків фінансової безпеки, роль інформаційних систем підприємства як об’єкта аудиту та важливого джерела аудиторських доказів.

Практико-орієнтована частина підручника зосереджена на цифрових інструментах аудитора і фахівця з фінансової безпеки. Розглянуто комп’ютеризовані засоби аудиту, використання табличних процесорів для типових процедур, а також можливості спеціалізованого програмного забезпечення. Важливе місце відведено технологіям виявлення шахрайства та підозрілих операцій у даних, роботі з «червоними прапорцями», моніторингу транзакцій і формуванню аналітичних ознак, що допомагають своєчасно ідентифікувати ризикові патерни. Окремо висвітлено питання інформаційної безпеки та кібербезпеки фінансових даних, оскільки надійність аудиторських висновків прямо залежить від захищеності цифрового середовища, управління доступами, резервного копіювання, відновлення та готовності організації до кіберінцидентів.

Сучасний розвиток технологій зумовлює інтеграцію штучного інтелекту в аудиторські процедури. У підручнику розкрито можливості застосування ШІ для аналітики, автоматизації та підвищення ефективності. Водночас наголошено на ризиках і етичних обмеженнях, які слід враховувати при використанні

інтелектуальних систем у професійних судженнях та формуванні висновків. Крім того, у виданні окремо розглянуто питання інклюзивного аудиту та окреслено можливості цифрових технологій для його проведення, методичної підтримки аудиторських процедур і належного оформлення результатів.

Підручник доповнено практикумом із кейсами та завданнями, які спрямовані на формування прикладних навичок роботи з цифровими даними, відкритими реєстрами й аналітичними сервісами. Практикум також дає можливість відпрацювати підходи до організації цифрового аудиту, виявлення ризикових операцій та оцінювання кіберризиків. Контрольні питання та тести для самоперевірки і підсумкового контролю забезпечують системне засвоєння матеріалу та допомагають визначити рівень сформованих компетентностей. Наприкінці підручника подано глосарій основних термінів, який полегшує роботу з ключовими поняттями та уніфікує їх розуміння.

Авторський колектив підручника висловлює глибоку вдячність рецензентам Ю. І. Клюс, доктору економічних наук, професору, завідувачу кафедри обліку і оподаткування Східноукраїнського національного університету імені Володимира Даля; Т. В. Шталь, доктору економічних наук, професору, проректору з наукової роботи та міжнародного співробітництва Харківського національного економічного університету імені Семена Кузнеця; А. В. Шлапак, доктору економічних наук, доценту, проректору з науково-педагогічної роботи та інноваційного розвитку Київського столичного університету імені Бориса Грінченка – за конструктивні зауваження, рекомендації та пропозиції, що сприяли вдосконаленню змісту та підвищенню практичної цінності навчального видання.

Розділ 1

Автори:
Леся Буяк
Вадим Шухманн

ТРАНСФОРМАЦІЯ БІЗНЕС-ПРОЦЕСІВ: ТРЕНДИ ТА ПЕРСПЕКТИВИ

РОЗДІЛ 1. ТРАНСФОРМАЦІЯ БІЗНЕС-ПРОЦЕСІВ: ТРЕНДИ ТА ПЕРСПЕКТИВИ

«Найбільша небезпека в часи турбулентності – не турбулентність, а дія за логікою вчорашнього дня.»

Пітер Друкер

1.1. Сутність цифрової трансформації бізнес-процесів та ключові драйвери змін
1.2. Технологічні тренди (хмари, дані, RPA, IoT) і їх вплив на облік, аудит та фінансову безпеку
1.3. Реінжиніринг процесів: організаційні зміни, IT-ризики та показники результативності
1.4. Контрольні питання для самоперевірки

1.1. Сутність цифрової трансформації бізнес-процесів та ключові драйвери змін

Цифрова трансформація бізнесу перестала бути «IT-проєктом» і стала способом системного оновлення того, як організація створює цінність для клієнта, партнерів і власників. У центрі цих змін перебувають бізнес-процеси – повторювані ланцюги робіт і рішень, що перетворюють ресурси на результат. Сучасні цифрові технології та дані прискорюють виконання процесів, знижують транзакційні витрати, змінюють структуру контролю і підвищують вимоги до прозорості. Одночасно цифровізація створює нові ризики: залежність від даних, платформ, постачальників та кіберстійкості. Тому для обліку, аудиту й фінансової безпеки важливо не лише впроваджувати системи, а й перебудовувати процеси, вимірювати ефект і керувати ризиками у логіці процесного підходу.

Цифрова трансформація бізнес-процесів один із визначальних трендів сучасного менеджменту. В епоху четвертої промислової революції нові цифрові технології докорінно змінюють спосіб ведення бізнесу, взаємодію з клієнтами та організацію операцій. Цифрова трансформація означає фундаментальне перебудування роботи компанії через масштабне впровадження сучасних технологій у всі сфери діяльності. На відміну від точкової автоматизації чи простої цифровізації, трансформація передбачає глибокі зміни бізнес-моделей і процесів, культури та підходів до управління. Іншими словами, це стратегічний перегляд того, як компанія створює цінність у цифрову еру, щоб залишатися конкурентоспроможною та ефективною (табл. 1.1).

Таблиця 1.1

Критерії відмінностей між оцифруванням, цифровізацією та цифровою трансформацією

Критерій	Оцифрування	Цифровізація	Цифрова трансформація
Суть	Переведення аналогової інформації в цифрову форму	Автоматизація існуючих процесів із використанням цифрових технологій	Повна перебудова бізнес-моделі з фокусом на цифрові цінності
Приклад	Сканування паперових документів	Впровадження CRM або електронного документообігу	Переорієнтація компанії на онлайн-сервіси замість фізичних офісів
Рівень змін	Тактичний	Операційний	Стратегічний
Технології	PDF, сканери, архіви	ERP, CRM, BPM-системи	ШІ, Big Data, IoT, хмари, блокчейн

Важливо розрізняти декілька суміжних понять, аби чітко розуміти суть цифрової трансформації. Нижче наведено визначення ключових термінів, які часто плутають між собою:

- ***Оцифрування (digitization)*** – переведення інформації з паперової або аналогової форми в електронну. Наприклад, сканування паперових документів і збереження їх як електронних файлів. Це створює цифровий фундамент даних, але не змінює самі процеси.
- ***Цифровізація (digitalization)*** – впровадження цифрових технологій у наявні бізнес-процеси для їх покращення та оптимізації. Іншими словами,

це автоматизація та перегляд окремих операцій за допомогою IT-інструментів, що підвищує ефективність існуючих процесів.

- ***Цифрова трансформація (digital transformation)*** – масштабне переосмислення клієнтського досвіду, процесів і бізнес-моделей компанії на основі цифрових технологій. Це не просто впровадження IT-рішень, а зміна корпоративної стратегії й культури. Цифрова трансформація спрямована на пошук нових способів генерування цінностей та доходів, а не лише на покращення поточних операцій.

Цифрова трансформація охоплює всі аспекти роботи компанії – від технологій та інфраструктури до структури організації, навичок персоналу і самої культури управління. Це комплексний процес змін, де новітні цифрові технології (хмарні обчислення, великі дані, штучний інтелект, Інтернет речей тощо) інтегруються у бізнес-процеси з метою суттєвого підвищення їх продуктивності та гнучкості. Важливо, що мова йде не лише про впровадження певного програмного забезпечення, а про трансформацію мислення компанії:

- *перехід до управління на основі даних;*
- *швидких експериментів;*
- *клієнтоорієнтованості;*
- *безперервних інновацій.*

У глобальному вимірі розвиток data-driven економіки розглядається як один із ключових чинників цифрової трансформації, який посилює конкуренцію і водночас створює дисбаланси та нові вимоги до управління даними. Для обліку це означає зростання важливості трасованості (звідки дані), цілісності (чи не спотворені) та відповідності (чи законно обробляються).

Хмара і цифрові екосистеми змінюють саму географію процесу, коли частина операцій виконується на сторонніх платформах, а контроль переноситься у сферу управління постачальниками та контрактними умовами. Європейська політика щодо даних підкреслює, що вони є ресурсом для конкурентоспроможності та інновацій, а отже, організації мають вибудовувати процеси доступу й використання даних із урахуванням прав і безпеки. У

підсумку цифрова трансформація визначається сукупністю взаємопов'язаних драйверів, які змінюють бізнес-процеси та підвищують вимоги до управління й контролю. Ключові з них та їх наслідки систематизовано в таблиці (табл. 1.2).

Таблиця 1.2

Ключові драйвери цифрової трансформації бізнес-процесів та їхні наслідки для управління й контролю

Драйвер змін	**Як змінює бізнес-процеси**	**Типові управлінські рішення**	**Критичні точки контролю (для обліку, аудиту, фінансової безпеки)**
Дані як стратегічний ресурс	процеси стають орієнтованими на дані, зростає роль аналітики та інтеграцій	управління даними, політики доступу, якість даних	цілісність даних, простежуваність, контроль змін, розмежування прав
Хмарні платформи та екосистеми	частина процесів виноситься за периметр (SaaS або аутсорс)	вибір постачальників, SLA, інтеграції	контроль третіх сторін, ризик залежності, безперервність, відповідність вимогам
Автоматизація та «розумні» інструменти (ШІ/RPA)	скорочення ручних операцій, зміна ролей і відповідальності	регламенти, нові KPI, навчання персоналу	контроль алгоритмів та скриптів, журналювання, розподіл обов'язків
Дистанційність і цифрові канали	процеси взаємодії переходять онлайн, збільшується поверхня атак	цифрова ідентичність, MFA, політики віддаленого доступу	управління обліковими записами, автентифікація, моніторинг, інцидент-менеджмент
Регуляторні вимоги до даних та звітності	потрібно проєктувати процеси з вбудованими комплаєнс-контролями.	комплаєнс-контури, політики збереження та видалення	доказовість, конфіденційність, аудит-трейл, контролі доступу
Конкуренція та очікування клієнтів	прискорення циклів, персоналізація, сервісність	аналіз клієнтського шляху, наскрізна оптимізація процесу	якість сервісу, контроль помилок, управління змінами
Кіберризики і стійкість	процеси мають містити механізми відновлення і реагування	BCP/DRP, резервне копіювання, тестування відновлення	резерви, RTO/RPO, контроль інцидентів, незалежність резервних копій

Дана таблиця показує, що драйвери трансформації одночасно є джерелами ефекту (швидкість, якість, масштабованість) і джерелами ризику (помилки даних, залежність від платформ, кіберінциденти). Саме тому в сучасних підходах

наголошується на необхідності цілісної політики цифрового розвитку на рівні організацій і держав, де довіра, безпека та інклюзивність є невід'ємними компонентами цифрових змін.

Автоматизація на основі RPA та ШІ змінює те, де саме виникають помилки і хто за них відповідає, адже замість помилки виконавця частіше маємо помилку в налаштуванні правила, у скрипті або в моделі. Тому контролю перевірки людиною вже недостатньо і його потрібно доповнювати контролями над автоматизацією, зокрема контролем налаштувань і змін, веденням журналів виконання, управлінням версіями та тестуванням перед запуском змін у роботу. У результаті цифрова трансформація є не разовим впровадженням технологій, а постійним управлінням змінами в процесах, що потребує зрозумілих регламентів і підтримки керівництва.

Дистанційні канали та цифрова ідентичність підвищують навантаження на контури доступу. Для фінансової безпеки ключове питання звучить просто хто саме ініціює операцію і чи має право її виконувати. Трансформація процесів без одночасного посилення контролів доступу створює прямий шлях до шахрайства, витоків і компрометації облікових даних. Отже, цифровий комфорт має супроводжуватися дисципліною доступу.

Регуляторні вимоги (конфіденційність, збереження даних, прозорість звітності) фактично вимагають будувати процеси за принципом ***compliance-by-design*** – коли дотримання вимог передбачають ще на етапі проєктування процесу та фіксують у регламентах, ролях, маршрутах погодження і контрольних точках.

За визначенням експертів McKinsey, ***«цифрова трансформація*** – це фундаментальна перебудова роботи компанії шляхом масштабного впровадження нових технологій, які проникають в усі сфери бізнесу». Ціль – створити стійку конкурентну перевагу, підвищивши якість обслуговування клієнтів і знизивши витрати завдяки новим технологічним рішенням.

Сьогодні цифрова трансформація для багатьох галузей стала питанням виживання бізнесу, основним рушієм якої виступає стрімкий розвиток

технологій. Водночас успішна трансформація стосується не тільки впровадження IT, а й людей та процесів, а також організаційної структури компанії (рис. 1.1).

Цифрова трансформація не зводиться до міграції в хмару чи створення мобільного додатку це, передусім, про зміну підходів до роботи. Компанія стає більш гнучкою та адаптивною, здатною швидко реагувати на змінні ринкові умови і потреби клієнтів.

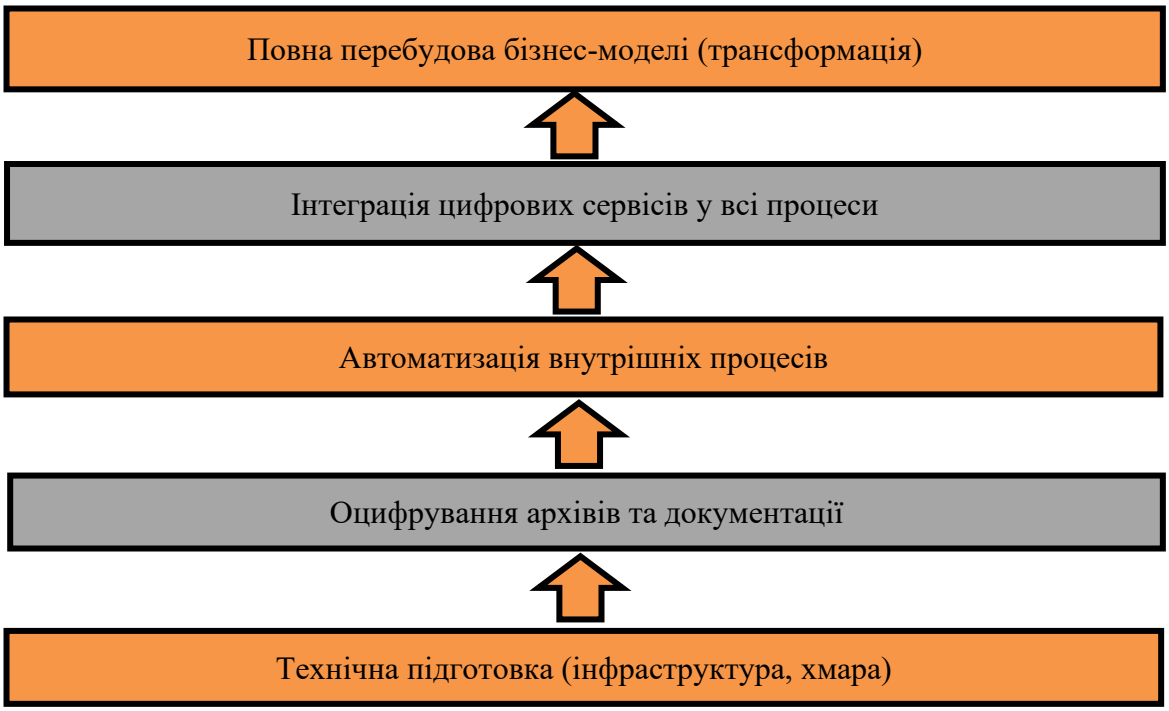


Рис. 1.1. Етапи цифрової трансформації підприємства

Трансформація бізнес-процесів означає, що рутинні операції автоматизуються, процеси перебудовуються «під цифру», зникають зайві ланки, натомість з’являються нові цифрові продукти або сервіси. Наприклад, використання аналітики Big Data дозволяє ухвалювати рішення на основі даних, а не інтуїції; впровадження IoT-пристроїв на виробництві автоматизує контроль за обладнанням і знижує ризик простоїв; застосування ШІ може прискорити обробку клієнтських запитів тощо. У результаті правильно реалізована цифрова трансформація підвищує ефективність компанії, покращує досвід клієнтів і відкриває нові можливості для росту. Причини, через які компанії починають цифрову трансформацію своїх процесів, можуть бути різними.

1. ***Зовнішні чинники:***
    - *ринок;*
    - *конкуренція;*
    - *регулятори.*
2. ***Внутрішні:***
    - *потреба в ефективності;*
    - *стратегічні цілі.*

Стрімкий прогрес інформаційних технологій є головним рушієм цифрових змін. Поява нових рішень, зокрема штучного інтелекту, машинного навчання, блокчейну, великих даних, хмарних платформ і мобільних застосунків, створює для бізнесу одночасно нові можливості та нові виклики. Компанії змушені впроваджувати сучасні технології, щоб зберігати конкурентоспроможність і технологічну сумісність у цифрових екосистемах. За результатами KPMG Global Tech Report 2024, пріоритетами інвестицій на найближчий рік для більшості організацій є XaaS та хмарні моделі, які обирають 86 % респондентів з фокусом на гнучкість і зниження витрат, а також кібербезпека 68 % і ШІ та автоматизація 65 %, що відображає прагнення одночасно підвищувати ефективність і посилювати стійкість операцій. Наприклад, впровадження хмарних сервісів дає змогу швидко масштабувати IT-інфраструктуру, а алгоритми ШІ відкривають шлях до персоналізації сервісів. Розвиток технологій фактично диктує бізнесу необхідність трансформації ті, хто ефективно застосовує інновації, отримують значні переваги на ринку.

Зміни на ринку і зростання очікувань клієнтів потужний драйвер цифрової трансформації. Сучасні споживачі звикли до цифрового досвіду – вони хочуть отримувати послуги онлайн, через зручні мобільні додатки, очікують миттєвого обслуговування та персоналізації. Бізнеси, що не відповідають цим очікуванням, ризикують втратити клієнтів. Все більше банків переходять на дистанційне обслуговування, ритейлери розвивають омніканальні продажі (поєднання онлайн- і офлайн-каналів), а служби таксі впроваджують мобільні додатки для замовлення поїздок.

Конкуренція теж змушує трансформуватися. Якщо один учасник ринку успішно оцифровує свої процеси, інші мусять реагувати, щоб не втратити частку ринку. ***Цифрові «аборигени»*** – компанії, що народилися одразу цифровими (на кшталт Amazon, Uber чи Monobank) встановлюють високий стандарт швидкості та сервісу. Традиційні компанії вимушені перебудовуватися, щоб не поступитися клієнтами більш технологічним конкурентам. Цифрові технології та інновації допомагають бізнесу диференціюватися від конкурентів і створити стійку конкурентну перевагу, оперативно реагуючи на потреби аудиторії та ринку. Іншими словами, цифрова трансформація стала інструментом виживання в умовах глобальної конкуренції.

Зовнішнє регуляторне середовище також відіграє свою роль. Уряди і міжнародні органи впроваджують нові правила, які фактично стимулюють бізнес до цифровізації. Яскравий приклад – законодавство щодо захисту даних (такі як європейський GDPR), компанії змушені впроваджувати сучасні системи управління даними і безпеки, щоб відповідати вимогам із прозорості та конфіденційності. Цифрова трансформація у цьому випадку стає засобом забезпечення комплаєнсу (відповідності нормам) та зниження регуляторних ризиків. Окрім того, держава нерідко сама задає тон, наприклад, в Україні через проєкти Міністерства цифрової трансформації («Дія» та ін.) бізнес-середовище адаптується до електронного документообігу, електронної звітності, онлайн-торгів тощо. Компаніям вигідно впроваджувати нові цифрові процеси, аби користуватися державними електронними сервісами, подавати документи онлайн, підключатися до державних реєстрів. Такі ініціативи виступають драйвером цифрових змін, особливо у фінансовому та державному секторах (рис. 1.2). З іншого боку, регулятори можуть вимагати від бізнесу певного рівня кібербезпеки, наявності резервних IT-систем, прозорості операцій. У сукупності

такі чинники додатково стимулюють модернізацію IT інфраструктури компаній.

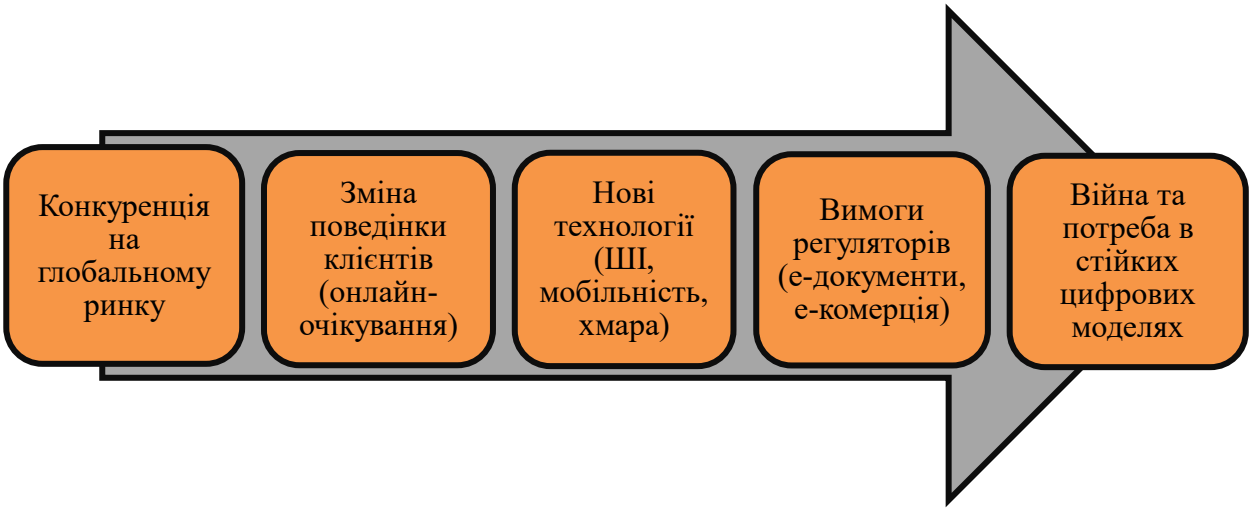


Рис. 1.2. Ключові драйвери цифрової трансформації в Україні

Внутрішні мотиватори – підвищення продуктивності та оптимізація витрат є не менш важливими драйверами цифрової трансформації. Автоматизація процесів і використання IT-рішень дають змогу компаніям робити більше меншими ресурсами. Тому керівники, шукаючи шляхів підвищити рентабельність, інвестують у цифрові технології.

Наприклад, впровадження ERP-системи чи CRM-платформи допомагає усунути дублювання функцій, скоротити ручну працю, мінімізувати помилки і прискорити операції. ***Автоматизація*** – ключовий інструмент економії завдяки якому рутинні завдання виконуються швидше і без участі людини, що знижує операційні витрати.

Використання хмарних технологій, штучного інтелекту, великих даних та цифрових каналів значно підвищує прозорість процесів і робить їх більш результативними. Зокрема, автоматизація щоденних рутинних задач, зменшення впливу людського фактору та економія часу і ресурсів напряму ведуть до зростання загальної ефективності роботи компанії. Отже, бажання отримати операційну досконаліть і кращі фінансові показники спонукає бізнес переглядати застарілі процеси й замінювати їх цифровими, більш ефективними аналогами.

1.2. Технологічні тренди (хмари, дані, RPA, IoT) і їх вплив на облік, аудит та фінансову безпеку

Українська фінансова сфера за останні роки переживає прискорену цифрову трансформацію. Виклики війни та глобальної конкуренції змусили бізнес і державний сектор переходити від паперових процесів до хмарних сервісів, аналітики великих даних (Big Data), роботизованої автоматизації процесів (RPA), Інтернету речей (IoT), штучного інтелекту (AI) і машинного навчання (ML), віртуальної реальності (VR), електронної комерції, блокчейну, смарт-контрактів. Регулятори теж стимулюють ці зміни. Зокрема, Національний банк України (НБУ) у 2022 році вперше дозволив банкам використовувати хмарні послуги (в дата-центрах ЄС, США, Британії, Канади) для забезпечення безперервної роботи під час війни. Цей крок допоміг підтримати стабільне функціонування банківської системи в умовах воєнного стану.

У 2025 році НБУ перейшов від тимчасових дозволів до повноцінного регулювання хмар. ***Постанова Правління НБУ №99*** встановила постійні вимоги з прозорості, інформаційної безпеки та управління ризиками при роботі фінансових установ у хмарі. Ця постанова зобов'язує банки забезпечити повний контроль над хмарною інфраструктурою та врахувати низку умов у контрактах з провайдерами (зокрема, процедуру видалення даних, право НБУ на аудит, звітність про локацію дата-центрів тощо). Банки повинні повідомляти НБУ про кожен хмарний контракт і сертифікації безпеки провайдера.

Одночасно Міністерство цифрової трансформації розвиває екосистему підтримки бізнесу «Дія.Бізнес» та інструменти оцінки цифрової зрілості, підкреслюючи, що цифрові інструменти стали головним фактором успіху. Компанії, що впровадили CRM, хмарні сервіси та автоматизовані облікові системи, як правило, демонструють вищу операційну ефективність і швидше адаптуються до змін, тоді як підприємства, які зберігають паперово орієнтовані процеси, поступово втрачають конкурентні позиції.

Успішне функціонування сучасних бізнес-структур неможливе без інтеграції широкого спектра цифрових інструментів. Їх використання

спрямоване на оптимізацію операційних процесів, підвищення якості комунікації з клієнтами та забезпечення конкурентоспроможності в умовах цифрової економіки. Систематизація зазначених технологій зазвичай здійснюється за трьома основними критеріями: їхнім функціональним призначенням і сферою застосування; специфікою інтерфейсу та способом взаємодії; а також здатністю забезпечувати необхідний рівень захисту та безпеки даних (рис. 1.3).

Рис. 1.3. Класифікація цифрових технологій для корпоративних підприємств

Розглянемо детальніше кожну групу згідно зі схемою.

Найширшу групу становлять технології, класифіковані за їхнім функціональним призначенням та сферою застосування в операційній діяльності

підприємства. Вони охоплюють рішення, що формують інфраструктурний базис, забезпечують інтелектуальну автоматизацію процесів, обробку даних, здійснення фінансових операцій, ведення електронної комерції та комплексне управління бізнесом. До технологій цієї групи належать:

1. ***Інфраструктурні технології*** – створюють базовий технологічний фундамент для функціонування інших систем:

- *хмарні технології* – забезпечують доступ до обчислювальних ресурсів та сховищ даних через інтернет за вимогою, дозволяючи масштабувати інфраструктуру без значних капітальних вкладень;
- *інтернет речей (IoT)* – мережа фізичних пристроїв, оснащених сенсорами та програмним забезпеченням для збору й обміну даними, що дозволяє здійснювати віддалений моніторинг та управління активами.

2. ***Інтелектуальні технології*** – спрямовані на автоматизацію складних завдань, що традиційно вимагають людського інтелекту:

- *штучний інтелект (AI) і машинне навчання (ML)* – системи, здатні аналізувати дані, навчатися на досвіді та приймати рішення, імітуючи когнітивні функції людини для оптимізації процесів;
- *роботизована автоматизація процесів (RPA)* – використання програмних роботів для автоматизації рутинних, повторюваних бізнес-завдань, що підвищує швидкість та точність операцій.

3. ***Аналітика та обробка даних*** – інструменти для роботи з інформацією з метою отримання цінних інсайтів:

- *аналітика великих даних* – методи та засоби обробки величезних масивів структурованих і неструктурованих даних для виявлення прихованих закономірностей та тенденцій ринку;
- *прогностична аналітика* – використання історичних даних та статистичних алгоритмів для прогнозування майбутніх подій, попиту чи поведінки клієнтів.

4. ***Фінансові технології*** – інновації у сфері фінансових послуг:

- *блокчейн* – децентралізована технологія розподіленого реєстру, що забезпечує прозорість, безпеку та незмінність записів про транзакції;
- *рішення для цифрових платежів* – системи, що дозволяють здійснювати миттєві та безпечні електронні розрахунки між контрагентами;
- *смарт-контракти* – самовиконувані контракти, умови яких записані в коді блокчейну, що автоматизує виконання угод при настанні певних умов.

5. Електронна комерція – технології для ведення торговельної діяльності онлайн:

- *платформи електронної комерції* – програмні рішення для створення онлайн-магазинів, управління каталогами товарів, замовленнями та взаємодією з покупцями;
- *прогностична аналітика (в e-commerce)* – застосування аналітичних інструментів для персоналізації пропозицій та оптимізації товарних запасів на основі передбачення поведінки покупців.

6. Управління бізнесом та клієнтськими відносинами – комплексні системи для автоматизації основних бізнес-процесів:

- *системи управління взаємовідносинами з клієнтами (CRM)* – програмне забезпечення для збору та аналізу інформації про клієнтів з метою покращення обслуговування та збільшення продажів;
- *системи планування ресурсів підприємства (ERP)* – інтегровані системи для управління всіма ключовими бізнес-процесами компанії (фінанси, виробництво, логістика, кадри) в єдиному інформаційному просторі.

Друга важлива класифікаційна ознака визначає інструменти за типом інтерфейсу та способом взаємодії з користувачем. Ця група технологій забезпечує мобільність доступу до даних, створює нові середовища для роботи, а також пропонує сучасні інтерактивні канали комунікації. Основними інструментами тут виступають:

1. Мобільні технології – забезпечують доступ до корпоративних систем з будь-якого місця:

➢ *аналітика великих даних (через мобільні інтерфейси)* – надання доступу до аналітичних звітів та дашбордів у реальному часі через смартфони та планшети для швидкого прийняття рішень.

2. Віртуальна реальність та імерсивні технології – створюють ефект занурення у цифрове середовище:

➢ *віртуальна реальність (VR)* – повне занурення користувача у змодельований цифровий світ, що використовується для навчання персоналу, прототипування чи презентацій;

➢ *доповнена реальність (AR)* – накладання цифрової інформації (графіки, тексту) на зображення реального світу в режимі реального часу, що застосовується у виробництві, логістиці та маркетингу.

3. Інтерактивні інтерфейси – забезпечують діалогову взаємодію з користувачем:

➢ *чат-боти та віртуальні помічники* – програми на основі ШІ, які можуть вести діалог з користувачами, відповідати на запити та виконувати прості завдання, автоматизуючи клієнтську підтримку.

Критично важливою складовою цифрового ландшафту є група технологій, виділених за функцією забезпечення захисту і безпеки. Вони спрямовані на захист інформаційних активів підприємства від зовнішніх та внутрішніх загроз, а також на забезпечення надійного контролю доступу. До цієї категорії входять:

1. Технології кібербезпеки – комплекс засобів для протидії цифровим загрозам:

➢ *рішення для кібербезпеки* – широкий спектр інструментів (антивіруси, фаєрволи, системи виявлення вторгнень) для захисту мереж, пристроїв та даних від кібератак.

➢ *біометрична автентифікація* – методи ідентифікації користувачів за їхніми унікальними фізичними характеристиками (відбиток пальця, розпізнавання обличчя) для посилення контролю доступу до систем.

Сучасні цифрові технології, зокрема хмарні обчислення, штучний інтелект і машинне навчання, роботизована автоматизація процесів, аналітика даних,

блокчейн і смарт-контракти, рішення для цифрових платежів, платформи електронної комерції, корпоративні системи CRM та ERP, мобільні й імерсивні технології, інтерактивні інтерфейси, зокрема чат-боти, а також інструменти кібербезпеки й біометрична автентифікація, істотно трансформують бухгалтерський облік і аудит та впливають на фінансову безпеку бізнесу. У цьому розділі розглядаються лише окремі з перелічених рішень, тоді як інші технології та їх прикладні ефекти детальніше аналізуються в наступних розділах.

Впровадження цих технологій є глобальним трендом і критично важливим для підвищення ефективності та прозорості фінансової інформації та звітності, у тому числі в українських компаніях. Водночас цифровізація підвищує залежність від якості даних, інтеграцій і зовнішніх провайдерів, що робить актуальними питання контролю доступу, аудит трейлу та безперервності. Для обліку й аудиту це означає необхідність поєднувати технологічні інновації з належним внутрішнім контролем і комплаєнсом.

Хмарні технології (Cloud technologies) дедалі активніше проникають у бухгалтерський облік і фінансову інфраструктуру України. Вони дозволяють винести IT-системи (облікові програми, бази даних) на віддалені сервери, забезпечуючи гнучкий доступ онлайн, масштабованість і зменшуючи витрати на власні дата-центри. Для українських компаній хмари стали особливо цінними під час війни: завдяки їм критичні фінансові системи можуть працювати навіть при фізичній недоступності офісів.

Переваги хмар для обліку – це доступність і гнучкість. Бізнес може працювати з бухгалтерськими даними з будь-якої точки, що полегшує віддалену роботу і співпрацю в реальному часі. Хмарна бухгалтерія не потребує власних серверів і складної IT-команди – оновлення і резервне копіювання забезпечує постачальник. Наприклад, багато українських компаній перейшли на SAP або інші ERP-системи, розгорнуті в хмарі (в тому числі на локальних хмарних майданчиках чи глобальних платформах на кшталт AWS, Azure). Міністерство фінансів також підтримує перехід державних установ на хмарні рішення для

бухгалтерського обліку (є нормативні акти щодо застосування хмар у державному секторі).

Цифровізація облікового процесу забезпечує оперативність і точність інформації, автоматизує рутинні задачі та мінімізує людський фактор. В результаті бізнес отримує достовірніші дані для прийняття рішень, скорочує витрати часу на обробку документів та підвищує рівень контролю. Вплив вищезазначених технологічних трендів на облік, аудит та фінансову безпеку, а також пов'язані ризики, контролі і показники ефективності цифровізації відображено нижче (табл. 1.3) та (рис. 1.4).

Таблиця 1.3

Порівняльний вплив сучасних технологій на облік, аудит і фінансову безпеку

Технологія	Вплив на бухгалтерський облік	Вплив на аудит	Вплив на фінансову безпеку
Хмарні технології (Cloud)	Перехід на електронні регістри та зберігання даних в хмарі, відмова від паперу. Автоматичне резервне копіювання та швидке відновлення даних, що гарантує безперервність облікового процесу. Мобільність доступу: бухгалтери можуть працювати з базами даних із будь-якого місця, де є інтернет. Зниження витрат на IT-інфраструктуру (сервери, ПЗ) провайдер забезпечує оновлення і підтримку систем	Централізований доступ до фінансових даних для аудиторів у режимі реального часу, спрощення дистанційного аудиту та співпраці. Прозорість операцій у хмарних ERP сприяє повнішому контролю: всі транзакції фіксуються і доступні для вибірки аудиторських тестів. Аудитори повинні врахувати ризики хмарних сервісів, тобто оцінювати ефективність IT-контролів провайдера та дотримання ним стандартів безпеки	Підвищення стійкості та захищеності даних: обмежений доступ, шифрування інформації, резервні копії та дублювання баз даних у хмарі покращують захист фінансової інформації. Зменшення ризику втрати даних у разі надзвичайних подій (аварій, атак) завдяки георозподіленим дата-центрам провайдера. Водночас виникають нові ризики: залежність від інтернет-з'єднання та стороннього провайдера, питання юрисдикції даних – це потребує посиленої кібербезпеки і контролю з боку компанії
Великі дані (Big Data)	Збір і аналіз великих обсягів різнорідної інформації відкриває нові можливості для бухгалтерів: від аналізу транзакцій в	Суцільний аудит даних, зокрема засоби аналітики дозволяють перевіряти 100 % транзакцій замість вибіркового методу, що	Моніторинг ризиків: аналітика Big Data використовується для постійного відстеження фінансових ризиків і шахрайських дій у

	режимі реального часу до прогнозування фінансових показників. Big Data розширюють горизонт обліку, бухгалтерія перестає обмежуватися лише фінансовою звітністю і включає аналіз нефінансових даних, трендів ринку, поведінки клієнтів тощо, що сприяє більш обґрунтованим управлінським рішенням. Підвищується автоматизація рутинних задач обліку: алгоритми можуть обробляти тисячі операцій і виявляти помилки чи невідповідності швидше за людину	значно підвищує ймовірність виявлення порушень. Аудитори отримують інструменти для автоматичного виявлення аномалій, шахрайських схем або ризикових операцій у масивах даних. Поєднання Big Data з ШІ дає проактивний аудит. Наприклад, аналіз соцмереж чи IoT-даних може сигналізувати про проблеми ще до традиційної перевірки. Вимагає нових компетенцій від аудиторів (обробка даних, робота з аналітичним ПЗ), оскільки ШІ та аналіз даних поки мало представлені в класичній освіті аудитора	режимі реального часу. Наприклад, банки в Україні вже застосовують аналіз великих даних для виявлення підозрілих транзакцій і кіберзагроз. Big Data підвищують прозорість, відповідно консолідація даних з різних підрозділів дає цілісне бачення фінансового стану, сприяє своєчасному виявленню відхилень. Захист даних стає критичним, тобто великі масиви фінансової інформації потребують надійного зберігання, контролю доступу та дотримання законів про конфіденційність. Неналежна якість даних або їх витік – серйозна загроза фінбезпеці, тому впроваджуються політики управління даними (Data Governance)
RPA (Robotic Process Automation)	RPA виконує монотонні, стандартні операції бухгалтерії (перенесення даних, формування звітів, звірки, розсилка довідок) цілодобово та без помилок. Це прискорює облік та усуває людський фактор. Автоматизація закриття періодів і обробки документів: боти можуть щомісяця закривати книги значно швидше, забезпечуючи, наприклад, готовність звітності на наступний день (T+1). Бухгалтери звільняються від	Прозорість операцій, тобто дії програмних роботів повністю логуються – кожен крок записується у журнал, що полегшує аудит та внутрішній контроль. Аудитори можуть побачити всі операції, виконані ботом, і перевірити їх на відповідність правилам. Підвищення якості контролю: RPA-системи суворо дотримуються заданих інструкцій, тому процеси з ними більш передбачувані та керовані, ніж ручні – це знижує ризик помилок і шахрайства. Аудит RPA-	Мінімізація людських помилок: роботизація процесів усуває фактор неуважності або змови персоналу, підвищуючи достовірність фінансових даних. Це напряму впливає на фінансову безпеку – менше помилок означає менше ризиків втрат чи санкцій. Прискорення реакції: RPA обробляє операції швидше, тож компанія може швидко виявляти відхилення (наприклад, бот одразу сигналізує про нестачу коштів чи перевищення ліміту). Швидка інформація дає змогу оперативно запобігти фінансовим проблемам

	рутинної роботи і переходять до аналітичних задач та контролю, що підвищує продуктивність фінансової служби. RPA легко інтегрується з наявними програмами (ERP, Excel тощо) без кардинальних змін інфраструктури, тому доступна навіть для середніх і малих підприємств	середовища, оскільки аудитор має оцінити налаштування RPA, тобто чи правильно визначені правила, чи забезпечено захист від несанкціонованих змін бота, чи є резервний сценарій на випадок збою. RPA доповнює роботу аудиту, але не замінює професійного судження (усі нестандартні ситуації все одно потребують участі людини)	Обмеження, оскільки RPA працює лише з формалізованими процесами. Якщо виникають нестандартні події, існує ризик, що бот їх не помітить. Тому для фінансової безпеки важливо визначити зони, де потрібен додатковий контроль людини (для сценаріїв, що виходять за рамки алгоритмів)
Інтернет речей (IoT)	Автоматизація первинного обліку: датчики IoT можуть збирати інформацію про господарські операції безпосередньо в момент їх здійснення. Наприклад, оснащення виробничого обладнання сенсорами дозволяє автоматично фіксувати показники випуску продукції чи споживання ресурсів. Ці дані передаються в облікову систему і формують електронні документи, усуваючи ручне заповнення накладних чи актів. Таким чином, від події до документа інформація проходить миттєво і без втручання людини. Зростає оперативність і точність обліку, оскільки IoT забезпечує своєчасний збір первинних даних з високою достовірністю (немає затримок і перекручень, що бувають при людському факторі)	Безперервний аудит: завдяки IoT-пристроям аудитори можуть отримувати доступ до даних про активи і операції у режимі online. Наприклад, GPS-трекери на автотранспорті чи складах дають можливість аудитору відстежувати рух товарів, що спрощує інвентаризацію і підтвердження залишків. Нове джерело аудиторських доказів зосереджене на тому, що аудитор може використати записи IoT (логи сенсорів, відеодані, показники лічильників) як незалежні докази при перевірці достовірності обліку. Це підвищує рівень впевненості в перевіреній звітності. Разом з тим IoT підвищує вимоги до аудиту IT-безпеки, адже потрібно оцінювати, чи захищені смарт-пристрої від втручань, чи калібровані вони	Віддалений контроль активів: фінансові установи і підприємства в Україні активно застосовують IoT для моніторингу матеріальних цінностей. Наприклад, банки через датчики і M2M SIM-карти відстежують стан банкоматів і терміналів у реальному часі, щоб запобігти збоям чи несанкціонованому доступу. Це підвищує фізичну безпеку і безперервність фінансових послуг (справність обладнання = безперервність операцій). Безпека транзакцій: IoT-технології (наприклад, безконтактні платежі NFC з біометрією) роблять фінансові транзакції зручними і захищеними, зменшуючи ризик шахрайства з картками. Кіберризики IoT, тобто кожен підключений пристрій – це потенційна вразливість. IoT передає великі обсяги конфіденційних даних (транзакції, особисті дані

	Впровадження IoT змінює роль бухгалтера – замість введення даних він більше зосереджується на контролі за системами збору даних та аналізі показників у реальному часі	правильно (інакше датчик може дати хибні дані). Аудитор має враховувати ризики кібератак на IoT-інфраструктуру, які можуть вплинути на фінансові показники	клієнтів), які є привабливими для хакерів. Відтак фінансова безпека потребує додаткових заходів, таких як: шифрування каналів зв'язку, сегментування мережі для IoT, систем моніторингу аномалій у трафіку та регулярних аудиторських перевірок IoT-платформ на захищеність

Як видно з таблиці 1.3, усі розглянуті технології мають значний позитивний вплив на ефективність та точність обліково-аудиторських процесів. Вони автоматизують операції, прискорюють отримання інформації та посилюють контроль, що зрештою підвищує фінансову стійкість бізнесу. Разом з тим, цифровізація породжує нові ризики – від кіберзагроз до технологічних збоїв. Тому важливо впроваджувати адекватні контрольні заходи та управління ризиками.

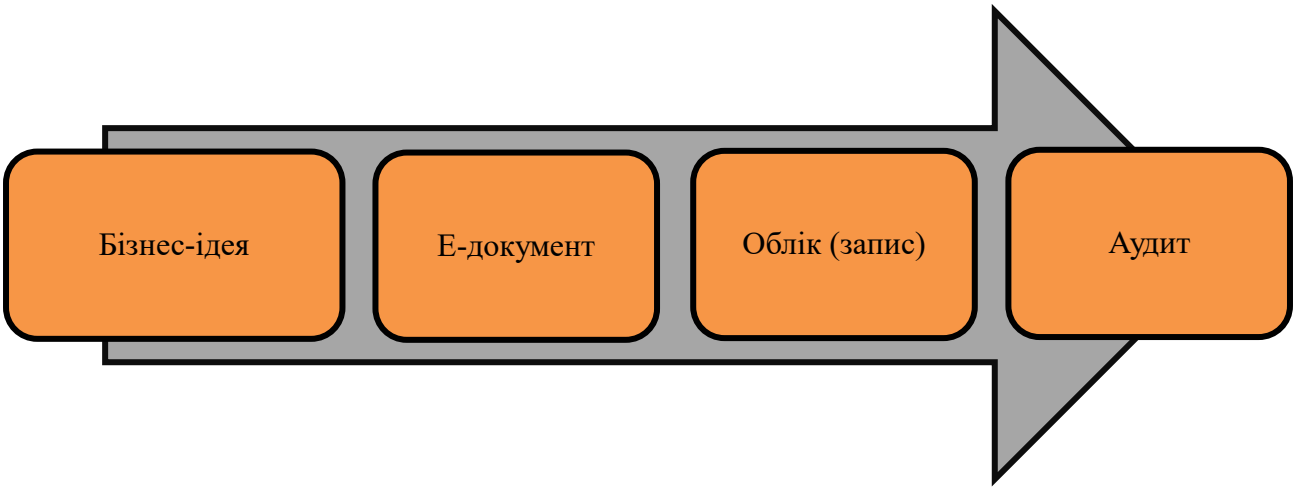


Рис. 1.4. Схематичний «цифровий ланцюг» від події до документа, обліку та аудиту

Така цифрова трансформація процесів означає, що інформація проходить шлях від бізнес-події до фінансової звітності безперешкодно і майже миттєво. Наприклад, подія (господарська операція) генерує електронний документ (запис у системі), який автоматично відображається у бухгалтерському обліку, а

аудитори можуть одразу його перевірити у цифровому середовищі. Це підвищує оперативність, прозорість та керованість фінансових даних. У традиційному середовищі між цими етапами були розриви (папери, затримки, ручні перевірки), але сучасні IT-рішення об'єднують їх в єдиний ланцюжок.

В аудиті перехід клієнтів на хмарні системи означає, що аудитори отримують більш оперативний доступ до даних (іноді навіть дистанційно). Аудиторські фірми впроваджують власні хмарні платформи для обміну документами з клієнтами та для використання аналітичних інструментів. У хмарному середовищі легше реалізувати концепцію ***безперервного аудиту*** – коли перевірка даних йде паралельно з їхнім створенням.

Водночас аудиторам важливо врахувати ризики:

- *чи надійно захищені фінансові дані клієнта у хмарі;*
- *чи є резервні копії;*
- *чи можна довіряти цілісності інформації.*

Контракти мають включати право аудитора (банк або НБУ) перевіряти хмарну інфраструктуру. Тобто навіть у хмарі забезпечується можливість аудиту даних та IT-контролів. Фінансова безпека при використанні хмар набуває нових аспектів.

Хмари підвищують надійність і безперервність бізнес-процесів, так як провайдери гарантують:

- *відмовостійкість;*
- *георезервування даних;*
- *захист даних від фізичного знищення серверів (стало актуальним через ракетні загрози).*

Наприклад, глобальні платформи дозволяють розгорнути системи у різних географічних зонах і швидко відновити роботу навіть після масштабних збоїв. Водночас перехід у хмару змінює профіль операційної та інформаційної стійкості, оскільки частина контролів реалізується на рівні провайдера, а частина – на рівні банку, що безпосередньо відображається на контурах фінансової безпеки (рис. 1.5).

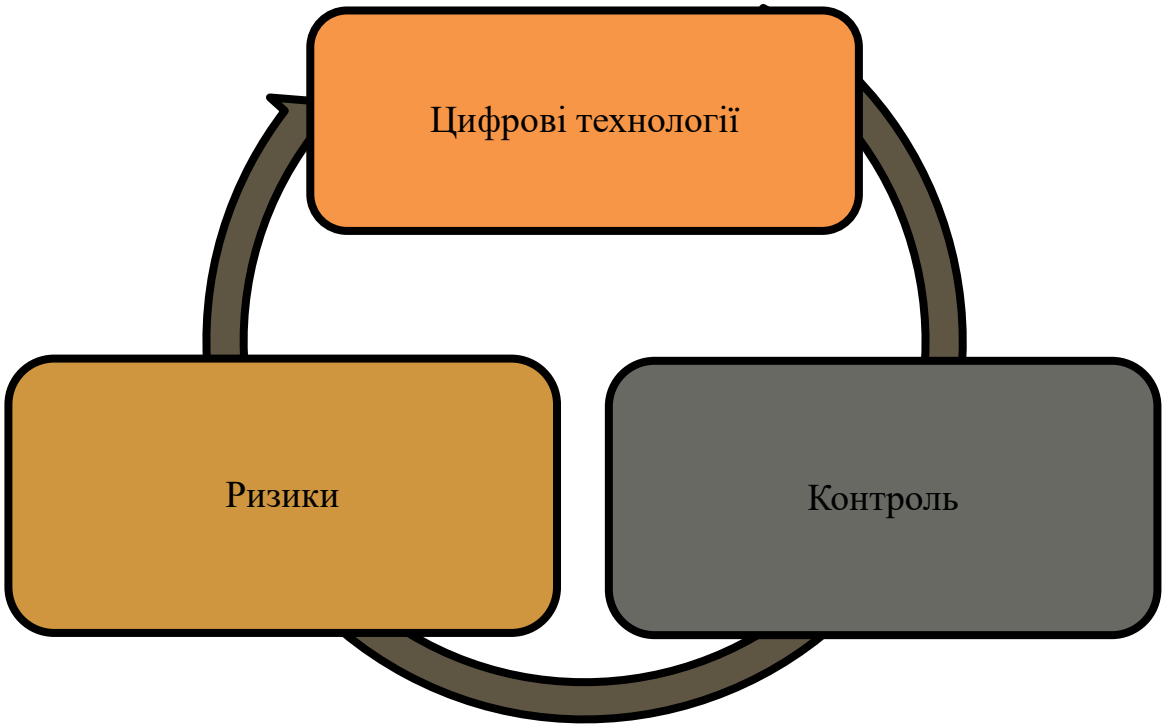


Рис. 1.5. Контур фінансової безпеки (взаємодія технології → ризики → контрольні заходи)

Контур на рисунку 1.5 фактично відображає цикл управління ризиками. Він є безперервним, оскільки із впровадженням нових ІТ-рішень повинні одразу оцінюватися потенційні ризики та оновлюватися засоби контролю. Такий підхід гарантує, що цифровізація буде не лише ефективною, а й безпечною для фінансової сфери компанії. Тому НБУ висуває вимогу моделі спільної відповідальності, коли провайдер відповідає за фізичну безпеку дата-центрів, а банк за налаштування внутрішніх контролів, таких як шифрування даних, управління доступом та постійний моніторинг активності. Заборонено розміщувати фінансові дані в небезпечних юрисдикціях (наприклад, в країні-агресорі), а дозволено лише в дата-центрах країн зі списку НБУ (ЄС, Північна Америка тощо). Також вимагається план виходу, оскільки компанія повинна мати можливість мігрувати з хмари іншого провайдера без втрати даних.

Українські банки вже почали переносити окремі сервіси в хмару. У 2023–2024 рр. кілька банківських ІТ-департаментів пілотували хмарні рішення для резервного копіювання даних та аналізу великих масивів транзакцій. Prozorro

(державна система закупівель) від самого початку побудована як хмарна платформа на принципах відкритих даних. Вона агрегує інформацію з численних торговельних майданчиків у центральній хмарній базі, що дозволило створити модуль аналітики та онлайн-моніторингу ризиків у публічних закупівлях. Ще одним прикладом є АТ «Укрпошта». Вони у 2023 році оголосили тендер на закупівлю резервних хмарних послуг вартістю понад 115 млн грн, плануючи зберігати копії критичних даних у хмарі. Дане рішення демонструє пріоритет безпеки і безперервності бізнесу на державному підприємстві. Отже, хмарні рішення стрімко інтегруються як у приватному, так і в державному секторі економіки.

Big Data – це технології збору, зберігання та аналізу надвеликих масивів даних для виявлення закономірностей, тенденцій та аномалій. У фінансовій сфері України Big Data застосовується як в корпоративному сегменті (банки, великі компанії), так і у державному нагляді й аудиті. Аудит особливо виграє від аналітики даних, адже замість вибіркових перевірок з'являється можливість аналізувати 100 % транзакцій і документів.

Так, у системі публічних закупівель Prozorro запроваджено автоматизовані ризик-індикатори, де 35 алгоритмічних індикаторів аналізують тендерні дані і автоматично виявляють підозрілі закупівлі (наприклад, відсутність цифрового підпису учасника, надто багато лотів в одному тендері, порушення строків оскарження тощо). Якщо сукупний «ризик-бал» високий, така закупівля автоматично надходить на перевірку Державній аудиторській службі.

Для бухгалтерського обліку великі дані відкривають можливості більш глибокої фінансової аналітики і прогнозування. Традиційний облік оперує регламентованими проведеннями і звітами, але Big Data дозволяє накладати на ці дані додаткові шари інформації. Наприклад, торговельна мережа може аналізувати мільйони транзакцій продажів, аби виявити приховані тренди у виторгу, кореляцію між поведінкою клієнтів і фінансовими показниками. Фінансові директори все більше використовують дашборди і системи бізнес-

аналітики, що беруть дані з бухгалтерських систем і комбінують їх з великими масивами зовнішніх даних (економічних показників, курсів валют, новин).

Міністерство фінансів та НБУ публікують багато відкритих даних. До них відносять:

- *показники банківського сектору;*
- *бюджетні витрати;*
- *статистику боргу.*

Аналітики можуть обробляти ці масиви для аудиту та фінансового аналізу. Великі українські банки впровадили системи аналізу транзакцій у режимі реального часу для цілей фінансового моніторингу. Це також приклад Big Data, коли потоки даних з карткових операцій, переказів, платежів аналізуються алгоритмами, які виявляють підозрілі шаблони (типу структурування платежів, нетипову активність) і виставляють «червоні прапорці» для служби комплаєнсу. В наглядовій аналітиці НБУ використовує великі дані для макропруденційного аналізу, які агрегують показники по всіх банках, щоб моделювати стрес-тести, аналізувати кредитні ризики по секторах економіки тощо.

Бюро економічної безпеки України (БЕБ) з 2021 року будує Єдину інформаційно-аналітичну систему. За даними БЕБ, ця система матиме 18 модулів, включно з аналітичним модулем та модулем ризик-орієнтованого підходу. Фактично, Бюро планує інтегрувати дані з податкової, митниці, банків та інших джерел у єдине сховище і застосувати алгоритми Big Data для виявлення схем ухилення від податків, відмивання коштів та інших загроз економічній безпеці. Тобто, ***аналітика великих масивів даних*** – ключовий інструмент проактивного виявлення загроз, який дозволяє передбачати і випереджати незаконні дії.

RPA (Robotic Process Automation) – це технологія, що дозволяє налаштувати програмних роботів для виконання рутинних операцій так, ніби їх виконував працівник вручну. RPA-боти можуть імітувати дії людини у різних програмах, тобто натискати кнопки, копіювати й вставляти дані, переносити файли, заповнювати форми тощо. В обліку RPA за останні 5 років набуло значної

популярності, адже багато бізнес-процесів тут добре структуровані і підлягають формалізації. Перехід від ручної праці до роботизації бухгалтерських операцій дає змогу компаніям суттєво підвищити ефективність і точність фінансової роботи.

Типові застосування RPA в обліку:

1. ***Обробка первинних документів*** (рахунків, актів, накладних). RPA-бот може автоматично зчитувати рахунки (наприклад, з PDF чи електронної пошти) та витягувати потрібні реквізити, звіряти їх із замовленнями чи договорами, а потім вносити дані в облікову систему. На практиці це означає, що рахунки до сплати можуть опрацьовуватися без участі бухгалтера – від отримання до проведення платежу. Така автоматизація ліквідує затримки, усуває помилки ручного вводу і покращує комунікацію з постачальниками.
2. ***Банківська реконсиляція.*** Бот підключається до виписок банку та бухгалтерських регістрів і щоденно звіряє рух коштів. Він знаходить невідповідності (наприклад, платежі, які є в банку, але не відображені в обліку, або навпаки) і формує звіт для бухгалтера з переліком розбіжностей. Це значно прискорює закриття місяця, адже те, що раніше бухгалтер робив годинами вручну, тепер виконується за хвилини. RPA забезпечує повну трасованість таких процедур – кожна дія бота протоколюється, що важливо для аудиту і контролю.
3. ***Нарахування заробітної плати і кадрові операції.*** RPA може збирати дані про відпрацьований час з HR-системи, розраховувати зарплату, податки та відрахування за заданими формулами і формувати платіжні відомості. У великих компаніях із тисячами співробітників це знімає величезне навантаження з бухгалтерів і мінімізує ризик помилок у нарахуванні заробітної плати.
4. ***Податковий комплаєнс і звітність.*** Програмні роботи здатні заповнювати податкові декларації, перевіряти правильність заповнення форм, звіряти дані у різних системах. Деякі компанії використовують RPA

для автоматичного формування податкових накладних та реєстрації їх у Єдиному реєстрі, адже це економить час і гарантує вчасну реєстрацію.

Internet of Things (Інтернет речей) – це мережа фізичних пристроїв, обладнаних сенсорами і підключених до інтернету для збору та обміну даними. На перший погляд, IoT більше стосується виробництва чи логістики, але й у обліку та аудиті ця технологія знаходить застосування. Суть у тому, що розумні пристрої можуть автоматично фіксувати господарські операції і передавати їх прямо в облікові системи, без участі людини.

Практичне застосування IoT в обліку:

1. ***Ритейл.*** Торгові мережі встановлюють смарт-каси та датчики покупців. Вони охоплюють великий обсяг даних про продажі, який автоматично аналізується (суміжно з Big Data). IoT-термінали банків збирають телеметрію, що допомагає фінансовим установам проактивно планувати інкасацію, ремонт (АТМ зламався – банк бачить по датчиках і одразу реагує, мінімізуючи втрати).
2. ***Сільське господарство.*** Датчики вологості ґрунту і GPS-навігація сільгосптехніки передають дані у фінансові модулі агрокомпаній для розрахунку собівартості (скільки палива витрачено, який урожай зібрано з поля).
3. ***Логістика.*** Компанії відстежують переміщення товарів у реальному часі, й інформація про доставку автоматично закриває дебіторську заборгованість (наприклад, як тільки вантаж доставлено і це підтверджено IoT-сканером, у системі генерується бухгалтерський документ про виконання зобов'язань).

Щоб оцінити успішність цифрової трансформації, компанії визначають ***ключові показники ефективності (Key Performance Indicators, KPI). KPI*** – це кількісні метрики, які відображають ступінь досягнення поставлених цілей і дозволяють виміряти результати змін. Вони охоплюють як фінансові, так і нефінансові аспекти діяльності. Правильно підібрані KPI дають змогу

керівництву відстежувати прогрес трансформації, своєчасно виявляти проблемні місця та приймати обґрунтовані рішення.

Впровадження цифрових технологій у фінансові процеси дозволяє суттєво поліпшити ***ключові показники ефективності (KPI) бухгалтерського обліку і аудиту.*** Нижче наведено матрицю KPI із типових метрик, їх значеннями після цифровізації (табл. 1.4). Один із ключових показників є тривалість (цикл) закриття звітного періоду (місяця). До автоматизації багато українських компаній закривали місяць за 7–10 календарних днів, особливо коли процеси були переважно ручними. Після впровадження ERP, RPA та ШІ-інструментів тривалість закриття звітного періоду суттєво скорочується.

Таблиця 1.4

KPI-матриця ефективності цифровізації обліку

KPI цифровізації	**Опис показника та цільове значення**
Швидкість закриття періоду (T+1)	Час, необхідний для підготовки повного комплекту фінансової звітності після закінчення звітного періоду. T+1 означає, що місяць (або квартал) закривається на наступний день - це можливе за умови високої автоматизації обліку і консолідації даних в режимі реального часу. Для традиційних систем цей процес може тривати 5–10 днів, а цифрові рішення (ERP, RPA) дозволяють скоротити його до 1 дня або навіть годин. Підвищення цього показника свідчить про оперативність обліку та гнучкість компанії реагувати на фінансові результати
Рівень автоматизації процесів (%)	Частка транзакцій або облікових операцій, що виконуються автоматично без участі людини, у загальній кількості операцій вимірюється у відсотках. Цифровізація направлена на збільшення цього показника – наприклад, до 80–90 %. Високий рівень автоматизації означає менше ручної роботи, менше помилок і швидший облік. Проте 100 % автоматизації може бути недосяжним або навіть небажаним (через наявність нестандартних ситуацій, що потребують ручного втручання)
Кількість помилок на 1000 операцій	Показник якості облікового процесу. Розраховується як число виявлених помилкових проводок або виправлень, що були необхідні, у розрахунку на кожні 1000 транзакцій. При впровадженні перевірок та автоматизації (напр. контрольні алгоритми, RPA) цей коефіцієнт має різко знижуватися. Ціль - прагнути до <1 помилки на 1000 операцій (6 рівень якості). Зменшення цього показника свідчить про зростання точності обліку і менші ризики викривлення фінансової звітності

Щоб оцінити вплив цифрових рішень не лише на терміни закриття звітного періоду, а й на щоденну продуктивність облікової служби, розглянемо операційні KPI обліку та документообігу:

1. Трудомісткість обліку. Цей KPI вимірюється як сумарний час співробітників, витрачений на обробку документів, введення даних, виправлення помилок тощо. Дослідження Innora показало, що українські офісні працівники витрачають 10-25 % робочого часу на ручне введення даних. Бухгалтер маленької фірми – до 20-30 год/міс на ручні операції, а в період звітності – понад 50 годин. Після впровадження електронного документообігу, OCR та RPA ці цифри значно зменшуються. KPI, кількість документів на одного бухгалтера оброблених за місяць зросла у кілька разів (за рахунок автоматизації один співробітник може контролювати те, що раніше робили 3-4 людини).

2. Тривалість обробки **одного документа**. До автоматизації обробка рахунку-фактури від надходження до проведення займала, приміром, 30-60 хвилин (з урахуванням черги, ручного введення, перевірок). Після впровадження RPA+IDP цей цикл скорочується до 5-10 хвилин, а в ідеалі – секунди (більшість часу йде на автоматичне розпізнавання).

3. Кількість помилок у обліку. Показник можна виміряти як кількість виправних бухгалтерських довідок, або число виявлених помилкових транзакцій на 1000 операцій. Ручний облік дає певний відсоток помилок - наприклад, 1 % транзакцій потребують виправлення. Після автоматизації багато компаній звітують про зменшення помилок на 90 %. ШІ-алгоритми самі знаходять невідповідності і попереджають їх, система прогнозує відсутній рахунок або дублікат і сигналізує бухгалтеру. Отже, KPI частка помилкових проводок може знизитися з 10 на 1000 до менш ніж 1 на 1000 після впровадження контролів на основі RPA або ШІ.

4. Частка автоматизованих операцій. Це інтегральний показник цифровізації. Він відображає, яка частина операцій (в штуках або в гривнях) проходить без участі людини. У фінансових відділах компаній, що впровадили навіть базові RPA, можна очікувати автоматизації 50-70 % операцій (наприклад,

70 % платіжних документів генеруються і проводяться автоматично, 30 % – вручну через нестандартні випадки). Цей KPI прямо пов'язаний із продуктивністю, адже чим більша частка автоматизації, тим більше операцій на одного працівника і тим менше витрати на обробку одиниці транзакції.

5. ***Час на підготовку управлінської звітності.*** Цей показник стосується вже аналітики. З цифровими інструментами (BI, BigData) час на збір даних і складання, наприклад, бюджету або прогнозу може скоротитися з кількох тижнів до декількох днів. Якщо раніше фінансовий аналітик витрачав 60 % часу на зведення цифр і 40 % на аналіз, то з BI-системою 90 % часу йде на аналіз (зведення – автоматичне). Це якісно покращує обґрунтованість рішень.

Інші можливі KPI цифровізації обліку включають:

- *час реагування на запит керівництва* (скільки часу потрібно, щоб отримати потрібний фінансовий аналітичний звіт – в ідеалі, це on-line через BI-системи);
- *який відсоток використання електронних документів* (частка документів, що існують лише в електронній формі, без паперових дублікатів);
- *економія трудових витрат (*скорочення людино-годин на облікові процедури завдяки IT).

Показники мають відображати швидкість, точність та продуктивність фінансової функції, які й покращуються завдяки новітнім технологіям. Вимірювання KPI до і після впровадження дає кількісні докази успіху цифрової трансформації або вказує на сфери, які ще потребують вдосконалення.

Цифрові KPI допомагають не лише оцінювати результати змін, а й постійно відстежувати стабільність процесів обліку та аудиту під час цифрової трансформації. Щоб краще показати, як цифрові KPI відображають реальні зміни в обліку, на рисунку 1.6 наведено їхній зв'язок із загальною ефективністю процесів.

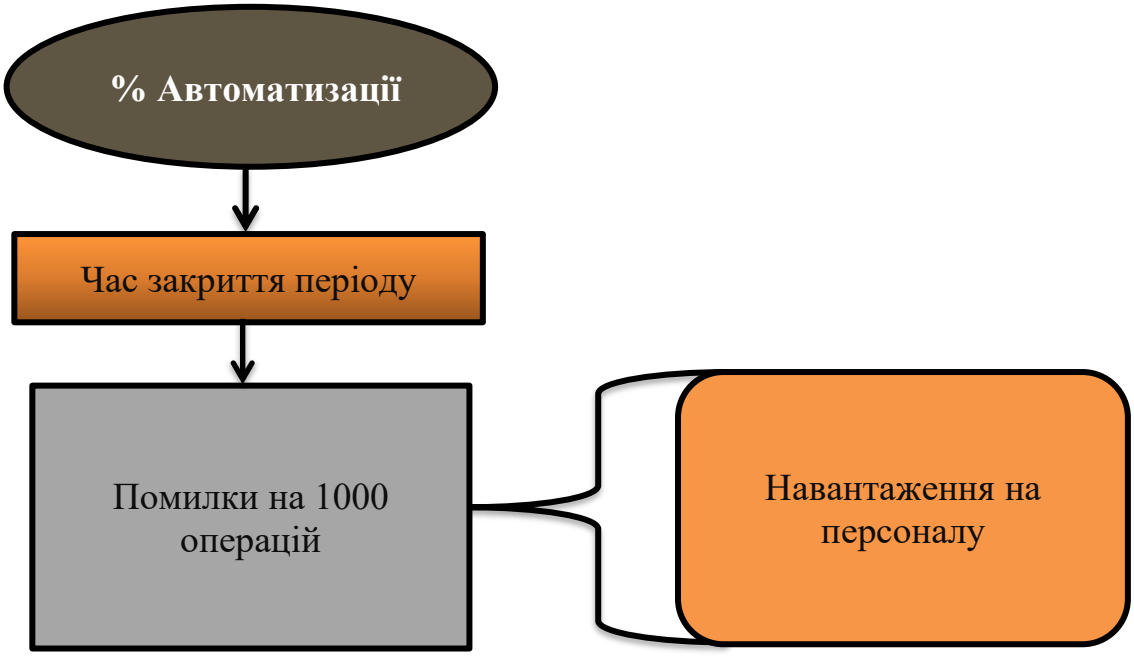


Рис. 1.6. Зв'язок цифрових KPI з ефективністю обліку

Цей рисунку ілюструє, як зростання рівня автоматизації безпосередньо впливає на ключові показники ефективності в бухгалтерії. У першу чергу скорочується час, необхідний для закриття звітного періоду, що дозволяє оперативніше ухвалювати управлінські рішення.

Отже, ***технологічні тренди***, а саме: хмари, дані, роботи, IoT докорінно трансформують бухгалтерський облік та аудит, роблячи їх більш ефективними, оперативними та прозорими. Адже, саме вони надають нові інструменти для забезпечення фінансової безпеки (через автоматизацію контролів, проактивний моніторинг, кіберзахист).

За правильного впровадження цифрові рішення помітно підсилюють облікову функцію, роблячи її більш точною, відтворюваною та контрольованою. Це підтверджують українські підприємства, які внаслідок оцифрування процесів фіксують підвищення продуктивності й контрольованості господарських операцій та звітних даних.

1.3. Реінжиніринг процесів: організаційні зміни, IT-ризики та показники результативності

У сучасних умовах цифрової трансформації бізнеси змушені переглядати свої основні процеси, щоб залишатися конкурентоспроможними. ***Реінжиніринг бізнес-процесів (Business Process Reengineering, BPR)*** – це підхід до радикального перепроектування ключових процесів компанії з метою досягнення суттєвих покращень показників діяльності. Іншими словами, BPR означає «почати з чистого аркуша» і спроєктувати процеси заново, ніби компанія створюється сьогодні. М. Хаммер, один із ідеологів концепції BPR, визначав реінжиніринг як «фундаментальне переосмислення і радикальне перепланування бізнес-процесів компанії з метою різкого поліпшення ключових показників, таких як витрати, якість, сервіс, швидкість». Таким чином, реінжиніринг передбачає не поступове вдосконалення, а кардинальні зміни процесів, що особливо актуально, коли дрібні покращення вже не дають ефекту.

Цифрова трансформація передбачає інтеграцію сучасних цифрових технологій у всі аспекти діяльності компанії. Реінжиніринг процесів відіграє при цьому ключову роль, оскільки впровадження нових технологій часто вимагає перегляду застарілих підходів до роботи (табл. 1.5). Якщо автоматизувати старий неефективний процес без змін, то технологія лише закріпить його недоліки. Натомість BPR дозволяє перебудувати процеси під цифрові рішення і максимально використати їхній потенціал.

Таблиця 1.5

Вплив цифрових змін на організаційні ролі та процеси

Процес	Типова зміна	Організаційний ефект	Відповідальні
Обробка первинних даних	Автоматизація через RPA	Зменшення ручної праці	Оператор процесу, IT-інтегратор
Звітність	Хмарні шаблони та електронна подача	Прискорення циклів звітності	Data-контролер, е-звіт-менеджер
Контроль транзакцій	Аналітика Big Data	Зниження помилок і шахрайства	Аналітик даних, аудит-контролер

Погодження витрат	КЕП, маршрути узгодження документів	Прозорість, контроль	КЕП-адміністратор, контролер витрат

Внаслідок реінжинірингу компанія може отримати кратне підвищення продуктивності, якості та швидкості роботи процесів. Наприклад, перехід від паперових процедур до ERP-систем чи платформ автоматизації часто супроводжується перепроектуванням бізнес-процесів, тобто замість багатоетапної обробки даних у різних відділах створюються єдині цифрові потоки, що прискорюють виконання завдань і зменшують кількість помилок. Реінжиніринг є частиною інноваційної стратегії управління, яка допомагає організації адаптуватися до змін та досягати стратегічних цілей за рахунок нових підходів до роботи. В результаті успішного BPR підприємство стає гнучкішим, клієнтоорієнтованим і краще підготовленим до викликів ринку в цифрову еру.

Реінжиніринг бізнес-процесів впливає не лише на технології, а й на організаційну структуру, культуру та управлінські підходи компанії. ***Впровадження нових цифрових рішень*** часто супроводжується організаційними змінами – адаптацією внутрішніх правил і взаємозв'язків у компанії для підтримки оновлених процесів (рис. 1.7).

Традиційно компанії були організовані за функціональним принципом (окремі відділи для різних функцій), але після реінжинірингу можливий перехід до процесно-орієнтованої структури. Це означає об'єднання фахівців з різних функцій у крос-функціональні команди, відповідальні за виконання процесу «від початку до кінця». Ієрархія може стати більш прозорою, з'являються нові ролі (наприклад, власники процесів), які відповідають за результати процесу через декілька підрозділів. Такий підхід розмиває межі між відділами і зменшує бюрократію, прискорюючи прийняття рішень.

Цифрова трансформація вимагає культури інновацій та гнучкості. Співробітники повинні бути готові навчатися новим інструментам, експериментувати з поліпшеннями і швидко адаптуватися до змін. Організація формує цифрову культуру, що заохочує обмін знаннями, креативність та орієнтацію на дані при прийнятті рішень. Водночас долається організаційна

інерція – опір змінам з боку персоналу, який звик працювати по-старому. Активна комунікація про цілі змін і навчання персоналу допомагають зменшити спротив і залучити команду до трансформації.

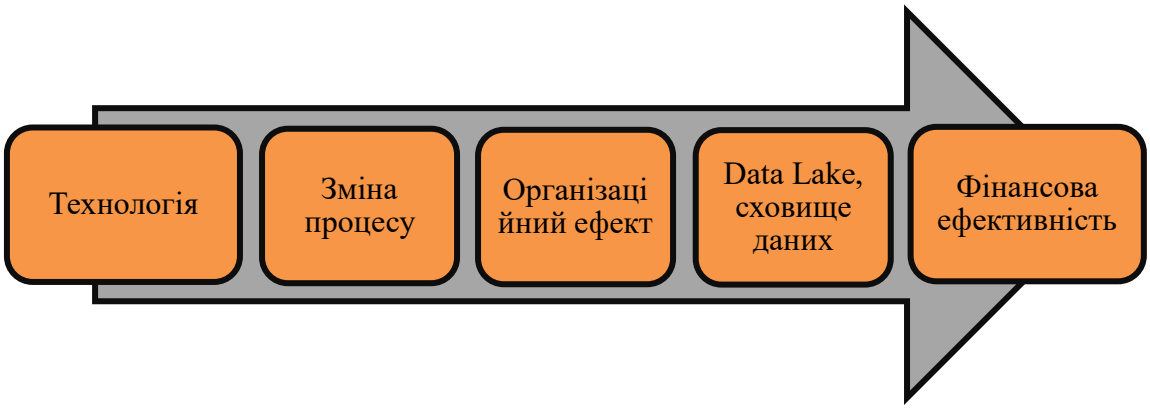


Рис. 1.7. Цифровий контур змін при реінжинірингу

Внаслідок впровадження сучасних технологій керівники переходять від жорстких бюрократичних методів до більш гнучких стилів управління. Гнучкі підходи до управління проєктами та співпраця між різними командами стають дедалі популярнішими. Роль керівників зміщується від контролю до підтримки змін. Топменеджери беруть на себе відповідальність за цифрові ініціативи, формують культуру постійного вдосконалення та забезпечують проєкти оновлення процесів потрібними ресурсами. Відкрите обговорення прогресу, підтримка ініціатив працівників і прозора оцінка результатів поступово стають нормою в сучасному управлінні.

Реінжиніринг процесів веде до глибинних організаційних перетворень. BPR неминуче зачіпає розподіл влади, ролі та стандарти взаємодії – фактично змінюються «правила гри» в компанії. Компанія, що впроваджує нові технології, повинна перебудувати внутрішні процеси та структури так, щоб максимально використати їхні переваги. Без готовності змінюватися з боку людей навіть найсучасніша технологія не дасть результату, тому управління змінами є критично важливим складником успішної трансформації.

Впровадження інформаційних технологій у перероблені процеси несе низку ризиків. ***IT-ризики*** – це потенційні проблеми і втрати, пов’язані з використанням інформаційних систем та цифрових рішень у бізнес-операціях.

Під час реінжинірингу процесів найбільш поширеними є такі IT-ризики (табл. 1.6).

Таблиця 1.6

IT-ризики та відповідні контрольні заходи

IT-ризик	Потенційний вплив	Мінімізувальний захід
Втрата доступу до сервісу	Зупинка облікових процесів	План безперервності, резерви
Компрометація облікового запису	Несанкціоновані зміни	MFA, логування, обмеження прав
Помилка в автоматизованому сценарії	Масові помилки в обліку	Тестування, контроль змін
Збої в інтеграції	Неповні або дубльовані дані	Контроль цілісності, моніторинг

Радикальна перебудова процесів зазвичай супроводжується впровадженням нового програмного забезпечення або IT-інфраструктури. Один із ризиків відмова цих систем або їх непрацездатність у критичний момент. Наприклад, збій ERP-системи, на яку перевели ключові процеси, може паралізувати роботу підприємства. Такі збої призводять до простоїв, невиконання замовлень і фінансових втрат, тому важливо забезпечити резервні плани (резервні копії даних, дублювання серверів, тощо) та тестування нових рішень перед повноцінним запуском.

При переході на нові цифрові процеси існує ризик втрати даних - через помилки міграції, апаратні збої або кібератаки. Дані є основою сучасного бізнесу, тому їхня втрата чи пошкодження можуть серйозно вплинути на операційну діяльність. Також важливо враховувати ризик порушення цілісності даних, якщо нові системи або інтеграції працюють неправильно, дані можуть спотворитися. Для мінімізації цього ризику застосовують:

- *резервне копіювання;*
- *шифрування;*
- *ретельне тестування процесів міграції;*
- *налаштування контролів якості даних.*

Зміни технологій і процесів неминуче впливають на працівників, які ними оперують. Помилки користувачів або недостатня кваліфікація кадрів становить серйозний ризик, оскільки співробітники можуть неправильно користуватися

новими системами, що призведе до збоїв або помилкових даних. Також існує опір персоналу, деякі з них можуть несвідомо перешкоджати впровадженню нових процесів, якщо не розуміють їхньої цінності або побоюються втратити роботу. Відсутність цифрових навичок і негативне ставлення до змін названо серед головних бар'єрів цифрової трансформації. Щоб знизити цей ризик, компанії інвестують у навчання співробітників, залучають їх до проєктування нових процесів та поступово впроваджують зміни (наприклад, починаючи з пілотних проєктів).

Переведення ключових операцій на цифрові платформи підвищує ризики, пов'язані з кібератаками та витоком даних. Нові системи можуть мати вразливості, якими скористаються зловмисники, якщо компанія не впровадить належних заходів безпеки. Справді, залежність від IT-рішень та проблеми із захистом даних значно підвищують рівень ризиків для бізнесу. Типові загрози включають:

- *несанкціонований доступ до конфіденційної інформації;*
- *віруси й шкідливе ПЗ;*
- *атаки типу ransomware* (вимагання викупу за розблокування даних).

Наслідками можуть бути як зупинка процесів, так і фінансові втрати чи шкода репутації. Тому під час трансформації необхідно впроваджувати ***сучасні засоби кібербезпеки***, а саме: автентифікацію MFA (Multi-Factor Authentication), системи моніторингу трафіку, шифрування даних, регулярне оновлення програмного забезпечення та навчання персоналу основам інформаційної безпеки.

Інші ризики, що можуть супроводжувати IT-проєкти реінжинірингу, включають перевищення бюджету чи термінів впровадження, а також невідповідність кінцевого результату початковим вимогам бізнесу (якщо задачі були сформульовані нечітко). Проте ключовим є те, що кероване управління ризиками – ідентифікація, оцінка і план реагування дозволяє мінімізувати негативний вплив більшості загроз.

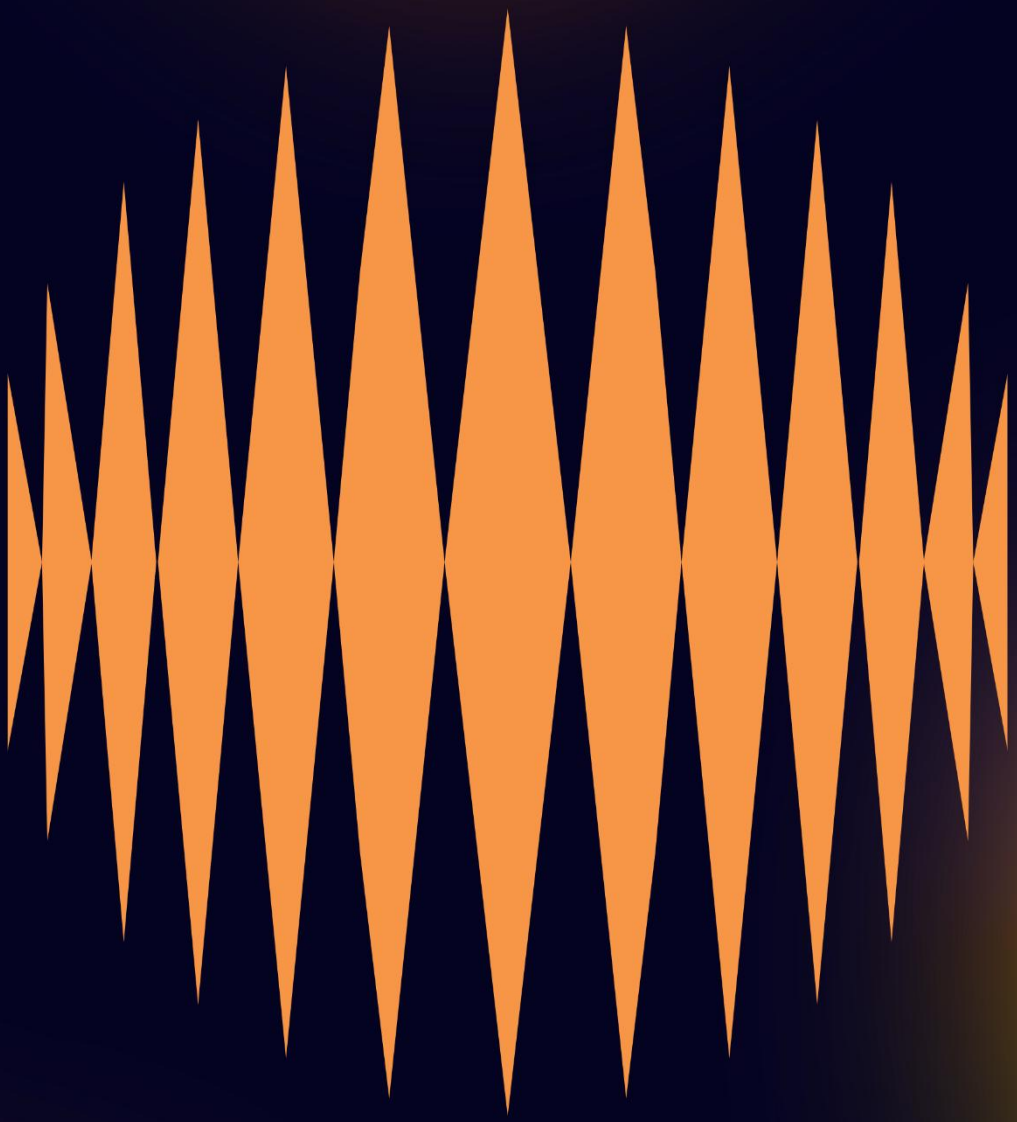
Рівень задоволеності клієнтів сервісом після змін є одним із ключових індикаторів результативності реінжинірингу та може вимірюватися через опитування або індекси схожі на NPS (індекс лояльності клієнтів). Сюди ж відносять швидкість реагування на запити клієнтів, відсоток своєчасно виконаних замовлень, кількість скарг. Зростання задоволеності та лояльності клієнтів свідчить про позитивний вплив реінжинірингу на якість сервісу.

1.4. Контрольні питання для самоперевірки

1. Які основні переваги хмарних обчислень для бухгалтерського обліку?
2. Які ризики супроводжують використання хмарних технологій в обліку та аудиті?
3. Що таке audit trail і яку роль він відіграє в системі внутрішнього контролю?
4. Як Big Data змінює підхід до контролю та аудиту?
5. Які приклади застосування Big Data для фінансового моніторингу ви можете назвати?
6. У чому полягає користь RPA для автоматизації бухгалтерських процесів?
7. Які потенційні ризики пов’язані з впровадженням RPA?
8. Яким чином IoT може впливати на точність бухгалтерського обліку?
9. Назвіть приклади контролю за допомогою IoT-пристроїв.
10. Які ключові контрольні заходи мають бути впроваджені незалежно від обраної технології?
11. Як цифрові технології впливають на фінансову безпеку підприємства?

Розділ 2

Автори:
Леся Буяк
Юрій Семененко



МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ В ОБЛІКУ ТА АУДИТІ

РОЗДІЛ 2. МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ В ОБЛІКУ ТА АУДИТІ

«Якщо ви не можете описати те, що робите, як процес, ви не знаєте, що робите.»

Вільям Едвардс Демінг

2.1 Процесно-орієнтовані моделі обліково-аудиторської діяльності та їх методологічні основи

У традиційній практиці організації обліково-аудиторської діяльності переважає функціональний підхід. Його логіка сформувалася історично та тривалий час вважалася ефективною, оскільки дозволяла чітко розподіляти обов'язки між підрозділами та відповідальними особами. Саме тому більшість систем бухгалтерського обліку, внутрішнього контролю та аудиту будувалися за функціональним принципом. Проте в умовах ускладнення господарських процесів і зростання вимог до якості управлінських рішень недоліки такого підходу стають дедалі очевиднішими.

Функціональний підхід – це підхід до організації діяльності підприємства, за якого управління та виконання робіт здійснюються за окремими функціями та структурними підрозділами, кожен з яких відповідає за власний напрям діяльності, без орієнтації на наскрізну логіку формування результату.

Функціональний підхід передбачає організацію діяльності підприємства за окремими функціями. У межах обліку та аудиту це означає поділ робіт за напрямами:

- *бухгалтерський облік;*
- *податкові розрахунки (податковий облік);*
- *управлінський облік;*
- *внутрішній контроль;*
- *внутрішній аудит;*
- *фінансова звітність.*

Кожна з цих функцій має власні завдання, відповідальних осіб і регламент виконання робіт.

У такій моделі увага зосереджується не на процесі формування результату, а на виконанні окремих функціональних операцій. Наприклад, бухгалтер фіксує первинні документи, інший працівник формує звітність, аудитор перевіряє правильність відображення операцій. При цьому кожен етап розглядається як відносно самостійний. У загальному вигляді функціональний підхід можна охарактеризувати як підхід, за якого діяльність організації структурується за видами робіт, а не за логікою їх послідовного виконання. Такий підхід добре описаний у класичних працях з менеджменту та організації управління.

Одним із ключових наслідків функціонального підходу є ***фрагментація інформації.*** Під фрагментацією в даному контексті слід розуміти розподіл інформаційних потоків між окремими функціональними підрозділами без чіткої прив'язки до загального процесу створення облікової інформації.

Фрагментація виникає з кількох причин.

1. ***Кожна функція орієнтована на виконання власних завдань.*** Бухгалтер зосереджується на правильності оформлення документів і відображенні операцій на рахунках. Підрозділ внутрішнього контролю перевіряє дотримання процедур. Аудитор аналізує відповідність звітності встановленим вимогам. У результаті кожен учасник бачить лише «свій фрагмент» загальної картини.

2. ***Функціональний підхід передбачає використання різних регламентів, форм документів і показників для різних напрямів діяльності.*** Це ускладнює узгодження інформації між підрозділами та призводить до дублювання даних або, навпаки, до їх втрати на окремих етапах.
3. ***У межах функціональної організації відсутній єдиний відповідальний за весь процес формування облікової інформації.*** Відповідальність розподіляється між функціями, але не закріплюється за процесом у цілому. Це ускладнює виявлення причин помилок і відхилень.

З методологічної точки зору така ситуація суперечить сучасному уявленню про управління процесами. Згідно з міжнародним стандартом ***ISO 9000***, процес розглядається як «сукупність взаємопов'язаних або взаємодіючих видів діяльності, які перетворюють входи на виходи» (ISO 9000:2015). Саме ця логіка дозволяє простежити повний шлях формування результату, чого не забезпечує функціональний підхід.

Для аудиту фрагментація інформації має особливо негативні наслідки. Аудитор працює не лише з окремими документами або показниками, а з логікою формування фінансової інформації в цілому. Коли інформація розподілена між функціями, аудит зводиться до перевірки окремих елементів без глибокого розуміння причин відхилень.

У таких умовах аудит часто набуває формального характеру. Перевіряється відповідність документів вимогам стандартів, але не аналізується, як саме організований процес їх формування. У результаті виявляються помилки, але не завжди встановлюються їхні першопричини.

Крім того, функціональний підхід ускладнює оцінювання ризиків. Аудиторські ризики формуються на рівні процесів, а не окремих функцій. Наприклад, ризик викривлення фінансової звітності може бути наслідком недоліків у процесі закупівель, обліку запасів або нарахування витрат. Якщо ці етапи розглядаються окремо, ризик оцінюється фрагментарно.

Міжнародні стандарти аудиту також наголошують на необхідності розуміння процесів. Зокрема, ***Міжнародний стандарт аудиту (МСА) 315***

«Ідентифікація та оцінка ризиків суттєвого викривлення через розуміння суб'єкта господарювання і його середовища» визначає, що аудитор повинен отримати розуміння діяльності суб'єкта господарювання та його внутрішнього контролю для ідентифікації та оцінки ризиків суттєвого викривлення фінансової звітності. Функціональний підхід без доповнення процесним аналізом негативно впливає на якість аудиторських висновків. Висновки часто ґрунтуються на перевірці окремих показників, а не на аналізі логіки їх формування. Це знижує аналітичну глибину аудиту. Аудиторські рекомендації в такому випадку мають обмежений ефект. Вони спрямовані на усунення окремих порушень, але не на вдосконалення процесу в цілому. Наприклад, рекомендується посилити контроль на окремій ділянці, але не переглядається структура процесу. Функціональний підхід ускладнює комунікацію результатів аудиту з керівництвом. Керівнику важливо розуміти, як зміни в одному процесі вплинуть на інші елементи системи. Фрагментарні висновки не дають такого розуміння.

У підсумку функціональна організація обліково-аудиторської діяльності не відповідає сучасним вимогам до управління, прозорості та аналітичності. Вона створює основу для формального аудиту, але не забезпечує умов для глибокого аналізу та оптимізації діяльності. Функціональний підхід, незважаючи на його поширеність, обмежує можливості обліку та аудиту через фрагментацію інформації та відсутність цілісного бачення процесів. Саме ці обмеження зумовлюють потребу у переході до процесно-орієнтованих моделей, які дозволяють аналізувати не окремі функції, а логіку формування облікової інформації в цілому.

У сучасних умовах ведення обліку та здійснення аудиту дедалі більшого значення набуває не лише правильність окремих облікових операцій, а й розуміння того, яким чином ці операції пов'язані між собою та як вони в сукупності формують облікову інформацію. Саме на цьому рівні виникає потреба в такому інструменті, який дозволяє побачити діяльність підприємства не як набір розрізнених дій, а як цілісну, логічно впорядковану систему. Таким інструментом виступає процесно-орієнтована модель.

Процесний підхід – це підхід до управління діяльністю організації, за якого вона розглядається як сукупність взаємопов'язаних процесів, що перетворюють вхідні ресурси на результати та створюють цінність, а управління зосереджується на логіці виконання цих процесів і взаємозв'язках між ними.

Процесно-орієнтована модель у контексті обліку та аудиту слугує способом представлення діяльності підприємства через послідовність взаємопов'язаних дій, що приводять до формування облікових даних, звітності та аудиторських висновків. На відміну від функціонального підходу, де увага зосереджується на окремих підрозділах або виконавцях, процесна модель акцентує увагу на логіці виконання робіт і на взаємозв'язках між ними (табл. 2.1). Це дозволяє перейти від фрагментарного сприйняття обліково-аудиторської діяльності до її системного бачення.

Таблиця 2.1

Порівняння функціонального та процесно-орієнтованого підходів

Критерій порівняння	Функціональний підхід	Процесно-орієнтований підхід
Об'єкт управління	Окремі функції та підрозділи обліку й аудиту	Наскрізні обліково-аудиторські процеси
Логіка організації діяльності	Поділ за видами робіт і відповідальністю підрозділів	Послідовність взаємопов'язаних дій від операції до результату
Представлення облікової інформації	Фрагментоване, за функціями	Цілісне, у межах процесу
Відповідальність	Закріплена за окремими функціями	Орієнтована на результат процесу в цілому
Роль внутрішнього контролю	Окрема функція або підрозділ	Інтегрований елемент процесу
Підхід до аудиту	Перевірка окремих ділянок і показників	Аналіз логіки формування інформації та процесів
Виявлення ризиків	Фрагментарне, за функціями	Системне, на рівні процесів
Причини помилок і відхилень	Часто залишаються неочевидними	Чітко простежуються в межах процесу
Аналітична глибина аудиту	Обмежена перевіркою відповідності	Орієнтована на причини та наслідки

Придатність до оптимізації	Низька, зміни мають локальний характер	Висока, можливе комплексне вдосконалення процесів
Зручність для управлінських рішень	Обмежена	Висока, забезпечує прозорість і прогнозованість

Процесно-орієнтована модель не є складною технічною конструкцією. У навчальному контексті її слід сприймати як узагальнене відображення того, як на практиці рухається облікова інформація – від виникнення господарської операції до її перевірки та використання у звітності. Така модель допомагає структурувати знання та побачити причинно-наслідкові зв'язки між окремими етапами діяльності.

У межах процесної моделі обліково-аудиторської діяльності можна виокремити низку ключових елементів, які забезпечують її цілісність і практичну цінність. Першим таким елементом є вхід процесу. В обліку це, як правило, первинні документи, господарські операції або управлінські рішення, які потребують облікового відображення. Саме з них починається формування інформації, що згодом стане об'єктом аудиторської перевірки.

Наступним елементом є ***сукупність дій та операцій,*** які виконуються в межах процесу. До них належать перевірка достовірності первинних даних, їх обробка, відображення в облікових регістрах, узагальнення та підготовка звітної інформації. У процесно-орієнтованій моделі ці дії розглядаються не ізольовано, а як послідовні етапи єдиного процесу. Такий підхід дозволяє зрозуміти, як помилки або недоліки на одному етапі можуть впливати на кінцевий результат.

Важливим елементом процесної моделі є ***контрольні точки.*** Саме на цих етапах здійснюється перевірка правильності виконання операцій, дотримання встановлених процедур та відповідність вимогам законодавства і внутрішніх регламентів. Для обліку це можуть бути процедури внутрішнього контролю, а для аудиту – аналітичні та перевірочні процедури. Наявність таких контрольних точок у моделі дозволяє заздалегідь визначити зони підвищеного ризику та сфокусувати на них увагу аудитора.

Завершальним елементом процесної моделі є ***результат процесу.*** У системі обліку ним виступає сформована облікова інформація або фінансова звітність. У системі аудиту – аудиторські докази, висновки та рекомендації. Важливо, що результат розглядається як логічний наслідок усього процесу, а не як самостійний об'єкт аналізу, відірваний від попередніх етапів.

Процесно-орієнтована модель також дозволяє наочно показати взаємозв'язок між процесами обліку, внутрішнього контролю та аудиту. У практичній діяльності ці елементи часто сприймаються як окремі напрями роботи. Однак з позиції процесного підходу вони є взаємопов'язаними складовими єдиної системи формування та перевірки інформації.

Процеси обліку забезпечують фіксацію та узагальнення господарських операцій. Процеси внутрішнього контролю спрямовані на запобігання помилкам і порушенням у межах цих операцій. Аудит, у свою чергу, оцінює надійність облікових процесів і ефективність системи контролю. У процесно-орієнтованій моделі всі ці елементи розглядаються в єдиному логічному ланцюгу, що дозволяє уникнути дублювання функцій і підвищити прозорість діяльності.

Застосування процесної моделі має важливе значення для систематизації інформації в аудиті. Коли облікові дані представлені у вигляді логічно пов'язаних процесів, аудитору легше зрозуміти, де саме можуть виникати ризики викривлення інформації. Це дозволяє перейти від формальної перевірки окремих документів до аналізу причин і умов виникнення помилок.

Крім того, процесно-орієнтована модель полегшує комунікацію результатів аудиту з керівництвом підприємства. Представлення проблем через призму процесів є більш зрозумілим і наочним, ніж перелік окремих порушень. Керівництво отримує можливість побачити, як саме організована діяльність і які зміни доцільно внести для її вдосконалення.

Процесно-орієнтована модель виступає не лише засобом опису обліково-аудиторської діяльності, а й основою для її аналізу, контролю та подальшої оптимізації. Саме така модель дозволяє поєднати облік, внутрішній контроль та

аудит у цілісну систему, орієнтовану на якість інформації та обґрунтованість управлінських рішень.

Побудова процесно-орієнтованих моделей не є довільною діяльністю. Для того щоб така модель виконувала аналітичну та прикладну функцію, вона має ґрунтуватися на певних методологічних принципах (рис. 2.1). Саме ці принципи забезпечують логічність моделі, її відповідність реальній діяльності підприємства та можливість практичного використання результатів моделювання в обліку, аудиті й управлінні.

Важливо розуміти, що методологічні принципи не ускладнюють моделювання, а навпаки – допомагають уникнути помилок і формального підходу. Дотримання таких принципів дозволяє перетворити процесну модель на інструмент аналізу, а не на абстрактний опис діяльності.

Одним із базових принципів побудови процесно-орієнтованих моделей є ***принцип цілісності.*** Він передбачає, що діяльність організації має розглядатися як єдина система взаємопов'язаних процесів, а не як сукупність окремих, ізольованих дій. У межах цього принципу кожен процес повинен бути логічно пов'язаний з іншими процесами та займати визначене місце в загальній структурі діяльності.

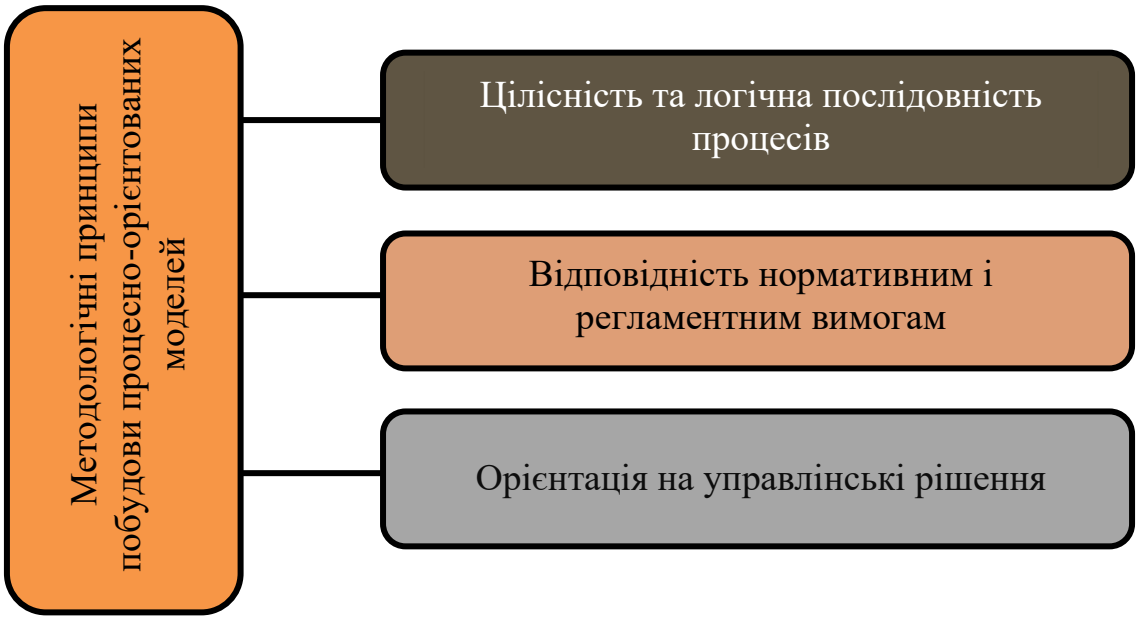


Рис. 2.1. Методологічні принципи побудови процесно-орієнтованих моделей

Для обліку та аудиту це означає, що процес формування облікової інформації не може розглядатися окремо від процесів, які йому передують або слідують за ним. Наприклад, облік витрат пов'язаний з процесами закупівель, виробництва, внутрішнього контролю та формування звітності. Якщо модель відображає лише окремий фрагмент цього ланцюга, вона втрачає цілісність і не дозволяє зробити обґрунтовані висновки.

Логічна послідовність процесів є продовженням принципу цілісності. Вона означає, що всі етапи процесу мають бути впорядковані відповідно до реального порядку виконання робіт. Кожен етап повинен мати чітке місце між попереднім і наступним етапами. Для аудиту це має особливе значення, оскільки дозволяє простежити причинно-наслідкові зв'язки між подіями та результатами. Порушення логічної послідовності в моделі призводить до спотворення уявлення про діяльність. Наприклад, якщо контрольні процедури показані формально або «відірвані» від основних операцій, аудитору складно оцінити їх реальну ефективність. Саме тому принцип цілісності та послідовності є фундаментальним для побудови будь-якої процесно-орієнтованої моделі.

Процесно-орієнтована модель не існує поза нормативним середовищем. Облік і аудит здійснюються в межах чітко визначених законодавчих, нормативних і внутрішніх регламентів. Тому ще одним важливим методологічним принципом є принцип відповідності процесної моделі таким вимогам. У практиці обліку це означає, що модель повинна відображати порядок виконання операцій відповідно до вимог законодавства, стандартів бухгалтерського обліку та внутрішніх положень підприємства. Якщо модель ігнорує ці вимоги або подає процеси у спрощеному вигляді, який не відповідає реальним правилам, вона втрачає прикладну цінність. Для аудиту відповідність нормативним і регламентним вимогам має ще ширше значення. Аудитор оцінює не лише правильність відображення операцій, а й дотримання встановлених процедур. Процесна модель у цьому випадку стає інструментом зіставлення фактичного порядку виконання робіт з нормативно визначеним.

Важливо підкреслити, що цей принцип не обмежує можливості аналізу та вдосконалення процесів. Навпаки, саме зіставлення нормативної моделі з фактичним перебігом процесу дозволяє виявити відхилення, слабкі місця та зони ризику. Для майбутнього аудитора це формує розуміння того, що ***аудит – це не лише перевірка результату, а й аналіз відповідності процесів установленим правилам.***

Процесно-орієнтована модель має не лише описувати діяльність, а й бути корисною для прийняття управлінських рішень. Саме тому важливим методологічним принципом є ***орієнтація моделі на управлінський результат.***

У контексті обліку це означає, що модель повинна допомагати зрозуміти, як формуються показники, які використовуються керівництвом для планування, контролю та оцінювання діяльності. Якщо процесна модель не дозволяє відповісти на питання «чому отримано саме такий результат», вона не виконує своєї управлінської функції. Для аудиту орієнтація на управлінські рішення проявляється в тому, що результати аналізу процесів мають бути зрозумілими та корисними для керівництва. Аудиторські висновки, побудовані на основі процесної моделі, дозволяють не лише зафіксувати порушення, а й обґрунтувати необхідність змін у організації діяльності. Цей принцип також передбачає, що процесна модель повинна бути достатньо зрозумілою для користувачів, які не є фахівцями з моделювання. Керівник підприємства або менеджер має мати можливість на основі моделі побачити проблемні місця та оцінити можливі напрями вдосконалення процесів.

Методологічні принципи побудови процесно-орієнтованих моделей забезпечують цілісність, логічність, відповідність реальній діяльності та практичну цінність. Принцип цілісності та логічної послідовності дозволяє сформувати системне бачення процесів. Принцип відповідності нормативним і регламентним вимогам забезпечує коректність і прикладний характер моделі. Принцип орієнтації на управлінські рішення перетворює процесну модель на інструмент аналізу, контролю та вдосконалення діяльності.

Однією з важливих особливостей процесно-орієнтованого підходу є можливість описувати діяльність організації на різних рівнях деталізації (рис. 2.2). Це означає, що одна й та сама діяльність може бути представлена як у загальному, узагальненому вигляді, так і на рівні окремих дій та операцій. Для обліку та аудиту така багаторівнева логіка має принципове значення, оскільки дозволяє адаптувати модель до конкретних цілей аналізу.

Важливо розуміти, що не існує єдиного правильного рівня опису процесів. Вибір рівня деталізації залежить від того, яке управлінське або аналітичне завдання вирішується. Надмірна деталізація ускладнює сприйняття моделі, тоді як надто загальний опис не дає можливості виявити причини помилок і ризиків. Саме тому в процесному моделюванні зазвичай виокремлюють кілька рівнів опису, кожен з яких виконує власну функцію.

Загальний рівень опису є найвищим рівнем узагальнення процесів. На цьому рівні діяльність підприємства розглядається у вигляді ключових процесів без детального опису окремих операцій. У системі обліку та аудиту до таких процесів можуть належати, наприклад, процес формування фінансової звітності, процес обліку доходів і витрат, процес внутрішнього контролю, процес аудиторської перевірки.

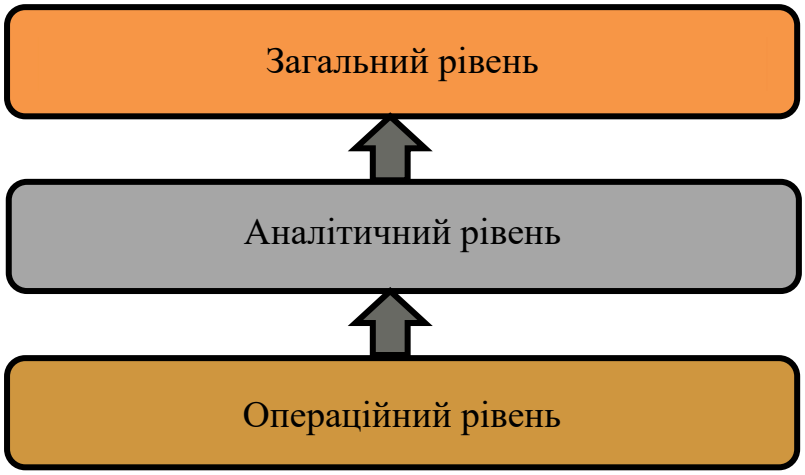


Рис. 2.2. Рівні деталізації опису діяльності організації

Основне завдання загального рівня опису полягає у формуванні цілісного уявлення про структуру діяльності. Саме на цьому рівні стає зрозуміло, які

процеси існують в організації, як вони пов’язані між собою та яке місце займають у загальній системі управління.

Для аудиту загальний рівень опису дозволяє визначити основні напрями перевірки та окреслити межі аудиторського дослідження. Аудитор отримує уявлення про те, які процеси є ключовими для формування фінансової інформації і які з них можуть бути пов’язані з підвищеними ризиками. Водночас на цьому рівні ще неможливо оцінити конкретні причини можливих відхилень або помилок.

У межах аналітичного рівня процес розкладається на окремі етапи або підпроцеси. Наприклад, процес обліку запасів може включати етапи надходження, зберігання, списання та інвентаризації. Такий опис дозволяє виявити, на яких саме етапах виникають ризики помилок або порушень.

Для аудиту аналітичний рівень є особливо важливим, оскільки саме на ньому формується розуміння логіки процесу. Аудитор може оцінити, наскільки узгодженими є дії різних учасників процесу, чи існують дублювання або прогалини, а також чи відповідає фактичний перебіг процесу встановленим регламентам.

Операційний рівень є найбільш детальним рівнем опису процесів. На цьому рівні відображаються конкретні дії, операції та процедури, які виконуються в межах процесу. У системі обліку це можуть бути оформлення первинних документів, проведення записів у регістрах, виконання контрольних перевірок. В аудиті – це конкретні аудиторські процедури, тести контролю та аналітичні перевірки.

Для аудиторської діяльності операційний рівень має особливе значення, оскільки саме на ньому здійснюється практична перевірка. Аудитор працює з конкретними операціями, документами та записами, оцінюючи їхню правильність і відповідність вимогам. Процесно-орієнтована модель на цьому рівні допомагає систематизувати аудиторські процедури та пов’язати їх з відповідними етапами процесу.

Одним із перших етапів аудиторської перевірки є ідентифікація ризиків. У традиційному підході ризики часто пов’язуються з окремими ділянками обліку або показниками звітності. Однак такий підхід не завжди дозволяє побачити джерела ризиків і зрозуміти, на якому етапі діяльності вони виникають.

Процесно-орієнтована модель дозволяє розглядати ризики як властивість процесів, а не окремих функцій. Це означає, що увага аудитора зосереджується на логіці виконання процесу, послідовності дій і взаємодії між учасниками. Саме в цих точках найчастіше виникають умови для помилок, викривлень або порушень. Наприклад, ризик викривлення інформації щодо запасів може бути пов’язаний не лише з неправильним відображенням операцій у бухгалтерських регістрах, а й з недоліками у процесі приймання, зберігання або інвентаризації. Процесна модель дозволяє аудитору побачити весь ланцюг дій і визначити, на якому етапі ризик є найбільш імовірним. Виявлення відхилень у процесі аудиту є лише першим кроком. Не менш важливим завданням є встановлення причин цих відхилень. Саме на цьому етапі процесно-орієнтовані моделі демонструють свою аналітичну цінність.

У межах функціонального підходу відхилення часто розглядаються як окремі помилки або порушення, пов’язані з діяльністю конкретного підрозділу або виконавця. Процесний підхід дозволяє подивитися на проблему ширше і з’ясувати, чи є відхилення наслідком системних недоліків у організації процесу.

Процесна модель дає змогу простежити, як інформація проходить через усі етапи процесу і де саме виникає збій. Наприклад, затримка у формуванні звітності може бути наслідком неефективної взаємодії між підрозділами, нечіткого розподілу відповідальності або відсутності контрольних процедур на проміжних етапах. Без процесної моделі такі причини залишаються неочевидними.

Для аудитора аналіз причин відхилень має принципове значення, оскільки саме він дозволяє перейти від констатації фактів до формування рекомендацій. Процесно-орієнтована модель у цьому випадку виступає інструментом

пояснення, який допомагає обґрунтувати, чому саме виникла проблема і які зміни доцільно запропонувати.

Аудиторські висновки мають бути не лише правильними з формальної точки зору, а й обґрунтованими та зрозумілими для користувачів. Процесно-орієнтовані моделі суттєво підвищують якість таких висновків, оскільки забезпечують їх логічну основу.

У результаті ***аудиторське судження,*** сформоване на основі процесно-орієнтованої моделі, має більш глибокий аналітичний характер. Воно ґрунтується не лише на перевірці відповідності, а й на розумінні логіки діяльності підприємства, що відповідає сучасним вимогам до професії аудитора.

Аналіз процесно-орієнтованих моделей у межах обліку та аудиту дозволяє зробити узагальнюючий висновок про їх системну роль у сучасній діяльності підприємств. Такі моделі виступають не окремим аналітичним інструментом і не допоміжним елементом аудиту, а основою цілісного бачення того, як формується облікова інформація, як здійснюється контроль та як приймаються управлінські рішення.

Процесно-орієнтований підхід дозволяє об’єднати облік, внутрішній контроль і аудит у межах єдиної логіки діяльності. ***Облік*** у цьому випадку розглядається як процес формування інформації, ***внутрішній контроль*** – як вбудований механізм запобігання помилкам, а ***аудит*** – як інструмент оцінювання надійності та ефективності всієї системи. Саме процесна модель забезпечує зв’язок між цими елементами та дозволяє розглядати їх не ізольовано, а як складові єдиного управлінського механізму.

Для майбутніх аудиторів таке системне бачення має принципове значення. Воно формує розуміння того, що якість аудиторських висновків безпосередньо залежить від глибини аналізу процесів, а не лише від обсягу перевірених документів. Процесно-орієнтовані моделі дозволяють перейти від фіксації окремих фактів до аналізу причин, умов і наслідків господарських операцій, що відповідає сучасним вимогам до професійного аудиту.

Водночас процесне моделювання не є самоціллю. Його основне призначення полягає у створенні передумов для вдосконалення діяльності підприємства. Побудова процесної моделі дозволяє виявити слабкі місця, неузгодженості та дублювання функцій, але не вирішує проблем автоматично. Саме на цьому етапі виникає логічна необхідність переходу від опису та аналізу процесів до їх цілеспрямованого вдосконалення.

Моделювання процесів і їх оптимізація є взаємопов’язаними етапами єдиного управлінського підходу. Процесна модель створює інформаційну основу для прийняття рішень, тоді як оптимізація спрямована на підвищення ефективності, надійності та прозорості діяльності. Без попереднього моделювання оптимізаційні заходи носять фрагментарний характер і часто не дають очікуваного результату.

З методологічної точки зору саме процесно-орієнтовані моделі забезпечують перехід від аналізу стану обліково-аудиторської діяльності до її цілеспрямованого розвитку.

2.2 Інструменти аналізу та оптимізації обліково-аудиторських процесів

Процесно-орієнтований підхід не обмежується лише описом діяльності підприємства у вигляді моделей. Опис процесів є необхідним, але недостатнім етапом роботи. Для того щоб процесна модель мала практичну цінність, вона повинна стати основою для аналізу. Саме на цьому етапі виникає потреба в застосуванні спеціальних інструментів, які дозволяють перейти від фіксації процесів до їх осмислення та оцінювання.

Перехід від опису процесів до їх аналізу означає зміну фокусу уваги. Якщо на етапі моделювання головним завданням є зрозуміти, як організована діяльність і які етапи вона включає, то на етапі аналізу ключовими стають питання ефективності, надійності та доцільності такої організації. Аналіз дозволяє виявити, наскільки існуючі процеси відповідають цілям підприємства, вимогам законодавства та потребам управління.

У практиці обліку та аудиту цей перехід має особливе значення. Облікові процеси можуть бути формально правильно описані, але водночас містити внутрішні суперечності, дублювання дій або надмірні контрольні процедури. Без застосування аналітичних інструментів такі проблеми залишаються непомітними. Саме аналіз дозволяє побачити не лише структуру процесу, а й його реальну якість.

Аналітичні інструменти в процесно-орієнтованому підході виконують роль засобів інтерпретації процесної моделі. Вони допомагають перетворити схематичне або описове представлення діяльності на основу для висновків і рішень. Важливо усвідомити, що інструменти аналізу не є універсальними або стандартними для всіх ситуацій. Їх вибір залежить від цілей перевірки, характеру процесів і рівня деталізації моделі.

У роботі аудитора аналітичні інструменти займають проміжне місце між процесною моделлю та аудиторським судженням. Процесна модель відповідає на питання «як організована діяльність», тоді як аналітичні інструменти

дозволяють відповісти на питання «наскільки ефективно та надійно вона організована?». Саме через застосування таких інструментів аудитор переходить від спостереження до оцінювання.

Важливо підкреслити, що аналітичні інструменти в аудиті не обмежуються лише перевірочними процедурами. Вони охоплюють засоби порівняння, узагальнення, групування та інтерпретації інформації, що дозволяє оцінювати процеси ще до детальної перевірки первинних документів. Зокрема, аналіз тривалості виконання етапів, оцінка кількості контрольних точок і співвідношення між обсягом операцій та використаними ресурсами дають змогу сформувати попередні висновки щодо ефективності й надійності організації процесу (рис. 2.3).

Рис. 2.3. Аналітичні інструменти оцінювання ефективності обліково-аудиторських процесів

Зв’язок між процесною моделлю та вибором інструментів аналізу є принциповим. Процесна модель визначає, які саме аспекти діяльності можуть і повинні бути проаналізовані. Якщо модель побудована на загальному рівні, інструменти аналізу також матимуть узагальнений характер і використовуватимуться для попередньої оцінки ризиків. Якщо ж модель

деталізована до рівня окремих етапів і операцій, з'являється можливість застосування більш точних і глибоких аналітичних інструментів.

Для аудитора це означає, що інструменти аналізу не застосовуються ізольовано від процесної моделі. Їх ефективність безпосередньо залежить від того, наскільки коректно та повно відображена діяльність у моделі. Неповна або формальна модель обмежує можливості аналізу і знижує якість аудиторських висновків.

Роль інструментів аналізу в процесно-орієнтованому підході полягає у забезпеченні переходу від опису діяльності до її оцінювання. Вони дозволяють аудитору системно аналізувати процеси, виявляти проблемні зони та формувати обґрунтовані висновки.

У сучасних умовах аналіз обліково-аудиторських процесів практично неможливий без використання програмних засобів. Саме вони формують середовище, в якому процеси фіксуються, виконуються та залишають цифрові сліди, що згодом стають основою для аналітичної роботи аудитора. Важливо підкреслити, що мова йде не про окремі програми як технічні рішення, а про цілі класи програмних засобів, кожен з яких відображає певну частину діяльності підприємства (рис. 2.4).

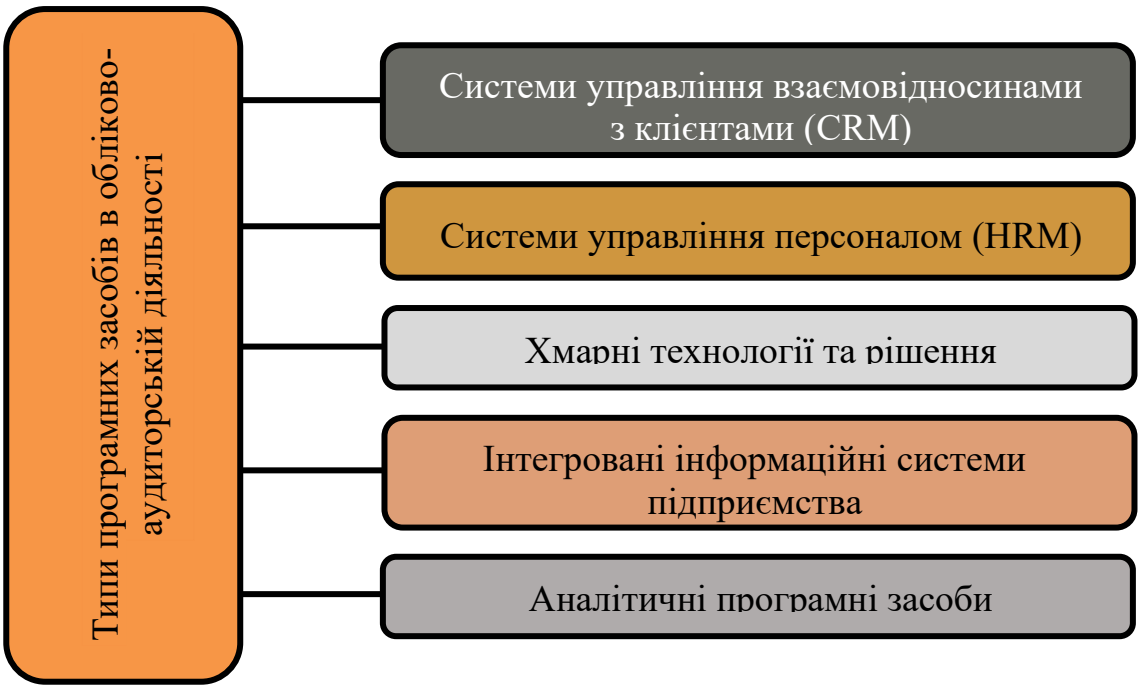


Рис. 2.4. Типи програмних засобів в обліково-аудиторській діяльності

Однією з найбільш поширених груп програмних засобів є системи управління взаємовідносинами з клієнтами. Такі системи використовуються для фіксації операцій, пов'язаних з продажами, договорами, рахунками, оплатами та комунікаціями з контрагентами. У контексті обліку вони формують значну частину первинної інформації щодо доходів та дебіторської заборгованості. Для аудитора ці системи є важливими не як інструмент маркетингу, а як джерело даних про реальний перебіг процесів реалізації. Аналіз даних із таких систем дозволяє оцінити повноту відображення доходів, узгодженість операцій з умовами договорів та логіку формування фінансових показників.

Іншою важливою групою програмних засобів є системи управління персоналом. У них зосереджується інформація про трудові відносини, нарахування заробітної плати, облік робочого часу, преміювання та інші виплати. З позиції процесного підходу такі системи відображають не лише кадрові процеси, а й значну частину витрат підприємства. Для аудитора вони дозволяють простежити, як формуються витрати на персонал, чи узгоджені між собою дані обліку, кадрових рішень і фактичних виплат, а також чи працюють контрольні механізми в цих процесах.

Окреме місце в аналізі обліково-аудиторських процесів займають хмарні технології. Їх роль полягає не стільки у зберіганні інформації, скільки у зміні логіки доступу до даних і виконання процесів. У хмарному середовищі облік, документообіг і контроль часто здійснюються в режимі реального часу. Це створює для аудитора нові можливості, але водночас і нові виклики. З одного боку, зростає прозорість процесів і доступність інформації. З іншого – виникає потреба оцінювати надійність доступів, розмежування прав користувачів і збереження даних. У процесному аналізі хмарні технології розглядаються як середовище, в якому відбувається більшість операцій, а не як окремий технічний інструмент.

Важливу роль у дослідженні обліково-аудиторських процесів відіграють також інтегровані інформаційні системи підприємства. Вони поєднують облік, управління ресурсами, логістику, виробництво та фінанси в межах єдиної

платформи. Для процесного підходу це має принципове значення, оскільки дозволяє аналізувати наскрізні процеси без розривів між підрозділами. Аудитор у такому середовищі може простежити шлях операції від її виникнення до відображення у фінансовій звітності, що суттєво підвищує якість аналізу.

Окрім систем, які безпосередньо підтримують виконання облікових процесів, дедалі більшого значення набувають аналітичні програмні засоби. Вони не створюють первинні дані, але дозволяють їх узагальнювати, візуалізувати та інтерпретувати. Саме через такі засоби аудитор отримує можливість працювати з великими обсягами інформації, виявляти закономірності та відхилення, які не помітні під час перевірки окремих операцій. У процесному аналізі ці інструменти виконують роль містка між даними та аудиторським судженням.

Важливо наголосити, що жоден із зазначених типів програмних засобів не використовується аудиторами ізольовано. Процесний підхід передбачає їх поєднання в єдиній аналітичній логіці. Дані з систем управління клієнтами, персоналом, ресурсами та фінансами розглядаються як елементи одного процесного середовища. Саме в такому середовищі стає можливим комплексний аналіз обліково-аудиторських процесів.

Ідентифікація ризиків є одним із центральних завдань аудиту, незалежно від його виду та об’єкта перевірки. У процесно-орієнтованому підході це завдання набуває особливого змісту, оскільки ризики розглядаються не як випадкові помилки або окремі порушення, а як наслідок організації процесів. Саме тому інструменти аналізу процесів стають основою для виявлення ризиків і визначення так званих вузьких місць у діяльності підприємства.

У межах процесного підходу ризик пов’язується з певним етапом процесу, його логікою, послідовністю дій або умовами виконання. Це означає, що аудитор аналізує не лише результат облікової операції, а й шлях, яким цей результат був отриманий. Такий підхід дозволяє перейти від поверхневого аналізу до розуміння внутрішніх причин виникнення ризиків.

Аналіз ризиків у межах процесів обліку та аудиту ґрунтується на зіставленні нормативної моделі процесу з його фактичним виконанням. Нормативна модель відображає, як процес має бути організований відповідно до законодавства, внутрішніх регламентів і встановлених процедур. Фактичне виконання процесу фіксується в інформаційних системах і проявляється у даних обліку, журналах подій, документах і результатах контролю. Саме розбіжність між цими двома станами є джерелом аудиторського ризику.

Процесний аналіз дозволяє аудитору побачити, на яких етапах виникають найбільші відхилення. Це можуть бути етапи, де відсутній належний контроль, де зосереджено надмірну кількість операцій або де відповідальність розподілена нечітко. У таких місцях зростає ймовірність помилок, несвоєчасного відображення операцій або навмисних викривлень інформації. Особливу увагу в процесному аналізі приділяють так званим вузьким місцям. ***Вузьке місце*** – це етап процесу, який обмежує його ефективність або створює умови для накопичення помилок і затримок.

У контексті обліку такими етапами можуть бути:

- *погодження документів;*
- *ручне введення даних;*
- *перенесення інформації між різними системами;*
- *виконання контрольних процедур після завершення операції.*

Виявлення вузьких місць можливе лише за умови аналізу процесу в цілому. Якщо аудитор працює лише з окремими документами, він може зафіксувати наслідки проблеми, але не її причину. Процесно-орієнтований аналіз дозволяє простежити, як затримка або помилка на одному етапі впливає на всі подальші дії та зрештою відображається у фінансовій звітності.

Інструменти аналізу, реалізовані через програмні засоби, значно підвищують ефективність виявлення таких проблем. Вони дозволяють аналізувати не окремі випадки, а масиви даних за певний період. Це дає можливість виявляти повторювані відхилення, типові помилки або системні затримки, які не помітні під час вибіркової перевірки.

Для аудитора важливо усвідомлювати, що не кожне відхилення є порушенням, але кожне відхилення є сигналом. Процесний аналіз не замінює професійне судження, але створює основу для його формування. Саме на цьому етапі аудитор визначає, які ризики є суттєвими, а які мають локальний характер і не впливають на достовірність фінансової інформації.

Значення процесного аналізу для управління ризиками полягає в тому, що він дозволяє перейти від реактивного до проактивного підходу. Замість того щоб виявляти помилки після їх виникнення, підприємство отримує можливість усувати причини ризиків на рівні організації процесів. Для аудиту це означає зміну ролі – від контролюючої до аналітично-консультативної.

Процесно-орієнтовані інструменти ідентифікації ризиків також сприяють підвищенню якості управлінських рішень. Інформація про ризики, прив'язані до конкретних процесів і етапів, є більш зрозумілою для керівництва, ніж загальні зауваження щодо окремих показників. Це дозволяє спрямовувати ресурси на вдосконалення саме тих ділянок діяльності, які мають найбільший вплив на результат.

Для майбутніх аудиторів опанування процесного підходу до ідентифікації ризиків формує системне професійне мислення. Воно дозволяє бачити діяльність підприємства як взаємопов'язану систему, у якій ризики виникають не випадково, а як наслідок конкретних управлінських і організаційних рішень.

Інструменти ідентифікації ризиків і вузьких місць у процесах є ключовим елементом процесно-орієнтованого аналізу в обліку та аудиті, оскільки дають змогу пояснити причини відхилень і підвищити обґрунтованість аудиторських висновків. Для практичного застосування такі інструменти розглядають як послідовний алгоритм робіт: від збирання процесних даних і їх підготовки – до виконання аналітичних процедур та отримання управлінських результатів (рис. 2.5).

Оптимізація обліково-аудиторських процесів є логічним продовженням їх аналізу. Якщо на попередніх етапах увага зосереджується на описі процесів, виявленні ризиків і вузьких місць, то оптимізація спрямована на практичне

вдосконалення діяльності. Важливо підкреслити, що в контексті обліку та аудиту оптимізація не означає спрощення за будь-яку ціну. Йдеться про досягнення такого стану процесів, за якого вони є ефективними, контрольованими та такими, що відповідають установленим вимогам.

У сфері обліку та аудиту оптимізація має специфічний зміст. На відміну від виробничих або логістичних процесів, де основним критерієм часто виступає швидкість або зменшення витрат, обліково-аудиторські процеси повинні забезпечувати насамперед достовірність інформації та її відповідність нормативним вимогам. Тому оптимізація тут завжди пов'язана з пошуком балансу між ефективністю виконання операцій і збереженням належного рівня контролю.

Рис. 2.5. Алгоритм застосування інструментів ідентифікації ризиків і вузьких місць у процесно-орієнтованому аудиті

Поняття оптимізації в цьому контексті розглядається як цілеспрямована зміна процесів на основі результатів аналізу з метою підвищення їх якості. Така зміна може стосуватися послідовності виконання дій, розподілу відповідальності, використання програмних засобів або організації контрольних процедур. Для аудитора важливо розуміти, що оптимізація не є разовою дією. Вона розглядається як безперервний процес удосконалення, який спирається на регулярний аналіз і переоцінку процесів.

Інструменти оптимізації обліково-аудиторських процесів ґрунтуються на результатах процесного аналізу. Саме процесна модель дозволяє визначити, які етапи є надмірно складними, де виникають затримки або дублювання

функцій, а де контроль є формальним і не виконує своєї захисної ролі. Без такого аналізу будь-які оптимізаційні заходи мають випадковий характер і можуть навіть погіршити ситуацію.

Одним із напрямів оптимізації є впорядкування послідовності виконання процесів. У багатьох організаціях облікові операції історично формуються як набір окремих дій, які виконуються за звичкою, а не за логікою процесу. Оптимізація в цьому випадку полягає у перегляді послідовності дій і усуненні зайвих або дублюючих етапів. Для аудитора важливо оцінити, чи така зміна не створює додаткових ризиків і чи зберігається контроль на ключових етапах.

Іншим важливим напрямом є вдосконалення розподілу відповідальності в межах процесів. Процесний аналіз часто виявляє ситуації, коли відповідальність за виконання або контроль процесу розмита між кількома підрозділами або, навпаки, зосереджена в одних руках. Оптимізація в цьому випадку передбачає чітке визначення ролей і повноважень, що знижує ризик помилок і підвищує прозорість процесів.

Суттєву роль в оптимізації відіграють програмні засоби. Вони дозволяють автоматизувати окремі етапи процесів, зменшити частку ручних операцій і забезпечити своєчасний контроль. Проте використання програмних інструментів саме по собі не гарантує оптимізації. Якщо цифрове рішення впроваджується без урахування процесної логіки, воно лише відтворює наявні проблеми в електронному вигляді. Саме тому оптимізація повинна починатися з аналізу процесів, а вже потім переходити до вибору або налаштування програмних засобів.

Особливу увагу в обліково-аудиторських процесах слід приділяти балансу між ефективністю, контролем і дотриманням вимог. Надмірне прагнення до скорочення часу або зменшення кількості процедур може призвести до ослаблення контролю і зростання ризиків. Водночас надмірна кількість контрольних дій уповільнює процеси, створює додаткове навантаження на персонал і знижує їхню ефективність.

Оптимізація в цьому випадку полягає у визначенні тих контрольних процедур, які є справді критичними для забезпечення достовірності інформації, і відмові від формальних або дублюючих перевірок. Процесно-орієнтований підхід дозволяє аудитору оцінити не кількість контролів, а їхнє місце в логіці процесу та вплив на кінцевий результат.

Для майбутніх аудиторів розуміння інструментів оптимізації є важливим етапом професійного становлення. Воно формує уявлення про аудит як про діяльність, спрямовану не лише на виявлення недоліків, а й на створення умов для підвищення ефективності та прозорості діяльності підприємства.

Інструменти оптимізації обліково-аудиторських процесів базуються на процесному аналізі, використовують можливості програмних засобів і спрямовані на досягнення балансу між ефективністю, контролем і дотриманням вимог. Саме такий підхід забезпечує сталий розвиток системи обліку та аудиту і підвищує цінність аудиторської діяльності для управління підприємством (рис. 2.6).

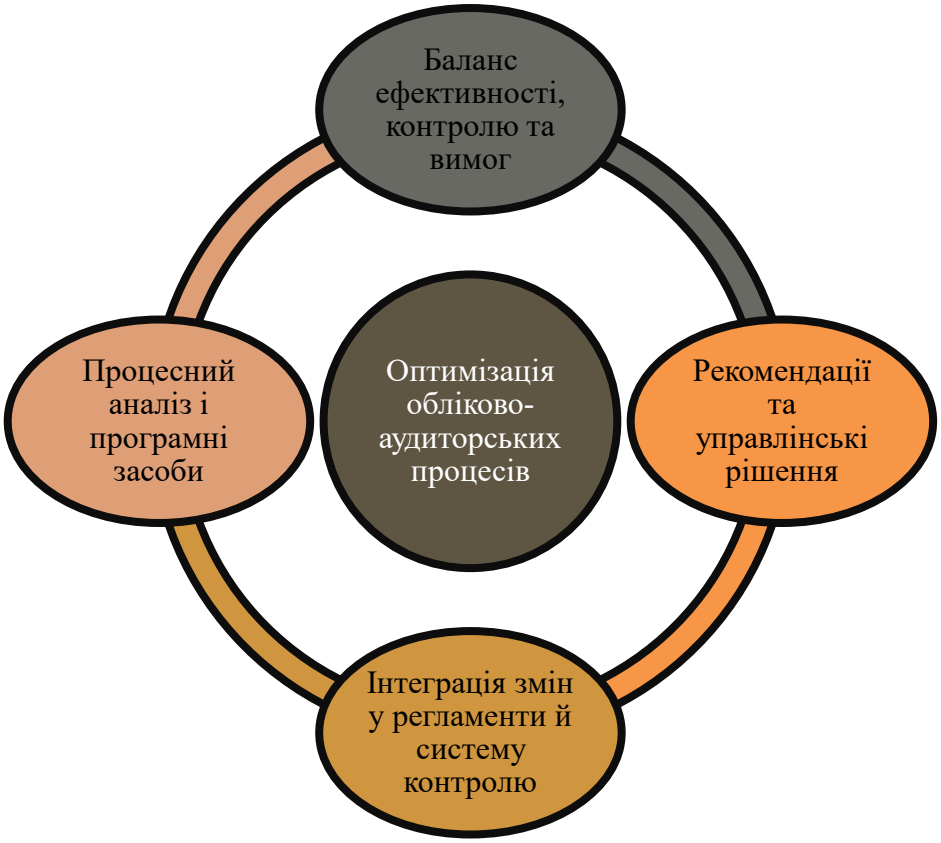


Рис. 2.6. Ключові складові оптимізації обліково-аудиторських процесів на основі процесного аналізу

Результати процесного аналізу мають практичну цінність лише тоді, коли вони трансформуються у конкретні дії та управлінські рішення. У практиці аудиту це насамперед проявляється у формуванні рекомендацій, спрямованих на вдосконалення обліково-аудиторських процесів. Такі рекомендації ґрунтуються не на окремих виявлених помилках, а на системному розумінні того, як організована діяльність і які саме елементи процесів потребують змін.

Формування рекомендацій на основі процесного аналізу передбачає перехід від опису проблем до пояснення їх причин. Аудитор, спираючись на результати аналізу, може аргументовано показати, які особливості організації процесу призводять до ризиків, затримок або зниження якості облікової інформації. У такому випадку рекомендації мають не формальний характер, а безпосередньо пов'язані з логікою виконання процесів. Це підвищує їхню практичну значущість і спрощує сприйняття для управлінського персоналу.

Важливим аспектом використання результатів аналізу є інтеграція оптимізаційних рішень у систему обліку та контролю. Оптимізація процесів не може розглядатися як окремий проєкт, відірваний від повсякденної діяльності підприємства. Зміни мають бути закріплені у внутрішніх регламентах, налаштуваннях програмних засобів, розподілі відповідальності та контрольних процедурах. Лише в такому разі результати аналізу стають частиною стабільно функціонуючої системи.

Для аудитора інтеграція результатів оптимізації означає оцінку того, наскільки запропоновані зміни узгоджуються з нормативними вимогами і не створюють нових ризиків. Процесний підхід дозволяє здійснювати таку оцінку не інтуїтивно, а на основі чіткого розуміння впливу змін на всі етапи процесу. Це особливо важливо в обліково-аудиторській діяльності, де будь-яке спрощення має бути збалансоване належним рівнем контролю.

Роль аудитора у впровадженні змін у межах процесного підходу поступово трансформується. Аудитор перестає бути лише стороннім контролером і набуває рис аналітичного партнера управління. Його завдання полягає не у прямому управлінні процесами, а у наданні обґрунтованої інформації, яка дозволяє

керівництву приймати зважені рішення щодо вдосконалення діяльності. Саме в цьому проявляється ***сучасне розуміння професійної ролі аудитора.***

Для майбутніх аудиторів важливо усвідомити, що використання результатів процесного аналізу вимагає не лише технічних знань, а й уміння комунікувати, пояснювати та аргументувати. Аудиторське судження, підкріплене процесною логікою, має значно більший вплив на управлінські рішення, ніж перелік окремих зауважень або формальних порушень.

2.3 Інтеграція результатів моделювання бізнес-процесів у систему управлінських рішень обліку та аудиту

У сучасній системі управління підприємством дедалі більшого значення набуває здатність приймати рішення на основі цілісної та узгодженої інформації. Управлінські рішення вже не можуть ґрунтуватися виключно на підсумкових показниках звітності або інтуїтивних оцінках керівництва. Вони потребують розуміння того, як саме формується результат, які процеси на нього впливають і де виникають ключові ризики. Саме в цьому контексті результати процесного моделювання займають важливе місце як аналітична основа управління.

Результати процесного моделювання відображають не лише структуру діяльності підприємства, а й логіку взаємодії між окремими етапами обліку, контролю та аудиту. На відміну від традиційних аналітичних матеріалів, які часто фокусуються на кінцевих показниках, процесні моделі дозволяють побачити шлях формування цих показників. Для управління це має принципове значення, оскільки рішення приймаються не лише щодо результатів, а й щодо способів їх досягнення.

Управлінські рішення, що спираються на результати процесного моделювання, мають більш обґрунтований характер. Керівництво отримує можливість оцінювати не лише те, що відбулося, а й чому це відбулося. Наприклад, замість загального висновку про зростання витрат з'являється розуміння того, на яких етапах процесу вони формуються, де виникають затримки або неефективні дії, і які управлінські впливи можуть змінити ситуацію.

Важливою особливістю процесного моделювання є його тісний зв'язок з обліковою інформацією. Облік у цьому випадку перестає бути лише інструментом фіксації фактів і перетворюється на джерело даних для аналізу процесів. Процесна модель дозволяє структурувати облікову інформацію відповідно до логіки виконання діяльності, а не лише за рахунками або статтями

звітності. Це створює передумови для більш глибокого аналізу та використання облікових даних у процесі прийняття рішень.

Зв'язок між процесною моделлю, обліковою інформацією та управлінськими рішеннями проявляється у тому, що кожне управлінське рішення може бути співвіднесене з конкретними процесами та етапами їх виконання. Наприклад, рішення про зміну регламенту обліку або впровадження нового програмного засобу оцінюється не абстрактно, а з позиції його впливу на перебіг процесів, які формують облікову інформацію. Такий підхід зменшує ризик непродуманих управлінських рішень і підвищує їхню результативність.

Особливу роль у трансформації результатів процесного моделювання в управлінські рішення відіграє аудит. Саме аудит виступає своєрідним перекладачем між аналітичними результатами та управлінською практикою. Аудитор, аналізуючи процеси, не лише виявляє проблеми або ризики, а й оцінює їх значущість для діяльності підприємства та можливі наслідки для фінансової інформації.

У процесно-орієнтованому підході аудит виходить за межі формальної перевірки відповідності. Він забезпечує інтерпретацію результатів моделювання з урахуванням нормативних вимог, управлінських цілей і реальних умов функціонування підприємства. Саме завдяки аудиту результати процесного аналізу набувають прикладного значення та можуть бути використані для прийняття управлінських рішень.

Для управління це означає, що аудиторські висновки, сформовані на основі процесного моделювання, мають значно вищу цінність, ніж традиційні зауваження щодо окремих порушень. Вони дозволяють керівництву побачити системні проблеми, оцінити альтернативні варіанти дій і приймати рішення, спрямовані на довгострокове вдосконалення діяльності.

У практиці моделювання бізнес-процесів використовується кілька основних методологій, кожна з яких відрізняється рівнем формалізації, логікою опису процесів і сферою застосування (рис. 2.7). Для обліку та аудиту важливо розуміти ці відмінності, оскільки вибір методології впливає на глибину аналізу,

зручність використання моделей і можливість інтеграції результатів у систему управлінських рішень.

BPMN (Business Process Model and Notation) – це стандартизована графічна нотація для моделювання бізнес-процесів, призначена для наочного та формалізованого опису послідовності дій, подій, точок прийняття рішень і ролей учасників процесу з метою однакового розуміння процесів різними групами користувачів – управлінцями, аналітиками, бухгалтерами та аудиторами.

BPMN є найбільш універсальною та поширеною методологією процесного моделювання. Вона орієнтована на опис послідовності дій, подій, точок прийняття рішень і ролей учасників процесу. BPMN добре підходить для моделювання облікових і аудиторських процесів, оскільки дозволяє наочно показати формування облікової інформації, місця контролю та виконання аудиторських процедур. Типові програмні засоби: Bizagi Modeler, Camunda Modeler, Signavio, ARIS, Draw.io (з підтримкою BPMN).

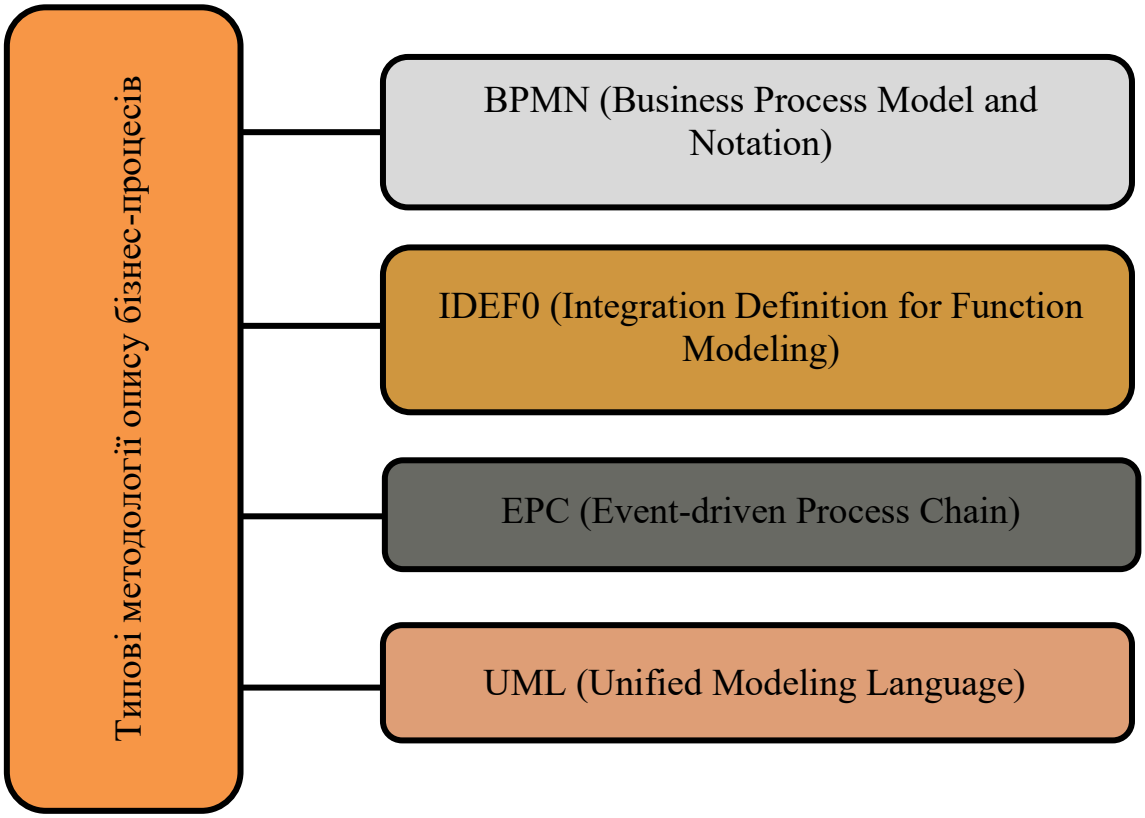


Рис. 2.7. Типові методології опису бізнес-процесів

IDEF0 (Integration Definition for Function Modeling) – це методологія функціонального моделювання, призначена для опису діяльності організації у вигляді ієрархічної системи функцій, які перетворюють вхідні ресурси на вихідні результати за наявності керуючих впливів і механізмів виконання.

IDEF0 використовується для функціонально-процесного опису діяльності. Основна увага в цій методології приділяється не послідовності дій, а зв'язку між функціями, ресурсами, вхідною та вихідною інформацією. Для обліку та аудиту IDEF0 доцільна на етапі узагальненого аналізу діяльності, коли потрібно показати, які функції виконуються і які ресурси вони використовують. Типові програмні засоби: BPwin, ERwin Process Modeler, AllFusion Process Modeler.

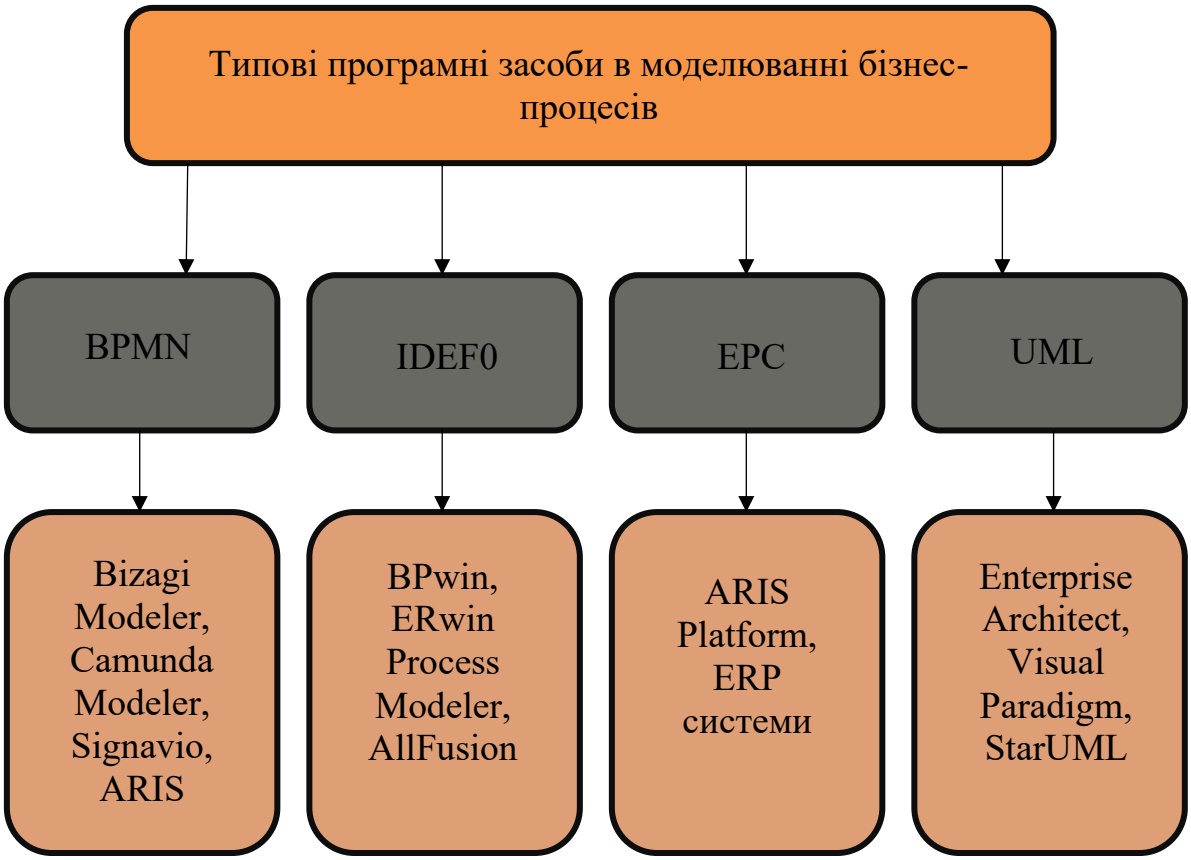


Рис. 2.8. Типові програмні засоби в моделюванні бізнес-процесів

EPC (Event-driven Process Chain, подієво-орієнтований ланцюг процесів) – це методологія моделювання бізнес-процесів, яка використовується для опису діяльності організації у вигляді послідовності подій та функцій, де події визначають умови початку або завершення процесу, а функції відображають дії, що виконуються в межах цього процесу.

EPC ґрунтується на логіці «подія → функція → подія» і часто використовується для опису процесів у корпоративних інформаційних системах. EPC дозволяє поєднати події, функції та організаційні одиниці, що робить її зручною для аналізу взаємодії обліку, контролю та управління. Типові програмні засоби: ARIS Platform, а також окремі корпоративні модулі ERP-систем.

UML (Unified Modeling Language, уніфікована мова моделювання) – це стандартизована мова графічного моделювання, призначена для опису структури, поведінки та взаємодії елементів інформаційних систем.

UML застосовується переважно для моделювання інформаційних систем, але окремі її діаграми можуть використовуватися для опису процесів. В обліку та аудиті UML має допоміжне значення і використовується здебільшого для пояснення логіки автоматизованих процесів і взаємодії між системами. Типові програмні засоби: Enterprise Architect, Visual Paradigm, StarUML.

У системі сучасного управління аудит поступово виходить за межі функції перевірки та контролю. Його результати дедалі частіше розглядаються як важливий інформаційний ресурс для прийняття управлінських рішень. Особливої ваги це набуває в умовах використання процесно-орієнтованих моделей, коли аудиторські висновки формуються не лише на основі фактів порушень, а з урахуванням логіки виконання процесів і причин виникнення відхилень.

Аудиторські висновки в такому підході перестають бути ізольованим документом. Вони стають елементом управлінської інформації, що доповнює облікові дані та результати процесного аналізу. Для керівництва підприємства цінність аудиторської інформації полягає не лише в оцінці відповідності, а й у

можливості зрозуміти, які саме процеси потребують змін і чому ці зміни є доцільними.

У процесно-орієнтованому середовищі аудиторські висновки тісно пов’язані з процесними моделями, зокрема з тими, що створюються за допомогою спеціалізованих програм для моделювання бізнес-процесів. Коли результати аудиту співвідносяться з конкретними етапами процесу, вони стають більш зрозумілими для управлінців. Наприклад, зауваження аудитора щодо ризиків або неефективності можуть бути безпосередньо пов’язані з елементами BPMN-моделі, що наочно демонструє, де саме виникає проблема.

Використання процесних результатів у внутрішньому управлінні дозволяє інтегрувати аудит у загальну систему прийняття рішень. Процесні моделі, доповнені аудиторськими оцінками, можуть використовуватися під час перегляду регламентів, оптимізації процедур обліку, налаштування контрольних механізмів і впровадження змін у програмних системах. У такому вигляді аудит перестає бути реакцією на помилки і перетворюється на інструмент підтримки розвитку організації.

Для внутрішнього управління важливо, що результати аудиту, подані через призму процесів, дозволяють уникнути фрагментарних рішень. Замість усунення окремих недоліків керівництво отримує можливість впливати на першопричини проблем.

Роль аудиту у підтримці стратегічних і операційних рішень у такому підході суттєво розширюється. На операційному рівні аудит допомагає вдосконалювати поточні процеси, підвищувати їх ефективність і знижувати ризики. На стратегічному рівні результати процесного аудиту можуть використовуватися для оцінювання доцільності змін у бізнес-моделі, вибору напрямів цифрової трансформації або перегляду системи управління (рис. 2.9).

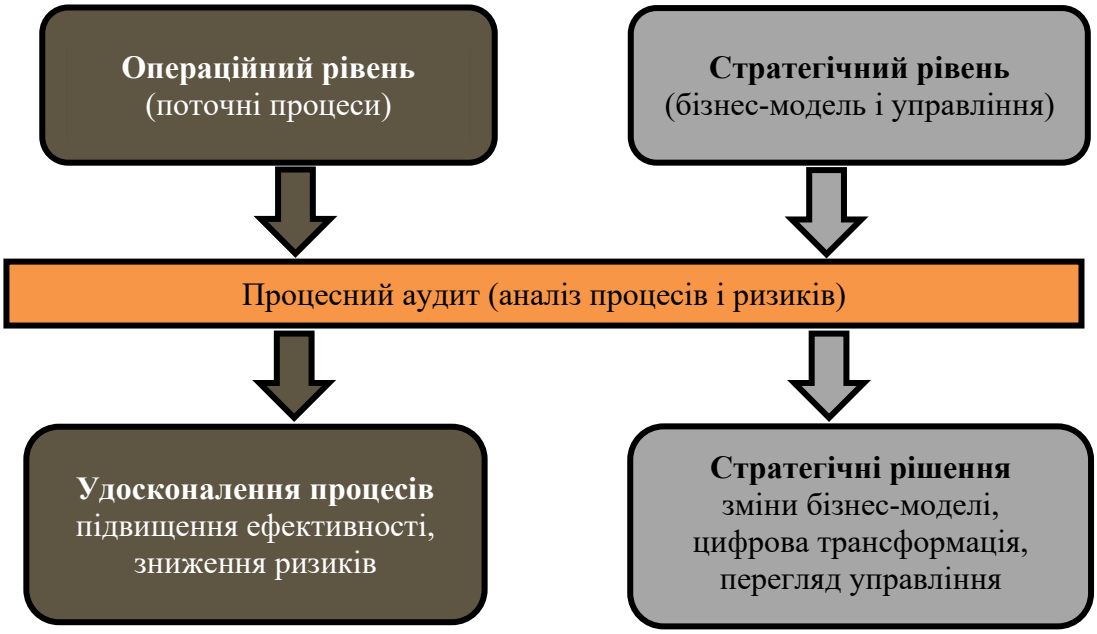


Рис. 2.9. Роль процесного аудиту в підтримці операційних і стратегічних управлінських рішень

Використання програм для моделювання бізнес-процесів підсилює цю роль аудиту. Процесні моделі, що постійно оновлюються і використовуються в управлінні, створюють спільний інформаційний простір для аудиторів і керівництва. У такому середовищі аудиторські висновки легше інтегруються в управлінські рішення, оскільки вони подаються не у вигляді абстрактних рекомендацій, а як конкретні пропозиції щодо зміни або вдосконалення процесів.

Для майбутніх аудиторів важливо усвідомити, що інтеграція результатів аудиту в систему управлінських рішень вимагає не лише знання стандартів і методик перевірки. Вона потребує розуміння процесної логіки діяльності підприємства, уміння працювати з процесними моделями та здатності пояснювати результати аналізу в управлінських термінах. Саме ці навички визначають ***сучасний професійний профіль аудитора.***

Таким чином, у процесно-орієнтованому підході аудит відіграє роль ключового елемента управлінської системи. Аудиторські висновки, інтегровані з результатами процесного моделювання і реалізовані через програмні засоби, стають основою для прийняття як операційних, так і стратегічних управлінських рішень у сфері обліку та аудиту.

У традиційній практиці управління рішення часто мають реактивний характер. Вони приймаються після того, як проблема вже проявилася у вигляді помилки в обліку, відхилення показників або зауважень аудитора. Такий підхід зосереджується на усуненні наслідків, але не завжди дозволяє впливати на причини їх виникнення. Процесно-орієнтований підхід змінює цю логіку і створює умови для переходу від реактивних до проактивних управлінських рішень.

Проактивність у процесному підході полягає в тому, що управлінські рішення приймаються на основі аналізу перебігу процесів, а не лише кінцевих результатів. Процесні моделі дозволяють заздалегідь ідентифікувати етапи, на яких можуть виникати ризики, затримки або помилки, і відповідно скоригувати організацію діяльності. Для обліку та аудиту це означає можливість впливати на якість інформації ще на етапі її формування, а не лише після її відображення у звітності.

Процесне мислення стає основою управлінської логіки в умовах цифровізації та зростання складності діяльності підприємств. Воно передбачає сприйняття організації не як набору окремих функцій або підрозділів, а як системи взаємопов’язаних процесів. Кожне управлінське рішення в такій системі розглядається з позиції його впливу на перебіг процесів, їхню узгодженість і кінцевий результат.

Для управління це має важливе значення, оскільки дозволяє уникати ситуацій, коли рішення, прийняті в одній сфері, створюють проблеми в іншій. Наприклад, зміна облікової процедури без урахування процесів внутрішнього контролю або аудиту може призвести до зростання ризиків. Процесне мислення допомагає бачити такі взаємозв’язки ще на етапі обговорення управлінських рішень.

Значення процесних моделей для прийняття управлінських рішень полягає в їх здатності забезпечувати узгодженість дій на різних рівнях управління. Процесна модель виступає спільною основою для обговорення рішень між бухгалтерами, аудиторами та керівництвом. Вона дозволяє перейти від

абстрактних формулювань до конкретного розуміння того, які зміни пропонуються і як вони вплинуть на діяльність підприємства (рис. 2.10).

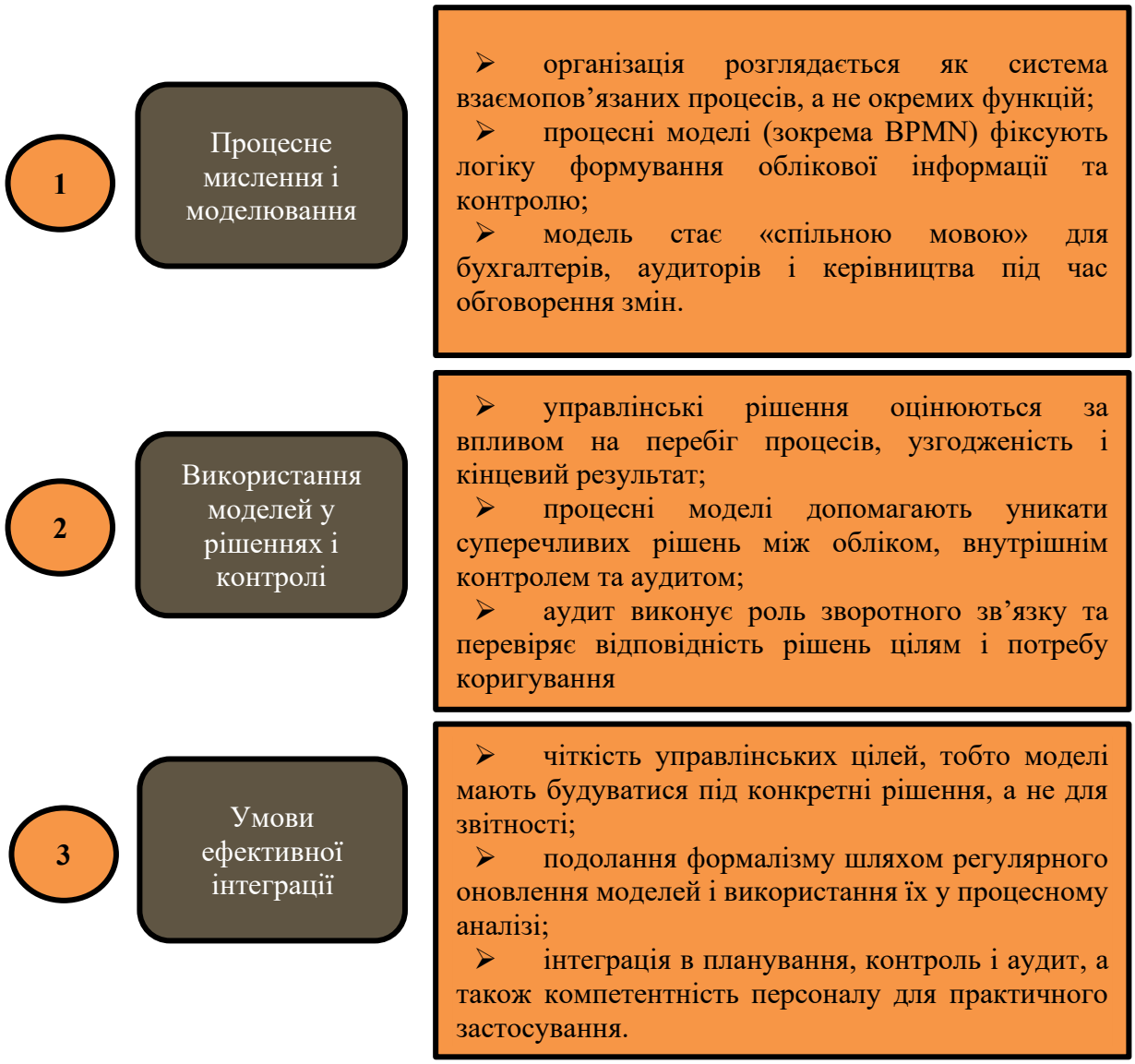


Рис. 2.10. Етапи використання процесних моделей у прийнятті управлінських рішень в обліку та аудиті

У контексті обліку та аудиту процесні моделі, зокрема створені з використанням методології BPMN, дозволяють пов'язати управлінські рішення з конкретними етапами формування облікової інформації та здійснення контролю. Це підвищує прозорість управління і зменшує ризик прийняття суперечливих або несумісних рішень. Керівництво отримує можливість оцінювати альтернативні варіанти дій не лише за їх результатами, а й за впливом на логіку процесів.

Процесно-орієнтований підхід також сприяє узгодженості стратегічних і операційних рішень. Стратегічні цілі підприємства знаходять відображення в організації ключових процесів, а операційні рішення спрямовуються на підтримку цих процесів у щоденній діяльності. Аудит у такій системі відіграє роль механізму зворотного зв'язку, який дозволяє оцінити, наскільки прийняті рішення відповідають задекларованим цілям і чи потребують вони коригування.

Незважаючи на значний потенціал процесного моделювання, ефективність використання його результатів у системі управлінських рішень не є автоматичною. Наявність процесних моделей, навіть створених за допомогою сучасних програмних засобів, сама по собі не гарантує підвищення якості управління в обліку та аудиті. Вирішальне значення мають умови, в яких ці результати інтегруються в управлінську практику.

Одним із ключових факторів, що впливають на використання результатів моделювання, є ***чіткість управлінських цілей.*** Якщо процесні моделі створюються без розуміння того, для яких саме рішень вони будуть використовуватися, їх практична цінність знижується. У такому випадку моделювання перетворюється на формальний опис діяльності, який не впливає на організацію обліку, контроль або аудит. Ефективна інтеграція можлива лише тоді, коли процесне моделювання безпосередньо пов'язане з конкретними управлінськими завданнями.

Суттєвою проблемою є ризик формального застосування процесних моделей. У практиці підприємств нерідко трапляються ситуації, коли моделі створюються «для звітності» або як вимога внутрішніх регламентів. У такому випадку вони не оновлюються, не використовуються в аналізі й не враховуються під час прийняття рішень. Формальне використання процесних моделей створює ілюзію системного підходу, але фактично не змінює управлінську логіку.

Ще однією важливою проблемою є ***розрив між процесними моделями та реальними управлінськими рішеннями.*** Якщо результати моделювання не інтегровані в процедури планування, контролю та аудиту, вони залишаються ізольованими аналітичними матеріалами. Для обліку та аудиту це означає втрату

можливості використовувати процесні результати як основу для оцінювання ризиків і формування рекомендацій.

Важливу роль у подоланні цих обмежень відіграє компетентність персоналу. Процесне моделювання вимагає не лише технічних навичок роботи з програмними засобами, а й розуміння процесної логіки діяльності підприємства. Бухгалтери, аудитори та управлінці мають однаково розуміти значення процесних моделей і вміти використовувати їх у своїй роботі. Без цього інтеграція процесних результатів у систему управління є обмеженою.

Не менш значущим чинником є організаційна культура. Процесно-орієнтований підхід передбачає відкритість до змін, готовність аналізувати власну діяльність і визнавати наявність проблем. У середовищі, де управлінські рішення приймаються виключно інтуїтивно або на основі традиційних підходів, процесні моделі сприймаються як додаткове навантаження, а не як інструмент підтримки управління.

2.4 Контрольні питання для самоперевірки

1. У чому полягає відмінність між функціональним і процесно-орієнтованим підходами в обліку та аудиті?

2. Чому функціональний підхід обмежує можливості комплексного аналізу обліково-аудиторської діяльності?

3. Яким чином процесно-орієнтована модель дозволяє представити обліково-аудиторську діяльність як цілісну систему?

4. Які елементи обліково-аудиторської діяльності відображаються в процесно-орієнтованих моделях?

5. У чому полягає роль процесного моделювання в систематизації інформації для аудиторського аналізу?

6. Які методологічні принципи лежать в основі побудови процесно-орієнтованих моделей?

7. Чим відрізняються загальний, аналітичний та операційний рівні опису процесів?

8. Як процесно-орієнтовані моделі використовуються у формуванні аудиторського судження?

9. Чому процесні моделі є основою для ідентифікації ризиків у обліку та аудиті?

10. Яку роль відіграють програмні засоби в аналізі обліково-аудиторських процесів?

11. Які типи програмних засобів застосовуються для дослідження та аналізу обліково-аудиторських процесів?

12. У чому полягає значення процесного аналізу для виявлення вузьких місць і неефективних етапів діяльності?

13. Як результати процесного аналізу використовуються для оптимізації обліково-аудиторських процесів?

14. Чому оптимізація в обліку та аудиті не зводиться лише до скорочення часу або витрат?

15. Яким чином результати процесного аналізу трансформуються в практичні аудиторські рекомендації?

16. Яку роль відіграє аудит у підтримці управлінських рішень у процесно-орієнтованому підході?

17. Що таке BPMN і з якою метою ця методологія використовується в обліку та аудиті?

18. Як процесні моделі, створені за допомогою BPMN, можуть бути інтегровані в систему управлінських рішень?

19. Які фактори обмежують ефективну інтеграцію результатів процесного моделювання в управлінську практику?

20. Чому компетентність персоналу та організаційна культура є важливими умовами використання процесного підходу в обліку та аудиті?

Розділ 3

Автори:
Валентина Панасюк
Оксана Черешнюк

ЦИФРОВА ТРАНСФОРМАЦІЯ АУДИТУ

РОЗДІЛ 3. ЦИФРОВА ТРАНСФОРМАЦІЯ АУДИТУ

«Зміни – закон життя. І ті, хто дивиться лише в минуле чи тільки на сьогодення, напевно пропустять майбутнє.»

Джон Кеннеді

3.1. Цифрова трансформація середовища обліку і аудиту

Сучасні умови розвитку економіки характеризуються прискоренням інформаційних потоків, цифровізацією фінансових відносин та зростанням складності господарських операцій. За таких обставин інтеграція цифрових технологій у систему бухгалтерського обліку, фінансового аналізу й аудиту набуває особливої актуальності. Стрімке збільшення обсягів даних, поява нових джерел інформації, таких як електронний документообіг, онлайн-платежі, платформи електронної комерції, інтегровані корпоративні системи та підвищення вимог користувачів до своєчасності й достовірності звітності обмежують можливості традиційних методів обробки й контролю даних. Відтак зростає потреба в дослідженні та впровадженні цифрових рішень, які забезпечують підвищення точності облікових даних.

Цифровізація виступає не лише фактором економічного розвитку, а й ключовим рушієм трансформації бізнес-процесів у різних сферах діяльності підприємств, зокрема в аудиті. Застосування сучасних технологій, а саме штучного інтелекту, блокчейну та хмарних сервісів, істотно модернізує методи проведення аудиту, підвищуючи його точність і швидкість.

Цифрова трансформація обліку та аудиту є закономірною відповіддю підприємств на зміни у зовнішньому середовищі та внутрішніх умовах ведення бізнесу. Вона не зводиться до впровадження окремих програмних продуктів, а передбачає комплексні зміни у процесах формування даних, їх обробці, контролі, зберіганні та використанні для управлінських рішень менеджменту підприємств і організацій.

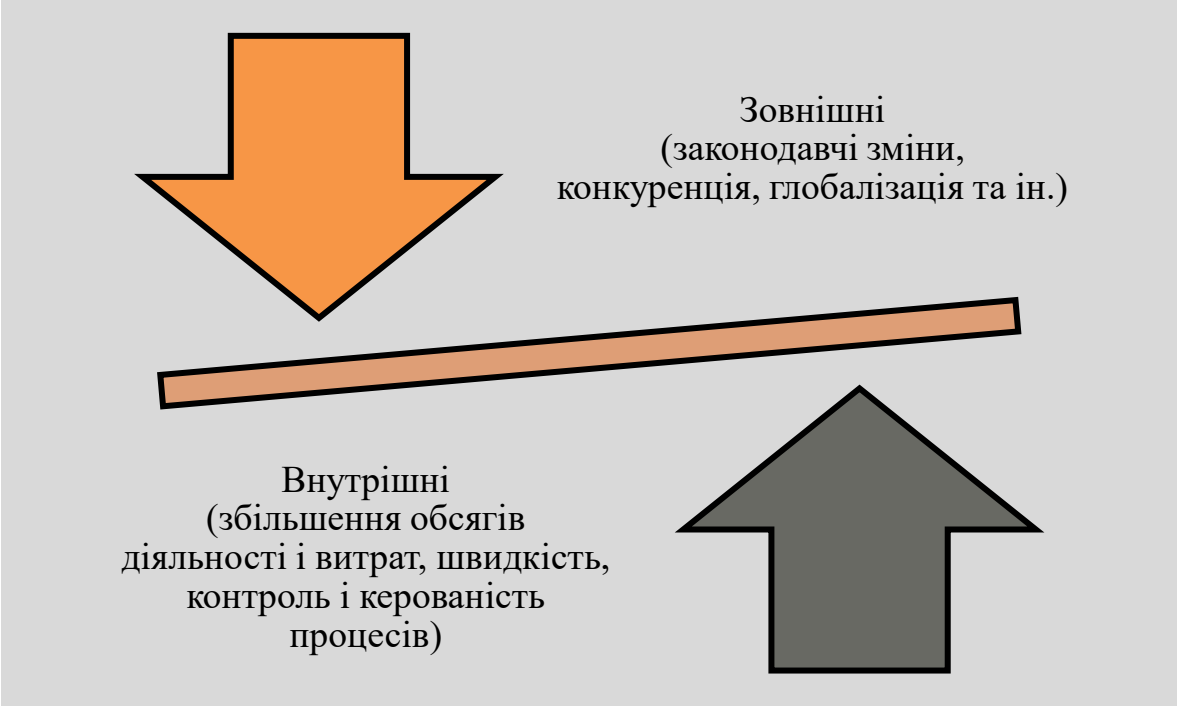


Рис. 3.1. Фактори цифрової трансформації обліку і аудиту

Цифрова трансформація обліку й аудиту відбувається під впливом зовнішніх і внутрішніх факторів. Зовнішній тиск, що формується законодавчими вимогами, конкуренцією та процесами глобалізації, і внутрішня потреба в підвищенні ефективності через зростання масштабів діяльності й витрат, прискорення обробки інформації та посилення контролю і керованості процесів.

Саме взаємодія цих блоків визначає темп, швидкість та пріоритети цифрової трансформації у конкретній організації, а також трансформує методики формування облікових даних і підходи до аудиторського підтвердження. Додатково слід враховувати, що важливим рушієм змін є технологічні можливості та супутні ризики, які одночасно відкривають нові інструменти автоматизації й висувають підвищені вимоги до захисту інформації та якості

даних. У результаті цифрова трансформація змінює не лише технічну інфраструктуру, а й компетентнісні вимоги до бухгалтерів і аудиторів, посилюючи потребу в цифровій грамотності, розумінні IT-контролів та роботі з електронними доказами.

Основні фактори цифрової трансформації у сфері обліку й аудиту вітчизняними вченими-економістами поділяються на такі групи:

- ***Законодавчі та державні вимоги***

Першочерговим стимулом цифровізації в обліку й аудиті виступають законодавчі зміни, що переводять взаємодію суб'єктів господарювання з державними інституціями в електронний формат. Це, насамперед, розвиток електронної звітності та електронних сервісів (податкових, статистичних, митних, соціальних реєстрів), розширення сфери застосування електронних документів і кваліфікованого електронного підпису (КЕП / ЕЦП) як юридично значущого підтвердження господарських операцій. Паралельно посилюються вимоги до прозорості, відповідальності та якості фінансової звітності, а також до системи контролю якості аудиторських послуг і наглядових процедур. Окрему групу формують вимоги щодо захисту даних, а саме персональних, комерційної таємниці, правил зберігання й архівування інформації, а також організації реагування на інциденти.

Вплив на облік і аудит проявляється у формуванні «електронного сліду» операцій, стандартизації форматів даних, підвищенні ролі контролів доступу, веденні журналів змін, забезпеченні довготривалого зберігання електронних доказів.

Цікавий факт. Сьогодні інформаційні технології активно впроваджуються у роботу державних і приватних структур у всьому світу, і Україна також рухається у цьому напрямі. У 2024 році Україна досягла значних результатів у сфері цифрового управління та взаємодії держави з громадянами. Згідно з даними United Nations, країна посіла 30-те місце серед 193 країн у Індексі розвитку е-урядування. При цьому Україна виборола 1-ше місце у рейтингу E-Participation Index, що вимірює ступінь залученості громадян до цифрових

платформ державного управління. Варто зазначити, що у 2022 році Україна посідала 57 місце.

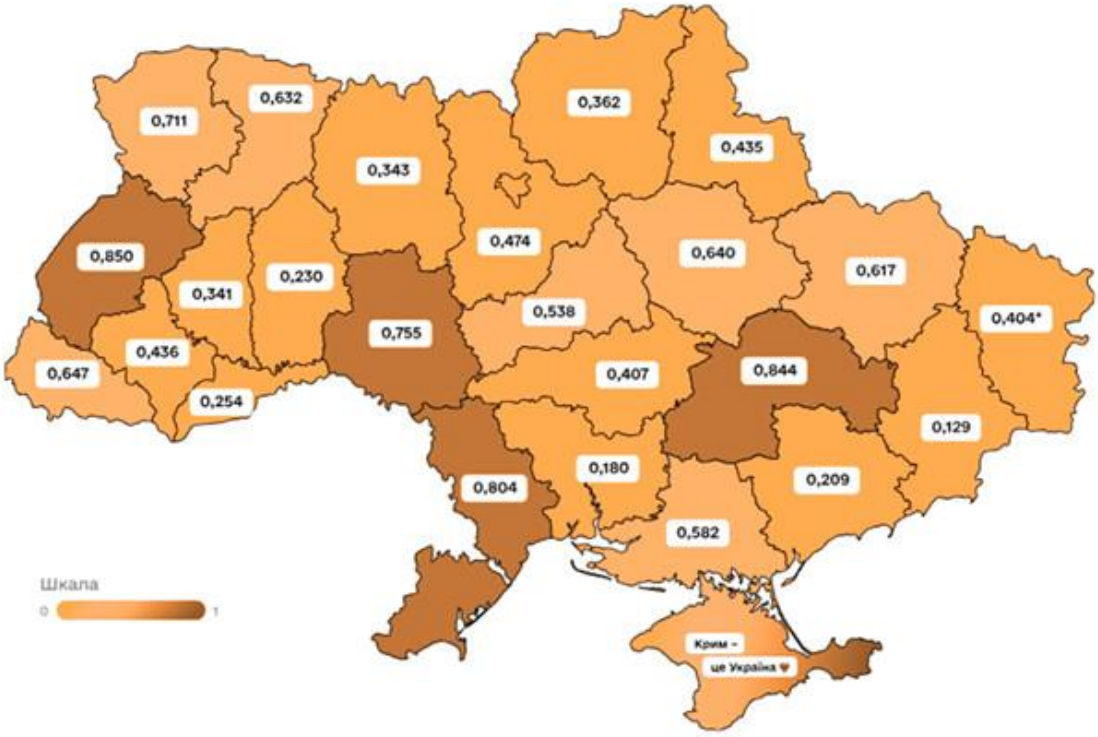


Рис. 3.2. Індекс цифрової трансформації України в 2024 році

- ***Ринкова конкуренція та очікування клієнтів та інвесторів***

Наступним фактором є ринковий тиск, що формує запит на швидкість, прозорість і прогнозованість діяльності. У практиці управління зростає потреба в рішеннях «майже в реальному часі», скороченні тривалості формування звітності для цілей менеджменту, підвищенні оперативності управлінської звітності. Інвестори, кредитори та бізнес-партнери очікують зрозумілої, порівнюваної та перевірюваної інформації, що підкріплює значення якісної облікової політики, контрольного середовища та незалежного підтвердження звітності. Одночасно цифрові канали взаємодії з клієнтами і персоналізація сервісів стають стандартом діяльності. Додатково глобалізація та участь у міжнародних ланцюгах створення вартості вимагають сумісності процесів, звітності та контрольних процедур.

- ***Технологічний прогрес і здешевлення цифрових рішень***

Розвиток і доступність технологій істотно знижують бар'єри входу в цифрову трансформацію. Хмарні моделі забезпечують масштабованість і

зменшують капітальні витрати на IT-інфраструктуру. Використання інтеграційних рішень дозволяє об'єднувати в єдиний простір облікові системи з банківськими сервісами, касою, маркетплейсами, логістикою. Аналітика даних переводить облік від суто реєстраційної функції до управління на основі даних. Роботизація процесів підсилює автоматизацію повторюваних операцій, звірок, перенесення даних, контролю лімітів, формування документів. Штучний інтелект додатково розширює можливості виявлення порушень, прогнозування, класифікації документів і підтримки професійних рішень бухгалтера й аудитора.

- ***Операційна ефективність і оптимізація витрат***

Економічна доцільність є базовим внутрішнім драйвером трансформації. Підприємства прагнуть скоротити обсяг ручної праці, мінімізувати помилки, усунути дублювання операцій і зменшити витрати часу на рутинні процедури. Цифровізація стає інструментом економії ресурсів і дисциплінування процесів, особливо в обліку, де домінують повторювані операції та регламентні процедури.

- ***Ризики, безпека та стійкість бізнесу***

Зростання цифрової залежності підвищує значущість ризиків, пов'язаних з IT-інфраструктурою і даними. Кіберзагрози вимагають захисту фінансової інформації, контролю доступів, моніторингу подій безпеки. Паралельно формується потреба у забезпеченні безперервності діяльності, можливості віддаленої роботи, резервного копіювання та відновлення після інцидентів. Посилюється контроль шахрайства, зокрема ризик підміни реквізитів, фішингових атак, фальсифікації електронних документів. Важливим елементом стає розподіл повноважень, що забезпечує довіру до облікових систем.

Вплив на облік і аудит проявляється у зміщенні аудиторського фокусу на IT-контроли, журнали подій і змін, права доступу, управління інцидентами, оцінювання надійності інформаційних систем.

- ***Кадрові та організаційні чинники***

Цифрова трансформація значною мірою зумовлена людським фактором. Дефіцит кваліфікованих кадрів та необхідність зменшення залежності від ручної

праці спонукають автоматизувати типові операції та формалізувати процедури. Паралельно відбувається зміна компетентностей – потрібні навички роботи з даними, розуміння логіки інформаційних систем, аналітичне мислення. Очікування працівників щодо цифрових інструментів і віддаленої взаємодії стають частиною кадрової політики. Інтеграція цифрових рішень у систему підготовки кадрів, управління знаннями, стандартизацію робочих процедур підвищують продуктивність праці.

- **Стратегічні зміни ведення бізнесу**

Найбільший рівень трансформації зумовлюється стратегічними змінами у створенні цінності. Поширюються платформні та екосистемні моделі, підписки, маркетплейси, цифрові продукти й сервіси, де фінансові потоки створюються онлайн. Це формує потребу у нових підходах до групування доходів, витрат, договорів, цифрових активів, а також до контролю й звітності, включно з нефінансовою.

Етапи цифрової трансформації у світі систем обліку та аудиту подано на рисунку 3.3.

Межі етапів цифровізації є умовними, оскільки різні країни та галузі проходили їх нерівномірно залежно від рівня розвитку економіки, доступності технологій та законодавчих вимог. Проте для потреб обліку й аудиту доцільно виділяти послідовні етапи, які відображають зміну інструментів ведення обліку, характеру даних та підходів до отримання аудиторських доказів.

Перший етап (1950-1970-ті) – автоматизація обчислень і обліку пов'язаний із використанням мейнфреймів, перфокарт і централізованих обчислювальних центрів. Його сутність полягала в переході від ручних розрахунків до машинної обробки, що дало змогу автоматизувати окремі облікові ділянки, насамперед розрахунки із заробітної плати, облік запасів і формування підсумкових регістрів.

Другий етап (1980-ті роки) – комп'ютеризація робочих місць характеризується поширенням персональних комп'ютерів, локальних мереж і офісних пакетів. Цифрові інструменти стають масовими, облікова інформація

починає накопичуватися у файлах і локальних базах даних, а продуктивність бухгалтерських та управлінських процедур суттєво зростає завдяки автоматизації розрахунків і документування.

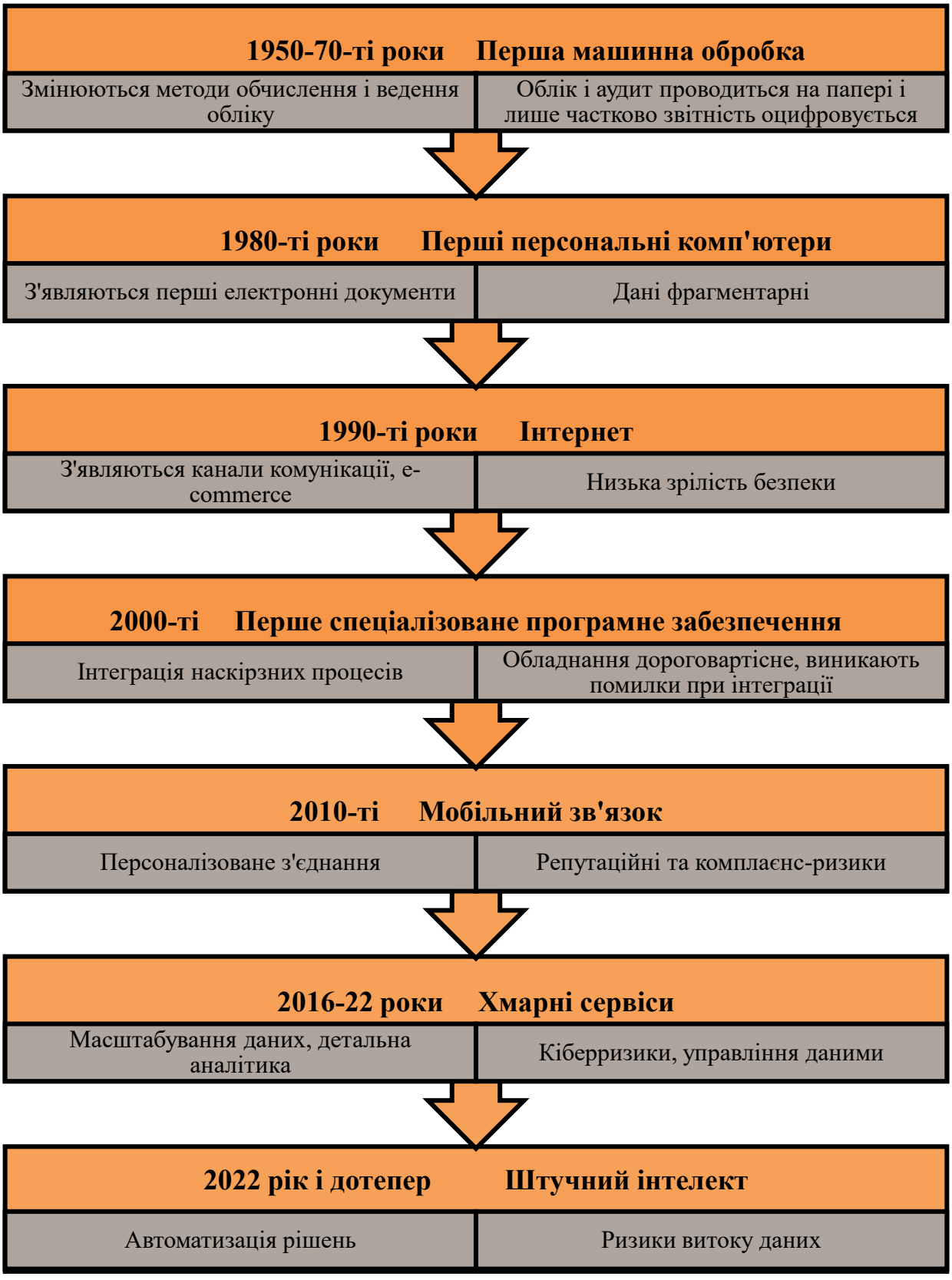


Рис. 3.3. Етапи цифрової трансформації обліку і аудиту в світі

Третій етап (1990-ті роки) – інтернетизація бізнесу пов'язаний із розвитком WWW, електронної пошти, появою корпоративних сайтів і клієнт-серверних систем.

Бізнес починає активно працювати в мережі, з'являються електронна комерція та онлайн-канали взаємодії з клієнтами, а також перші інтегровані IT-архітектури, що змінюють характер документообігу та комунікацій, у тому числі в аудиті.

Четвертий етап (2000–2009 роки) – інтеграція процесів і даних базується на розвитку ERP/CRM-систем, BI-аналітики, електронного документообігу й широкому впровадженні електронних платежів.

Центральним стає підхід до управління наскрізними бізнес-процесами (наприклад, procure-to-pay та order-to-cash), уніфікуються довідники і бази даних, стандартизуються управлінська й фінансова звітність, що розширює можливості аудиту щодо аналітики та контролів.

П'ятий етап (2010–2016 роки) – мобільність і платформні моделі визначається поширенням смартфонів, соціальних мереж, розвитком API-економіки, маркетплейсів і SaaS-рішень.

Цифрові канали стають основними у взаємодії з клієнтами, а бізнес дедалі частіше переходить до платформних моделей та екосистем, що ускладнює облік (через нові форми доходів, посередництво, комісії) і підсилює потребу в контролі інтеграцій та даних.

Шостий етап (2016–2022 роки) – хмарні технології та дані як актив характеризується масштабуванням IT через загальнодоступні хмари, розвитком сховищ даних і перетворенням кібербезпеки на управлінську функцію.

Аналітика та управління даними стають важелем конкурентоспроможності, а автоматизація процесів входить у масове застосування, що змінює підхід до аудиту, увага зосереджується на правильності формування електронних документів, IT-контролях, управлінні доступами, надійності даних і безперервності процесів.

Сьомий етап (2022 рік і дотепер) пов'язаний із розвитком машинного навчання та штучного інтелекту та автоматизованої аналітики.

Відбувається перехід від використання цифрових інструментів до впровадження рішень, які самі генерують аналіз, контент і рекомендації, що впливає на облік, фінансовий аналіз і аудит. У таких умовах зростає значення етики та прозорості моделей, управління якістю даних, відповідальності за результати автоматизованих рішень і посилення захисту інформації.

В Україні аудит почав активно формуватися після здобуття незалежності як відповідь на потреби становлення ринкової економіки та розвитку приватного сектору. Перехід до нових форм власності, поява комерційних структур і залучення інвестицій зумовили попит на незалежне підтвердження достовірності фінансової інформації. Паралельно виникла необхідність створення національної нормативно-правової бази та професійних інституцій, які б регулювали аудиторську діяльність і забезпечували її якість. У подальшому розвиток аудиту посилився під впливом євроінтеграційних процесів і гармонізації вимог до обліку та аудиторських процедур із міжнародними стандартами.

Таблиця 3.1

Періоди цифрової трансформації аудиту в Україні

Період	**Назва**	**Характеристика**	**Ключові передумови**	**Особливості цифровізації**
Перший *(1987-1989 рр.)*	Зародження аудиту	Виникають перші аудиторські структури, ревізійні групи та консалтингова фірма «Інаудит-Україна» у Києві, відбувається контроль підприємств із участю іноземного капіталу	Запит інвесторів і користувачів на незалежну перевірку нових форм господарювання	Обмежене застосування ІТ, а перевірки переважно документальні; цифрові дані фрагментарні. Перші підходи до перевірки електронних розрахунків (табличні форми, машинограми) без розвинутих інструментів аналізу даних

Другий *(1989-1992 рр.)*	Становлення українського аудиту	Зростає кількість аудиторських фірм та розширюється спектр послуг	Необхідність аудиторського підтвердження результатів діяльності фірм	Документи поступово переводилися в електронний формат, що спрощувало їх зберігання й обмін. Водночас більшість контрольних процедур і перевірочних розрахунків аудитори виконували переважно вручну, спираючись на паперові першоджерела та ручні перерахунки
Третій *(1993-2001 рр.)*	Юридичне формування аудиту	Формується нормативно-правова база аудиту, інституціоналізація професії та регулювання	Необхідність уніфікації аудиторської діяльності та розвитку ринку	Поступова автоматизація обліку (виникають перші спеціалізовані програми), поступовий перехід частини реєстрів у цифровий формат. Аудит розширює комп'ютерно-орієнтовані процедури
Четвертий *(2001-2006 рр.)*	Інституційне зміцнення	Розвиток практик і методик, професійне укрупнення ринку; підготовка до глибших реформ і зближення з міжнародними підходами	Потреба підвищення якості аудиторських послуг і методичного оновлення в умовах зростання складності бізнесу	Впровадження облікових систем, електронного банкінгу, перших елементів електронного документообігу. Аудитори застосовують комп'ютерні методи аудиту, суцільні/масові вибірки з реєстрів, тестування контролів доступу, перші підходи до аналізу даних

П'ятий *(2007-2017 рр.)*	Сучасний аудит	Реформування аудиту відповідно до міжнародно визнаних вимог; зміни до вітчизняного законодавства	Гармонізація аудиторських механізмів і національного обліку з європейськими вимогами	Аудит зміщується до ризик-орієнтованого підходу з опорою на дані; актуалізуються питання кіберризиків, цілісності баз даних, журналів змін, резервного копіювання
Шостий *(2017 – дотепер)*	Нова ера аудиту	Адаптація законодавства до норм ЄС; посилення вимог до якості, прозорості та нагляду	Євроінтеграція, інтернаціоналізація діяльності компаній і зростання вимог стейкхолдерів	Цифрова трансформація аудиту, виникають дистанційні процедури, хмарні середовища, автоматизація робочих документів, інтеграція з джерелами даних клієнта, е-докази. Поява фокусу на безперервному моніторингу, ШІ-інструментах, контролі відповідності, захисті персональних даних та управлінні

Отже, цифрова трансформація аудиту в Україні пройшла шлях від фрагментарного використання ІТ та переважно паперового контролю до дата-орієнтованих, дистанційних і частково автоматизованих процедур у хмарних середовищах із використанням е-доказів. Водночас гармонізація з вимогами ЄС і ускладнення ІТ-архітектур бізнесу змістили фокус аудиту з перевірки окремих документів на оцінку ІТ-контролів, якості даних, кіберризиків та прозорості рішень (зокрема ШІ).

3.2. Вплив цифровізації на цілі та завдання аудиту

Як показує світова історія, розвиток аудиту завжди прискорювався після економічних криз і корпоративних скандалів. У США після біржового краху 1929 р. зросла потреба інвесторів у перевіреній звітності, що сприяло інституційному закріпленню незалежного аудиту на ринку капіталу. Наприкінці XX ст. комп'ютеризація обліку зумовила появу комп'ютерно-орієнтованих методів аудиту, коли аудитори почали перевіряти не лише документи, а й цифрові масиви даних. Поворотним моментом стало посилення вимог до внутрішнього контролю після корпоративних скандалів початку 2000-х років, коли в багатьох країнах акцент змістився на оцінювання контрольного середовища та IT-контролів. Паралельно стандартизація електронної звітності підвищила порівнюваність даних і розширила можливості аналітичних процедур. У сучасний період ця еволюція логічно привела до концепцій безперервного аудиту та data-driven підходів, коли ключовим об'єктом підтвердження стає не лише фінансовий результат, а й надійність цифрових процесів, що його формують.

З огляду на цифровізацію зростає роль аудиту як інструменту, що забезпечує довіру не лише до підсумкових фінансових показників, а й до цифрових даних і каналів звітності. Електронні документи, кваліфіковані електронні підписи, журнали змін, системні логи та результати автоматизованих обробок стають джерелами аудиторських доказів, а отже, потребують перевірки їх автентичності, незмінності, простежуваності й захищеності. У цьому контексті аудит підтримує інформаційну прозорість для інвесторів, кредиторів та інших стейкхолдерів, оскільки підтверджує, що цифрові дані відображають реальні господарські процеси та формуються за належних умов контролю.

Згідно із Законом України «Про аудит фінансової звітності та аудиторську діяльність» ***завдання з обов'язкового аудиту фінансової звітності*** – завдання з надання обґрунтованої впевненості, що приймається і виконується суб'єктом аудиторської діяльності відповідно до вимог Закону та міжнародних стандартів

аудиту шляхом перевірки фінансової звітності або консолідованої фінансової звітності з метою висловлення незалежної думки аудитора про її відповідність в усіх суттєвих аспектах і відповідність вимогам міжнародних стандартів фінансової звітності або національних положень (стандартів) бухгалтерського обліку та законів України.

У цифровому середовищі завдання обов'язкового аудиту фінансової звітності зберігає свою сутність як завдання з надання обґрунтованої впевненості. Аудитор, діючи відповідно до Закону України та МСА, перевіряє фінансову (консолідовану) звітність і висловлює незалежну думку щодо її відповідності в усіх суттєвих аспектах вимогам МСФЗ або НП(С)БО та законодавства України, використовуючи при цьому цифрові дані й електронні докази, сформовані інформаційними системами.

Водночас відбувається зміщення акценту від моделі ретроспективного підтвердження інформації до більш широкого забезпечення впевненості щодо процесів і систем, які генерують облікову інформацію. У практиці це означає зростання значення оцінювання внутрішнього контролю, управління доступами, розподілу повноважень і контролю змін у системах, а також використання методів аналітики даних для виявлення відхилень і ризикових операцій. Отже, в цифровій економіці мета аудиту еволюціонує від підтвердження результату до підтвердження надійності механізму формування цього результату, що підвищує довіру стейкхолдерів до звітності та цифрового середовища підприємства в цілому.

Основним етапом аудиторської перевірки є збирання необхідної інформації, яка забезпечує отримання достатніх доказів для формування професійного висновку аудитора. Для цього застосовують різні методичні прийоми, що поділяються за спрямованістю на органолептичні, розрахунково-аналітичні та документальні. Ці групи методів подані на рисунку 3.4.

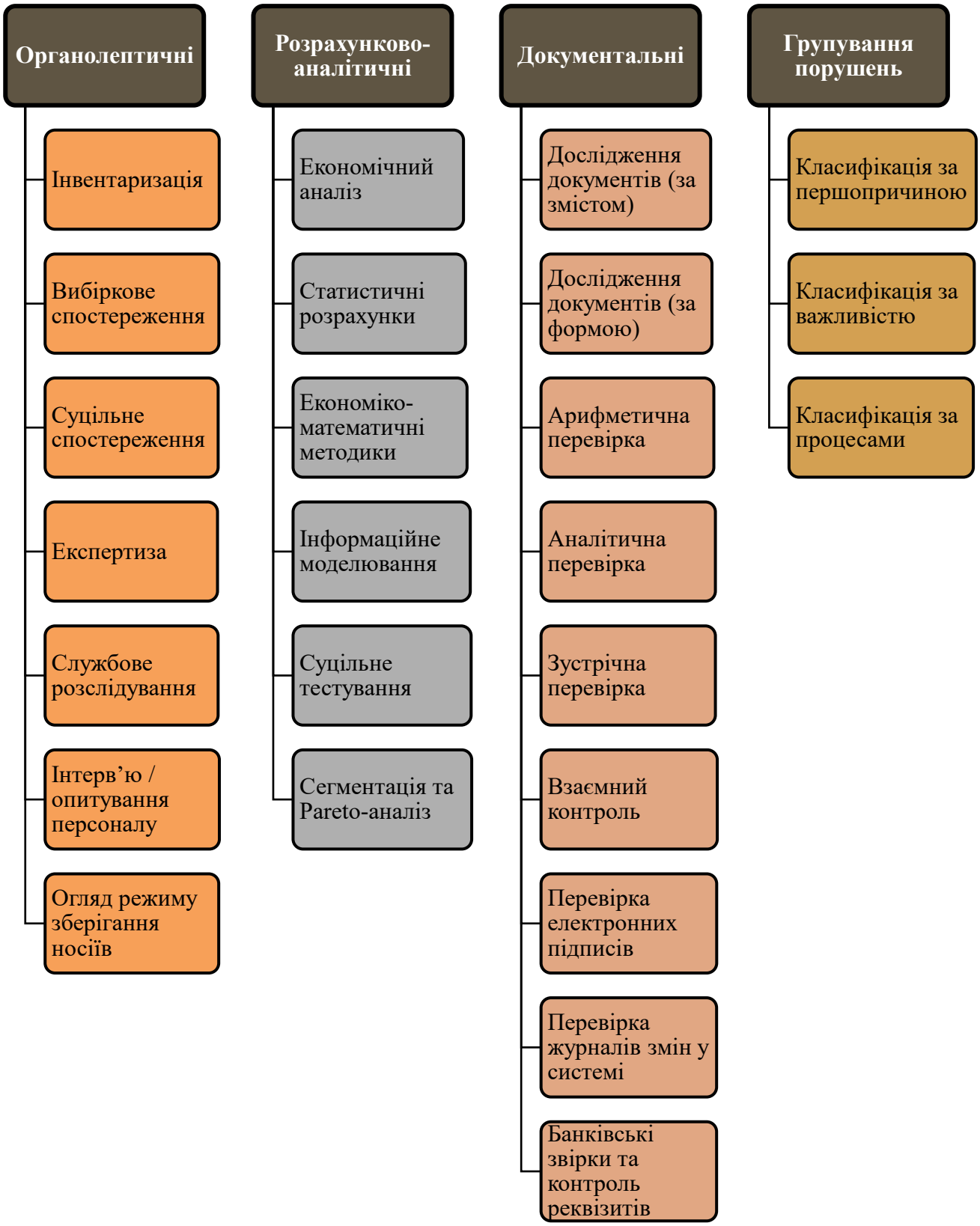


Рис. 3.4. Методичні прийоми аудиту в цифровому середовищі

Під час аудиторської перевірки аудитор формує набір робочих документів, які слугують основою для виконання необхідних процедур і фіксації результатів контролю. У процесі аналізу аудитор звертає увагу на можливі відхилення в

облікових даних, що можуть впливати на точність і достовірність показників фінансової звітності, та оцінює їхній вплив на загальний висновок.

Аудиторська перевірка складається з послідовних етапів. Під час проведення аудиторської перевірки, використовуючи спеціалізоване програмне забезпечення, аудитор може виконувати низку процедур, перелік яких подано на схемі (рис. 3.5).

Рис. 3.5. Процедури та етапи, визначені аудитором у цифровому середовищі

На початковому етапі аудитор уточнює мету перевірки, формулює конкретні завдання та визначає, які з них доцільно виконувати із застосуванням цифрових інструментів.

Паралельно оцінюється реалістичність виконання завдань з огляду на доступність даних, якість інформації, рівень автоматизації клієнта, наявні обмеження доступу та вимоги конфіденційності.

На етапі планування аудитор складає програму перевірки, визначає обсяг процедур, строки та відповідальних осіб.

Важливим елементом є аналіз облікової політики та практики її застосування в інформаційних системах. Додатково оцінюються можливості застосування відповідних програмних засобів і інструментів, а також технічні ресурси (доступи, формат вивантажень, потужність обробки даних, потреба в залученні IT-фахівців або аналітиків). Результатом етапу є погоджений план цифрових аудиторських процедур та критерії оцінювання.

На третьому етапі відбувається підготовка стандартних програмних засобів до роботи, налаштування шаблонів аналізу, правил відбору, контрольних звітів, форм вивантаження.

За потреби аудитор розробляє нові інструменти або процедури, спеціальні запити до баз даних, макроси, скрипти, робочі таблиці, а в сучасних умовах також підготовляє промпти й інструкції для використання інструментів зі штучним інтелектом (з урахуванням політик конфіденційності). Метою етапу є забезпечення відтворюваності й контрольованості цифрових процедур.

Четвертий етап передбачає отримання, завантаження та первинну верифікацію масивів даних з облікових систем (ERP, бухгалтерські програми, CRM, банківські системи).

Аудитор перевіряє повноту даних, коректність періоду, структуру файлів, узгодженість довідників, відсутність дублювань, а також забезпечує простежуваність (від транзакції до показників звітності). Фактично на цьому етапі формується надійна база для подальшого цифрового аналізу і тестування.

На підставі підготовлених даних аудитор проводить аналітичні процедури та тестування, оцінює правильність формування облікових показників і звітності. Застосовуються методи суцільної або вибіркової перевірки, виявлення аномалій і ризикових операцій, аналіз трендів, співвідношень, відповідності обліковій політиці. У цифровому середовищі це може доповнюватися використанням баз знань і спеціалізованого програмного забезпечення для інтерпретації результатів і формування висновків щодо рівня ризиків та надійності контрольних процедур.

На завершальному етапі результати цифрових процедур узагальнюються, оцінюється їх достатність і прийнятність як аудиторських доказів, формуються висновки щодо виявлених викривлень і недоліків контролю.

Далі готується аудиторський висновок і/або управлінський лист із рекомендаціями відповідно до визначених стандартів і методології організації. Важливо, що цифрові інструменти на цьому етапі використовуються для стандартизації звітування, документування виконаних процедур і забезпечення відтворюваності аудиторських результатів. У процесі проведення аудиторської перевірки застосування спеціального ПЗ суттєво розширює можливості аудитора та підсилює ефективність аудиторських процедур. Цифрові інструменти дозволяють поєднати традиційні методичні прийоми з новими технологічними можливостями, формуючи сучасний підхід до перевірки фінансової інформації.

Застосування цифрових технологій дозволяє пришвидшити роботу аудитора та аналітика, виявити складніші зв’язки, більш детально вивчити дані. У таблиці 3.2 подано переваги застосування цифрових технологій в аудиті у порівнянні з традиційними методами роботи.

Так, інструменти штучного інтелекту та аналізу даних дають змогу аудиторам опрацьовувати значні масиви фінансової інформації в стислі терміни та наближатися до режиму реального часу, що розширює можливості глибшого аналітичного оцінювання операцій.

Таблиця 3.2

Переваги застосування цифрових технологій в аудиті

Аспект	Традиційний аудит	Цифровий аудит
Обсяг даних	Обмежена кількість даних; використання вибіркових процедур	Обробка великих масивів даних у реальному часі
Методи збору даних	Ручна перевірка документів, паперові носії	Автоматизоване отримання даних з онлайн-платформ
Час на перевірку	Триваліший через поетапну ручну роботу	Значно швидший завдяки автоматизації
Точність аналізу	Вища ймовірність людських помилок; обмежена точність вибірок	Висока точність алгоритмів, мінімізація помилок
Виявлення шахрайства	Залежить від досвіду аудитора; потребує ручного аналізу	Автоматичне виявлення помилок та ризиків за допомогою штучного інтелекту
Методи аналізу	Простий аналіз, ручні розрахунки, тестування вибірок	Алгоритмічний аналіз, статистичні методи, прогнозування
Перевірка операцій	Аналіз вибірки транзакцій	Повний аналіз усіх операцій у реальному часі
Аналіз ризиків	Оцінка на основі вибіркових даних та досвіду аудитора	Прогнозування ризиків на основі штучного інтелекту
Інтеграція з системами	Мінімальна; робота з окремими документами	Повна інтеграція з ERP, CRM, бухгалтерськими системами
Регулювання та відповідність	Перевірка відповідності переважно вручну	Автоматичний контроль відповідності стандартам
Вимоги до персоналу	Переважно знання з бухгалтерського обліку та аудиту	Знання IT, аналітики даних, особливостей роботи з штучним інтелектом, кібербезпеки

Завдяки автоматизованому виявленню порушень, нетипових транзакцій і невідповідностей підвищується здатність своєчасно ідентифікувати помилки та ознаки потенційних порушень. Використання блокчейн-технологій посилює довіру до даних через механізми незмінності записів і простежуваності операцій, а хмарні сервіси забезпечують мобільність доступу, масштабованість обчислювальних ресурсів і можливість організації дистанційних аудиторських процедур. У сукупності ці технології формують передумови для переходу до більш ефективної, ризик-орієнтованої та аналітично посиленої моделі аудиту, що відповідає вимогам цифрової економіки.

Окремого значення набувають інтеграції між системами та обмін даними через інтерфейси, оскільки саме в інтеграційних вузлах часто виникають ризики втрати даних, дублювання, спотворення або неузгодженості показників. Тому аудит має охоплювати оцінювання надійності інформаційних потоків «від операції до звітності», включаючи коректність завантаження даних, правила трансформації та узгодження довідників. Відповідно, перевіряється не лише кінцевий результат, а й механізм його формування в цифровому контурі підприємства.

У цифровій економіці дані набувають ознак стратегічного активу, що також розширює об'єкти аудиторської уваги. Аудитор повинен враховувати питання якості даних, таких як:

- *повнота;*
- *точність;*
- *своєчасність;*
- *узгодженість;*
- *унікальність.*

Саме якість вихідних масивів визначає надійність фінансової та управлінської звітності. Крім внутрішніх даних облікових систем, дедалі частіше використовуються дані із зовнішніх джерел, зокрема банківські виписки, інформація від платіжних сервісів, маркетплейсів, логістичних операторів, державних реєстрів, що потребує оцінювання їх достовірності, зіставності та порядку включення в облікові процеси. Також розширюється коло об'єктів за рахунок нефінансової інформації, зокрема даних, які впливають на репутацію, доступ до капіталу та виконання вимог стейкхолдерів, а отже, можуть ставати предметом завдань із надання впевненості.

Зміни торкаються й ***джерел аудиторських доказів.*** Електронні документи, підписані кваліфікованим електронним підписом (КЕП / ЕЦП), набувають статусу повноцінних первинних документів і стають центральним елементом доказової бази. Водночас важливими джерелами доказів стають журнали подій і журналювання змін у системах, системні логи, метадані документів, цифрові

сліди користувачів, а також контрольні звіти, сформовані автоматизовано. Це зумовлює необхідність оцінювання автентичності, цілісності та простежуваності цифрових доказів, а також умов їх збереження й захисту.

Таким чином, у цифровому середовищі об’єкти аудиту охоплюють не тільки звітні показники, а й цифрову інфраструктуру їх формування, дані як актив та цифрові докази, що забезпечують належний рівень аудиторської впевненості.

3.3. Роль аудитора й фахівця з фінансової безпеки у цифровому середовищі

У системі корпоративного управління аудит і функція фінансової безпеки виконують роль ключових елементів забезпечення прозорості, підзвітності та стійкості діяльності підприємства. Вони підтримують прийняття управлінських рішень через формування та перевірку надійної інформаційної бази, оцінювання ризиків і контролів, а також попередження фінансових втрат. В умовах цифровізації їх значення зростає, оскільки управління дедалі більше спирається на дані, що створюються автоматизованими системами, а ризики зміщуються від суто облікових помилок до ризиків цифрового середовища, якості даних, правильності способів обробки, кіберзагроз, несанкціонованих змін і збоїв у цифрових ланцюгах створення вартості.

Цифровізація змінює роль аудиту від переважно ретроспективного аналізу підтвердження звітності до більш комплексної оцінки надійності процесів і систем, у яких формується фінансова інформація. Водночас функція фінансової безпеки переходить від фрагментарного реагування на окремі порушення до системного управління загрозами, пов’язаними з цифровими фінансовими потоками, інтеграціями, електронними документами, платіжними інструментами та віддаленим доступом. Унаслідок цього аудит і фінансова безпека дедалі частіше орієнтуються на попередження помилок, а раннє виявлення відхилень, моніторинг ризикових операцій і супровід менеджменту у створенні ефективного контрольного середовища.

Важливим є взаємозв’язок аудиту та фінансової безпеки з іншими складовими корпоративного управління, а саме:

- *комплаєнсом;*
- *ризик-менеджментом;*
- *внутрішнім контролем;*
- *ІТ-безпекою.*

Комплаєнс забезпечує дотримання вимог законодавства й внутрішніх політик, ризик-менеджмент формує підходи до ідентифікації та оцінювання ризиків, внутрішній контроль створює контрольні процедури в операційних процесах, а IT-безпека відповідає за захист інформаційної інфраструктури. У цифровому середовищі ці функції мають діяти узгоджено, оскільки більшість фінансових ризиків набуває змішаного характеру. Наприклад, порушення вимог комплаєнсу може бути наслідком помилкової інтеграції даних, а фінансові втрати результатом кіберінциденту або несанкціонованого доступу.

Концепція «трьох ліній захисту» (управління → контроль → внутрішній аудит) у цифровому середовищі зберігає свою актуальність, проте здобуває нового змісту.

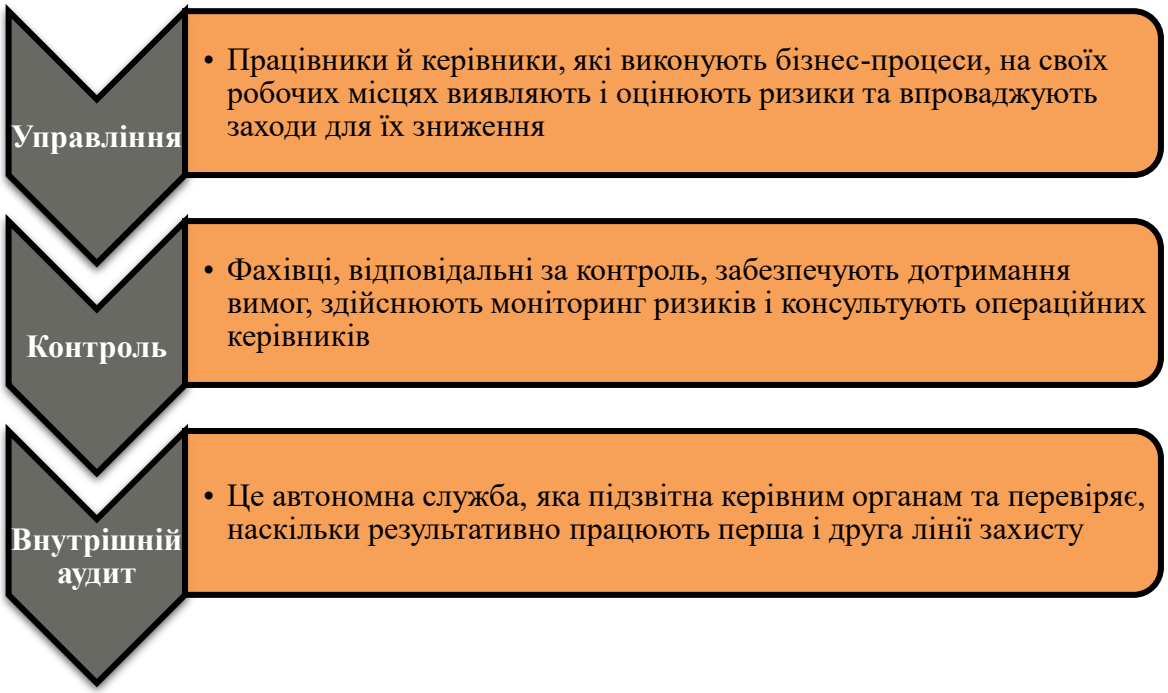


Рис. 3.6. Схема трьох ліній захисту підприємства

Отже, цифрове середовище посилює вимоги до координації між лініями захисту, формалізації контрольних процедур у системах та переходу від разових перевірок до більш безперервного контролю й аналітики. У цифровому середовищі чітке розмежування відповідальності між аудитором, підрозділами внутрішнього контролю та службою фінансової безпеки є необхідною умовою ефективного корпоративного управління. Це розмежування забезпечує, з одного боку, належний рівень захисту фінансових ресурсів і даних, а з іншого –

збереження незалежності аудитора та об'єктивності його висновків. Цифровізація ускладнює межі компетенцій, оскільки значна частина контролів реалізується в інформаційних системах, а ризики мають одночасно фінансовий, операційний та кібернетичний характер, що вимагає координації функцій при збереженні їх автономності.

Аудитор у системі контролю виконує насамперед функцію незалежного підтвердження. Його ключове призначення полягає у висловленні обґрунтованої думки щодо достовірності фінансової звітності та, за потреби, щодо надійності процесів і систем, які формують звітні показники.

Для цього аудитор оцінює ризики суттєвих викривлень, перевіряє ефективність внутрішніх контролів, отримує достатні й прийнятні аудиторські докази та формує висновки. Важливо підкреслити, що аудитор не відповідає за побудову системи контролю або за запобігання порушенням. Ці функції належать управлінському персоналу та контрольним підрозділам; аудитор лише оцінює, наскільки ці механізми є адекватними та ефективними в контексті завдань аудиту.

Фахівець з фінансової безпеки виконує превентивну та операційну функцію захисту. Його завданням є ідентифікація загроз фінансовим ресурсам і даним, таких як шахрайство, зловживання, підміна реквізитів, компрометація доступів, несанкціоновані зміни, організація постійного моніторингу ризикових подій, впровадження механізмів захисту та координація дій під час інцидентів.

У цифровому середовищі фінансова безпека тісно взаємодіє з IT-безпекою, оскільки значна частина загроз реалізується через цифрові канали та інформаційні системи, а доказова база для розслідувань формується у вигляді логів, журналів змін і метаданих.

Межа між аудитом, внутрішнім контролем і службою безпеки визначається насамперед відповідальністю за створення та виконання контролів і рівнем незалежності. Внутрішній контроль (перша та друга лінії захисту) відповідає за розробку, впровадження та функціонування контрольних процедур у процесах і системах, включаючи автоматизовані правила, маршрути

узгодження, ліміти та блокування. Служба фінансової безпеки забезпечує захист від загроз, організовує моніторинг і реагування, проводить перевірки й розслідування в межах своїх повноважень. Аудит, як третя лінія, здійснює незалежну оцінку ефективності цих механізмів і формує висновок, не підміняючи функції управління чи безпеки.

Щоб не втрачати незалежність, аудитор не повинен брати участь у прийнятті управлінських рішень щодо налаштування систем, розподілу прав доступу, впровадження контрольних процедур або оперативного реагування на інциденти. Допустимою є надання рекомендацій та повідомлення про виявлені недоліки, однак відповідальність за реалізацію заходів залишається за керівництвом і відповідними підрозділами. Таким чином, у цифровому середовищі ефективність контролю досягається через координацію функцій, але незалежність аудиту забезпечується чітким поділом ролей, адже безпека будує й захищає, контроль – забезпечує виконання процедур, аудит – незалежно оцінює та підтверджує.

Глобальні Стандарти внутрішнього аудиту вступили в дію в 2015 році. Вони містять 15 принципів стосовно діяльності, етичних особливостей та особливостей проведення внутрішнього аудиту. Цифровізація змінює інструменти й середовище внутрішнього аудиту, однак не змінює його базових етичних засад. Навпаки, робота з великим обсягом інформації, доступ до інформаційних систем, використання аналітики та автоматизованих інструментів підсилюють вимоги до чесності, об’єктивності, компетентності, професійної ретельності та конфіденційності аудитора.

Принципи стосовно етики і професіоналізму:

1. Демонструвати чесність

Внутрішній аудитор у цифровому середовищі має діяти доброчесно, не спотворювати результати аналізу та не використовувати доступ до систем і даних у власних інтересах. Чесність передбачає прозоре документування джерел цифрових доказів, коректне відображення обмежень доступу та якості даних, недопущення маніпулювання вибірками або налаштуваннями аналітичних

інструментів для отримання необхідного висновку. Аудитор також зобов'язаний повідомляти про виявлені порушення та ризики незалежно від їхньої чутливості для керівництва.

2. Підтримувати об'єктивність

Об'єктивність у цифрових умовах означає незалежність професійних суджень від впливу власників процесів, IT-підрозділу, постачальників програмного забезпечення та інших зацікавлених сторін. Аудитор має уникати ситуацій, коли він перевіряє результати власної участі у впровадженні систем, або коли його оцінки залежать від доступу, який надає перевірюваний підрозділ. Для збереження об'єктивності важливо розмежовувати ролі, де аудитор оцінює та рекомендує, але не налаштовує контрольні правила в системі й не управляє об'єктами перевірки.

3. Демонструвати компетентність

Компетентність внутрішнього аудитора в цифровому середовищі включає не лише знання методики аудиту, а й базове розуміння інформаційних систем і даних. Аудитор повинен орієнтуватися в принципах роботи програмного забезпечення, у ролях і правах доступу, а також у поняттях якості даних і цифрових доказів (електронні документи, КЕП/ЕЦП, метадані, журнали подій). За відсутності необхідних знань аудитор зобов'язаний залучати IT-спеціалістів або експертів з аналітики даних, забезпечуючи при цьому контроль якості їхньої роботи та збереження конфіденційності.

4. Застосовувати належну професійну ретельність

Належна професійна ретельність у цифровому аудиті передбачає критичну оцінку достовірності цифрових джерел, перевірку повноти та цілісності даних, а також правильності застосування аналітичних методів. Аудитор має перевіряти, чи дані, що аналізуються, є повними (повний період, усі підрозділи, всі типи операцій), чи не містять дублювань або пропусків, чи забезпечена простежуваність від внесення операцій до показника звітності. При використанні автоматизованих інструментів (аналітики, скриптів, ШІ) аудитор повинен документувати параметри їх застосування, межі точності та ризики помилкових

спрацювань, а також підтверджувати висновки альтернативними процедурами там, де це необхідно.

5. Дотримуватися конфіденційності

У цифровому середовищі конфіденційність охоплює захист не тільки змісту даних, але й доступів до систем, логів, метаданих і технічної інформації про контрольне середовище. Аудитор зобов'язаний використовувати принцип мінімально необхідного доступу, не копіювати надмірні масиви даних, забезпечувати захист робочих файлів (контроль доступу, шифрування, захищені канали обміну), а також дотримуватися правил збереження й знищення інформації після завершення завдання. Особлива увага приділяється роботі з персональними даними та комерційною таємницею, оскільки їх витік може спричинити правові наслідки та фінансові втрати для підприємства.

У межах виконання мандату внутрішнього аудиту аудитори, як правило, отримують широкий доступ до даних, документів і відомостей, необхідних для проведення перевірок. Така інформація може мати різний статус – службовий, конфіденційний або містити персональні дані і надходити як у паперовій, так і в електронній формі, а також під час усних комунікацій (офіційних чи неформальних зустрічей). Тому ключовою етичною вимогою є повага до цінності та права власності на отриману інформацію, її слід використовувати виключно для професійних цілей і забезпечувати належний захист від несанкціонованого доступу чи розголошення як усередині організації, так і за її межами.

Під час роботи з чутливою інформацією внутрішній аудит має застосовувати адекватні заходи інформаційної та цифрової безпеки.

До таких заходів належать:

- *організаційні та технічні контролі;*
- *керування доступами за принципом «необхідного мінімуму»;*
- *використання паролів;*
- *багатофакторної автентифікації;*
- *шифрування;*

- *обмеження копіювання та передавання даних;*
- *контроль за обміном через електронну пошту;*
- *правила поводження з документами у друкованому вигляді.*

Особливу небезпеку становить зловживання інформацією, наприклад використання внутрішніх фінансових, стратегічних або операційних відомостей у власних інтересах чи їх передавання третім сторонам, що може завдати організації прямих фінансових і репутаційних втрат.

Інформація, яку внутрішній аудит отримує, обробляє та створює (робочі документи, аналітичні файли, висновки, комунікації), підлягає захисту відповідно до законодавчих і нормативних вимог, а також внутрішніх політик організації. Такі політики зазвичай регламентують порядок доступу, зберігання, архівування та видалення даних, включаючи вимоги щодо фізичної охорони носіїв і цифрового захисту систем. У випадках, коли питання розкриття інформації має правові наслідки (наприклад, судові спори, запити контролюючих органів, правові привілеї чи адвокатська таємниця), керівнику внутрішнього аудиту доцільно взаємодіяти з юридичним радником для належного визначення меж допустимого розповсюдження та порядку зовнішнього оприлюднення.

Важливою практикою є контроль і простежуваність доступу до інформації, журнали доступу, реєстри документів, контроль використання прав у системах можуть застосовуватися для підтвердження дотримання методології та запобігання витокам. З метою мінімізації ризиків навмисного або випадкового розголошення використовують методи контролю, шифрування, захист паролями, обмеження фізичного доступу, правила поводження в соціальних мережах, а також процедурне вилучення доступів після завершення робіт. Коли потреба в інформації відпадає, цифрові дозволи мають бути відкликані, а паперові матеріали повернені, знищені або заархівовані відповідно до встановлених правил. Прикладом інформації, що потребує підвищеного рівня захисту, є відомості про індивідуальні винагороди, персональні дані працівників та інша чутлива кадрова інформація.

Керівник функції внутрішнього аудиту повинен періодично оцінювати, чи відповідає обсяг доступу аудиторів їхнім завданням, і чи є механізми управління доступом ефективними. Також важливо забезпечити навчання персоналу з питань захисту інформації та підтвердження того, що аудитори розуміють вимоги внутрішніх вимог і законодавчих норм. Дотримання конфіденційності та безпеки інформації має підтверджуватися документально і наявністю методологічних процедур, доказами впровадження контролів доступу, записами про навчання, підтвердженнями ознайомлення з правилами, визначенням обмежень щодо поширення робочих документів і фінальних звітів, а також оформленими рішеннями про санкціоноване розкриття інформації. Додатковим інструментом є угоди про конфіденційність та результати внутрішніх оглядів, які засвідчують дотримання встановленого порядку захисту і розкриття інформації.

У цифрових умовах етика та професіоналізм внутрішнього аудитора проявляються не лише в коректності висновків, а й у відповідальному поводженні з даними та цифровими інструментами, доброчесному формуванні доказів, незалежному судженні, достатній цифровій компетентності, ретельній перевірці якості даних і безумовному дотриманні конфіденційності (рис. 3.7).

Рис. 3.7. Етичні та правові засади проведення аудиту в цифровому середовищі

Цифровізація обліку та аудиту істотно розширює коло даних, з якими працюють аудитори й фахівці контрольних функцій, а отже, підвищує значущість етичних і правових вимог щодо їх використання. На відміну від традиційного середовища, де основними носіями доказів були паперові документи, у цифровому аудиті доказова база формується з електронних документів, баз даних, журналів подій, метаданих і цифрових слідів користувачів. Це потребує не лише технічної компетентності, а й чіткого дотримання принципів професійної етики, конфіденційності та законодавчих обмежень на обробку інформації.

1. Конфіденційність і доступ до персональних та комерційних даних

Під час аудиту в цифровому середовищі аудитор отримує доступ до значних масивів інформації, яка може містити персональні дані працівників і контрагентів, комерційну таємницю, фінансові й технологічні відомості. Відповідно, ключовою етичною вимогою є збереження конфіденційності та використання даних виключно в межах аудиторського завдання. Практично це означає застосування принципу «необхідного мінімуму» доступу, адже аудитор має отримувати лише ті права і лише до тих ресурсів, які потрібні для отримання достатніх і прийнятних доказів. Важливими є також вимоги до безпечного зберігання робочих файлів аудитора, контролю доступу до них, шифрування, використання захищених каналів передачі, а також недопущення несанкціонованого копіювання або передачі даних третім особам. Дотримання конфіденційності в цифровому аудиті охоплює не лише зміст даних, а й метадані та журнали подій, які можуть розкривати внутрішні процеси, структуру доступів та управлінські рішення.

2. Політика збереження та архівації і юридична значимість електронних доказів

Особливістю цифрового середовища є те, що докази існують у змінній формі, адже дані в системах можуть змінюватися внаслідок коригувань, оновлень або автоматизованої обробки, а доступ до них нерідко обмежений строками зберігання логів та архівів. Тому аудитор повинен враховувати

політики збереження, архівації та відтворюваності інформації, а саме хто і як забезпечує зберігання електронних документів, протягом якого часу доступні журнали подій, чи можна відновити історію змін і підтвердити цілісність даних. Юридична значимість електронних доказів визначається їх автентичністю та незмінністю, можливістю ідентифікувати автора окремої дії чи документа, підтвердити час створення і забезпечити простежуваність від первинної події до показника звітності. У практиці це пов'язується з використанням кваліфікованого електронного підпису, статусів електронного документообігу, метаданих, журналів змін і контрольних слідів. Для аудитора важливо документально підтверджувати походження цифрових доказів і зберігати їх у форматі, що забезпечує можливість перевірки в майбутньому, у тому числі в разі спорів або контролю якості аудиту.

3. Незалежність аудитора та конфлікти інтересів у цифрових проєктах

Цифрова трансформація підприємств часто реалізується через впровадження спеціального програмного забезпечення, хмарних сервісів, аналітичних платформ і автоматизації процесів, що створює додаткові ризики для незалежності аудитора. Потенційний конфлікт інтересів виникає тоді, коли аудитор або аудиторська фірма одночасно бере участь у розробці, налаштуванні чи супроводі систем, які потім підлягають аудиторській перевірці, адже це означає перевірку результатів власної роботи. Не менш значущими є загрози зацікавленості та залежності, наприклад, коли суттєва частка доходу аудитора пов'язана з цифровими консалтинговими послугами для того самого клієнта або коли аудитор залучає сторонні цифрові платформи, що можуть впливати на об'єктивність процедур чи доступ до даних. У зв'язку з цим принцип незалежності передбачає чітке розмежування аудиторських і консультаційних функцій, прозоре управління конфліктами інтересів, документування прийнятих запобіжних заходів, а також обмеження участі аудитора в рішеннях управлінського характеру щодо контролів і систем.

Отже, етичні та правові аспекти роботи з даними в цифровому аудиті охоплюють захист конфіденційності та законності доступу, забезпечення

юридичної значимості й відтворюваності електронних доказів, а також збереження незалежності аудитора в умовах активного впровадження цифрових технологій. Дотримання цих вимог є необхідною передумовою довіри до результатів аудиту та легітимності цифрової доказової бази.

Внутрішній аудит зосереджується на незалежній оцінці системи внутрішнього контролю та управління ризиками і надає рекомендації щодо її вдосконалення, тоді як фінансова безпека виконує превентивно-операційну функцію, виявляє та нейтралізує загрози, організовує моніторинг і реагування на інциденти (табл. 3.3). Обидві функції взаємодіють, але не повинні замінювати одна одну. Безпека будує та застосовує захист, а внутрішній аудит перевіряє, чи цей захист і контроль працюють ефективно.

Таблиця 3.3

Місце внутрішнього аудиту в системі фінансової безпеки підприємства в цифровій економіці

Критерій	**Внутрішній аудит**	**Фінансова безпека**
Головна мета	Надати незалежну в межах організації оцінку ефективності системи управління, внутрішнього контролю та корпоративного управління; допомогти покращити процеси	Запобігти фінансовим втратам і загрозам (шахрайство, зловживання, витоки, несанкціоновані операції) та забезпечити стійкість фінансових потоків і активів
Фокус	Системний і процесний: «Чи працює система контролю і ризик-менеджменту?»	Операційний і захисний: «Які загрози є зараз і як їх нейтралізувати?»
Ключові завдання	1) Оцінка внутрішнього контролю та ризик-менеджменту; 2) аудит бізнес-процесів (закупівлі, продажі, запаси тощо); 3) перевірка дотримання політик і процедур (комплаєнс); 4) надання рекомендацій і моніторинг їх виконання; 5) аудит інформаційних контролів і надійності даних	1) Виявлення та попередження шахрайства і зловживань; 2) моніторинг ризикових господарських операцій, контрагентів або платежів; 3) контроль фінансових потоків і протидія підміні; 4) розслідування інцидентів і збір доказів; 5) побудова захисних механізмів (визначення лімітів, правил, контролів доступу разом з IT)

Під час проведення аудиту фінансової безпеки внутрішній аудитор застосовує комплекс інструментів, що забезпечує обґрунтованість висновків і доказовість результатів. До таких інструментів належать:

- *аудиторські програми;*
- *робочі процедури;*
- *тести внутрішніх контролів;*
- *аналітичні методи;*
- *вибіркові перевірки операцій і залишків;*
- *аналітика даних;*
- *інтерв'ю з відповідальними працівниками;*
- *оцінювання ризиків і контрольного середовища.*

За підсумками перевірки формується звіт внутрішнього аудиту, у якому узагальнюються виявлені порушення або слабкі місця системи захисту, надаються рекомендації щодо їх усунення та визначається план коригувальних дій, а також організовується контроль виконання запропонованих заходів.

Аудит фінансової безпеки здійснюється переважно в межах планових перевірок відповідно до ризик-орієнтованого плану, однак може проводитися і позапланово за запитом керівництва або у зв'язку з інцидентами, суттєвими змінами в процесах чи підвищенням рівня ризиків. Важливою умовою ефективності такої роботи є організаційна незалежність внутрішнього аудиту, що забезпечується підзвітністю наглядовій раді або аудиторському комітету та дає змогу об'єктивно оцінювати діяльність підрозділів і контрольних функцій. При цьому внутрішній аудитор не виступає «власником» процесів і контролів та не замінює управлінський персонал у впровадженні захисних механізмів; його роль полягає в незалежному оцінюванні ефективності системи фінансової безпеки, виявленні недоліків і наданні рекомендацій щодо вдосконалення.

3.4. Контрольні питання для самоперевірки

1. У чому полягає сутність цифрової трансформації обліку й аудиту та чим вона відрізняється від простої автоматизації?
2. Які ключові зовнішні фактори стимулюють цифровізацію обліку й аудиту?
3. Які внутрішні фактори визначають потребу цифрових змін на підприємстві?
4. Які етапи цифрової трансформації обліку й аудиту у світі можна виокремити та які їх характерні риси?
5. Як розвивався аудит в Україні?
6. Охарактеризуйте методичні прийоми аудиту в цифровому середовищі
7. Охарактеризуйте періоди цифрової трансформації аудиту в Україні.
8. Які переваги застосування цифрових технологій в аудиті
9. Опишіть схему створення трьох ліній захисту підприємства.
10. Які етичні та правові вимоги є критичними для аудитора в цифрових умовах згідно з Глобальниими стандартами внутрішнього аудиту?

Розділ 4

Автори:
Віталій Бобрівець
Дмитро Сушко

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО АУДИТУ

РОЗДІЛ 4. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО АУДИТУ

«Свобода полягає в можливості робити все те, що дозволено законом.»

Шарль Монтеск'є

4.1. Міжнародні стандарти аудиту щодо використання ІТ та цифрових інструментів

Стрімкий розвиток інформаційних технологій сьогодення та масштабна цифровізація економічних процесів істотно трансформували середовище функціонування суб'єктів господарювання. Переважна більшість господарських операцій здійснюється з використанням автоматизованих систем, електронних платформ та цифрових сервісів. У результаті трансформується не лише бухгалтерський облік, а й підходи до його перевірки. Аудитор сьогодні працює не з паперовими документами чи вибірковими даними, а з комплексними інформаційними середовищами, де значна частина процесів виконується алгоритмами.

Використання програм аналізу великих масивів інформації, автоматизованих процедур тестування, електронних доказів та дистанційного доступу до облікових систем змінило характер аудиторських процедур. Такі зміни поставили перед професією аудитора нові вимоги від загальнометодологічних до нормативних. Без чітких правил застосування

технологій зростає ризик помилкового тлумачення результатів перевірки або неналежної оцінки інформаційних ризиків.

Міжнародні стандарти аудиту встановлюють вимоги щодо оцінювання ризиків суттєвого викривлення у середовищі інформаційних систем, використання комп'ютеризованих засобів аудиту, отримання та документування електронних доказів, а також формування професійного судження при застосуванні автоматизованих інструментів. Вони орієнтовані на забезпечення якості аудиторських процедур незалежно від рівня технологічної складності діяльності клієнта. Разом із тим, швидкість розвитку цифрових технологій ставить перед професійною спільнотою завдання постійного оновлення підходів та адаптації стандартів до нових викликів.

Далі систематизовано в таблиці міжнародні стандарти аудиту щодо використання ІТ та цифрових інструментів (відповідно до чинної системи МСА, розробленої IAASB) (табл. 4.1).

Таблиця 4.1

Міжнародні стандарти аудиту щодо використання ІТ та цифрових інструментів

Стандарт (МСА)	Назва стандарту	Аспекти, пов'язані з ІТ та цифровими інструментами	Практичне значення для аудитора
МСА 200	Загальні цілі незалежного аудитора та проведення аудиту відповідно до МСА	Визначає необхідність застосування професійного судження та скептицизму незалежно від форми даних (у тому числі електронної)	Формує загальні принципи роботи аудитора в цифровому середовищі
МСА 220	Управління якістю під час аудиту фінансової звітності	Передбачає належний контроль якості при використанні спеціалізованого програмного забезпечення та ІТ-інструментів	Забезпечує надійність результатів аудиту в умовах автоматизації
МСА 230	Аудиторська документація	Визначає вимоги до оформлення та зберігання електронних робочих документів	Регулює створення цифрових аудиторських файлів і архівів

Стандарт (МСА)	Назва стандарту	Аспекти, пов’язані з ІТ та цифровими інструментами	Практичне значення для аудитора
МСА 240	Відповідальність аудитора щодо шахрайства	Передбачає врахування ризиків шахрайства в автоматизованих системах обліку	Орієнтує аудитора на аналіз ІТ-контролів і логів операцій
МСА 315	Ідентифікація та оцінка ризиків суттєвого викривлення	Містить вимоги щодо розуміння ІТ-середовища, загальних ІТ-контролів та автоматизованих процесів	Ключовий стандарт для оцінки ризиків у цифрових системах
МСА 330	Реагування аудитора на оцінені ризики	Передбачає застосування автоматизованих процедур перевірки та тестування контролів	Дозволяє використовувати CAATs та аналітичні інструменти
МСА 402	Аудиторські міркування щодо суб’єкта, який використовує організацію з надання послуг	Регулює перевірку даних, що обробляються сторонніми ІТ-провайдерами (хмарні сервіси, аутсорсинг)	Актуальний при використанні хмарних технологій
МСА 500	Аудиторські докази	Визначає вимоги до достатності й належності електронних доказів	Легітимізує використання цифрових джерел інформації
МСА 520	Аналітичні процедури	Дозволяє застосування програм аналізу великих масивів даних	Підтримує використання Data Analytics
МСА 530	Аудиторська вибірка	Передбачає можливість автоматизованого відбору вибірки	Використання програмного забезпечення для статистичного аналізу
МСА 540	Аудит облікових оцінок	Враховує використання складних моделей і алгоритмів при формуванні оцінок	Вимагає розуміння автоматизованих розрахункових систем
МСА 550	Пов’язані сторони	Передбачає використання електронних баз даних для ідентифікації пов’язаних осіб	Застосування цифрового пошуку та перехресного аналізу
МСА 570	Безперервність діяльності	Вимагає аналізу прогнозних даних, сформованих в ІТ-системах	Використання цифрових фінансових моделей

Стандарт (МСА)	Назва стандарту	Аспекти, пов’язані з ІТ та цифровими інструментами	Практичне значення для аудитора
МСА 700	Формування думки та надання звіту	Допускає складання та подання аудиторського звіту в електронній формі	Забезпечує юридичну силу електронного аудиторського висновку

Міжнародні стандарти аудиту не виділяють окремого стандарту, присвяченого виключно цифровим інструментам, проте більшість із них містить положення, що регулюють роботу аудитора в умовах автоматизованого середовища. Найбільш вагоме значення для оцінки ІТ-систем має МСА 315, який деталізує вимоги щодо розуміння інформаційних технологій клієнта та пов’язаних ризиків.

МСА 315 зосереджує увагу аудитора на глибокому розумінні інформаційного середовища суб’єкта господарювання як складової системи внутрішнього контролю. У сучасних умовах це означає обов’язкове дослідження архітектури ІТ-систем, рівня автоматизації бізнес-процесів, характеру доступу до даних та наявності загальних і прикладних ІТ-контролів.

Оцінка ІТ-систем не обмежується технічним описом програмного забезпечення. Аудитор має з’ясувати, яким чином інформаційні технології впливають на формування облікових записів, автоматичні розрахунки, обробку транзакцій та підготовку фінансової звітності. Особлива увага приділяється існуванню автоматизованих контрольних процедур, які можуть запобігати або своєчасно виявляти суттєві викривлення.

На рисунку 4.1 представлено особливості МСА 315.

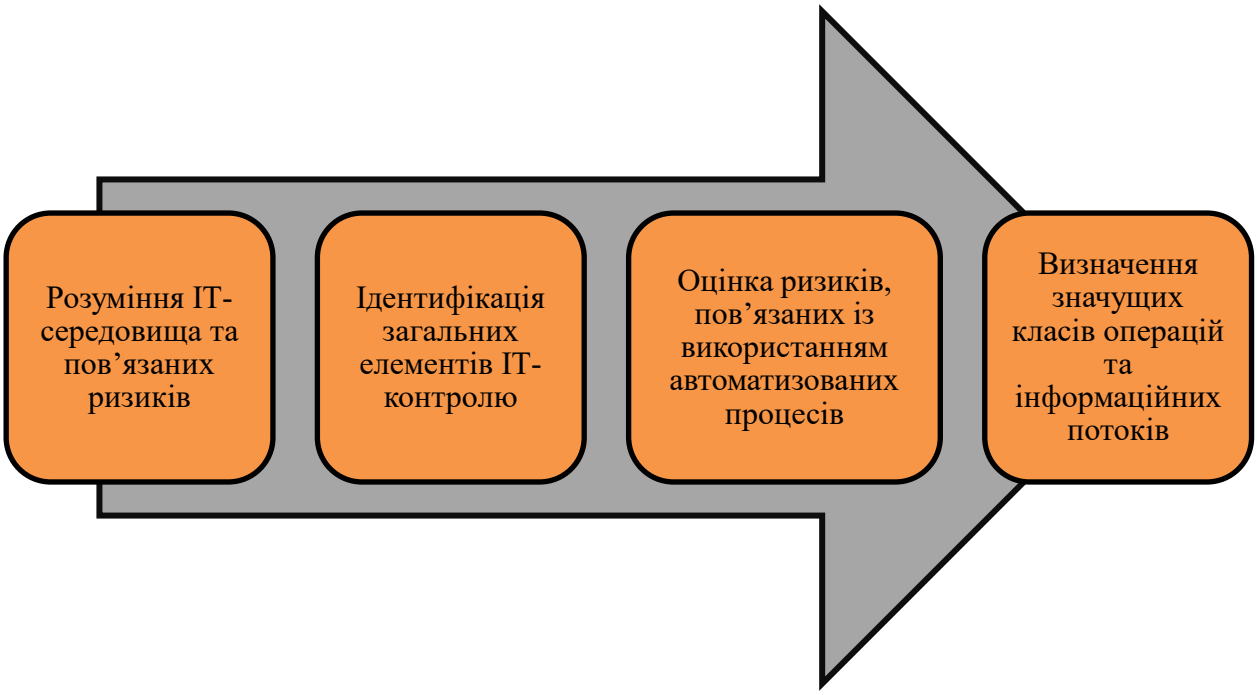


Рис. 4.1. Ключові особливості МСА 315

Зауваження

Якщо підприємство використовує складні ERP-системи, хмарні рішення або інтегровані платформи обробки даних, аудитор повинен оцінити не лише логіку обробки операцій, а й надійність середовища, у якому ці операції здійснюються. Недостатній контроль доступу, відсутність належного управління змінами програмного забезпечення чи слабка система резервного копіювання можуть підвищити ризик суттєвого викривлення фінансової звітності.

Таким чином, МСА 315 формує структурований алгоритм дій аудитора при роботі з IT-системами, орієнтований на ризик-орієнтований підхід і взаємозв'язок між технологічним середовищем та фінансовими показниками.

В подальших таблицях наведено вимоги МСА 315 з відповідними параграфами щодо IT-середовища (табл. 4.2) та порівняння МСА 315 з МСА 330 (табл. 4.3; табл. 4.4; рис. 4 .2).

Таблиця 4.2

Розширена таблиця вимог МСА 315 з прив’язкою до параграфів щодо ІТ-середовища

Параграф / Розділ стандарту	Суть вимоги	Зміст у контексті ІТ	Практичне значення для аудитора
п. 19	Аудитор повинен сформувати розуміння суб’єкта діяльності та його середовища	Оцінює, як ІТ інтегрована в операції і впливає на обробку даних	Дає загальне уявлення про роль ІТ у бізнес-процесах
п. 25(a)	Розуміння інформаційної системи та комунікації	Вивчення ІТ-інфраструктури, шляхів обробки даних, програмного забезпечення	Виявлення ключових потоків інформації, що впливають на звітність
п. 25(b)	Розуміння комунікацій у межах контролю	Як дані передаються між підрозділами/системами	Визначення, чи забезпечено належну передачу інформації
п. 26	Вивчення ресурсів ІТ	Ідентифікація облікових систем, серверів, ERP-середовищ	Дає змогу оцінити технічні складові обробки фінансових даних
п. 28	Загальні ІТ-контролі (GITC)	Контроль доступу, управління змінами, резервне копіювання тощо	Оцінка здатності таких контролів запобігати викривленням
п. 29	Прикладні ІТ-контролі	Автоматизовані перевірки, валідації введення даних	Перевірка правильності побудови автоматичних контрольних процедур
п. 31	Визначення ІТ-ризиків	Ризики, пов’язані з обробкою, доступом і цілісністю даних	Ідентифікація факторів, що можуть призвести до викривлень
п. 32–33	Значущі класи операцій	Визначення процесів, що обробляються ІТ та впливають на звітність	Фокусування на ті ІТ-процеси, що створюють найбільші ризики
п. 34	Оцінка ризиків суттєвого викривлення	Використання отриманого розуміння ІТ для оцінки ризиків	Формування переліку ризиків і напрямів аудиту
п. 36	Документування результатів розуміння	Зафіксоване розуміння ІТ-середовища та оцінених ризиків	Формує основу для наступних аудиторських процедур

Таблиця 4.3

Порівняльна таблиця МСА 315 з МСА 330 щодо ІТ

Критерій порівняння	МСА 315	МСА 330
Функціональне призначення	Визначення ризиків, що випливають із ІТ-середовища	Реалізація процедур у відповідь на ці ризики
Етап аудиту	Планування та оцінка ризиків	Виконання перевірок і тестів
ІТ-компоненти, що оцінюються	Розуміння ІТ-систем, їх ролі у внутрішньому контролі	Перевірка операційної ефективності ІТ-контролів
Загальний ІТ-контроль (GITC)	Ідентифікація і оцінка дизайну	Тестування фактичного функціонування
Прикладний ІТ-контроль	Розуміння логіки автоматизації	Перевірка результатів автоматизованих аудиторських процедур
Обробка даних та системні ризики	Оцінювання ризиків суттєвих викривлень у ІТ	Докази щодо достатності й належності доказів
Документування	Фіксація розуміння ІТ як частини оцінки ризиків	Докази виконання процедур, обґрунтування висновків
Результат застосування	Перелік ризиків, що потребують аудиторської уваги	Перелік аудиторських процедур і їх результатів

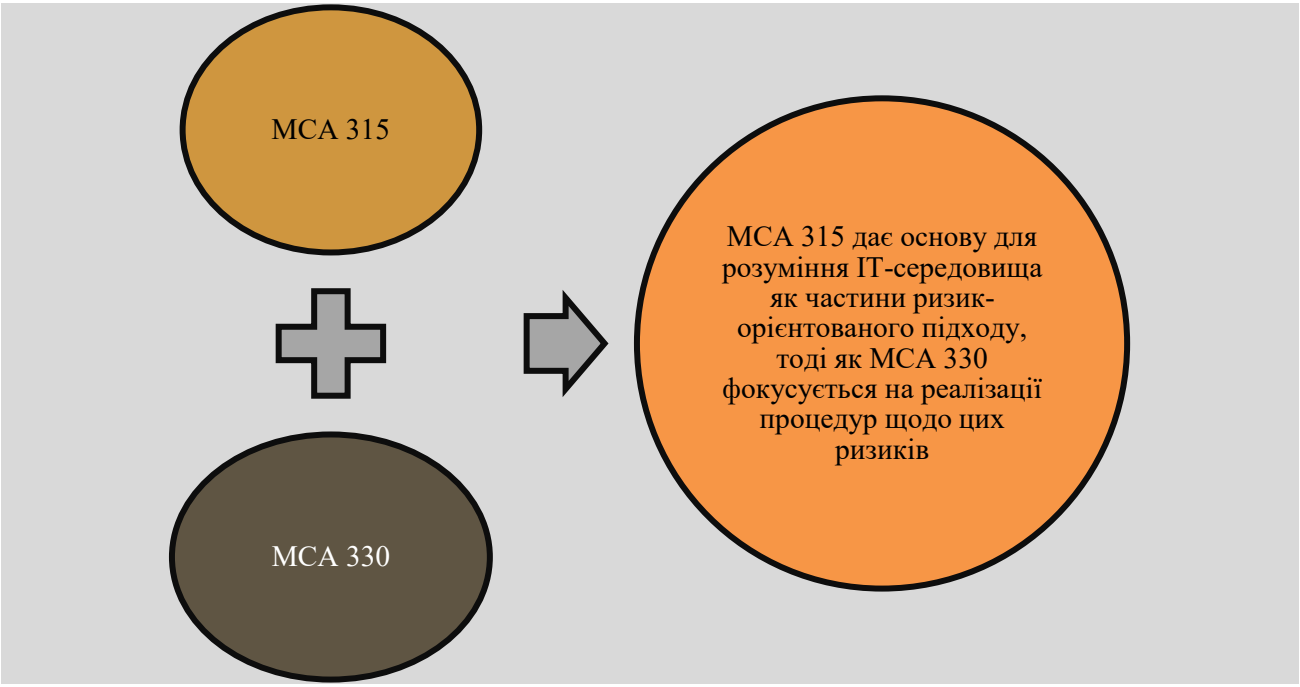


Рис. 4.2. Особливості МСА 315 та МСА 330

Таблиця 4.4

Практичні приклади аудиторських процедур щодо IT-контролю (МСА 315 та МСА 330)

Вид IT-контролю	Етап за МСА 315 (оцінка ризиків)	Процедури за МСА 330 (реагування)	Приклад практичного виконання	Очікуваний аудиторський доказ
Контроль доступу до системи (GITC)	Визначення, хто має доступ до облікової системи та рівнів прав	Тестування ефективності контролю доступу	Перевірка переліку користувачів, аналіз прав адміністратора, вибіркова перевірка звільнених працівників	Підтвердження обмеженого та санкціонованого доступу
Управління змінами програмного забезпечення	Оцінка наявності процедури затвердження змін	Перевірка документального підтвердження внесених змін	Вибіркова перевірка змін у конфігурації ERP та наявності погоджень	Доказ контрольованого внесення змін
Резервне копіювання та відновлення даних	Аналіз політики збереження та архівування	Тестування фактичного створення резервних копій	Перевірка журналів backup, тест відновлення даних	Підтвердження цілісності інформації
Автоматизовані розрахунки (прикладні контролі)	Визначення алгоритмів автоматичного нарахування (ПДВ, амортизації)	Перерахунок або повторне виконання процедур	Перевірка правильності формул у системі на вибіркових операціях	Доказ коректності автоматичних обчислень
Логування операцій (audit trail)	З'ясування наявності журналів операцій	Аналіз логів щодо підозрілих змін	Вибірковий перегляд журналів змін проведень	Доказ відсутності несанкціонованих втручань
Інтеграція з хмарними сервісами	Встановлення залежності від сторонніх IT-провайдерів	Оцінка контролів організації-постачальника послуг	Аналіз договору, отримання звіту типу ISAE 3402 (за наявності)	Підтвердження надійності обробки даних третьою стороною
Автоматичне формування фінансової звітності	Розуміння процесу трансформації даних у звітність	Тестування узгодженості між обліковими регістрами і звітами	Звірка даних Головної книги зі сформованим звітом	Підтвердження повноти та точності звітності

Вид IT-контролю	Етап за МСА 315 (оцінка ризиків)	Процедури за МСА 330 (реагування)	Приклад практичного виконання	Очікуваний аудиторський доказ
Контроль розмежування обов'язків (SoD)	Аналіз розподілу ролей у системі	Тестування відсутності конфлікту повноважень	Перевірка, чи не поєднує одна особа функції введення та затвердження операцій	Підтвердження належного розподілу функцій

Таким чином, сучасна практика аудиторської діяльності під впливом цифрових змін змінює свою сутність та переходить на новий рівень, який визначається прозорістю з одного боку та підвищеними кіберризиками з іншого. При цьому основними міжнародними стандартами аудиту для України, що регламентують аудиторську діяльність в цифровому форматі, є наступні:

1. Міжнародний стандарт контролю якості 1 «Контроль якості для фірм», що виконують аудити та огляди фінансової звітності, а також інші завдання з надання впевненості, і супутні послуги». Цей стандарт вимагає від аудиторських організацій розробки та впровадження політик і процедур, які враховують сучасні технології, що використовуються в аудиторському процесі.

2. Міжнародний стандарт аудиту 315 «Ідентифікація та оцінювання ризиків суттєвого викривлення через розуміння суб'єкта господарювання і його середовища». Цей стандарт дозволяє аудиторам розуміти ризики, пов'язані з комп'ютеризованими системами, та вживати відповідних заходів щодо їх управління.

3. Міжнародний стандарт аудиту 330 «Дії аудитора у відповідь на оцінені ризики». Цей стандарт дозволяє аудитору зрозуміти, як суб'єкт господарювання відповів на ризики, що походять з IT.

4.2. Законодавче регулювання аудиту в Україні в умовах цифровізації

Законодавче регулювання аудиторської діяльності в Україні формується на основі поєднання національних норм та міжнародних стандартів, що визначають загальні принципи організації, здійснення та контролю якості аудиту. В умовах цифровізації облікових процесів та поширення автоматизованих інформаційних систем особливого значення набуває здатність чинного законодавства адаптуватися до використання цифрових інструментів без порушення фундаментальних засад аудиторської професії.

Основним нормативно-правовим актом, що визначає правові засади аудиторської діяльності в Україні, є Закон України ***«Про аудит фінансової звітності та аудиторську діяльність»*** від 21.12.2017 р. № 2258-VIII. Його положення мають принциповий характер і не обмежуються конкретними технологічними рішеннями, що дозволяє розглядати цифровий аудит не як окремий вид діяльності, а як еволюційний етап розвитку аудиторських процедур. Закон закріплює базові вимоги до статусу аудитора, принципів професійної етики, незалежності, професійного скептицизму, належного документування та контролю якості, які однаковою мірою поширюються як на традиційні, так і на цифрові форми проведення аудиту.

У контексті цифровізації цей Закон закріплює такі принципи:

- *належного документування;*
- *професійного судження;*
- *незалежності та відповідальності аудитора.*

Вони застосовуються незалежно від формату виконання процедур – традиційного чи з використанням цифрових технологій, автоматизованих засобів обробки даних та комп'ютеризованих засобів аудиту (CAATs). Закон встановлює, що аудит має здійснюватися з дотриманням міжнародних стандартів аудиту, що створює правове підґрунтя для застосування аналітичних платформ, автоматизованого аналізу даних та електронного документообігу як елементів професійної аудиторської практики.

Закон України ***«Про аудит фінансової звітності та аудиторську діяльність»*** прямо не містить спеціальних норм щодо цифрових інструментів, його загальні положення не обмежують аудитора у виборі технічних засобів виконання аудиторських процедур, що фактично створює правові передумови для їх використання, зокрема для автоматизованого збору, обробки, аналізу та збереження цифрових аудиторських доказів. При цьому належність застосовуваних процедур до вимог закону і стандартів визначається методологічною відповідністю, відтворюваністю, документованістю та здатністю забезпечувати аудиторські докази професійної якості, незалежно від того, чи формуються вони в електронних середовищах чи на паперових носіях.

Таким чином, сучасна редакція Закону України «Про аудит фінансової звітності та аудиторську діяльність» забезпечує гібридну правову модель, у якій цифрові інструменти є не зовнішнім доповненням, а невід'ємною частиною реалізації професійних норм аудиту в електронному середовищі, що відповідає вимогам адаптації національного регулювання до умов глобальної цифрової економіки та інформаційних стандартів професійної практики.

Відсутність у Законі прямої регламентації конкретних цифрових інструментів або програмних продуктів не є нормативною прогалиною, а навпаки – створює гнучке правове середовище для впровадження комп'ютеризованих засобів аудиту (CAATs), спеціалізованого програмного забезпечення, інструментів аналізу великих масивів даних та автоматизованих процедур тестування. Водночас відповідальність за правильність їх застосування та інтерпретацію результатів повністю покладається на аудитора, що відповідає концепції професійного судження, закріпленої в законодавстві та міжнародних стандартах.

Системний аналіз норм Закону України «Про аудит фінансової звітності та аудиторську діяльність» дозволяє виокремити положення, які мають безпосереднє значення для розвитку та практичного застосування цифрового аудиту. Узагальнення таких норм та їх функціональне значення наведено в таблиці 4.5

Таблиця 4.5

Основні складові Закону України «Про аудит фінансової звітності та аудиторську діяльність» та їх значення для цифрового аудиту

Стаття закону	Зміст вимог	Значення для цифрового аудиту
Стаття 1. Визначення термінів	Встановлює базові поняття аудиторської діяльності, зокрема дає визначення термінів: «аудит фінансової звітності», «аудитор», «аудиторська діяльність», «аудиторська мережа», «аудиторська фірма», «аудиторський звіт», «аудиторські послуги», «добра репутація аудиторської фірми», «професійний скептицизм», «робочі документи аудитора» тощо	Формує базову правову та методологічну основу для визнання результатів цифрових аудиторських процедур (аналізу електронних масивів даних, автоматизованих тестів контролів, результатів IT-аналітики та спеціалізованого програмного забезпечення) як повноцінних аудиторських доказів. Забезпечує єдине тлумачення понять «професійний скептицизм» і «робочі документи аудитора», що дозволяє правомірно включати цифрові файли, аналітичні звіти та електронні робочі документи до складу аудиторської документації за умови дотримання критеріїв належності, достатності та відтворюваності доказів
Стаття 4. Аудитор	Визначає правовий статус аудитора як суб'єкта професійної діяльності, встановлює вимоги до його кваліфікації, професійної компетентності, знань і навичок, а також персональну відповідальність за дотримання стандартів аудиту, норм професійної етики та якість наданих аудиторських послуг	У контексті цифровізації підкреслює необхідність володіння аудитором сучасними IT-компетенціями, включно зі здатністю використовувати комп'ютеризовані засоби аудиту, спеціалізоване програмне забезпечення та інструменти аналізу великих масивів даних. Норма закріплює вимогу до професійного судження аудитора при інтерпретації результатів автоматизованих аналітичних процедур і покладає на нього відповідальність за обґрунтованість висновків, сформованих на основі цифрових доказів
Стаття 6. Аудиторська діяльність	Регламентує зміст, види та межі аудиторської діяльності, визначає основні принципи її здійснення, а також обов'язковість застосування міжнародних стандартів аудиту, стандартів контролю якості та професійного судження аудитора під час виконання аудиторських процедур	Створює нормативну основу для інтеграції цифрових інструментів у всі етапи аудиторського процесу, оскільки міжнародні стандарти аудиту передбачають використання інформаційних технологій і аналітики даних для ідентифікації та оцінки ризиків, планування перевірки, виконання процедур по суті та формування аудиторських доказів. Норма легітимізує застосування комп'ютеризованих засобів аудиту як повноцінного елементу методології сучасного ризик-орієнтованого аудиту

Стаття закону	Зміст вимог	Значення для цифрового аудиту
Стаття 8. Професійна етика	Встановлює обов'язок дотримання аудиторами принципів професійної етики відповідно до міжнародних етичних стандартів, зокрема принципів чесності, об'єктивності, професійної компетентності та належної ретельності, конфіденційності та професійної поведінки	У цифровому аудиті істотно зростає значення етичних вимог до роботи з даними, оскільки аудитор отримує доступ до великих масивів електронної інформації та автоматизованих аналітичних результатів. Стаття формує нормативні орієнтири щодо забезпечення конфіденційності електронних даних, захисту прав доступу, недопущення несанкціонованого використання інформації та маніпулювання результатами автоматизованих процедур, а також відповідального застосування алгоритмів і професійного судження при інтерпретації цифрових доказів
Стаття 9. Професійний скептицизм	Закріплює обов'язок аудитора застосовувати професійний скептицизм впродовж усього аудиторського завдання, передбачаючи критичну оцінку отриманих доказів, уважність до умов, що можуть свідчити про можливі викривлення внаслідок помилки або шахрайства, а також обґрунтоване використання професійного судження при плануванні та виконанні аудиторських процедур	Застосування цифрових інструментів і автоматизованої аналітики не знижує відповідальності аудитора за результати перевірки. Результати цифрових тестів, аналізу великих масивів даних та IT-звітів мають підлягати критичній оцінці з урахуванням можливих системних викривлень, обмежень алгоритмів, якості вхідних даних і налаштувань програмного забезпечення. Професійний скептицизм виступає ключовим запобіжником проти надмірної довіри до автоматизованих рішень та забезпечує належну інтерпретацію цифрових аудиторських доказів
Стаття 10. Незалежність і об'єктивність аудитора та суб'єкта аудиторської діяльності	Визначає вимоги щодо забезпечення незалежності та об'єктивності аудитора і суб'єкта аудиторської діяльності, передбачає ідентифікацію, оцінку та управління загрозами незалежності, зокрема загрозами власного інтересу, самоперевірки, близьких стосунків, тиску та адвокатування позиції клієнта, а також обов'язок застосування належних запобіжників для запобігання конфлікту інтересів	Використання цифрових платформ клієнта, віддаленого доступу до інформаційних систем, спільних IT-середовищ та інтегрованих ERP-рішень створює додаткові ризики порушення незалежності та об'єктивності аудитора. Це зумовлює необхідність запровадження спеціальних організаційних і технічних запобіжників, зокрема розмежування прав доступу, облік операцій аудитора в інформаційних системах клієнта, застосування принципу мінімально необхідних повноважень, а також документального підтвердження відсутності впливу клієнта на налаштування аудиторських процедур

Стаття закону	Зміст вимог	Значення для цифрового аудиту
Стаття 18. Оприлюднення інформації про діяльність Органу суспільного нагляду за аудиторською діяльністю	Визначає обов'язок забезпечення прозорості та публічності діяльності Органу суспільного нагляду за аудиторською діяльністю шляхом оприлюднення інформації про його повноваження, рішення, результати контролю якості аудиторських послуг, а також відомостей, що підлягають розкриттю відповідно до законодавства	Сприяє цифровій трансформації системи аудиторського нагляду шляхом впровадження та використання електронних реєстрів, онлайн-інструментів звітування і відкритого доступу до інформації про результати перевірок якості аудиту. Це підвищує прозорість цифрових аудиторських практик, посилює довіру користувачів до результатів аудиту та формує додаткові стимули для належного застосування цифрових інструментів і дотримання стандартів якості в умовах автоматизації аудиторських процедур
Стаття 19. Атестація аудиторів	Регулює порядок атестації аудиторів, умови допуску до професії, підтвердження професійної придатності, а також вимоги до рівня знань, навичок і компетентностей осіб, які мають право здійснювати аудиторську діяльність	В умовах цифровізації аудиторської діяльності атестація аудиторів набуває розширеного змісту та має враховувати рівень володіння інформаційними технологіями, знання електронних облікових систем, принципів функціонування ERP-систем, методів аналізу великих масивів даних, а також практичні навички застосування комп'ютеризованих засобів аудиту та спеціалізованого програмного забезпечення. Це забезпечує здатність аудитора професійно оцінювати результати автоматизованих процедур, належно ідентифікувати цифрові ризики та формувати обґрунтовані аудиторські судження в умовах цифрового середовища
Стаття 23. Вимоги до внутрішньої організації суб'єктів аудиторської діяльності, які мають право проводити обов'язковий аудит фінансової звітності	Визначає обов'язкові вимоги до внутрішньої організації суб'єктів аудиторської діяльності, зокрема щодо функціонування системи внутрішнього контролю якості, управління професійними та аудиторськими ризиками, розподілу повноважень і відповідальності, а також належного документування аудиторських процедур і результатів перевірки	Створює нормативні передумови для впровадження в аудиторських фірмах цифрових систем управління якістю, використання електронних робочих файлів аудитора, автоматизованих журналів аудиторських процедур, систем контролю доступу та IT-контролів. У контексті цифровізації ця стаття забезпечує інституційну інтеграцію комп'ютеризованих засобів аудиту у внутрішні процеси аудиторських фірм, підвищує рівень стандартизації та відтворюваності аудиторських процедур, а також сприяє посиленню контролю за дотриманням вимог незалежності, професійного судження і якості аудиторських послуг

Стаття закону	Зміст вимог	Значення для цифрового аудиту
Стаття 36. Звіт для органів нагляду	Регламентує обов'язок суб'єктів аудиторської діяльності подавати органам суспільного нагляду встановлену звітність щодо результатів аудиторської діяльності, системи внутрішнього контролю якості, дотримання вимог незалежності та виконання професійних обов'язків у визначених законом випадках і формах	Закріплює правові підстави для використання електронної звітності та цифрових форматів подання інформації до органів нагляду, включно з передачею структурованих даних, електронних форм звітів і супровідних матеріалів. У контексті цифровізації аудиту ця норма сприяє уніфікації форматів звітності, підвищенню прозорості та оперативності наглядових процедур, а також забезпечує можливість застосування цифрових інструментів аналізу, моніторингу та контролю якості аудиторських послуг на рівні державного та професійного регулювання
Стаття 40. Контроль якості аудиторських послуг	Встановлює порядок, принципи та процедури здійснення контролю якості аудиторських послуг, включно з перевіркою дотримання суб'єктами аудиторської діяльності вимог законодавства, міжнародних стандартів аудиту, норм професійної етики, а також ефективності функціонування систем внутрішнього контролю якості	Контроль якості в умовах цифровізації охоплює оцінку адекватності застосування комп'ютеризованих засобів аудиту (CAATs), обґрунтованості використання спеціалізованого програмного забезпечення та коректності виконання автоматизованих аналітичних процедур. Методичною передумовою цифрового аудиту є здатність аудитора встановити належність і достатність електронних аудиторських доказів, забезпечити відтворюваність цифрових процедур, гарантувати захищеність облікових та аналітичних даних, а також підтвердити відповідність електронної аудиторської документації вимогам міжнародних стандартів аудиту та чинного законодавства України

Закон України «Про аудит фінансової звітності та аудиторську діяльність» не містить спеціалізованих норм, безпосередньо присвячених цифровому аудиту як окремому виду аудиторської діяльності. Водночас його системні положення формують повноцінне й методологічно нейтральне правове середовище для застосування цифрових технологій, комп'ютеризованих засобів аудиту та спеціалізованого програмного забезпечення у сучасній аудиторській практиці. Закріплені Законом принципи незалежності та об'єктивності аудитора, професійного скептицизму, належного документування, відповідальності за

результати перевірки та контролю якості є універсальними й однаковою мірою поширюються на всі форми аудиту – незалежно від ступеня автоматизації аудиторських процедур і характеру використаних цифрових інструментів.

Відтак, ***чинне законодавство України створює правові передумови для розвитку цифрового аудиту шляхом інтеграції інформаційних технологій у традиційну методологію аудиту,*** забезпечуючи баланс між інноваційністю аудиторських підходів і дотриманням фундаментальних вимог професійної відповідальності, доказовості та якості аудиторських послуг.

Разом із тим, аналіз національного законодавства буде неповним без урахування ролі міжнародних стандартів аудиту, які в Україні мають обов'язковий характер застосування та фактично визначають методологічну основу аудиторської діяльності.

Важливою особливістю національного регулювання є орієнтація на імплементацію Міжнародних стандартів аудиту (МСА), які визнаються обов'язковими до застосування в Україні. Через це правова модель аудиту фактично інтегрує міжнародну методологію, зокрема положення щодо використання інформаційних технологій, суцільного аналізу даних, автоматизованих аудиторських процедур та електронних аудиторських доказів. З огляду на те, що цифровізація аудиту реалізується не шляхом ухвалення спеціальних «цифрових» законів, а через функціональне розширення та сучасне тлумачення традиційних норм професійного регулювання, закріплених у МСА та національному законодавстві.

Окреме місце в системі законодавчого забезпечення цифрового аудиту посідають норми, що регулюють електронний документообіг та інформаційні відносини (рис. 4.3).

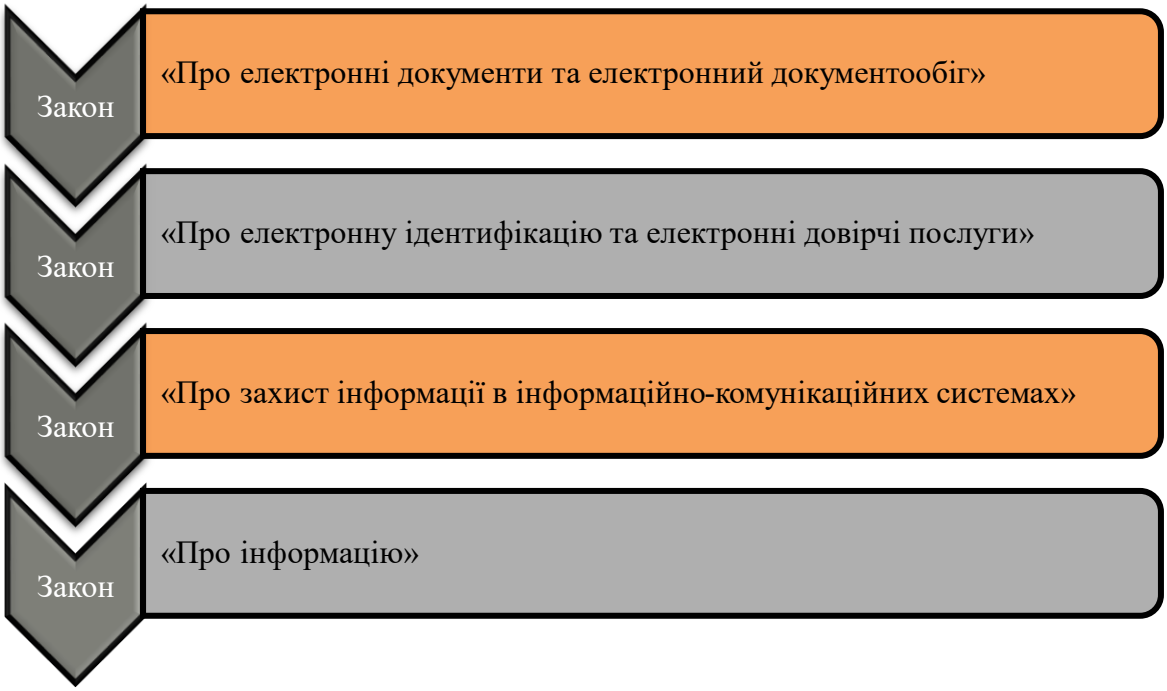


Рис. 4.3. Законодавче забезпечення цифрового аудиту

Саме вони формують правову основу для використання електронних первинних документів, електронного підпису, цифрових регістрів обліку та електронних баз даних як юридично значущих і рівноцінних паперовим джерелам аудиторських доказів.

Значення цих норм полягає не лише у визнанні правового статусу електронних документів, а й у встановленні вимог до їх автентичності, цілісності, захищеності та відтворюваності, що безпосередньо впливає на оцінку належності й достатності аудиторських доказів. Це набуває особливої актуальності в умовах масового впровадження ERP-систем, хмарних платформ обліку та віддаленого доступу до фінансових даних, коли аудитор повинен оцінювати не лише зміст інформації, а й надійність цифрового середовища її формування та зберігання.

Закон України ***«Про електронні документи та електронний документообіг»*** встановлює організаційно-правові засади електронного документообігу та правовий статус електронних документів, електронного підпису та супутніх реквізитів, а також регламентує порядок створення,

оброблення, передавання, отримання, зберігання, використання й знищення електронних документів.

Закон визначає такі ключові поняття:

- *електронний документ;*
- *електронний підпис;*
- *оригінал електронного документа;*
- *електронний документообіг;*
- *суб'єктів електронного документообігу.*

Він встановлює, що електронні документи є юридично значущими та не можуть втрачати правової сили виключно через свою електронну форму. Ці положення закладають основи державної політики у сфері електронного обігу документів і забезпечують правову певність у відносинах, що виникають під час обміну електронними документами між фізичними та юридичними особами, органами влади й іншими учасниками інформаційних процесів.

З погляду цифрового аудиту, цей Закон є фундаментальним нормативним актом, який легітимізує використання електронних первинних документів, електронного підпису та електронного документообігу як джерел аудиторських доказів**,** що формуються, обробляються і зберігаються в цифровому середовищі. Він встановлює правові умови для підтвердження аутентичності, цілісності та юридичної сили електронних документів, що є критично важливим для оцінки аудитором належності й достатності електронних доказів, відтворюваності цифрових процедур та забезпечення збереженості робочих електронних файлів. Закон також регламентує порядок організації електронного документообігу, що визначає вимоги до інформаційної інфраструктури, захисту та доступу до електронних даних, необхідних для проведення аудиту в умовах цифровізації облікового середовища.

Закон України ***«Про електронну ідентифікацію та електронні довірчі послуги»*** встановлює правові, організаційні та технічні засади функціонування системи електронної ідентифікації та надання електронних довірчих послуг на території України.

Закон визначає сутність електронної ідентифікації, електронного підпису та електронних довірчих послуг, порядок їх надання, статус суб'єктів, що їх здійснюють, вимоги до безпеки, а також механізми взаємодії в межах національної та міжнародної електронних довірчих інфраструктур.

Нормативно визначено такі поняття:

- *кваліфікованого електронного підпису;*
- *некваліфікованого електронного підпису;*
- *електронної довірчої послуги;*
- *вимоги до сертифікації провайдерів таких послуг;*
- *правовий статус електронних сертифікатів;*
- *правовий статус засобів ідентифікації;*
- *умови визнання таких послуг в інших юрисдикціях.*

Закон також інтегрується з положеннями Європейського регламенту eIDAS та міжнародними стандартами у сфері електронних довірчих послуг, забезпечуючи правове підґрунтя для їх використання у публічних та приватних інформаційних системах.

У контексті цифрового аудиту Закон України «Про електронну ідентифікацію та електронні довірчі послуги» має важливе значення для забезпечення автентичності, цілісності та юридичної сили електронних аудиторських доказів**.** Норми Закону створюють правову основу для використання кваліфікованих електронних підписів, електронних печаток, засобів електронної ідентифікації та довірчих сервісів у процесі формування, надсилання, збереження та обміну електронними документами у сфері аудиту. Це дозволяє аудиторам сприймати електронні документи та звіти, підписані кваліфікованими електронними підписами, як належні з точки зору законодавчої сили, а також безпечно ідентифікувати суб'єктів, що створюють та передають цифрові аудиторські дані. Такі вимоги є критично важливими для збереження доказової сили електронних робочих документів, гарантування цілісності даних при використанні ERP-систем, хмарних платформ та автоматизованих

аналітичних процедур, що підвищує надійність і достовірність аудиторських висновків у цифровому середовищі.

Закон України ***«Про інформацію»*** регулює суспільні відносини, пов'язані з формуванням, використанням, розповсюдженням, доступом до інформації та її охороною, встановлює загальні принципи інформаційної політики, права та обов'язки суб'єктів інформаційних відносин, а також правовий режим роботи з інформаційними ресурсами в Україні.

Закон визначає основні поняття й категорії, включно з інформацією як об'єктом правовідносин, відкритістю доступу до публічної інформації, обмеженням доступу у визначених законом випадках, а також правовими гарантіями забезпечення прав громадян і юридичних осіб на вільний доступ до інформації.

Законом України «Про інформацію» нормативно визначено:

- *механізми реалізації права на інформацію;*
- *порядок поводження з інформацією в державних інформаційних системах;*
- *порядок поводження з інформацією в комунальних інформаційних системах;*
- *порядок поводження з інформацією в приватних інформаційних системах;*
- *відповідальність за порушення законодавства про інформацію.*

Закон є фундаментальним актом інформаційного права України та створює загальні правові рамки для регулювання відносин у сфері обміну, обробки, зберігання та захисту інформації.

З урахуванням потреб цифрового аудиту Закон України «Про інформацію» відіграє визначальну роль у визначенні правових умов доступу до інформації, регулюванні обігу даних та забезпеченні законних підстав для їх використання аудитором у процесі виконання професійних процедур. У цифровому середовищі аудиторська діяльність передбачає збір, обробку, зберігання та аналіз великих обсягів електронних даних з різних джерел, включно з

інформаційними системами підприємств та відкритими даними. Норми Закону створюють правові підстави для забезпечення доступу до публічної та обмеженої інформації, одночасно визначаючи механізми захисту персональних даних, комерційної та службової таємниці, що є критично важливим для дотримання етичних та правових вимог при роботі з цифровими доказами. Це дозволяє аудитору правомірно збирати, обробляти та інтерпретувати електронні дані відповідно до загальних принципів інформаційного права, що посилює якість, достовірність і доказову силу аудиторських процедур в умовах цифровізації обліково-аудиторського середовища.

Закон України ***«Про захист інформації в інформаційно-комунікаційних системах»*** визначає правові та організаційні засади захисту інформації, що обробляється в інформаційно-комунікаційних системах, незалежно від форми власності та сфери застосування.

Закон регламентує вимоги до створення, впровадження та функціонування комплексних систем захисту інформації, встановлює повноваження суб'єктів інформаційних відносин, а також визначає відповідальність за порушення режиму захисту інформації. Особлива увага приділяється захисту інформації від несанкціонованого доступу, модифікації, знищення чи блокування, що є критично важливим в умовах використання електронних баз даних, мережевих інформаційних систем та хмарних технологій.

Значення цього Закону для цифрового аудиту полягає в тому, що він формує нормативну основу для забезпечення конфіденційності, цілісності та доступності електронних аудиторських доказів.

Вимоги щодо захисту інформації безпосередньо впливають на організацію доступу аудитора до:

- *облікових і фінансових систем клієнта;*
- *використання віддалених підключень;*
- *обробку даних у ERP-середовищах;*
- *збереження електронної аудиторської документації.*

Дотримання положень Закону є необхідною умовою належності цифрових аудиторських доказів, відтворюваності аналітичних процедур та зниження ризиків компрометації даних, що має принципове значення як для якості аудиту, так і для відповідності вимогам професійних стандартів і законодавства.

З позицій контрольної та наглядової логіки цифровізація аудиту знаходить безпосереднє відображення у діяльності ***Органу суспільного нагляду за аудиторською діяльністю та Аудиторської палати України.***

Система зовнішнього контролю якості аудиторських послуг поступово трансформується від формальної перевірки дотримання процедур до оцінки здатності аудитора ефективно працювати з цифровими масивами даних, використовувати комп'ютеризовані засоби аудиту, забезпечувати інформаційну безпеку, відтворюваність аналітичних процедур і належне зберігання електронних робочих документів.

У цьому контексті цифрові інструменти перестають бути виключно технічним елементом аудиторського процесу та набувають статусу об'єкта регуляторної і контрольної уваги, оскільки їх застосування безпосередньо впливає на якість аудиторських доказів, обґрунтованість висновків і рівень аудиторського ризику.

Отже, ***законодавче регулювання аудиту в Україні в умовах цифровізації*** характеризується еволюційним, а не революційним підходом. Цифрові інструменти інтегруються у традиційну правову модель через розширене тлумачення професійних стандартів, норм інформаційного права та практики контролю якості.

Це дозволяє забезпечити баланс між інноваційністю аудиторських процедур та дотриманням фундаментальних принципів професійної відповідальності, належного документування та якості аудиторських послуг.

Судова практика та діяльність органів нагляду підтверджують, що електронні документи, цифрові вибірки та результати автоматизованих процедур можуть визнаватися належними аудиторськими доказами за умови забезпечення їх автентичності, цілісності, захищеності та належного документування. Таким

чином, чинне законодавство України створює правове середовище, яке стимулює розвиток цифрового аудиту, водночас покладаючи на аудитора персональну відповідальність за обґрунтованість висновків та коректне використання цифрових технологій у процесі формування аудиторських доказів.

4.3. Електронні документи, електронний підпис та е-документообіг

Документування та документообіг в умовах цифровізації зазнають якісних змін, оскільки цифрові технології забезпечують створення, обробку, передавання та зберігання документів переважно без використання паперових носіїв. У результаті підвищуються оперативність і точність обробки первинної інформації, посилюється інтеграція з сервісами електронної звітності та іншими цифровими рішеннями, забезпечує керованість документних потоків, а також посилюється прозорість управлінських процедур завдяки фіксації маршрутів погодження, статусів документів і відповідальних осіб.

Важливою особливістю є можливість створення і передачі електронного документу, адже він дедалі частіше поєднується з бухгалтерськими програмами в єдиний інформаційний простір організації.

Електронний документообіг у світі формувався поступово у відповідь на вимоги часу. Його витоки зазвичай відносять до 1960-х років у транспортному секторі США, де електронні повідомлення почали застосовувати для швидшої взаємодії між залізницями, авіакомпаніями та автоперевізниками. Першими електронними документами стали заявки на перевезення, відвантажувальні повідомлення, накладні, рахунки та інші супровідні документи.

Державна політика України підтримує масштабне впровадження цифрових технологій у процеси документування та розвиток електронного урядування. Зокрема, у стратегічних документах національного рівня наголошується на необхідності розбудови ефективної міжвідомчої електронної взаємодії як у державному секторі, так і в підприємницькому середовищі.

Згідно із Законом України ***«Про електронні документи та електронний документообіг»*** «електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа».

Електронний документ складається з сукупності змістових та атрибутивних частин. В українському законодавстві визначено перелік обов'язкових реквізитів електронного документа (рис. 4.4).

Рис. 4.4. Обов'язкові реквізити документа

Сукупність взаємопов'язаних електронних документів та операцій із ними, таких як створення, погодження, підписання, передавання, зберігання й архівування, формує електронний документообіг, який забезпечує упорядкований рух документів між учасниками та контроль виконання бізнес-процесів у цифровому середовищі. Правове регулювання електронного документообігу ґрунтується на принципі збалансування приватних і публічних інтересів, оскільки цифрові документи одночасно виконують функції господарського підтвердження операцій і юридично значущих доказів. Сфера застосування електронного документообігу є багатокомпонентною:

- *у цивільно-правових відносинах між контрагентами порядок обміну електронними документами здебільшого визначається домовленістю сторін і умовами договору;*
- *внутрішній документообіг підприємства визначається обліковою політикою та внутрішніми наказами;*

- *взаємодія з державними органами регламентується відповідними нормативно-правовими актами, що діють у конкретній сфері.*

Окреме значення має використання електронних документів у публічному управлінні, зокрема для інформаційної взаємодії між органами влади, місцевого самоврядування та іншими суб'єктами, які реалізують публічно значущі функції.

На рисунку 4.5 подано нормативно-правове регулювання електронного документообігу, яке визначає порядок створення, підписання, обміну, зберігання та використання електронних документів, а також встановлює вимоги до їх юридичної значущості й захисту інформації.

Рис. 4.5. Нормативно-правове регулювання електронного документообігу в Україні

Загалом, цифрове середовище потребує постійного оновлення та адаптації бізнес-процесів, оскільки технології змінюють характер комунікацій, швидкість обробки інформації та можливості контролю. У наукових підходах підкреслюється, що цифровізація формує конкурентні переваги підприємств і розширює їхні комунікаційні можливості, створюючи сприятливі умови для

розвитку в сучасній економіці. У контексті обліку й аудиту це посилює значення електронного документообігу як фундаменту для якісних облікових даних, ефективних контрольних процедур та формування достовірної звітності.

Електронний документообіг пройшов кілька етапів розвитку від простого оцифрування паперових документів і створення електронних архівів до впровадження систем керування документами з регламентованими маршрутами погодження та контролем виконання. На рисунку 4.6 подано етапи розвитку електронного документообігу у відповідь на вимоги цифрового середовища.

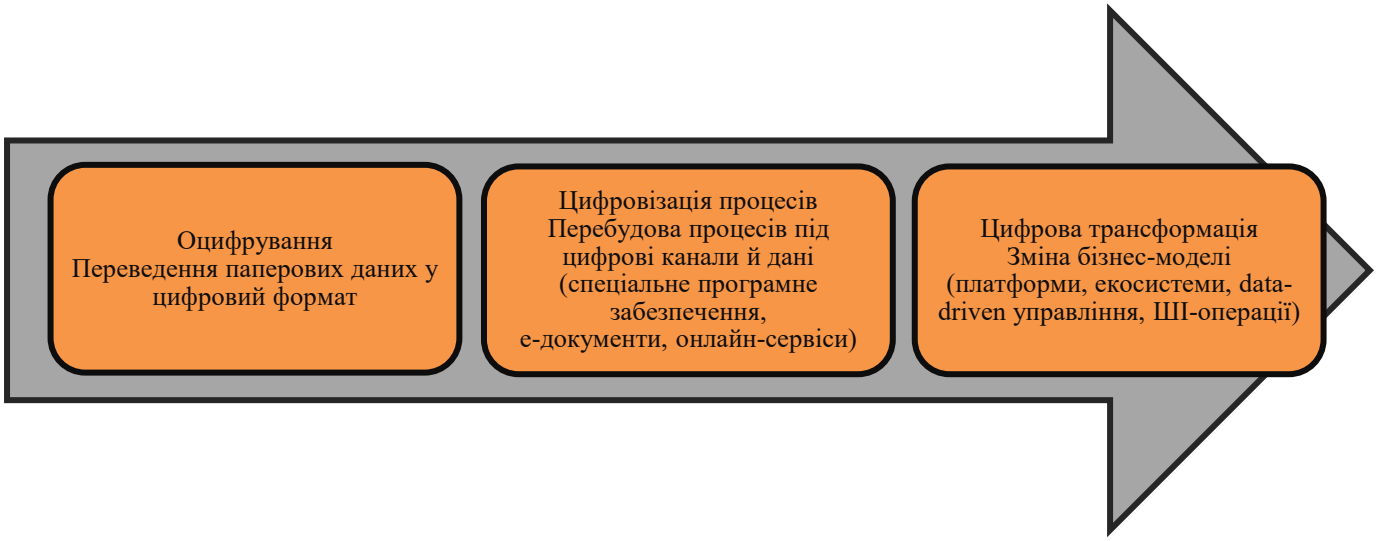


Рис. 4.6. Етапи цифрової трансформації документів

Подальша еволюція пов’язана із стандартизованим обміном між контрагентами, юридичним підтвердженням електронного підпису та інтеграцією електронних документів з обліковими системами й державними сервісами, що перетворило документи на повноцінні цифрові докази та елемент наскрізних бізнес-процесів.

Відтак, у сьогоденні ***електронний документообіг*** – це організована система створення, обробки, погодження, підписання, передавання, зберігання та використання документів у цифровій формі з використанням визначених правил і технологій.

На відміну від паперового обігу, електронний документообіг забезпечує швидку взаємодію між підрозділами підприємства, контрагентами та державними органами, а також формує цифровий слід операцій, адже електронні документи набувають юридичної значимості та можуть використовуватися як належні докази за умови їх підтвердження електронним підписом.

У Законі України ***«Про електронний цифровий підпис»*** визначено, що «електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних, а електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа».

Електронний цифровий підпис (ЕЦП або КЕП) є ключовим інструментом функціонування електронного документообігу, оскільки забезпечує можливість повноцінної роботи фізичних і юридичних осіб з електронними документами. Його застосування дає змогу встановити, хто саме підписав документ, а також підтвердити, що дані після підписання не були змінені, тобто забезпечує цілісність і доказовість електронної інформації.

Використання електронного цифрового підпису не змінює правових вимог до оформлення документів і не скасовує вимог щодо письмової форми правочинів, адже електронне підписання є лише сучасним технологічним способом реалізації підпису, передбаченого законодавством. Тобто договори та інші документи, які законом мають бути підписані у письмовій формі, можуть оформлюватися в електронному вигляді із застосуванням ЕЦП або КЕП за умови дотримання встановлених вимог.

Технічно електронний підпис ґрунтується на парі ключів та сертифікаті відкритого ключа, який «прив'язує» ключ до конкретної особи чи організації. Закритий ключ створює підпис, відкритий його перевіряє. Дійсність сертифіката

може перевірятися, зокрема, через сервіси пошуку сертифікатів і списки відкликаних сертифікатів. На рисунку 4.7 подано способи отримання електронного підпису.

Рис. 4.7. Способи отримання електронного підпису

Електронний цифровий підпис формується на основі криптографічної пари ключів, а саме особистого (закритого) ключа та відкритого ключа. Підписувач накладає підпис саме особистим ключем, який має залишатися лише у його володінні й забезпечує унікальність підпису. Перевірка підпису здійснюється за допомогою відкритого ключа, що міститься в сертифікаті. Він дозволяє

підтвердити, хто підписав документ, і встановити, чи не було змінено дані після підписання. На рисунку 4.8 подано обов'язкові дані сертифіката ключа.

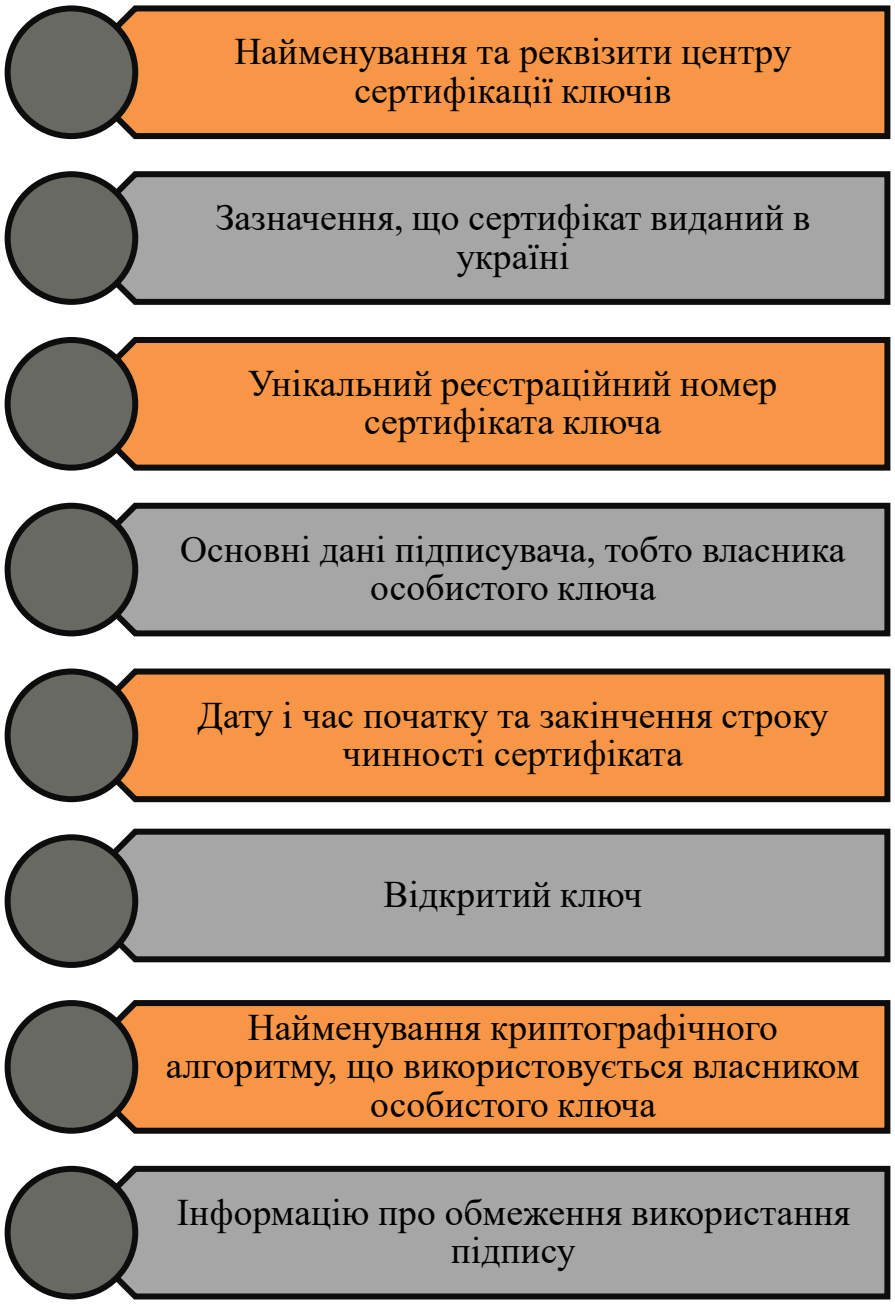


Рис. 4.8. Обов'язкові дані сертифіката ключа

Електронний і паперовий документообіг мають низку спільних і відмінних характеристик, адже обидва забезпечують фіксацію господарських операцій, рух документів між учасниками та контроль їх погодження і зберігання, однак відрізняються формою носія, швидкістю обміну, способами підписання й підтвердження юридичної значимості, а також вимогами до захисту, архівації та доступу до інформації (табл. 4.6).

Таблиця 4.6

Особливості паперового і електронного документообігу

Критерії	Електронний документообіг	Паперовий документообіг
1. Швидкість доставки документа користувачу	Документ доставляється миттєво за умови наявності ЕЦП у відправника й отримувача та доступу до телекомунікаційних мереж	Доставка повільна, оскільки вимагає друку, підпису, проставлення печаток, а також фізичного відправлення поштою, кур'єром або особисто
2. Оформлення та відправка документів	Процес включає лише три етапи, такі як створення документа, накладання електронного цифрового підпису та відправлення адресату	Містить багатоетапну процедуру, а саме друк, підписання, пакування, пересилання, доставка, а також ручне внесення інформації з документів
3. Способи зберігання та обліку документів	Документи зберігаються на електронних носіях, що спрощує пошук і доступ	Потребує фізичних архівів (шаф, сейфів), які займають багато місця. Пошук документів трудомісткий і тривалий
4. Витрати на канцелярські товари	Значна економія паперу, картриджів та інших канцелярських матеріалів	Високі витрати на папір, друк та інші матеріали
5. Система безпеки	Високий рівень захисту завдяки ЕЦП; мінімізується ризик несанкціонованого доступу	Нижчий рівень безпеки; існує ризик втрати, пошкодження або спотворення документів

У практиці бухгалтерського обліку електронний документообіг передбачає створення та передачу первинних документів, таких як рахунки, накладні, договори, внутрішні розпорядчі документи, документи з кадрових і адміністративних питань та інші. На рисунку 4.9 представлено етапи електронного документообігу.

Рис. 4.9. Основні етапи електронного документообігу

Ефективність електронного документообігу залежить від якості внутрішніх норм та правил системи контролю. До ключових елементів належать

визначення відповідальних осіб і прав доступу, правила підписання та делегування повноважень, контроль версій документів, вимоги до архівування і строків зберігання, а також заходи кіберзахисту, такі як шифрування, резервне копіювання, багатофакторна автентифікація. Отже, електронний документообіг є базовим елементом цифрової трансформації обліку й аудиту, який підвищує оперативність і прозорість процесів, але потребує належного управління даними та контролями для забезпечення довіри до електронних доказів. На рисунку 4.10 подано переваги та ризики електронного документообігу.

Рис. 4.10. Переваги та ризики електронного документообігу

Ключовою перевагою електронного документообігу є скорочення часу обробки документів, зменшення витрат на папір і друк, зниження ризику втрати або дублювання документів, а також можливість автоматизованого контролю строків та повноважень. Для управління обліковими даними електронний документообіг забезпечує своєчасність і повноту відображення операцій, оскільки документи можуть передаватися до бухгалтерії автоматично або через спеціалізовані сервіси. Разом з тим цифрове середовище ставить вимоги до якості даних та визначає необхідність правильності реквізитів, узгодженості

довідників, відповідності шаблонам, оскільки помилки в електронному документі можуть швидко поширюватися в інтегрованих системах.

Для аудиту електронний документообіг є важливим джерелом доказів, оскільки містить не лише зміст документів, а й ключові дані про документ, а саме дату створення, автора, маршрут погодження, час підписання, відомості про підписанта, історію змін і журнали подій.

Це дозволяє аудитору оцінювати правильність, доцільність та цілісність документів, підтверджувати факт їх погодження уповноваженими особами і простежувати зв'язок ***«господарська операція → документ → відображення в обліку → показник звітності».***

Водночас аудит повинен враховувати ризики електронного документообігу, такі як несанкціоновані зміни, помилки в налаштуваннях, недостатній контроль доступів, втрату журналів подій через короткі строки зберігання, а також загрози витоку конфіденційної інформації.

4.4. Контрольні питання для самоперевірки

1. У чому полягає сутність цифрового аудиту та які особливості його правового регулювання порівняно з традиційним аудитом?

2. Які нормативно-правові акти регулюють аудиторську діяльність у сфері цифрових технологій?

3. Які вимоги законодавства висуваються до збереження та захисту електронних доказів під час проведення цифрового аудиту?

4. Які правові аспекти використання хмарних технологій у процесі аудиторської перевірки?

5. У чому полягає відповідальність аудитора при роботі з автоматизованими інформаційними системами клієнта?

6. Які вимоги встановлюються до електронного документообігу в аудиторській діяльності?

7. Які ризики виникають у процесі цифрового аудиту та як вони враховуються в нормативно-правових документах?

8. Яким чином державне регулювання впливає на впровадження інноваційних цифрових інструментів в аудиті?

9. Які зміни в законодавстві спричинила цифровізація фінансової звітності?

10. Як забезпечується юридична сила електронного аудиторського висновку?

Розділ 5

Автори:
Олена Птащенко
Дмитро Сушко

ОРГАНІЗАЦІЯ ЦИФРОВОГО АУДИТУ ТА МОНІТОРИНГУ ФІНАНСОВОЇ БЕЗПЕКИ

РОЗДІЛ 5. ОРГАНІЗАЦІЯ ЦИФРОВОГО АУДИТУ ТА МОНІТОРИНГУ ФІНАНСОВОЇ БЕЗПЕКИ

«Гідність людини та права мають бути критерієм для нових технологій.»

Папа Франциск

5.1. Організація та інструменти моніторингу фінансової безпеки

Моніторинг фінансової безпеки – це систематичне спостереження, вимірювання та оцінювання фінансового стану підприємства і ключових ризиків, щоб завчасно виявляти загрози, наприклад втрати ліквідності, касові розриви, шахрайство, критичні борги, податкові ризики та вчасно запускати управлінські й контрольні дії.

Основна мета моніторингу фінансової безпеки подана на рисунку 5.1.

Моніторинг фінансової безпеки як термін оформився відносно пізно, однак сама ідея постійного спостереження за ресурсами, доходами, боргами та ризиками існує стільки ж, скільки й організовані фінанси. Ще в найдавніших державах Месопотамії та Стародавнього Єгипту «безпека» скарбниці забезпечувалася обліком і звіркою запасів зерна, податків та видачі ресурсів, а контроль зводився до перевірки записів, відповідальних осіб і фактичних залишків. В античних полісах і в Римі посилилася роль звітності посадовців, адже фінансова стабільність держави залежала від прозорого збору податків і контролю витрат, що заклало принцип відповідальності за публічні кошти та їх перевірюваності. У середньовічній Європі виникли спеціальні органи ревізії

доходів і видатків казни та міських зборів, де контроль переважно здійснювався постфактум, але вже формував практику регулярного нагляду за фінансовими потоками.

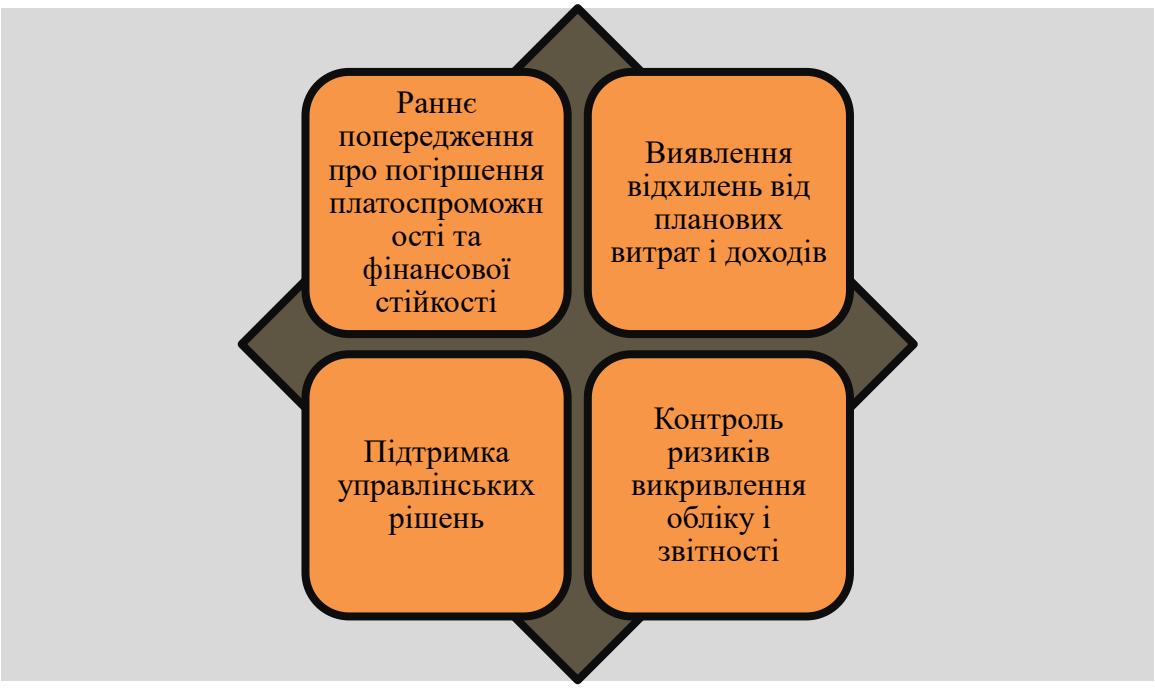


Рис. 5.1. Мета моніторингу фінансової безпеки

Поширення подвійного запису в XIV–XVI століттях стало ключовою віхою, оскільки забезпечило взаємоперевірку рахунків і можливість системно оцінювати фінансовий стан через баланс та обороти, що наблизило моніторинг до сучасної логіки аналітики. У XVII–XVIII століттях із розвитком акціонерних компаній зросла потреба в незалежній перевірці звітів управителів, що стимулювало становлення аудиту як інструменту захисту інтересів власників та інвесторів. Індустріалізація XIX століття зробила моніторинг більш регулярним і планово-аналітичним: великі підприємства почали застосовувати бюджетування, калькуляцію собівартості, управлінські звіти та контроль відхилень, щоб своєчасно реагувати на фінансові загрози. У XX столітті професіоналізація обліку й аудиту змістила акцент з перевірки окремих документів на оцінку надійності системи внутрішнього контролю, а фінансові кризи посилили вимоги до прозорості й стандартизації звітності як основи стабільності ринків.

З появою комп’ютерів у середині XX століття компанії отримали можливість будувати управлінські інформаційні системи, які забезпечували регулярні «сигнальні» показники для керівництва, а розвиток фінансової аналітики привів до використання моделей раннього попередження, зокрема оцінки ризику неплатоспроможності на основі коефіцієнтів. Наприкінці XX – на початку XXI століття інтегровані програмні рішення дали ефект «єдиного джерела даних», коли моніторинг фінансової безпеки став спиратися на транзакції у реальному часі, ліміти, розмежування доступів, журналювання подій та правила закриття періодів. Сьогодні моніторинг дедалі більше набуває форми безперервного контролю, поєднуючи автоматизовані звірки, аналітику даних, виявлення відхилень від планових показників і контроль змін в інформаційних системах, завдяки чому ризики можна не лише фіксувати, а й попереджати на ранніх етапах.

Об’єкти фінансового моніторингу подано на рисунку 5.2.

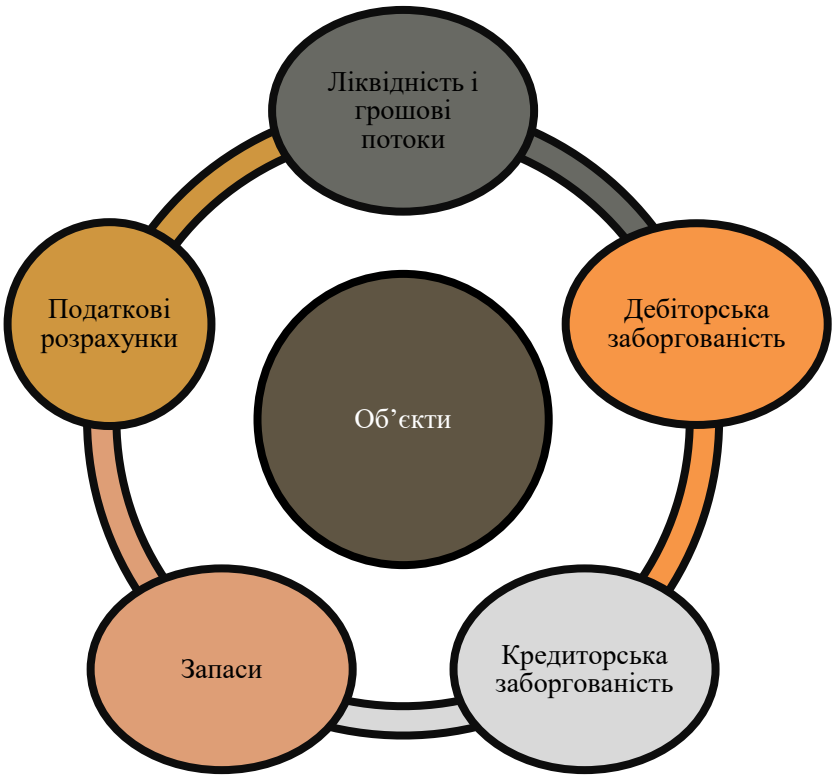


Рис. 5.2. Об’єкти моніторингу фінансової безпеки

Моніторинг фінансової безпеки має системний і безперервний характер та здійснюється протягом усіх циклів життєдіяльності учасників фінансового ринку від створення і зростання до стабілізації, трансформації або

реструктуризації. На кожному етапі розвитку змінюються цілі, структура ресурсів і рівень уразливості, тому контроль фінансових ризиків і загроз повинен супроводжувати діяльність суб'єкта постійно, а не епізодично. У практиці управління моніторинг інтегрується в усі етапи ризик-менеджменту: він забезпечує раннє виявлення факторів ризику, оцінку їхнього впливу, відбір заходів реагування, контроль виконання рішень та перевірку результативності застосованих інструментів. Завдяки цьому підприємство або інша фінансова установа отримує можливість своєчасно коригувати політики, ліміти, процедури та управлінські рішення. Водночас моніторинг фінансової безпеки є ключовим елементом антикризового управління і застосовується на всіх його стадіях: попередження кризових явищ, діагностика та стабілізація, відновлення платоспроможності й подальша адаптація.

У системі моніторингу фінансової безпеки важливо заздалегідь налаштувати періодичність контролю показників залежно від їх важливості та швидкості змін. Найоперативніші ділянки, пов'язані з рухом грошових коштів і банківськими операціями, доцільно контролювати щоденно, оскільки будь-які затримки платежів, нестача ліквідності або несанкціоновані списання потребують негайного реагування. Показники розрахунків із контрагентами, а саме дебіторська та кредиторська заборгованість, зазвичай аналізуються щотижнево, щоб вчасно виявляти прострочення, ризик неповернення коштів, накопичення боргів і порушення договірної дисципліни. Комплексні узагальнюючі процедури виконують щомісячно, тобто проводять закриття звітного періоду, оцінюють маржинальність і фінансові результати, перевіряють правильність нарахування податків та узгодженість облікових даних. Такий розподіл частоти перевірок забезпечує баланс між оперативністю контролю і системністю аналізу, дозволяючи своєчасно виявляти відхилення та підтримувати керованість фінансового стану підприємства.

Індикатори фінансової безпеки як компоненти моніторингу подано на рисунку 5.3.

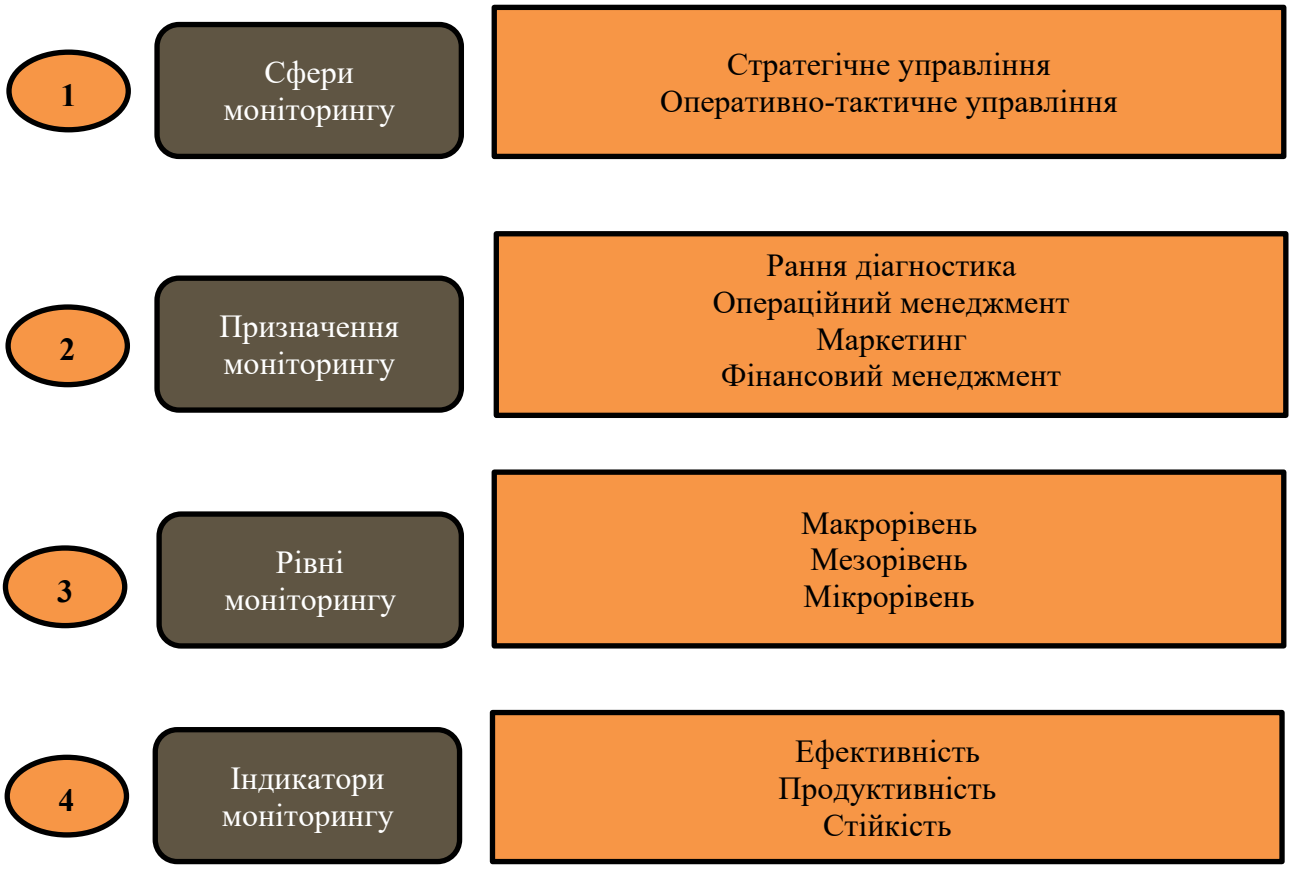


Рис. 5.3. Індикатори фінансової безпеки як компоненти моніторингу

У практиці моніторингу фінансової безпеки важливим елементом є встановлення порогів ризику – кількісних або якісних критеріїв, при перевищенні яких ситуація вважається потенційно небезпечною і потребує управлінської реакції. Такі пороги задають «сигнали тривоги», що дозволяють швидко відокремити нормальні коливання показників від відхилень, здатних спричинити фінансові втрати, викривлення обліку або порушення контролю. Наприклад, прострочення дебіторської заборгованості понад 30 днів може виступати тригером кредитного ризику, оскільки підвищує ймовірність неповернення коштів і потребує посилення претензійної роботи чи перегляду умов співпраці. Відхилення витрат більш ніж на 10 % від планових або середніх значень є сигналом ризику неефективності, помилок класифікації витрат чи можливих зловживань, тому вимагає деталізації причин і перевірки первинних документів. Від'ємні залишки на складі вказують на порушення порядку оформлення руху запасів, помилки в документах або проблеми інтеграції між підсистемами, що впливає на собівартість і достовірність звітності. Окремою

групою ризиків є контрольні події в обліковій системі щодо перепроведення документів після закриття періоду, які сигналізують про ризик зміни показників датою, що минула, тому потребує аналізу журналу подій, встановлення відповідальних осіб і оцінки впливу на звітність. Отже, правильно визначені пороги ризику забезпечують автоматизоване виявлення відхилень, дисциплінують роботу з даними та роблять моніторинг фінансової безпеки системним і керованим.

Моніторинг фінансової безпеки є важливим елементом системи управління, оскільки забезпечує своєчасне виявлення загроз і підтримує прийняття управлінських рішень. У сфері стратегічного управління його основним завданням є прогнозування та довгострокова оцінка негативних впливів зовнішнього і внутрішнього середовища з метою завчасної мінімізації або усунення загроз. Такий моніторинг має орієнтацію на перспективу, дозволяє формувати сценарії розвитку подій і планувати заходи зі зміцнення фінансової стійкості.

У сфері оперативно-тактичного управління моніторинг фінансової безпеки виконує іншу роль, адже він забезпечує експрес-контроль, експрес-аналіз та експрес-оцінку поточної ситуації, щоб організація могла швидко реагувати на актуальні ризики. Це означає систематичне відстеження ключових змін у діяльності та середовищі, оперативне виявлення відхилень і прийняття рішень щодо негайних дій з нейтралізації загроз.

Індикатори фінансової безпеки застосовуються як практичні інструменти моніторингу в різних управлінських механізмах – ризик-менеджменті, операційному та фінансовому менеджменті, менеджменті персоналу і маркетингу. Їхня особливість полягає в тому, що вони можуть формуватися як на основі показників фінансового стану, наприклад, ліквідності, платоспроможності, фінансової стійкості, рентабельності, так і на основі показників стану системи фінансової безпеки. При цьому індикатори системи фінансової безпеки можуть розраховуватись не лише за фінансовою звітністю, а й за іншими джерелами інформації – управлінською та нефінансовою звітністю,

даними про організацію процесів, параметрами технічного забезпечення та документацією на елементи системи захисту. У підсумку базовий перелік таких індикаторів створює основу для комплексного й доказового оцінювання фінансової безпеки та підвищує керованість ризиків у діяльності учасника фінансового ринку. Індикатори стану системи фінансової безпеки подано в таблиці 5.1.

Таблиця 5.1

Індикатори стану системи фінансової безпеки

№ п/п	Індикатор	Характеристика	Формула розрахунку	Опис складових
Індикатори ефективності				
1	Ефективність системи безпеки	ступінь, у якому заходи безпеки реально знижують ризики та втрати і забезпечують виконання вимог	$К_{еф} = \frac{ЗВ_{лз}}{ЗВ_{з}} \rightarrow 1$	$ЗВ_{лз}$ – можлива максимальна вартість втрат від попереджених та ліквідованих суттєвих загроз за період; $ЗВ_{з}$ – загальна вартість втрат від суттєвих загроз за період
2	Окупність	співвідношення отриманого ефекту від впровадження і підтримки безпеки до витрат на неї	$К_{ок} = \frac{ЗВ_{лз}}{ЗВ_{системи}} \rightarrow max$	$ЗВ_{системи}$ – загальна вартість системи фінансової безпеки учасника фінансового ринку
3	Швидкодія	час реакції системи безпеки на загрозу та швидкість виконання контрольних і захисних процедур	$t_{шв} = t_{зн} + t_{лікв} \rightarrow min$	$t_{зн}$ – час виявлення загрози системою в результаті моніторингу; $t_{лікв}$ – час на видачу і реалізацію управлінських рішень з ліквідації загрози
Індикатори продуктивності				
4	Частота моніторингу	встановлена періодичність збору, оновлення та аналізу показників (індикаторів) для своєчасного виявлення відхилень і загроз та оперативного реагування	$v_{мон} \rightarrow min$	Час між замірами *i*-го індикатора

5	Можливість модернізації та розширення	здатність системи моніторингу адаптуватися до змін у бізнес-процесах і ризиках шляхом додавання нових індикаторів, звітів, правил контролю, користувачів і функцій без суттєвого порушення її роботи	Експертна оцінка	–
6	Сумісність з іншими системами	спроможність системи обмінюватися даними та інтегруватися з іншими інформаційними системами підприємства	Експертна оцінка	–
Індикатори стійкості				
7	Надійність	здатність системи стабільно та безперервно працювати в заданих умовах, забезпечуючи правильність обробки даних і мінімальну кількість збоїв та помилок протягом визначеного часу	$t_{\text{бр}} \rightarrow max$	$t_{бр}$ – час безвідмовної роботи технічних засобів системи за даними виробника
8	Захищеність	сукупність організаційних і технічних заходів, що забезпечують конфіденційність, цілісність і доступність даних, запобігаючи несанкціонованому доступу, зміні, видаленню або витоку інформації	$\text{К}_{\text{зах}} = \frac{\text{К}_{\text{ат}}}{\text{К}_{\text{сбс}}} \rightarrow max$	$К_{ат}$ – загальна кількість шкідливих атак на систему; $К_{сбс}$ – кількість збоїв системи

9	Відновлюваність	здатність системи відновлювати працездатність і дані після збоїв, помилок шляхом використання резервних копій, процедур відновлення та контрольних перевірок цілісності	$t_{\text{повт}} \rightarrow min$	$t_{повт}$ – час повернення системи в працездатний стан у випадку збою

Для дотримання фінансової безпеки підприємство має сформувати комплекс управлінських і контрольних заходів, спрямованих на стабільність функціонування та захист фінансових інтересів. Передусім необхідно забезпечити подальший стійкий розвиток підприємства, тобто підтримувати його здатність зберігати конкурентоспроможність, прибутковість і платоспроможність у довгостроковій перспективі. Важливим завданням є також підтримання стійкості грошових розрахунків і досягнення ключових фінансово-економічних параметрів, а саме ліквідності, фінансової стійкості, рентабельності, що гарантує безперервність операційної діяльності та виконання зобов'язань.

Окремий напрям фінансової безпеки пов'язаний із нейтралізацією негативних впливів зовнішнього середовища: фінансових і банківських криз, нестабільності ринків, а також потенційно шкідливих дій конкурентів і тіньових структур. Для цього підприємство повинно застосовувати ризик-орієнтоване управління, диверсифікувати канали збуту й фінансування, мати резерви ліквідності та сценарні плани реагування. Водночас фінансова безпека залежить і від внутрішньої узгодженості інтересів, тому необхідно запобігати конфліктам між акціонерами, менеджерами та кредиторами, забезпечуючи прозорий розподіл, використання та контроль грошових потоків, чіткі повноваження і належну систему корпоративного управління.

Не менш важливим є формування оптимальної структури капіталу і підприємство має залучати й використовувати найбільш вигідні джерела

фінансування з урахуванням вартості ресурсів, строків, ризиків і впливу на платоспроможність. Завершальним, але критично значущим компонентом є попередження злочинів і адміністративних правопорушень у сфері фінансових правовідносин, що передбачає дієвий внутрішній контроль, комплаєнс-процедури, фінансову дисципліну, протидію шахрайству та регулярні перевірки дотримання законодавчих вимог. Заходи для забезпечення фінансової безпеки підприємства подано на рисунку 5.4.

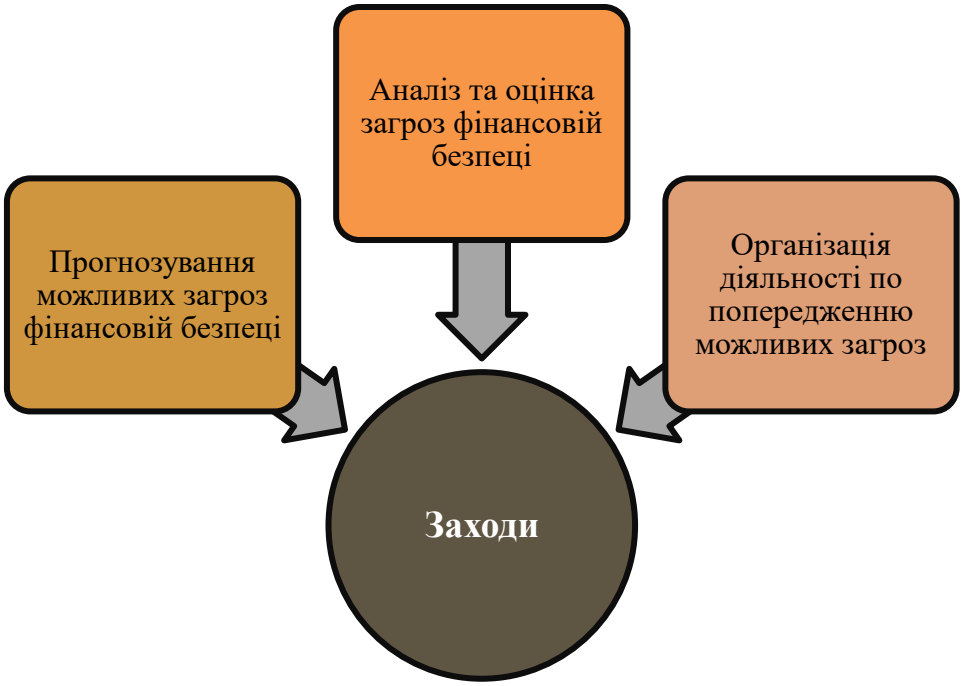


Рис. 5.4. Заходи для забезпечення фінансової безпеки підприємства

Доцільність аудиту в цьому контексті полягає в тому, що результати аудиту дають можливість виявити слабкі місця внутрішнього контролю та суттєво знизити ймовірність викривлень у фінансовій звітності, що підвищує довіру користувачів до звітних показників і прийняття управлінських рішень.

5.2. Планування аудиту з урахуванням IT-ризиків та ризиків фінансової безпеки

Глобальне економічне середовище сучасності характеризується високою залежністю бізнесу від інформаційних технологій, цифрових каналів обробки даних та автоматизованих систем управління. За таких умов фінансова звітність підприємств формується з урахуванням інтегрованих IT-платформ, хмарних сервісів, електронного документообігу та постійного обміну даними з контрагентами. Аудит, при такому динамічному розвитку економічного простору, не може обмежуватися перевіркою традиційних бухгалтерських процедур. Планування аудиту потребує глибокого врахування IT-ризиків і ризиків фінансової безпеки, які здатні суттєво вплинути на достовірність звітності та стабільність діяльності суб'єкта господарювання.

IT-ризики охоплюють технічні збої, втрату даних, несанкціонований доступ до облікових систем, помилки в алгоритмах автоматизованих розрахунків, некоректні налаштування контролів, кіберзагрози та залежність від сторонніх постачальників програмного забезпечення. Будь-який із цих елементів може призвести до спотворення фінансової інформації або створити передумови для здійснення шахрайства. Ризики фінансової безпеки включають загрози ліквідності, платоспроможності, фінансової стійкості, ризики маніпулювання показниками звітності з метою приховування реального стану справ.

На етапі планування аудиту зазначені вище аспекти визначають глибину та спрямованість подальших процедур. На наступному рисунку представлено ті особливості, які необхідно оцінити аудитору на початковому етапі аудиторського процесу (рис. 5.5).

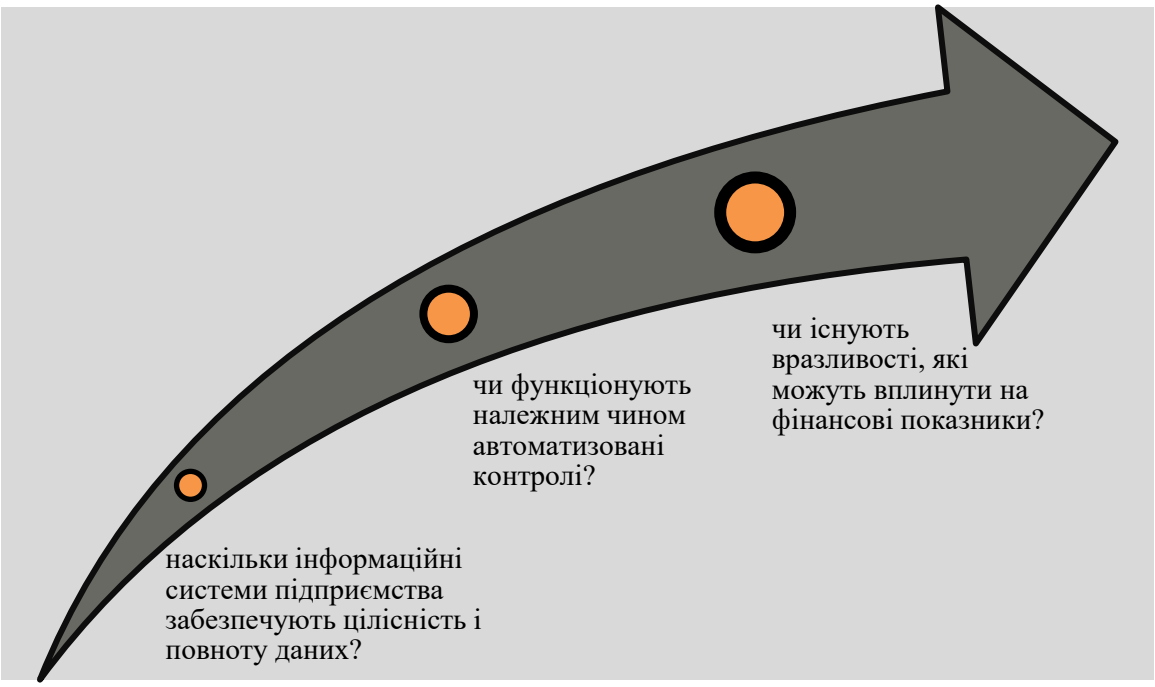


Рис. 5.5. Питання, які розглядає аудитор на першому етапі аудиторського процесу

Особливість сучасного планування полягає в тому, що IT-ризики та ризики фінансової безпеки взаємопов’язані.

Приклад. Сучасні недоліки у захисті інформаційних систем можуть спричинити несанкціоновані зміни в облікових даних. Такий негативний процес безпосередньо вплине на фінансову стійкість підприємства та довіру інвесторів. За таких умов аудитор повинен розглядати ризики комплексно та не ізольовано.

Врахування факторів ризику у процесі планування дозволяє сформувати обґрунтовану аудиторську стратегію, визначити пріоритетні напрями перевірки та розподілити ресурси. Зазначений підхід сприяє підвищенню якості аудиту, зменшенню ймовірності можливого невиявлення суттєвих викривлень і посиленню довіри до фінансової звітності в умовах цифрової економіки.

На рисунку представлено систематизацію IT-ризиків (рис. 5.6).

Рис. 5.6. Систематизація IT-ризиків

На етапі планування аудиту аудитор має ідентифікувати IT-ризики, що впливають на формування облікових даних, а також визначити, які контролі знижують імовірність викривлень. Така ідентифікація дає змогу обґрунтувати вибір процедур тестування контролів і змістовних перевірок, а також правильно розподілити ресурси аудиту. Основні IT-ризики та їхній потенційний вплив на фінансову звітність подано в таблиці 5.2.

Таблиця 5.2

Основні IT-ризики в діяльності підприємницьких структур

Вид IT-ризику	**Сутність ризику**	**Можливі наслідки для фінансової звітності**	**Особливий акцент**
Несанкціонований доступ до облікових систем	Сторонні або невповноважені працівники отримують доступ до бухгалтерських програм або баз даних	Викривлення облікових записів, зміна залишків, приховані операції	Перевірка політики доступу, ролей користувачів, журналів входу в систему
Неналежне розмежування повноважень	Одна особа має можливість створювати, затверджувати і відображати операції в обліку	Підвищений ризик шахрайства або маніпулювання даними	Аналіз матриці розподілу обов'язків, тестування внутрішніх контролів
Помилки в налаштуваннях програмного забезпечення	Некоректні алгоритми розрахунку податків, амортизації, резервів	Систематичні помилки у фінансових показниках	Оцінка параметрів системи, перевірка правильності автоматичних розрахунків
Відсутність або неналежне резервне копіювання	Дані не зберігаються належним чином або не відновлюються після збою	Втрата первинної інформації, неможливість підтвердити операції	Перевірка резервних копій та відновлення даних
Кіберзагрози та шкідливе програмне забезпечення	Вірусні атаки, фішинг, втручання хакерів	Порушення цілісності даних, блокування доступу до систем	Оцінка антивірусного захисту, систем кібербезпеки, реагування на інциденти

Вид IT-ризику	Сутність ризику	Можливі наслідки для фінансової звітності	Особливий акцент
Залежність від зовнішніх IT-постачальників	Використання хмарних сервісів або аутсорсингових компаній без належного контролю	Ризик втрати даних або обмеженого доступу до них	Аналіз договорів з провайдерами, наявність звітів про контроль (наприклад, ISAE 3402)
Відсутність журналів змін у системі	Не фіксуються зміни в довідниках, налаштуваннях або облікових даних	Неможливо простежити, хто і коли змінив інформацію	Перевірка наявності журналу записів та логування подій
Неналежне тестування оновлень програм	Оновлення систем впроваджуються без попереднього тестування	Помилки в обліку після змін у програмі	Аналіз процедур управління змінами
Використання застарілого програмного забезпечення	Програми не оновлюються, не підтримуються виробником	Підвищена вразливість до збоїв та атак	Оцінка актуальності версій програмного забезпечення
Недостатній контроль за електронним документообігом	Відсутність перевірки автентичності електронних документів	Використання підроблених або змінених документів	Перевірка цифрових підписів та систем шифрування
Ризик втрати даних при інтеграції систем	Помилки під час обміну даними між різними програмами	Неповнота або дублювання операцій	Тестування коректності інтеграції між системами

Оскільки більшість облікових процесів автоматизовані, IT-ризики мають прямий вплив на достовірність фінансової звітності. Для аудитора важливо не лише перевірити комплекс цифрового інструментарію підприємства, а також оцінити, наскільки надійно вони захищені, правильно налаштовані та контрольовані. Комплексна увага до IT-ризиків дозволяє своєчасно виявити потенційні викривлення та зменшити загальний аудиторський ризик.

На наступному рисунку представлено систематизацію ризиків фінансової безпеки (рис. 5.7).

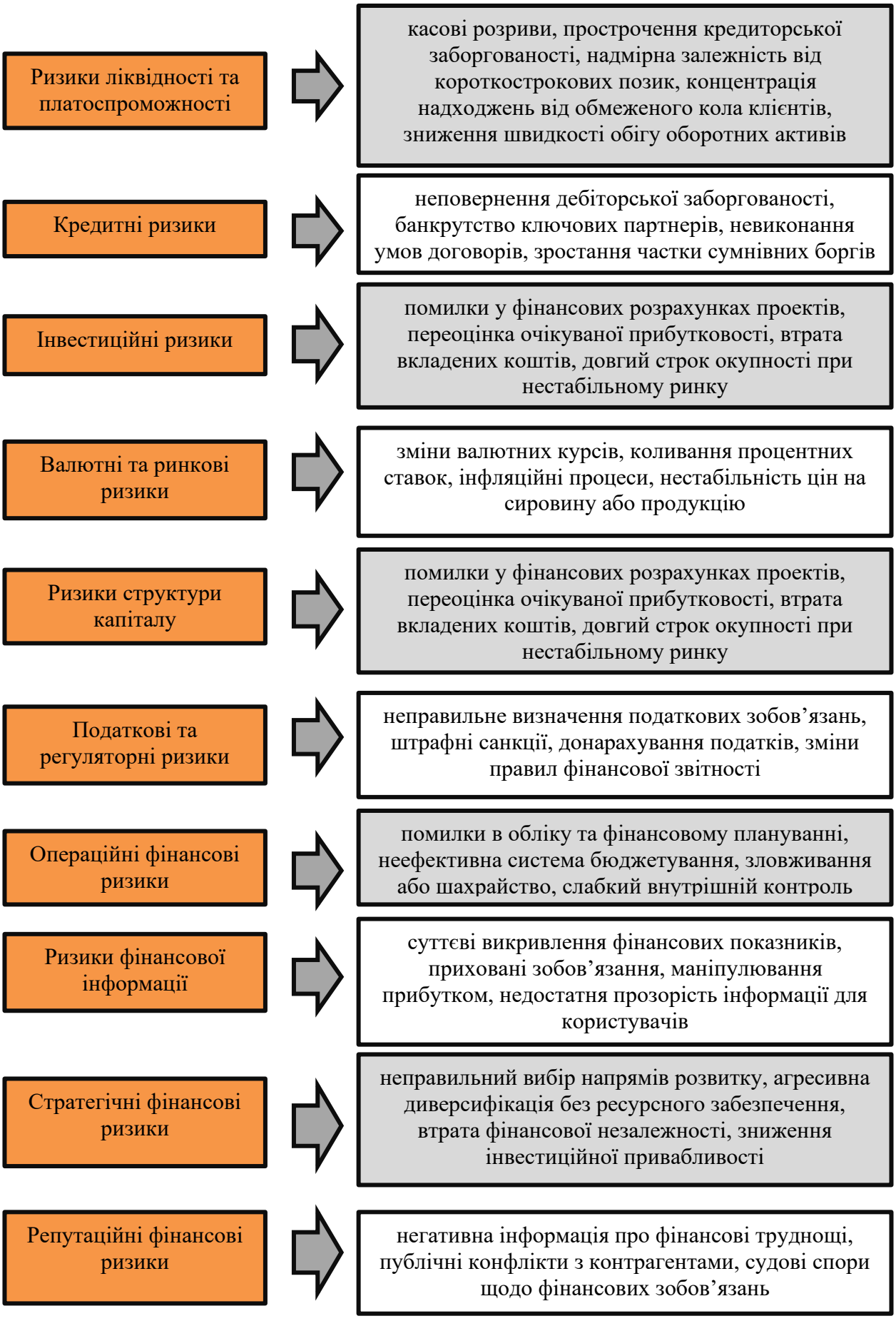


Рис. 5.7. Систематизація ризиків фінансової безпеки

В наступній таблиці представлено ризики фінансової безпеки суб'єктів господарювання (підприємницьких структур) (табл. 5.3).

Таблиця 5.3

Основні ризики фінансової безпеки підприємницьких структур

Група ризиків	Суть ризику	Типові причини виникнення	Можливі наслідки для підприємства	Проблема
Ризики ліквідності	Брак грошових коштів для розрахунків	Нерівномірні надходження, затримки платежів від клієнтів, надмірні запаси	Прострочені платежі, штрафи, втрата довіри партнерів	Зростання кредиторської заборгованості, часті касові розриви
Ризики платоспромож-ності	Неможливість погасити борги в довгостроковій перспективі	Високе боргове навантаження, зниження прибутковості	Реструктуризація боргу, загроза банкрутства	Погіршення фінансових коефіцієнтів, зменшення власного капіталу
Кредитні ризики	Контрагенти не виконують свої зобов'язання	Робота з ненадійними клієнтами, відсутність перевірки партнерів	Неповернення дебіторської заборгованості	Зростання частки прострочених боргів
Валютні ризики	Втрати через коливання валютних курсів	Зовнішньоекономічна діяльність, кредити в іноземній валюті	Додаткові витрати, курсові різниці	Нестабільність валютних платежів
Процентні ризики	Збільшення витрат через зміну ставок	Кредити з плаваючою ставкою	Зростання фінансових витрат	Підвищення витрат на обслуговування боргу
Інвестиційні ризики	Невдалі вкладення коштів	Недостатній аналіз проєктів, переоцінка попиту	Заморожені кошти, збитки	Відхилення фактичних результатів від планових
Податкові ризики	Неправильне нарахування або сплата податків	Помилки в обліку, часті зміни законодавства	Штрафи, донарахування, перевірки	Невідповідність звітності вимогам контролюючих органів

Група ризиків	Суть ризику	Типові причини виникнення	Можливі наслідки для підприємства	Проблема
Податкові ризики	Неправильне нарахування або сплата податків	Помилки в обліку, часті зміни законодавства	Штрафи, донарахування, перевірки	Невідповідність звітності вимогам контролюючих органів
Операційні фінансові ризики	Втрати через внутрішні помилки або зловживання	Слабкий внутрішній контроль, відсутність розмежування повноважень	Шахрайство, фінансові втрати	Невідповідність даних обліку фактичним показникам
Ризики структури капіталу	Неправильне співвідношення власних і позикових коштів	Агресивна кредитна політика, нестача власного капіталу	Залежність від кредиторів	Погіршення показників фінансової стійкості
Ризики грошових потоків	Нестабільність руху коштів	Незаплановані витрати, сезонність бізнесу	Порушення операційної діяльності	Нерегулярність надходжень і виплат
Ризики фінансової інформації	Недостовірні або викривлені фінансові дані	Помилки в обліку, свідоме спотворення показників	Неправильні управлінські рішення	Розбіжності між звітами та фактичними результатами
Репутаційні фінансові ризики	Втрата довіри через фінансові проблеми	Публічні конфлікти, невиконання зобов’язань	Відтік клієнтів, складність залучення інвестицій	Негативна реакція партнерів і банків

Приклад підтвердження комплексного розгляду ризиків фінансової безпеки.

Приклад. Проблеми з ліквідністю можуть спричинити порушення кредитних договорів, що, у свою чергу, погіршить репутацію та ускладнить доступ до фінансування. Систематизація таких ризиків є основою для формування ефективної політики фінансової стійкості та внутрішнього контролю.

Фінансова безпека підприємницької структури залежить від збалансованості всіх складових від ліквідності, боргового навантаження, якості фінансового управління до надійності партнерів. Ризики виникають поступово, завдання аудитора вчасно їх виявити. Систематичний моніторинг показників та налагоджений внутрішній контроль дозволяють зменшити ймовірність серйозних фінансових втрат і підтримувати стійкий розвиток бізнесу.

Таким чином, нижче представлено таблицю, де відображені етапи аудиторського процесу з врахуванням розглянутих ризиків (табл. 5.4).

Таблиця 5.4

Планування аудиторського процесу з врахуванням різних видів ризиків

Етап планування	**Врахування IT-ризиків**	**Врахування ризиків фінансової безпеки**	**Дії аудитора на стадії планування**	**Очікуваний результат для подальшої перевірки**
1. Попереднє ознайомлення з бізнесом клієнта	Залежність від інформаційних систем, використання хмарних сервісів, рівень автоматизації обліку	Структура капіталу, ліквідність, кредитне навантаження	Аналіз моделі бізнесу, джерел фінансування, IT-інфраструк-тури	Розуміння середовища функціонування підприємства
2. Оцінка середовища внутрішнього контролю	Розмежування доступу, наявність журналів змін, політика кібербезпеки	Система фінансового контролю, бюджетування, внутрішній нагляд	Опитування відповідальних осіб, аналіз регламентів і процедур	Попередня оцінка надійності системи контролю
3.Ідентифікація суттєвих ризиків	Можливість несанкціонованого втручання в облікові дані, помилки в налаштуваннях програм	Ризик викривлення звітності, маніпулювання прибутком, приховані зобов’язання	Визначення зон підвищеної уваги, формування карти ризиків	Виділення ділянок із високою ймовірністю викривлень
4. Аналіз інформаційних потоків	Некоректна інтеграція систем, втрата даних при передачі інформації	Неповнота обліку доходів і витрат	Перевірка логіки формування фінансових показників	Встановлення джерел можливих помилок

Етап планування	Врахування IT-ризиків	Врахування ризиків фінансової безпеки	Дії аудитора на стадії планування	Очікуваний результат для подальшої перевірки
5. Оцінка ризиків ліквідності та грошових потоків	Помилки в автоматичному формуванні платіжних операцій	Касові розриви, затримки платежів	Аналіз руху коштів, тестування коректності обліку платежів	Визначення потреби у поглиблених процедурах щодо грошових коштів
6. Перевірка залежності від зовнішніх IT-провайдерів	Ризик втрати або блокування доступу до даних	Переривання операційної діяльності через технічні збої	Оцінка договорів із постачальниками послуг, наявності резервних копій	Розуміння стійкості IT-середовища
7. Формування загальної стратегії аудиту	Рівень автоматизації процедур клієнта	Фінансова стійкість та ризик неплатоспроможності	Визначення обсягу тестів контролю та процедур по суті	Оптимальний розподіл аудиторських ресурсів
8. Визначення суттєвості	Можливість системних помилок у програмному забезпеченні	Вплив можливих викривлень на фінансовий результат	Розрахунок порогу суттєвості з урахуванням ризикових ділянок	Чіткі критерії оцінки виявлених відхилень
9. Планування процедур щодо шахрайства	Використання IT для прихованого редагування даних	Навмисне спотворення фінансової інформації	Передбачення додаткових аналітичних процедур	Підвищення рівня професійного скептицизму
10. Документування ризиків і запланованих дій	Відсутність повної історії змін у системі	Недостатня прозорість фінансових операцій	Формування робочої документації з описом ризиків і запланованих процедур	Забезпечення обґрунтованості подальших аудиторських дій

На наступному рисунку відображено основі особливості врахування різних ризиків при плануванні аудиту (рис. 5.8).

Рис. 5.8. Позитивні сторони підходу планування аудиторського процесу з врахування ІТ-ризиків та ризиків фінансової безпеки

Планування аудиту з урахуванням ІТ-ризиків і ризиків фінансової безпеки передбачає комплексний підхід. При такому підході аудитор має оцінювати не лише правильність бухгалтерських записів, а й те, наскільки надійно функціонує цифрове середовище підприємства та чи здатна компанія зберігати фінансову стійкість у короткостроковій і довгостроковій перспективі.

5.3. Аудиторські докази та робочі документи аудитора в цифровому середовищі

Аудиторські докази та робочі документи є фундаментальними складовими процесу аудиту, на їх основі формується професійне судження аудитора щодо достовірності фінансової звітності підприємницької структури. Аудит неможливий без належного документування фактів, операцій та контрольних процедур, такий процес забезпечує прозорість перевірки, можливість відстеження рішень аудитора та підтвердження відповідності міжнародним стандартам.

Аудиторські докази – це будь-яка інформація, отримана аудиторами для підтвердження правильності і повноти фінансової звітності.

Аудиторські докази можуть мати різний характер від документального, усного, аналітичного до емпіричного, їх обсяг та достовірність визначаються сутнісною характеристикою і ризиком конкретних операцій. Ключовим завданням аудитора є оцінка отриманих доказів з точки зору їх надійності, актуальності та достатності для формування обґрунтованого аудиторського висновку.

Робочі документи аудитора виконують роль «дорожньої карти» аудиторського процесу. Вони фіксують виконання всіх процедур, результати тестів контролю та аналітичних перевірок, а також аргументацію щодо професійних суджень. Також вони забезпечують належне документування внутрішніх перевірок і полегшують повторну перевірку результатів, як у межах внутрішнього контролю аудиторської фірми, так і при зовнішньому нагляді.

Особливе значення робочі документи набувають у сучасному цифровому середовищі, де фінансові потоки і дані автоматизовані, а інформаційні системи інтегровані. Використання електронних робочих файлів дозволяє підвищити ефективність збору доказів, контролювати версії файлових документів та

забезпечити захищене зберігання інформації. Зазначене не знімає відповідальності аудитора за оцінку виявлених відхилень і правильність професійних висновків.

В наступній таблиці представлено види аудиторських доказів (табл. 5.5).

Таблиця 5.5

Види аудиторських доказів

Категорія доказів	Опис	Приклади застосування	Джерело, Метод збору
Фізичні	Матеріальні об’єкти або активи, що підтверджують існування чи стан	Перевірка наявності товарів на складі, огляд обладнання	Інспекція, інвентаризація
Документальні	Письмові або електронні документи, що містять інформацію	Контракти, рахунки-фактури, платіжні доручення	Перегляд документації, перевірка автентичності
Аналітичні	Порівняння даних, розрахунки та тренди для виявлення відхилень	Аналіз фінансових показників, порівняння минулорічних даних	Обробка звітності, математичні моделі
Зовнішні джерела	Інформація, підтверджена зовнішніми джерелами	Банківські виписки, письмові підтвердження постачальників	Запити, письмові підтвердження, зовнішні сервіси
Інтерв’ю	Усні пояснення, підтвердження або роз’яснення від співробітників	Інтерв’ю з менеджментом, співробітниками бухгалтерії	Проведення співбесід, опитувань
IT-докази	Дані з інформаційних систем, що підтверджують операції або події	Журнали транзакцій, контрольні звіти систем	Експорт даних, перевірка логів, системні тести
Спостереження	Докази, отримані шляхом безпосереднього спостереження процесів	Огляд виробничих процесів, контроль робочих операцій	Неперервне спостереження, інспекція процесу
Тестові	Тести та моделювання для перевірки достовірності систем	Перевірка розрахунків у бухгалтерських програмах, тестові транзакції	Симуляція, тестування, контрольні приклади

Особливості аудиторських доказів в цифровому середовищі представлено в таблиці 5.6.

Таблиця 5.6

Особливості аудиторських доказів в цифровому середовищі

Особливість	Опис	Приклади	Методи збору / перевірки	Ризики та обмеження
Електронна форма	Докази існують у вигляді цифрових файлів або записів	Електронні рахунки, цифрові контракти, журнали транзакцій	Експорт даних, перевірка цифрових підписів, контроль версій	Можлива фальсифікація, втрати даних
Автоматизованість процесів	Дані генеруються або обробляються системами без ручного втручання	ERP-звіти, автоматичні облікові записи	Перевірка логів систем, тестові операції, контроль алгоритмів	Ризик технічних збоїв або помилок алгоритму
Швидкість накопичення даних	Великі обсяги даних формуються миттєво	Транзакції онлайн-магазинів, інтегровані системи обліку	Аналітичні перевірки, вибірковий аудит, програмні засоби аналізу	Перевантаження, пропуск аномалій у вибірках
Множинність джерел	Дані надходять із різних систем та платформ	Хмарні сервіси, внутрішні сервери, зовнішні контрагенти	Порівняння та узгодження даних, підтвердження від третіх сторін	Несумісність форматів, різна ступінь достовірності
Логування та сліди	Докази зберігають історію змін та дій користувачів	Журнали операцій, контрольні записи змін	Аналіз логів, трасування операцій, перевірка прав доступу	Можливість видалення або зміни логів
Дистанційність доступу	Дані можуть зберігатися віддалено та доступні онлайн	Хмарні документи, віддалені бази даних	Перевірка доступу, аудит облікових записів, контроль автентичності	Ризик несанкціонованого доступу або втрати з’єднання
Вразливість до кібератак	Дані можуть бути змінені або викрадені	Втручання у систему обліку, підробка електронних документів	Аналіз безпеки, перевірка цифрових підписів, контроль цілісності	Високий ризик маніпуляцій або шкідливого впливу

Особливість	Опис	Приклади	Методи збору / перевірки	Ризики та обмеження
Можливість автоматичного аналізу	Дані піддаються швидкій обробці аналітичними інструментами	Масові фінансові операції, електронні журнали	Аналітика, статистичний аудит, тестування систем	Неправильне налаштування алгоритмів може спотворити результати

Робочі документи аудитора є основою доказової бази та організаційного порядку перевірки, проте цифровізація бізнес-процесів суттєво змінила їх природу та способи використання. У сучасному середовищі робочі документи перестали бути виключно паперовими носіями інформації і здобули нові форми (електронні файли, інтегровані таблиці, журнали транзакцій та аналітичні звіти, автоматично згенеровані системами обліку).

Основне завдання робочих документів у цифровому аудиті – це забезпечення надійного та відтворюваного сліду перевірки. Робочі документи фіксують результати тестування і перевірки операцій, методи, критерії та джерела, що дозволяє відтворити процес аудиту у будь-який момент. Ключовим аспектом є адаптація до специфіки цифрових систем, де кожен запис у базі даних або у журналі подій може містити інформацію про автора зміни, часову мітку та параметри системи, що суттєво розширює можливості аудитора у відстеженні ризиків і контролі достовірності.

Робочі документи слугують інструментом комунікації та координації між суб'єктами аудиту. Електронні платформи дозволяють спільне використання документів, коментування та верифікування, що особливо важливо при дистанційних перевірках або залученні зовнішніх фахівців. При цьому зберігається принцип цілісності та конфіденційності.

У цифровому середовищі документи поділяються на такі категорії:

- *фінансові дані;*
- *аналітичні розрахунки;*
- *результати тестів;*

- *письмові підтвердження;*
- *лог-файли систем.*

Така організація забезпечує швидкий доступ до потрібної інформації, знижує ризик втрати доказів та підвищує ефективність аудиту.

Робочі документи в цифровому аудиті мають потенціал для автоматизації частини процесів, де створення контрольних таблиць, зведення показників та підготовка аналітичних звітів частково довірено системам (табл. 5.7). Проте остаточний аудит завжди потребує професійної оцінки та інтерпретації отриманих даних, щоб уникнути помилкових висновків та забезпечити достовірність висновків аудиторської перевірки.

Таблиця 5.7

Робочі документи аудитора в цифровому середовищі

Категорія документів	**Види документів**	**Призначення**	**Методи збору та використання**	**Особливості цифрового середовища**
Фінансові документи	Електронні бухгалтерські записи, звіти, рахунки-фактури, платіжні доручення	Підтвердження операцій, оцінка достовірності фінансових даних	Експорт із систем обліку, перевірка автентичності, порівняння із банківськими даними	Можливість швидкої аналітики, великий обсяг даних, цифровий слід змін
Аналітичні та розрахункові документи	Зведені таблиці, фінансові моделі, трендові графіки, KPI-аналітика	Аналіз показників, виявлення відхилень, прогнозування ризиків	Створення у програмних пакетах, порівняння періодів, обчислювальні перевірки	Автоматичне оновлення даних, інтеграція з іншими системами, ризик помилок алгоритмів
Документи підтвердження від третіх сторін	Листи від банків, постачальників, партнерів; електронні сертифікати	Підтвердження балансів, зобов'язань, наявності активів	Письмові або електронні запити, перевірка автентичності цифрових підписів	Часто зберігаються у хмарних системах, необхідна перевірка цілісності
Тестові та контрольні документи	Журнали транзакцій, результати тестових операцій	Перевірка функціонування систем та процесів, виявлення помилок	Тестування систем, вибіркові перевірки, аналіз логів	Автоматизоване ведення, збереження детальних логів, можливість трасування змін

Категорія документів	Види документів	Призначення	Методи збору та використання	Особливості цифрового середовища
Документація процедур та робочих кроків	План аудиту, чек-листи, внутрішні методики, інструкції	Організація роботи аудитора, фіксація процесу	Створення в електронному вигляді, спільний доступ для команди, створення нових версій та веріфікація	Можливість централізованого контролю, інтеграція з проєктними платформами
Комунікаційні документи	Електронні листи, записи зустрічей, коментарі у документах, повідомлення в системах	Фіксація обговорень, отриманих пояснень, підтверджень	Збереження копій, системні журнали повідомлень, аудіо/відеозаписи зустрічей	Доступність для спільної роботи, збереження цифрового сліду змін, необхідність контролю конфіденційності
Безпекові та IT-докази	Логи доступу, журнали змін у системах, звіти про безпеку	Перевірка кібербезпеки, контролю прав доступу, аудиту змін	Аналіз системних журналів, перевірка контрольних точок, аудит налаштувань безпеки	Висока деталізація даних, інтеграція з аналітичними інструментами, уразливість до втручання
Архівні документи	Старі електронні звіти, історичні журнали, резервні копії	Підтвердження минулих операцій, аналіз тенденцій	Доступ через архіви систем або хмарні сховища, відновлення даних	Збереження історії змін, необхідність перевірки цілісності та достовірності

Цифрове середовище змінює характер аудиторського процесу, тому представимо в таблиці основні хмарні сервіси та платформи в роботі аудитора (табл. 5.8).

Таблиця 5.8

Хмарні сервіси та платформи в роботі аудитора

Тип платформи / сервісу	Приклади	Призначення в аудиті	Методи використання	Особливості та ризики
Хмарні бухгалтерські системи	QuickBooks Online, Xero	Ведення обліку, формування фінансової звітності	Експорт звітів, контроль транзакцій, аналітична перевірка	Висока швидкість обробки даних, залежність від доступу до Інтернету, ризик несанкціонованого доступу
Платформи для документообігу	Google Workspace, Microsoft 365, Dropbox Business	Збереження та обмін робочими документами, спільна робота	Спільний доступ до файлів, контроль версій, коментування	Потреба у контролі прав доступу, можливість витоку конфіденційної інформації
Системи для здійснення аудиту	CaseWare, TeamMate, IDEA, ACL, Аксіома-Аудит, AuditXP	Планування аудиторських робіт, моніторинг виконання завдань	Створення завдань, відстеження прогресу, зберігання робочих документів	Необхідність стандартизації даних, ризик втрати інформації при некоректних налаштуваннях
Аналітичні та BI-платформи	Power BI, Tableau, Google Data Studio	Аналіз великих обсягів фінансових та операційних даних	Підключення до баз даних, формування дашбордів, візуалізація трендів	Можливі помилки при інтеграції даних, ризик некоректної інтерпретації
Сервіси для підтверджень третіх сторін	DocuSign, Adobe Sign, банківські онлайн-сервіси	Отримання електронних підтверджень, підписання документів	Верифікація електронних підписів, контроль цілісності документів	Потрібна перевірка автентичності, залежність від сторонніх провайдерів
Хмарні сховища даних	AWS S3, Google Cloud Storage, OneDrive for Business	Архівування робочих документів, резервне зберігання	Зберігання документів, доступ у будь-який час, контроль версій	Високий рівень доступності, але ризик кібератак та втрати даних
Сервіси для комунікацій та відеоконференцій	Zoom, Microsoft Teams, Google Meet	Проведення інтерв'ю, обговорення робочих документів	Запис зустрічей, ведення протоколів, обмін матеріалами	Потрібен контроль конфіденційності, ризик несанкціонованого запису або витоку інформації

Сучасна аудиторська діяльність у цифровому середовищі значною мірою залежить від інтеграції хмарних сервісів та онлайн-платформ. Такі інструменти забезпечують ефективне зберігання та обробку великих обсягів даних, створюють умови для більш гнучкого та оперативного виконання аудиторських процедур.

Хмарні бухгалтерські системи та платформи документообігу дозволяють аудиторам швидко отримувати фінансові та операційні дані, контролювати їх достовірність і формувати робочі документи в електронному вигляді. Платформи управління проєктами і аналітичні BI-системи забезпечують структуроване планування, моніторинг виконання аудиторських завдань та проведення глибокого аналізу трендів і відхилень, що підвищує якість висновків.

Особлива увага приділяється сервісам, які дозволяють отримувати підтвердження від третіх сторін та автоматизувати перевірки. Використання таких сервісів підвищує надійність доказової бази та скорочує ручну роботу аудитора. Цифрове середовище вимагає пильної уваги до безпеки, контролю прав доступу та перевірки автентичності, оскільки хмарні сервіси і онлайн-платформи залишають цифровий слід, який може бути змінений або скомпрометований.

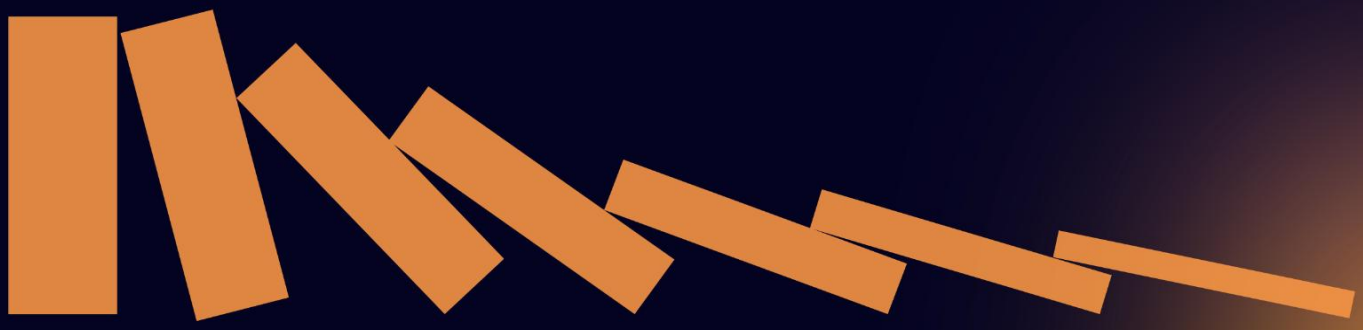
Таким чином, для сучасного аудитора важливо поєднувати класичні методи перевірки з грамотним використанням цифрових інструментів. Хмарні сервіси та онлайн-платформи підвищують ефективність аудиту та дозволяють більш точно оцінювати ризики, здійснювати контроль над великими обсягами даних і забезпечувати відтворюваність аудиторських процедур. Вони зобов’язують аудитора дотримуватися строгих стандартів безпеки, організації даних та налаштування прав доступу, щоб гарантувати достовірність і цілісність доказів.

5.4. Контрольні питання для самоперевірки

1. Які ключові завдання цифрового аудиту у фінансових структурах?
2. В чому полягає відмінність між традиційним аудитом та цифровим аудитом фінансових процесів?
3. Як цифрові технології змінюють підхід до оцінки фінансових ризиків?
4. Які основні етапи моніторингу фінансової безпеки в організації?
5. Як системи раннього попередження допомагають зменшувати фінансові ризики?
6. Які типи даних найчастіше використовуються для аналізу фінансової безпеки?
7. Які технології дозволяють автоматизувати контроль фінансових операцій?
8. Які фактори можуть впливати на ефективність цифрового аудиту та моніторингу фінансової безпеки?
9. Як цифровий аудит сприяє прозорості та довірі до фінансових інститутів?
10. Як організаційна структура та кваліфікація персоналу впливають на ефективність цифрового моніторингу фінансової безпеки?

Розділ 6

Автори:
Валентина Панасюк
Оксана Черешнюк



ІНФОРМАЦІЙНІ СИСТЕМИ ПІДПРИЄМСТВА ЯК ОБ’ЄКТ АУДИТУ

РОЗДІЛ 6. ІНФОРМАЦІЙНІ СИСТЕМИ ПІДПРИЄМСТВА ЯК ОБ'ЄКТ АУДИТУ

«Хто володіє інформацією, той володіє світом.»

Натан Ротшильд

6.1. Основні типи інформаційних систем підприємства

6.2. Бухгалтерські інформаційні системи та їх роль у формуванні аудиторських доказів

6.3. Внутрішній контроль в IT-середовищі

6.4. Контрольні питання для самоперевірки

6.1. Основні типи інформаційних систем підприємства (ERP, CRM, бухгалтерські системи)

Інформаційні системи підприємства – це сукупність програмних засобів, баз даних, технічної інфраструктури та організаційних процедур, які забезпечують збирання, обробку, зберігання і передавання інформації для ведення обліку, управління бізнес-процесами та підготовки звітності.

Вони підтримують внутрішню і зовнішню роботу підрозділів, забезпечуючи здійснення продажів, організацію закупівель, ведення складів, роботу персоналу, інтегрують дані між процесами та формують цифрові документи, що використовуються в контролі, аудиті та прийнятті управлінських рішень.

Перші інформаційні системи підприємства фактично були картотеками й друкарськими машинами. Саме IBM розвивала перфокарткову обробку даних, складів і витрат. Бізнес дуже швидко підхопив цю ідею для обліку працівників, що і стало раннім прообразом автоматизації. Спочатку підприємства планували ресурси, потім – виробництво і фінанси, а далі об'єднали в єдину систему продажі. Саме ця інтеграція дала підприємствам ефект «одного джерела інформації», коли дані вводяться один раз, а використовуються всіма підрозділами.

Основні типи інформаційних систем підприємства подано на рисунку 6.1.

Рис. 6.1. Основні типи інформаційних систем підприємства

Інформаційна система повинна забезпечити достовірність, повноту, своєчасність і захищеність облікових даних у системі, а також їх простежуваність від первинного документа до звітності. Для цього встановлюються правила доступу, фіксації та контролю змін, етапи та періодичність перевірок і закриття періодів, щоб мінімізувати помилки й несанкціоновані дії та своєчасно виявляти відхилення.

Основні завдання інформаційних систем підприємства такі:

- *збирання та реєстрація даних про господарські операції й події;*
- *обробка інформації, а саме класифікація, формування проводок і регістрів, проведення розрахунків;*
- *зберігання та архівація даних і документів із забезпеченням цілісності, можливості оновлення та доступності;*
- *передавання й обмін інформацією між підрозділами та зовнішніми контрагентами і державними системами;*
- *формування фінансової, податкової і управлінської звітності;*
- *автоматизація бізнес-процесів і контроль виконання;*
- *забезпечення внутрішнього контролю та безпеки;*
- *підтримка відповідності і дотримання вимог законодавства, внутрішніх стандартів та вимог.*

Її роль в управлінні полягає в тому, щоб надавати керівництву своєчасні й достовірні дані для планування, контролю, аналізу та прийняття управлінських рішень, а також узгоджувати роботу підрозділів через єдині правила й визначені показники. Класифікація інформаційних систем підприємства потрібна, щоб упорядкувати різні типи систем і чітко розуміти, яке завдання система вирішує та які ресурси для цього потрібні. Вона допомагає правильно обрати, порівняти й впровадити результати, визначити вимоги до інтеграції й безпеки, розподілити відповідальність, а також оцінити ризики й побудувати адекватні процедури контролю та аудиту. У таблиці 6.1 подано класифікаційні ознаки інформаційних систем підприємства.

Таблиця 6.1

Класифікація інформаційних систем підприємства

Класифікаційна ознака	Види	Коротка характеристика
За розміром охоплення	Одиничні	Працюють на одному пристрої без мережі та мають кілька простих модулів із спільними даними
	Групові	Для робочих груп, локальна мережа спільна
	Корпоративні	Для великих компаній, де територіально розподілені підрозділи, існує ієрархія серверів
	Глобальні	Охоплюють країну чи континент (державні платформи, міжнародні мережі)
За сферою застосування	Бази даних	Реєстрація й обробка операцій у режимі реального часу (облік, склад, продажі)
	Система підтримки рішень	Аналіз даних через запити, зрізи, моделі (управлінська аналітика)
	Інформаційно-довідкові	Пошук і доступ до інформації чи довідників, баз документів
	Офісні ІС	Автоматизація діловодства, електронний документообіг, перетворення паперових документів на електронні
За способом організації (архітектурою)	Файл-сервер	Дані у файлах на сервері, а обробка відбувається часто на робочих станціях
	Клієнт-сервер	Ролі розподілено між клієнтом і сервером
	Багаторівнева	Кожну частину можна змінювати або оновлювати окремо
	Інтранет-технології	Доступ через корпоративну мережу або веб-інтерфейс
За сферою діяльності	Державні	На рівні держави (е-звітність та інші)
	Територіальні (регіональні)	Для регіонів, громад і адміністрацій
	Галузеві	Для конкретної галузі (наприклад банківські, медичні, освітні)
	Підприємства чи установи	Внутрішні корпоративні інформаційні системи
	Технологічних процесів	Для виробництва чи функціонування обладнання
За типом підтримки управління	Системи обробки операцій	Реєструють і обробляють дані систематично або в реальному часі

	Автоматизовані системи управління технологічним процесом	Керування технологічними процесами, типові рішення для виробництва
	Системи співробітництва	Комунікація й координація, такі як групова робота, спільні ресурси
	Менеджерські системи	Звіти для менеджменту, контроль показників
За ступенем інтеграції	Автономні	Окремі програми без інтеграцій
	Інтегровані	Єдиний формат даних і процесів
	Платформні	Підключення зовнішніх сервісів
За способом розгортання	Локальні	На серверах підприємства
	Хмарні	У хмарі постачальника, доступ через інтернет
	Гібридні	Частина сервісів у хмарі, частина локально
За режимом обробки даних	Пакетний	Обробка періодами
	Онлайн або реального часу	Операції й контроль одразу при введенні
За рівнем автоматизації	Інформаційні	Фіксують і зберігають дані, підтримують документообіг
	Автоматизовані	Частину операцій виконує система, частину – користувач
	Інтелектуальні	Аналітика та ШІ для прогнозування і розробки рекомендацій
За критичністю для бізнесу	Критичні	Відсутність обладнання означає зупинку бізнесу
	Важливі	Впливають на ефективність
	Допоміжні	Сервісні функції, такі як довідники, внутрішні сервіси
За доступом користувачів	Внутрішні	Для працівників підприємства
	Зовнішні	Для клієнтів і контрагентів
	Змішані	Частина функцій відкрита назовні, частина – внутрішня

У розвитку та впровадженні інформаційної системи підприємства виділяють послідовні етапи її життєвого циклу від формування задуму до супроводу в експлуатації. ***На етапі розробки концепції інформаційної системи*** проводять обстеження об’єкта автоматизації, аналізують бізнес-процеси, вивчають форми вхідних і вихідних документів та методики розрахунку показників. Додатково оцінюють вимоги замовника, добирають підходи до

моделювання процесів, здійснюють пошук можливих програмних рішень і порівнюють альтернативні варіанти проєкту.

На етапі розроблення технічного завдання формується технічне завдання як основний документ, що визначає мету створення системи, її функції, вимоги до якості, безпеки та інтеграцій, а також порядок розробки й приймання в експлуатацію. За потреби можуть складатися окремі технічні завдання для підсистем або модулів.

Розробляється концепція інформаційної бази, створюються моделі даних, визначаються вимоги до структури інформаційних масивів, технічних засобів і програмного забезпечення. Також формуються системи класифікації та кодування техніко-економічної інформації. Результатом є комплект проєктної документації, технічний проєкт (опис задач, алгоритмів, інформаційного, організаційного, технічного і програмного забезпечення) та робочий проєкт.

На етапі реалізації і адаптації програмного продукту виконується створення програмного забезпечення відповідно до затвердженої проєктної документації, налаштовуються модулі та інтерфейси, готується продукт до тестування. Підсумком етапу є готовий програмний продукт або налаштована система.

Впровадження в експлуатацію, тестування та налагодження передбачає перевірку відповідності системи вимогам технічного завдання, дослідна експлуатація для виявлення можливих недоліків та їх усунення. Паралельно здійснюється навчання персоналу, готується робоча документація, виконуються приймальні випробування, після чого система передається замовнику в промислову експлуатацію.

На основі гарантійних і сервісних зобов'язань забезпечується технічна підтримка системи, усуваються помилки, здійснюються оновлення та адаптація до змін у законодавстві, процесах або технологіях. Цей етап забезпечує стабільну роботу інформаційної системи протягом усього періоду її використання.

Впровадження інформаційних систем на підприємстві зазвичай приводить до стандартизації бізнес-процесів і формування єдиного інформаційного

простору, де дані вводяться один раз і використовуються всіма підрозділами. У результаті підвищується оперативність управління, оскільки керівництво отримує своєчасні та узгоджені показники для планування, контролю й аналізу. Автоматизація зменшує кількість ручних операцій і помилок, прискорює документообіг та покращує простежуваність «операція → регістр → звітність». Одночасно зростає прозорість і керованість внутрішнього контролю завдяки розмежуванню доступів, журнал реєстрації подій та правил закриття періодів. Сукупно це знижує ризики викривлення облікових даних, підвищує якість звітності та створює надійну інформаційну основу для аудиту й прийняття управлінських рішень. Найтиповіші результати впровадження цифрових технологій подано на рисунку 6.2.

Рис. 6.2. Результати впровадження цифрових технологій та застосування інформаційних систем

Отже, інформаційні системи підприємства є основою сучасного обліку й управління, оскільки забезпечують інтегроване збирання, обробку та зберігання даних і формування звітності за принципом «одного джерела інформації». У результаті впровадження таких систем підприємство отримує стандартизовані процеси, прозорий внутрішній контроль, кращу простежуваність операцій і більш надійну інформаційну базу для прийняття управлінських рішень та аудиту.

6.2. Бухгалтерські інформаційні системи та їх роль у формуванні аудиторських доказів

Для бізнесу бухгалтерська інформаційна система – це сукупність програмних і організаційних засобів, що забезпечують реєстрацію господарських операцій, їх обробку, зберігання, формування облікових регістрів і звітності, а також контроль доступу й відстеження змін. У сучасному аудиті бухгалтерські інформаційні системи є одночасно джерелом інформації для перевірки і об'єктом оцінки наскільки система надійна та чи можна покладатися на дані.

Програмні продукти BAS, зокрема «BAS Бухгалтерія» та «BAS ERP», широко застосовуються для ведення обліку й формування звітності згідно чинних вимог. Послідовність роботи BAS спирається на такий зв'язок:
первинний документ → проведення → регістри або обороти → звітність.

Тому для аудитора BAS це середовище, де можна простежити повний «ланцюг доказів» від події до показника у фінансовій звітності. Програма має ряд переваг, адже містить вичерпну інформацію про всі внесені господарські операції. У BAS особливу роль відіграють:

- *первинні документи з обов'язковими реквізитами, які фіксують факт операції;*
- *звітність, що заповнюється на основі даних інформаційної бази та розрахунків у системі;*
- *журнал реєстрації подій, який дозволяє встановити, які дії виконували користувачі та які події відбувалися в інформаційній базі.*

У «BAS Бухгалтерія» головне меню побудоване за логікою господарських процесів і ділянок обліку. Така структура допомагає користувачу працювати «від події до звітності», а саме спочатку вводяться первинні документи і відбувається фіксація факту господарської операції. Далі система формує проведення та накопичує дані в регістрах, після чого ці дані відображаються у звітних формах. Тому кожен розділ меню відповідає певній групі операцій і водночас певному

набору аудиторських доказів, які можна отримати із системи. Нижче на рисунках подано характеристику програми за вкладками (рис. 6.3 – рис. 6.14).

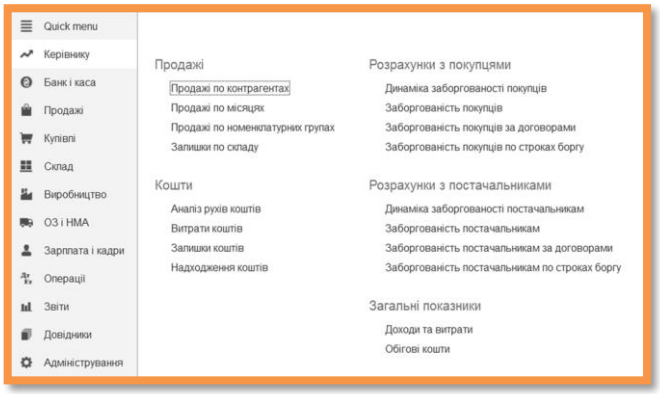


Рис. 6.3. Інтерфейс вкладки «Керівнику» в програмі BAS

Розділ «Керівнику» орієнтований не на введення документів, а на огляд результатів. У ньому зазвичай доступні зведені показники, короткі аналітичні огляди та ключові підсумки, наприклад, стан розрахунків, грошей, продажів чи витрат. У навчальному сенсі цей розділ демонструє, як оперативні дані, введені бухгалтерами, перетворюються на управлінську картину для керівництва.

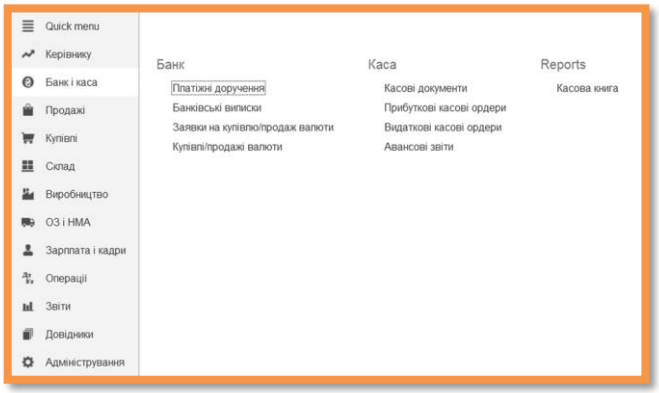


Рис. 6.4. Інтерфейс вкладки «Банк і каса» в програмі BAS

У розділі «Банк і каса» зосереджені всі операції, пов’язані з рухом грошових коштів. Саме тут оформлюють банківські виписки та платіжні документи, касові ордери, відображають надходження і витрати готівки, а також контролюють взаєморозрахунки й залишки коштів. Для обліку це область розрахункових операцій, а для аудиту – джерело доказів щодо існування, повноти та правильності відображення грошових потоків і розрахунків.

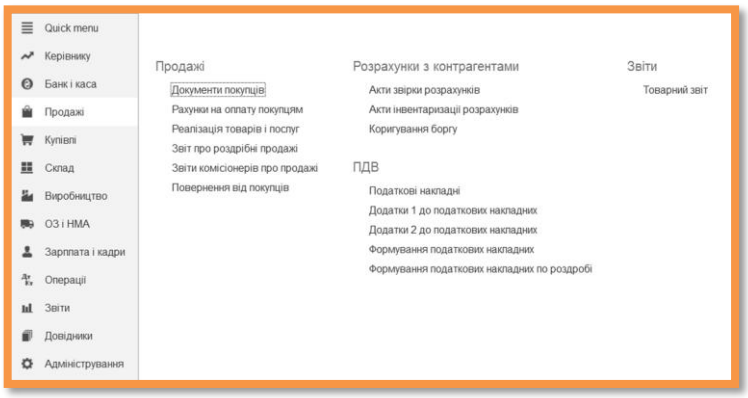


Рис. 6.5. Інтерфейс вкладки «Продажі» в програмі BAS

Розділ «Продажі» охоплює операції реалізації стосовно підготовки та оформлення документів відвантаження, актів виконаних робіт і наданих послуг, повернень від покупців, а також супровід розрахунків із клієнтами. Через цей розділ формується дохід, ПДВ та дебіторська заборгованість. Важливо, що в «BAS Бухгалтерія» продажі пов’язані з договорами та контрагентами, тому користувач може простежити ланцюг договір → документ → проведення → звіт.

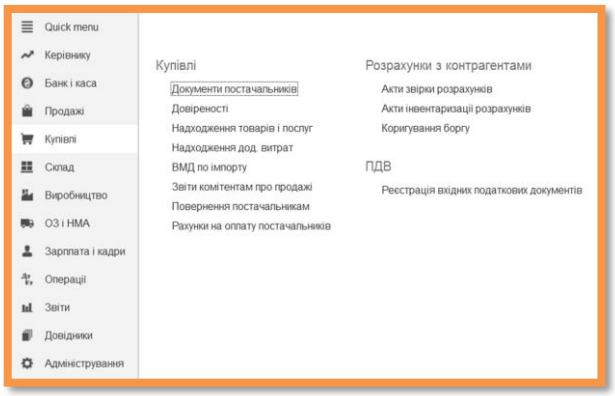


Рис. 6.6. Інтерфейс вкладки «Купівлі» в програмі BAS

Розділ «Купівлі» призначений для обліку закупівель і витрат на придбання. Тут вводять документи надходження товарів і послуг, повернення постачальникам, відображають супутні витрати, наприклад доставку, якщо це налаштовано, і контролюють кредиторську заборгованість. У підручнику цей розділ зручно пояснювати як «вхідний потік» ресурсів, який потім впливає на склад, витрати та собівартість.

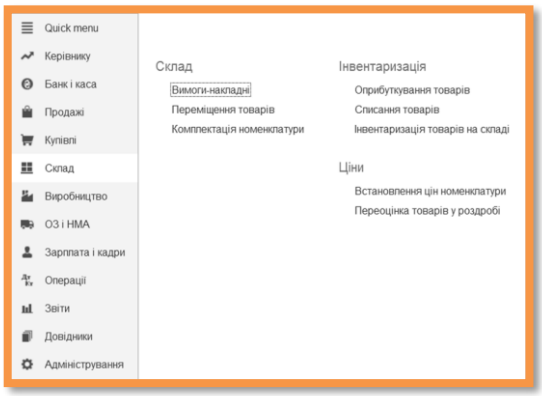


Рис. 6.7. Інтерфейс вкладки «Склад» в програмі BAS

Розділ «Склад» містить операції з товарно-матеріальними цінностями стосовно переміщення між складами, списання, оприбуткування, інвентаризацію та контроль залишків. Він показує, як BAS забезпечує кількісний і вартісний облік запасів, а також як документи складського руху формують підставу для витрат і собівартості. Для аудиту цей розділ є базою для перевірки повноти відображення запасів і правильності їх оцінки.

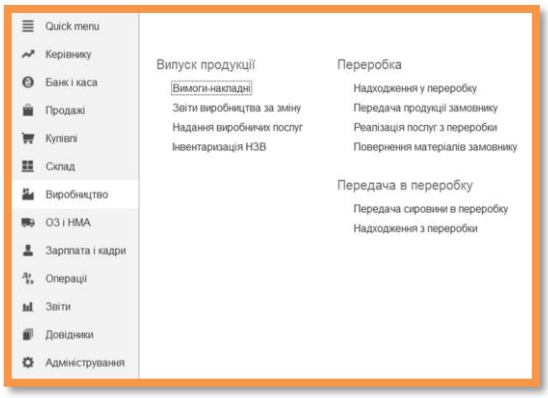


Рис. 6.8. Інтерфейс вкладки «Виробництво» в програмі BAS

Розділ «Виробництво» у «BAS Бухгалтерія» використовується тоді, коли підприємство веде виробничі операції і списує матеріали у виробництво, відображає випуск готової продукції, облік напівфабрикатів та елементи калькулювання. Навчально цей блок ілюструє перетворення запасів на готову продукцію та послідовність формування виробничої собівартості.

Рис. 6.9. Інтерфейс вкладки «Основні засоби (ОЗ) і нематеріальні активи (НМА)» в програмі BAS

Розділ «ОЗ і НМА» відповідає за облік основних засобів і нематеріальних активів від надходження та введення в експлуатацію до модернізації, переміщення, вибуття й нарахування амортизації. Він демонструє, як BAS підтримує довгострокові активи протягом усього життєвого циклу, забезпечуючи коректне відображення їх вартості та зносу в обліку і звітності.

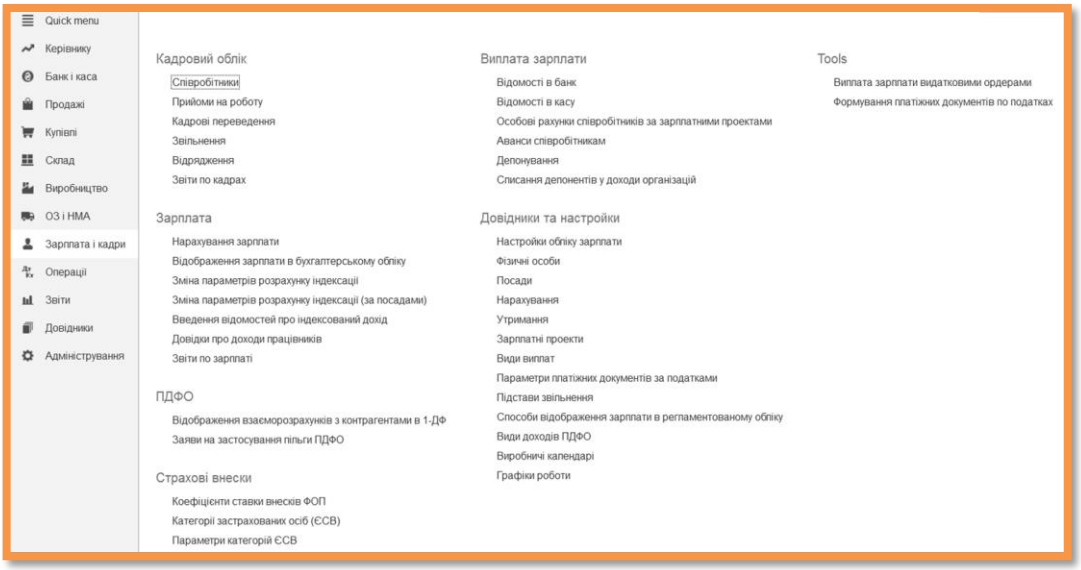


Рис. 6.10. Інтерфейс вкладки «Зарплата і кадри» в програмі BAS

У розділі «Зарплата і кадри» зібрані кадрові події та нарахування, такі як прийом, звільнення, табель, відпустки, лікарняні, розрахунок заробітної плати, утримань і виплат. Для системного розуміння важливо, що дані цього розділу впливають і на витрати, і на розрахунки з персоналом та бюджетом.

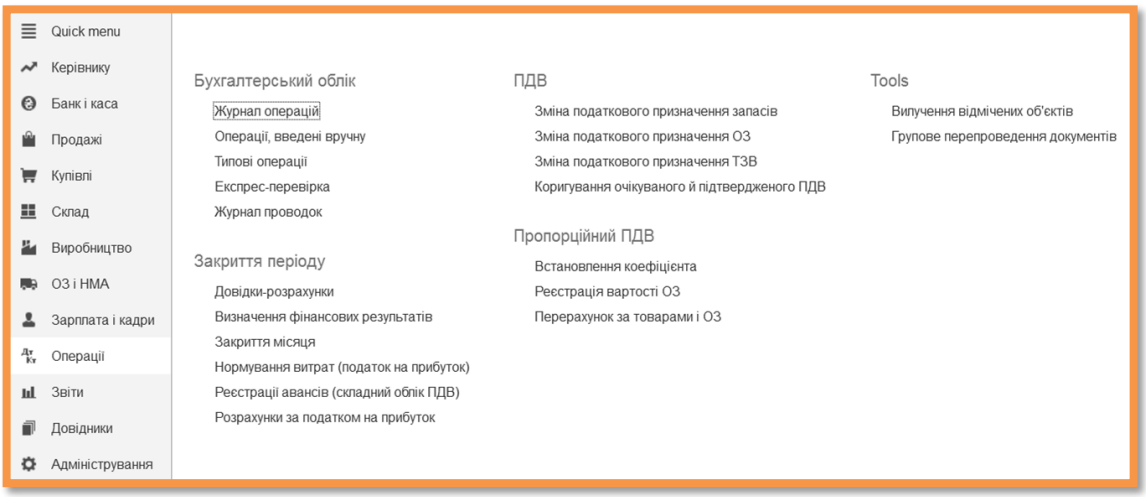


Рис. 6.11. Інтерфейс вкладки «Операції» в програмі BAS

Розділ «Операції» виконує роль «бухгалтерського ядра», де зосереджені інструменти для типових бухгалтерських коригувань і процедур. Тут можуть бути доступні ручні операції, коригування, а також процедури закриття місяця, залежно від налаштувань. Методично важливо пояснювати це як блок, що забезпечує завершення облікового циклу та узгодження даних перед формуванням звітності.

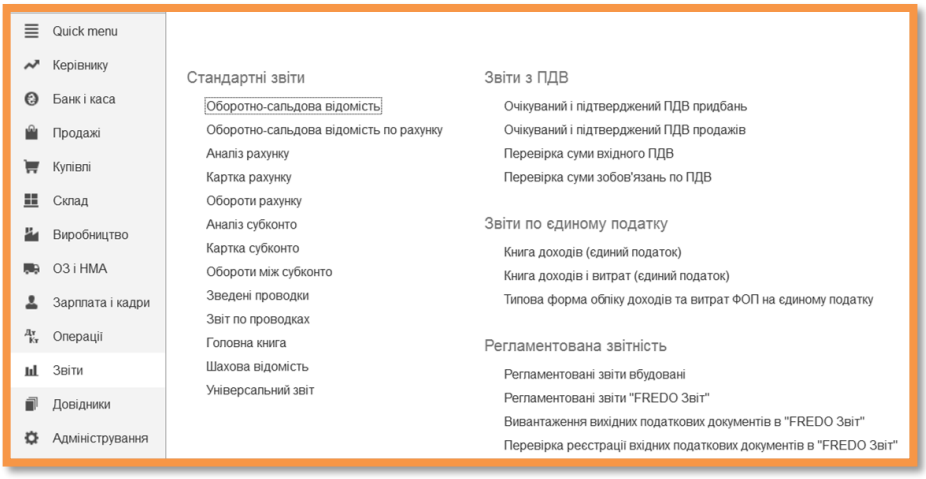


Рис. 6.12. Інтерфейс вкладки «Звіти» в програмі BAS

Розділ «Звіти» – це підсумкова частина системи, де користувач отримує регістри та аналітичні форми, а саме оборотно-сальдові відомості, картки рахунків, аналізи субконто, звіти щодо розрахунків, запасів, грошових потоків тощо. Саме звіти перетворюють масив документів і проведень на інформацію для контролю та управління, а також дають аудитору інструмент вибірки й перевірки.

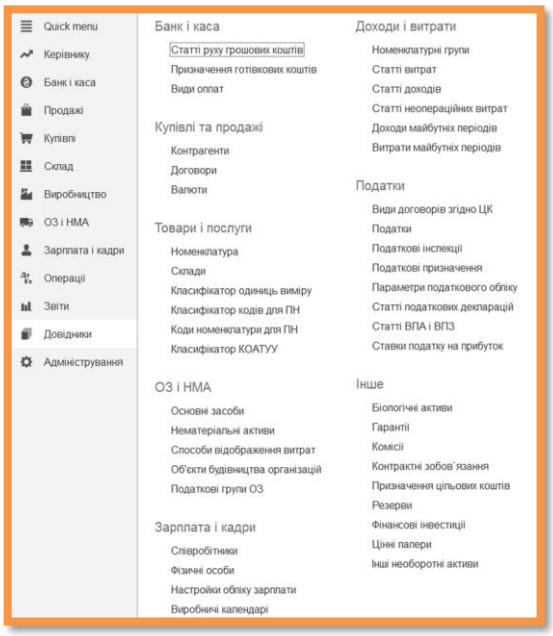


Рис. 6.13. Інтерфейс вкладки «Довідники» в програмі BAS

Розділ «Довідники» містить нормативно-довідкову інформацію про систему, а саме дані про контрагентів, номенклатуру, склади, договори, статті доходів і витрат, підрозділи та інші класифікатори. Довідники є основою єдиного кодування і стандартизації даних, правильність заповнення довідників безпосередньо впливає на якість обліку й достовірність звітів.

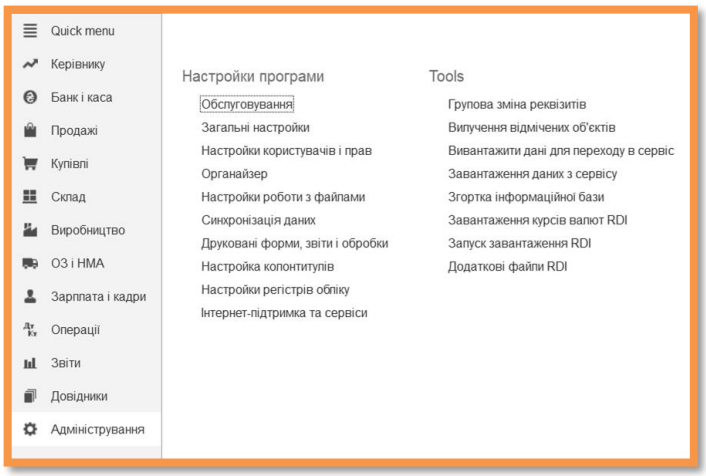


Рис. 6.14. Інтерфейс вкладки «Адміністрування» в програмі BAS

«Адміністрування» охоплює налаштування системи, параметри обліку, користувачів і права доступу, службові функції, обмін даними та інші технічні дані. Цей розділ пов’язаний із поняттям загальних IT-контролів, а саме через адміністрування забезпечується, хто і що може змінювати в системі, а отже наскільки надійними є дані, сформовані в «BAS Бухгалтерія».

Міжнародний стандарт аудиту 500 зазначає, що якість аудиторських доказів визначається їх доречністю та надійністю, а надійність залежить від джерела та характеру інформації і умов її отримання. У контексті BAS це означає, що навіть якщо дані взято з програми, аудитор має оцінити їх достовірність, перевіривши доступи, журнали подій, послідовність проведення, заборону редагування періодів, резервне копіювання тощо.

У «BAS Бухгалтерія» аудитору доступні різні види доказів, які подано на рисунку 6.15.

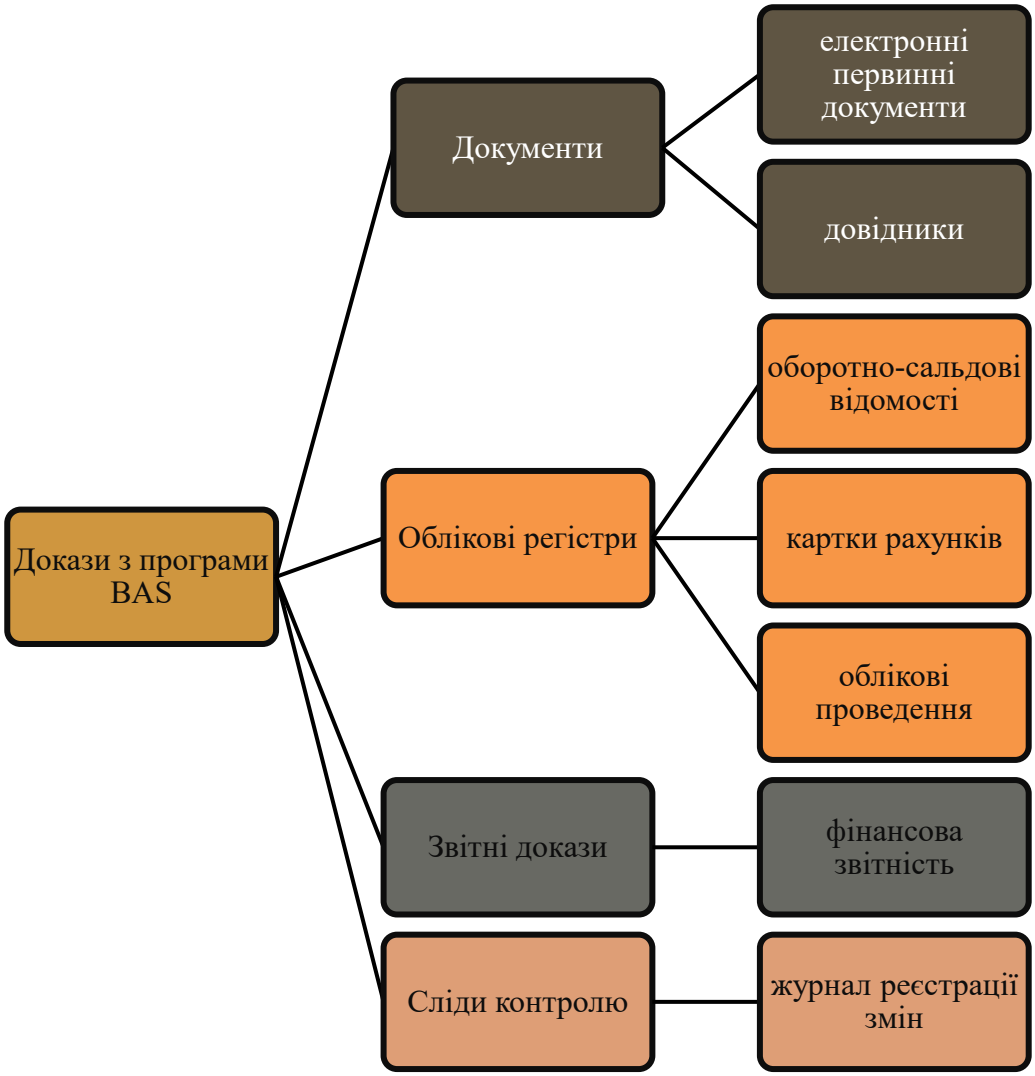


Рис. 6.15. Види доказів у «BAS Бухгалтерія»

У практиці аудитор проводить роботу у двох напрямках, а саме:

- від звітності до першоджерела;
- від первинного документа до звітності.

Такий підхід допомагає зрозуміти, як показник у фінансовій звітності формується з конкретних господарських операцій, і водночас як окрема операція впливає на підсумкові дані обліку. Практичну перевірку в середовищі BAS зручно вибудовувати як послідовність взаємопов'язаних кроків.

Спочатку аудитор визначає, які саме показники звітності підлягають перевірці. Залежно від цілей завдання та оцінених ризиків обирають ключові статті, наприклад виручку, собівартість, запаси, дебіторську або кредиторську заборгованість. Вибір показників важливий, оскільки саме він задає перелік облікових ділянок, документів і звітів, з якими працюватиме аудитор.

Далі аудитор отримує розшифровку вибраного показника у BAS через стандартні регістри та звіти. На цьому етапі формуються потрібні звіти, наприклад, оборотно-сальдова відомість, аналіз рахунку, розрахунки з контрагентами, складські залишки тощо і обов'язково фіксуються параметри формування період, організація, відбори, групування, інші налаштування. Саме коректність параметрів визначає, чи буде розшифровка репрезентативною та порівнюваною, а також чи можна буде відтворити результати перевірки.

Після цього аудитор перевіряє від рядка звіту до документів-джерел, які формують відповідні суми. Для вибірки операцій він відкриває конкретні документи, перевіряє їх реквізити, такі як дату, контрагента, номенклатуру, суму, склад, рахунки, підставу операції, а також відповідальних осіб і наявність підтвердних даних. У такий спосіб забезпечується простежуваність, а показник звіту підтверджується сукупністю конкретних первинних документів і проведень у системі.

Окремим обов'язковим етапом є оцінка IT-контролів, які забезпечують надійність інформації, що використовується як аудиторські докази. Насамперед аналізуються права доступу і ролі користувачів, щоб встановити, чи не має одна особа надмірних повноважень, які дозволяють одночасно створювати, змінювати і підтверджувати дані.

Далі перевіряється наявність і фактичне використання журналу реєстрації, який фіксує події та зміни в системі. Також оцінюються механізми

контролю змін і закриття періодів, що зменшують ризик правок заднім числом, а також процедури резервного копіювання як елемент загальних IT-контролів, що підтримує цілісність і доступність облікових даних.

Завершальним кроком є документування результатів перевірки. Висновки аудитора мають бути відображені у робочих документах так, щоб інший досвідчений аудитор міг зрозуміти обсяг виконаної роботи, застосований підхід і підстави для висновків (відповідно до логіки ISA 230). На практиці це означає збереження параметрів сформованих звітів, переліків відібраних операцій, скріншотів або вивантажень, а також опису отриманих доказів і оцінки їхньої якості. Такий порядок роботи забезпечує відтворюваність перевірки, прозорість аудиторського судження та належний рівень доказовості висновків.

Оскільки BAS – це система, в якій дані можуть змінюватися, аудитор повинен враховувати типові ризики, які подано на рисунку 6.16.

Рис. 6.16. Типові ризики при отриманні інформації з BAS

Відповідно, доказовість даних із BAS зростає, коли контроль доступу налаштований коректно, журнал реєстрації реально використовується для контролю подій, первинні документи містять обов’язкові реквізити та логічно узгоджуються з реальними операціями.

6.3. Внутрішній контроль в ІТ-середовищі

Внутрішній контроль в ІТ-середовищі – це система організаційних правил і технічних механізмів, яка забезпечує достовірність, повноту, своєчасність і захищеність інформації, що обробляється в інформаційних системах підприємства.

На відміну від традиційного «паперового» контролю, де головним доказом часто є підпис і печатка, в ІТ-середовищі ключовою стає здатність системи гарантувати, хто саме виконав дію, коли вона відбулася, що було змінено, і чи можна відтворити ланцюг від господарської операції до показника у звітності. Тому внутрішній контроль в ІТ-середовищі не зводиться лише до програмних налаштувань й поєднує політики управління доступом, дисципліну роботи з даними, регламенти закриття періодів, механізми журналювання та процедури забезпечення безперервності.

Контроль як суспільна потреба виник тоді, коли люди почали накопичувати ресурси й розподіляти їх між членами громади. У найдавніших державах Месопотамія та Стародавній Єгипет контроль пов’язувався з обліком зерна, податків і робіт, а записи на глиняних табличках і папірусі слугували підтвердженням виконаних операцій. З розвитком торгівлі та появою державної адміністрації зросла потреба у перевірці правильності збору податків і використання скарбниці. У середньовічних містах і цехах контроль підтримував довіру між учасниками обміну, адже перевіряли ваги, якість товарів, виконання зобов’язань і дотримання правил ремесла. Формування великих торгових компаній у Європі та відокремлення власників від управителів посилили запит на регулярну звітність і незалежну перевірку. Поширення подвійного запису в бухгалтерії створило системну основу для контролю через взаємоперевірку рахунків і підсумків. Індустріалізація XIX століття спричинила ускладнення виробництва та фінансів, тому з’явилися внутрішні регламенти, розподіл повноважень і спеціалізовані служби контролю.

У XX столітті контроль набув стандартизованих форм у вигляді внутрішнього контролю, внутрішнього аудиту та державного фінансового контролю, які почали спиратися на професійні норми. Наприкінці XX – на початку XXI століття комп'ютеризація й спеціальні програми змістили акцент із перевірки паперових документів на оцінку процесів, доступів, журналів подій і надійності даних у IT-середовищі. Сьогодні контроль еволюціонує у напрямі безперервного моніторингу, аналітики даних і автоматизованих перевірок, де головною цінністю є прозорість, простежуваність і своєчасне виявлення ризиків.

Практично внутрішній контроль в IT-середовищі будується на двох взаємопов'язаних рівнях. На рисунку 6.17 подано рівні контролю.

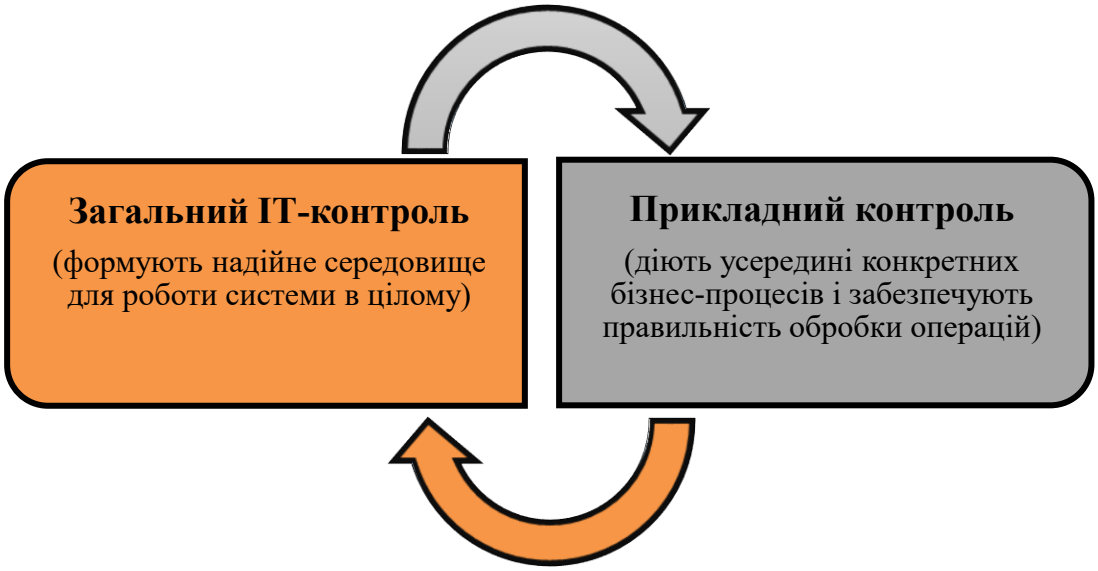


Рис. 6.17. Рівні контролю інформаційного середовища

Загальні IT-контролі формують надійне середовище для роботи системи в цілому і вони визначають, хто має доступ до інформаційної бази, як захищаються дані, як виконуються оновлення, резервне копіювання та відновлення, як контролюються технічні зміни. Прикладні контролі діють усередині конкретних бізнес-процесів і забезпечують правильність обробки операцій, перевірку повноти реквізитів, правильність розрахунків, логіку проведення документів, узгодженість записів між підсистемами та формування коректних вихідних звітів.

Основою загальних IT-контролів є контроль доступу. Він передбачає індивідуальні облікові записи користувачів, автентифікацію, встановлення ролей і прав, а також принцип мінімально необхідних повноважень – користувач повинен мати лише ті права, які потрібні для виконання його функцій. Важливим елементом є розподіл несумісних обов'язків.

Наприклад, небажано, щоб одна особа могла одночасно створювати довідники, вводити первинні документи, проводити їх і ще й виконувати коригування або змінювати налаштування системи. Такий розподіл зменшує ризик зловживань і робить процес прозорим, оскільки обмежує можливості однієї людини.

Другим критичним компонентом є журнал реєстрації подій і контроль змін. У надійному IT-середовищі будь-яка суттєва дія має залишати інформаційний слід.

Вхід користувача, створення або редагування документів, зміни довідників, повторне проведення, видалення записів, виконання масових операцій, запуск регламентних процедур записуються в історії користування програмою. Журнал подій перетворюється на інструмент контролю дисципліни обліку та на джерело доказів у випадку спірних ситуацій. Наявність журналу важлива, але ще важливіше особливості його аналізу.

Третій важливий блок загальних контролів є управління періодами та закриття облікового циклу. У цифровому обліку існує ризик, що документи можуть вводитися або змінюватися датою, що минула, впливаючи на показники звітного періоду.

Тому підприємства встановлюють правила закриття місяця і обмеження змін у закритих періодах. Така дисципліна забезпечує стабільність даних після формування звітності і подання її зовнішнім користувачам, а облікові показники не повинні змінюватися без оформленої процедури коригування.

Окремо виділяють контролі безперервності та збереження даних. До них належать:

- *регулярні резервні копії;*

- *контроль доступу до архівів;*
- *тестові відновлення;*
- *також плани дій на випадок технічних збоїв.*

Якщо облікова база буде втрачена або пошкоджена, жодні інші контролі не зможуть забезпечити достовірність і повноту звітності, тому резервне копіювання і контроль відновлення вважаються базовою умовою надійного IT-середовища.

Не менш важливим є управління змінами, оновлення програмного забезпечення, зміна алгоритмів розрахунків, налаштування форм документів, інтеграції з іншими системами.

Контроль тут полягає в тому, щоб зміни були санкціоновані, протестовані на окремому середовищі, задокументовані і впроваджені у визначений час із можливістю повернення. Без такого підходу зростає ризик, що система почне формувати інші проводки, ідентичні операції будуть обліковуватися по-новому, а порівнюваність даних між періодами погіршиться.

Прикладні контролі, на відміну від загальних, вбудовані у процес обробки господарських операцій. Їхня основна мета попередити або виявити помилки на етапі введення й обробки даних. До таких контролів належать:

- *перевірки обов'язкових реквізитів документів;*
- *контроль допустимих значень;*
- *контроль допустимих довідників;*
- *автоматичні розрахунки;*
- *логіка проведення операцій;*
- *контроль відповідності аналітики;*
- *процедури узгодження* (наприклад, погодження платежів або затвердження документів перед проведенням).

На виході прикладні контролі доповнюються контрольними звірками. Відбувається порівняння оборотів і залишків, виявлення від'ємних залишків запасів, аналіз непроведених документів, звірка розрахунків із контрагентами, контроль невідповідностей між підсистемами.

Важливо розуміти, що внутрішній контроль в IT-середовищі не є одноразовою подією. Це постійний систематичний контроль передбачає встановлення правил, їх виконання, моніторинг, аналіз відхилень і вдосконалення. Ефективний контроль має бути пропорційним ризикам. Для критичних ділянок, таких як грошові розрахунки, склад, податки запроваджують більш жорсткі правила доступу, детальні журнали і регулярні звірки; для менш ризикових – спрощені процедури.

У підсумку ***внутрішній контроль в IT-середовищі*** забезпечує підприємству дві ключові переваги. По-перше, підвищує якість управлінських рішень, бо дані стають надійними. По-друге, формує основу для підтвердження звітності та отримання аудиторських доказів, оскільки прозорі контролі роблять цифрові дані відтворюваними, перевірюваними і захищеними від викривлень.

В умовах цифрового ведення обліку внутрішній контроль все більше зміщується з перевірок лише документів у паперовому вигляді у площину контролів IT-середовища. Для «BAS Бухгалтерія» це означає, що достовірність облікових даних забезпечується не лише професійністю бухгалтера, а й тим, як налаштована система, хто має доступ, які дії фіксуються, як запобігають помилкам і несанкціонованим змінам. Внутрішній контроль у BAS розглядається як сукупність організаційних правил і програмних механізмів, які гарантують, що операції відображаються вчасно, правильно та повному обсязі, а дані захищені від викривлення.

Внутрішній контроль у «BAS Бухгалтерія» характеризують як систему послідовних «контрольних точок», розміщених уздовж усього життєвого циклу господарської операції від підготовки даних до завершення звітного періоду та забезпечення безперервності роботи. Такий підхід дозволяє не лише запобігати помилкам, а й своєчасно виявляти відхилення, фіксувати відповідальність і забезпечувати простежуваність даних від первинного документа до звітності.

Розрізняють наступні рівні контролів.

Перший рівень контролю формується до введення операції. На цьому етапі підприємство налаштовує середовище, у якому працює облік,

визначаються права доступу і ролі користувачів, встановлюються правила роботи з інформаційною базою, а також підтримуються актуальні довідники, контрагенти, номенклатура, статті витрат, склади тощо.

Саме тут закладається основа надійності даних. Якщо користувачі мають надмірні повноваження або довідники містять дублікати й некоректні параметри, то навіть правильно введені документи можуть породжувати неточні результати в регістрах і звітах.

Друга контрольна точка діє під час введення операції. У BAS її забезпечують вимоги до заповнення документів, обов'язкові реквізити, перевірки правильності введення, використання стандартизованих довідників і типових форм.

Завдяки цьому зменшується ризик технічних помилок, неправильний контрагент, склад, дата, кількість, одиниця виміру, а операція набуває належного документального оформлення в цифровому середовищі. Фактично BAS не дозволяє створити якісний облік без мінімального набору даних, потрібних для коректного відображення події.

Третій рівень контролю реалізується під час обробки введеної інформації. Ключовим механізмом BAS є проведення документів, яке автоматично формує бухгалтерські записи за вбудованими правилами.

На цьому етапі важливими стають контроль логіки проведень, правильність рахунків обліку та аналітики, а також автоматичні розрахунки, що забезпечують однакове відображення однотипних операцій. Саме тут відбувається перетворення первинної інформації на облікові дані і документ стає джерелом записів у регістрах і формує підґрунтя для звітності.

Четверта контрольна точка настає після відображення операції в обліку. Вона пов'язана з перевіркою результату, адже BAS надає звіти для звірок, інструменти контролю непроведених документів, аналіз оборотів, залишків, розрахунків із контрагентами, складських показників та інших ключових ділянок.

На практиці це означає регулярне виявлення невідповідностей:

- *непроведені документи;*
- *нетипові проводки;*
- *від'ємні залишки;*
- *незвичні відхилення у витратах чи виручці.*

Такі перевірки виконують роль оперативного контролю, який дозволяє коригувати помилки до закриття періоду.

П'ята контрольна точка пов'язана з етапом після закриття періоду. Її зміст – забезпечити стабільність даних і унеможливити несанкціоновані правки датою, що минула.

Для цього застосовують обмеження змін у закритих періодах, контроль коригувань через визначені процедури, а також використання журналу подій, що дозволяє відстежити дії користувачів і зміни в системі. У підсумку формується контрольоване середовище, у якому будь-яке коригування має бути обґрунтоване, документально підтверджене та прозоро відображене.

Нарешті, ***окремим наскрізним блоком виступає контроль безперервності.*** Він охоплює резервне копіювання та перевірку можливості відновлення даних, а також контроль оновлень і змін у системі, впровадження нових версій, налаштувань, доопрацювань.

Без цього підприємство ризикує втратити дані або отримати некеровану зміну облікової логіки, що прямо впливає на достовірність звітності.

Отже, модель контрольних точок у «BAS Бухгалтерія» дозволяє вибудувати внутрішній контроль як логічно завершену систему від правильно організованого доступу й довідників до перевірки результатів, закриття періоду та забезпечення безперервної роботи. Саме така послідовність робить цифровий облік керованим, прозорим і придатним для надійного формування звітності та аудиторських доказів.

Належно налаштований ***внутрішній контроль в IT-середовищі BAS*** має подвійний ефект. По-перше, він зменшує ризик помилок і зловживань, підвищуючи достовірність обліку та звітності. По-друге, він підвищує

доказовість інформації з BAS якщо доступи розмежовані, зміни фіксуються, періоди закриваються, а звірки виконуються регулярно, то дані системи стають надійною основою для управлінських рішень і аудиторських висновків.

Система контролю ризиків у BAS має не лише виявляти помилки, а й попереджати їх на ранніх етапах життєвого циклу операції. Завдяки такій системі внутрішнього контролю дані BAS стають більш надійними, підвищується якість аудиторських доказів, а підприємство отримує стабільний, прозорий та керований облік, який можна впевнено використовувати і для звітності, і для управління. У таблиці 6.2 подано перелік ризиків, які виникають в програмному продукті «BAS Бухгалтерія», перелік відповідних осіб при їх виникненні та шляхи їх зменшення.

Таблиця 6.2

Ризики інформаційного середовища «BAS Бухгалтерія»

Ризик	Контроль у BAS	Відповідальна особа	Доказ виконання
Несанкціонований доступ до бази, перегляд або зміна даних	Індивідуальні користувачі, ролі та права доступу (мінімально необхідні), заборона спільних логінів	Адміністратор BAS	Перелік користувачів і ролей, звіт налаштувань прав, журнал входів
Зловживання через надмірні права	Розподіл повноважень, розділити права створення довідників, проведення документів	Головний бухгалтер і адміністратор BAS	Список ролей і прав, наказ або розпорядження про розподіл функцій, скрін або звіт прав
Проведення документів датою, що минула для маніпуляції періодом	Закриття періоду і обмеження редагування, встановлення «коригування тільки через окремі документи»	Головний бухгалтер	Наказ про закриття, скрін параметрів в періоді, список документів, створених або перепроведених після закриття
Зміна проведених документів без контролю	Заборона редагування проведених документів для певних ролей, контроль повторного проведення, журнал подій	Головний бухгалтер і адміністратор BAS	Журнал реєстрації подій, історія змін, перелік повторно проведених документів за період

Ризик шахрайства	Права на створення і зміну довідника «Контрагенти» або «Договори» лише обмеженій групі, процедура погодження нового контрагента	Керівник і головний бухгалтер	Реєстр створених контрагентів, заявки і погодження, журнал змін довідника або скрін чи вивантаження документа
Дублювання документів (подвійне відображення операції)	Нумерація, контроль унікальності, регулярний перегляд оборотів і взаєморозрахунків, контроль повторень за реквізитами (номер, дата, сума)	Бухгалтер ділянки і головний бухгалтер	Реєстр документів із фільтрами, звіт по оборотах, акт внутрішньої перевірки дублів
Пропуск операцій (неповнота обліку)	Систематичний контроль непроведених документів, контроль розривів у ланцюгу замовлення → надходження або реалізація	Бухгалтер ділянки	Список непроведених документів, аналіз рахунку
Некоректне віднесення на рахунки (помилки класифікації)	Заблокувати ручні проводки для більшості операцій, стандартизувати рахунки обліку в номенклатурі і статтях витрат, контроль налаштувань рахунків	Головний бухгалтер	Налаштування рахунків обліку, ОСВ або аналіз рахунку з вибіркою підозрілих субрахунків
Помилки ПДВ чи податкового обліку через неправильні реквізити	Обов’язкові реквізити податкових документів, контроль заповнення рахунків, звірка реєстрів	Бухгалтер із розрахунків за податками	Реєстри ПДВ і податкової звітності, протоколи перевірок заповнення, звірка з первинними документами
Маніпуляції і помилки зі складом	Заборона від’ємних залишків, інвентаризація, контроль списань і переміщень, права на складські документи	Завідувач складом, бухгалтер складу	Інвентаризаційні відомості, звіти залишків, реєстр складських документів, акти списання чи переміщення
Неправильна собівартість, помилки закриття місяця і розподілу витрат	Регламент «закриття місяця» тільки після контрольних звірок, права на операції закриття періоду лише окремим особам	Головний бухгалтер	Протокол закриття місяця, звіти собівартості чи відхилень, фіксація виконання окремих операцій

Помилки чи зловживання в зарплаті (неправильні нарахування)	Обмежити доступ до кадрових довідників, погодження кадрових наказів, контроль змін окладів чи ставок	Головний бухгалтер, бухгалтер з нарахування оплати праці	Накази і розпорядження, реєстр змін по співробітниках
Втрата даних через збій, вірус і помилку користувача	Регулярне резервне копіювання і перевірка відновлення, контроль доступу до файлів копій	Головний бухгалтер і адміністратор BAS	Журнал резервних копій, акт тестового відновлення, політика зберігання повідомлень
Неконтрольовані оновлення чи доопрацювання	Процедура управління змінами, тестова база, погодження, фіксація версій, план впровадження	Головний бухгалтер і адміністратор BAS	Заявка на зміни, акт тестування, перелік версій чи оновлень, послідовність впровадження

Приклади проведення контролю у програмі «BAS Бухгалтерія» подано нижче.

Приклад 1. Перевірка проведення документів за певний період.

Мета. Виявити непроведені документи, які не відображені в обліку та звітності.

Період проведення. Щоденно або щотижнево, перед закриттям місяця.

Етапи здійснення контролю подано на рисунку 6.18.

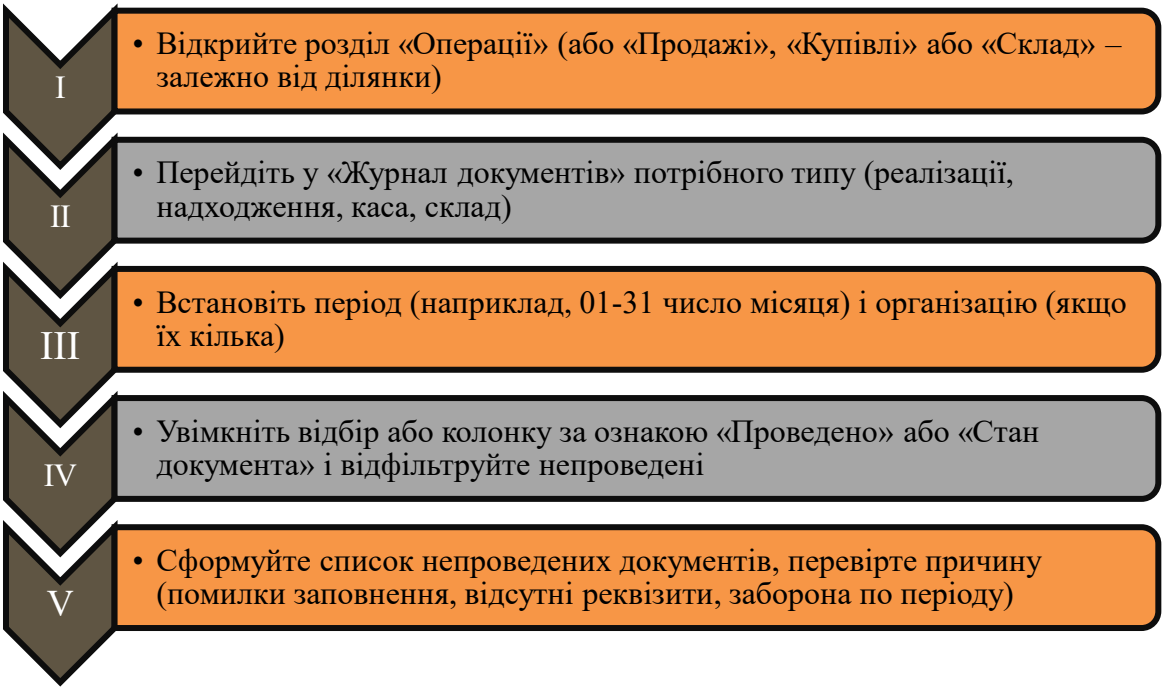


Рис. 6.18. Етапи здійснення контролю проведення операцій

За підсумками перевірки непроведених документів у «BAS Бухгалтерія» відповідальна особа повинна прийняти обґрунтоване рішення щодо кожного такого документа. Якщо документ не проведений через помилки заповнення або відсутність необхідних реквізитів, його спочатку виправляють, уточнюють контрагента, договір, номенклатуру, склад, рахунки, дату тощо, після чого проводять, щоб операція коректно потрапила в регістри та звітність. Якщо ж документ за своєю суттю не повинен проводитися, наприклад це чернетка, дубль, помилково створений запис або документ, який не підтверджено первинними підставами, тоді оформлюють службову примітку із зазначенням причини та відповідальної особи, щоб рішення було прозорим і відтворюваним у подальшому контролі.

Факт виконання перевірки має бути підтверджений документально. Як доказ зберігають скріншот або вивантаження переліку непроведених документів до проведення чи виправлення і після виконаних дій, а також складають короткий протокол перевірки, де фіксують дату, період, відповідального виконавця, кількість виявлених непроведених документів, прийняті рішення (проведено або не проводиться з обґрунтуванням) і підсумковий висновок. Такий підхід забезпечує контрольованість облікового процесу і створює належні підстави для внутрішнього контролю та аудиторської перевірки.

Приклад 2. Перевірка відповідності банківської виписки і облікових даних

Мета. Переконатися, що всі надходження і списання з банку відображені в BAS коректно.

Період проведення. Щоденно або при отриманні виписки.

Етапи здійснення контролю подано на рисунку 6.19.

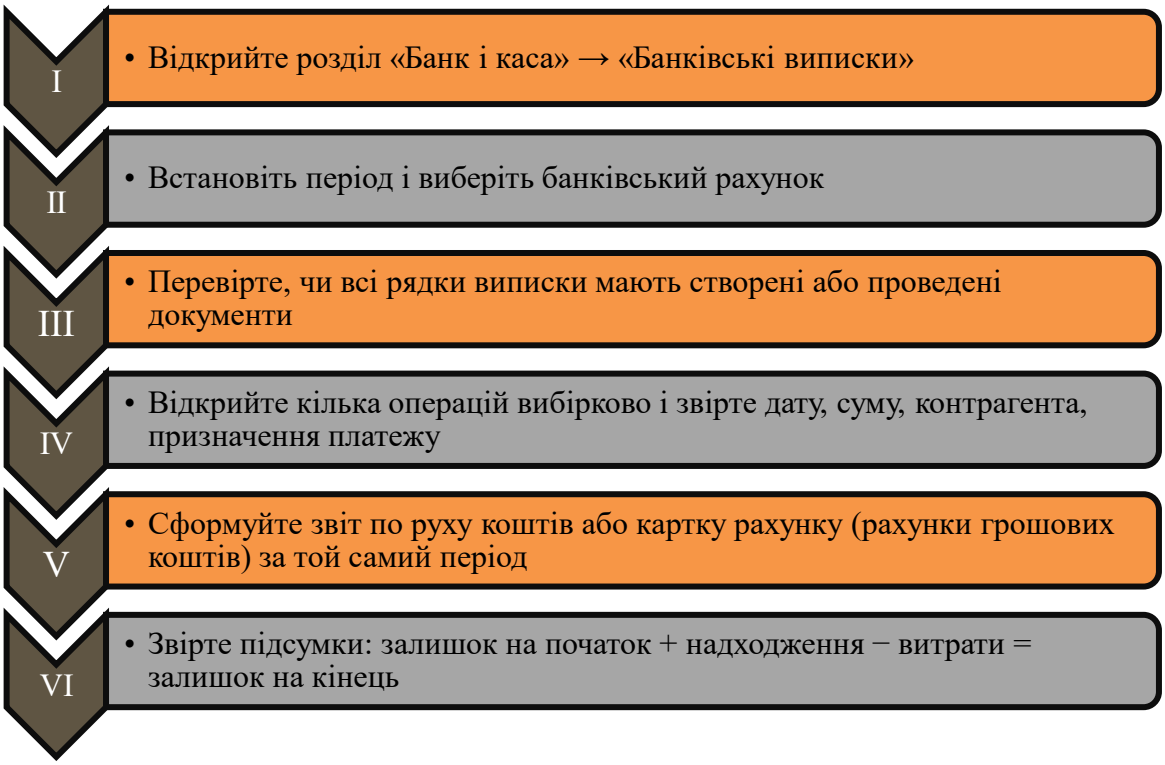


Рис. 6.19. Етапи здійснення контролю банківських операцій

Ця ситуація описує процедуру внутрішнього контролю, коли підприємство звіряє банківську виписку з даними в «BAS Бухгалтерія», щоб упевнитися, що всі надходження та списання коштів повністю і правильно відображені в обліку.

Приклад 3. Перевірка правильності відображення господарської операції.

Мета. Підтвердити, що конкретна господарська операція правильно потрапляє в регістри і звітність.

Період проведення. Щоденно або при отриманні виписки.

Етапи здійснення контролю подано на рисунку 6.20.

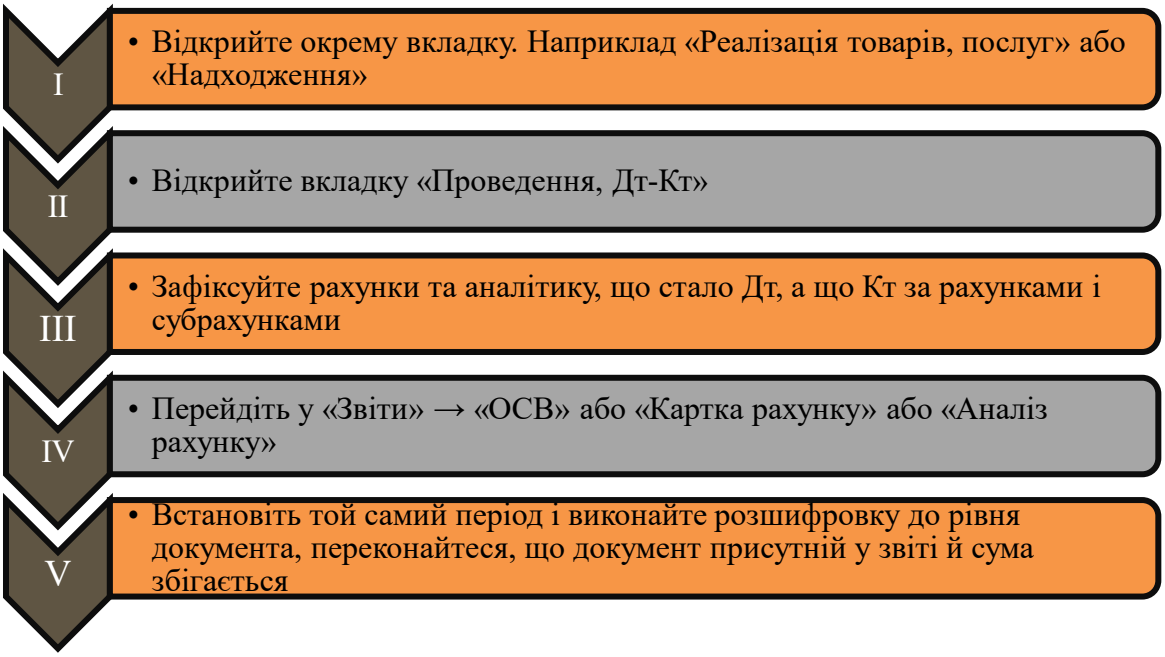


Рис. 6.20. Етапи здійснення контролю

Метою контролю є підтвердження, що введений первинний документ сформував коректні проведення, потрапив до відповідних регістрів і відобразився у звітності без помилок у сумі, даті, рахунках та аналітиці. Перевірка виконується систематично або за потреби при появі операції, яка має підвищений ризик помилок.

Приклад 4. Перевірка залишків на складах та недостач.

Мета. Виявити від'ємні залишки, помилки списання, неправильні переміщення.

Період проведення. Перед закриттям місяця, після інвентаризації.

Етапи здійснення контролю подано на рисунку 6.21.

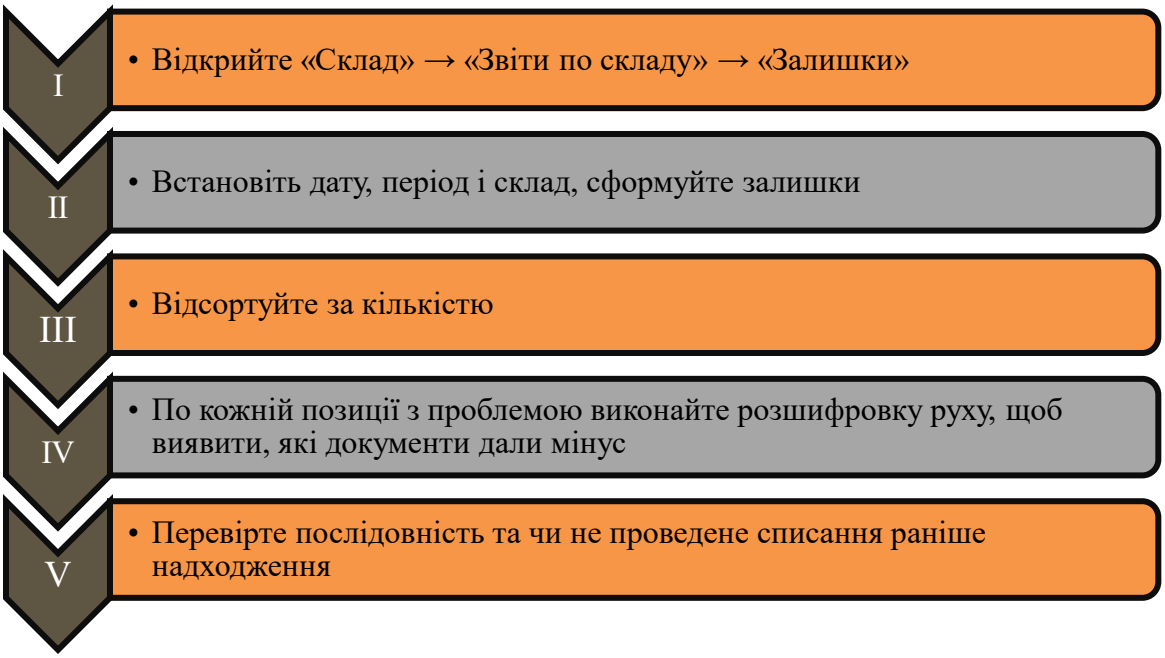


Рис. 6.21. Етапи здійснення контролю складських операцій

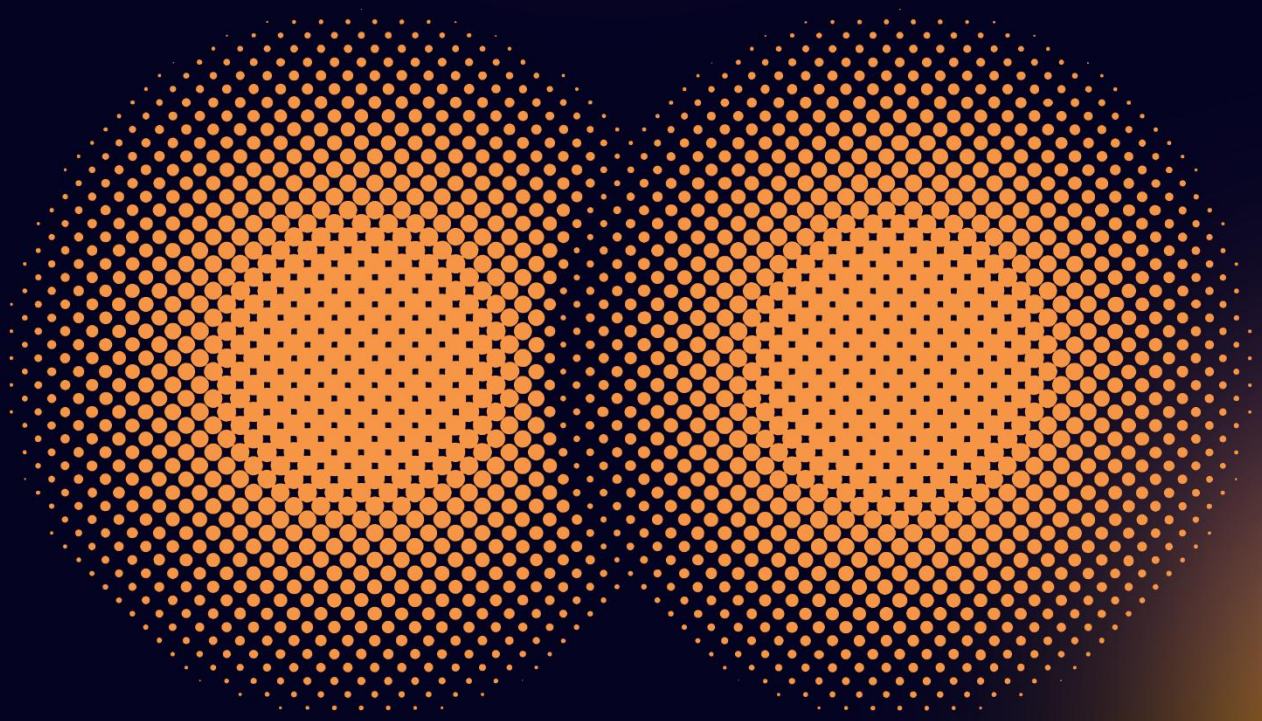
Ця ситуація описує процедуру внутрішнього контролю в «BAS Бухгалтерія», спрямовану на перевірку складських залишків і виявлення можливих недостач. Її мета – своєчасно знайти від'ємні залишки, помилки під час списання, а також неправильні переміщення товарно-матеріальних цінностей між складами, які можуть призводити до викривлення обліку запасів і собівартості. Перевірку проводять перед закриттям місяця та після інвентаризації, щоб підтвердити коректність даних у регістрах складу, узгодити фактичні залишки з обліковими та забезпечити достовірність звітності.

6.4. Контрольні питання для самоперевірки

1. Що таке інформаційна система підприємства і з яких основних компонентів вона складається?
2. Які ключові завдання виконує інформаційна система в управлінні підприємством?
3. У чому полягає принцип «одного джерела інформації» та чому він важливий для контролю і аудиту?
4. Яку роль відіграють бухгалтерські інформаційні системи у формуванні фінансової звітності?
5. Що означає ланцюг «первинний документ → проведення → регістри → звітність» у BAS?
6. Які види аудиторських доказів можна отримати із «BAS Бухгалтерія»?
7. Чому довідники, такі як контрагенти, номенклатура, статті витрат є важливими для якості обліку?
8. Які основні ризики виникають при некоректно налаштованих правах доступу в системі?
9. Для чого потрібний журнал реєстрації подій і які дії він має фіксувати?
10. Чому контроль змін і закриття періодів важливі для достовірності звітності?
11. Які контрольні процедури застосовують для виявлення непроведених документів?
12. Як виконують звірку банківської виписки з даними обліку та що саме перевіряють?

Розділ 7

Автори:
Оксана Коваль
Марія Шестерняк



ЦИФРОВІ ІНСТРУМЕНТИ АУДИТОРА ТА ФАХІВЦЯ З ФІНАНСОВОЇ БЕЗПЕКИ

РОЗДІЛ 7. ЦИФРОВІ ІНСТРУМЕНТИ АУДИТОРА ТА ФАХІВЦЯ З ФІНАНСОВОЇ БЕЗПЕКИ

«Технологія – це лише інструмент. Вона допомагає людям спілкуватися й робити свою роботу, але не замінює їх.»

Білл Ґейтс

7.1. Поняття та класифікація комп’ютеризованих засобів аудиту (CAATs)
7.2. Робота з табличними процесорами (Excel, Google Sheets) для аудиторських процедур
7.3. Базові можливості спеціалізованого ПЗ для аудиту (огляд інструментів)
7.4. Контрольні питання для самоперевірки

7.1. Поняття та класифікація комп’ютеризованих засобів аудиту (CAATs)

В умовах цифровізації економічних процесів та зростання обсягів оброблюваної інформації суттєво зростає роль інформаційних технологій у здійсненні аудиторської діяльності. Використання комп’ютеризованих засобів аудиту зумовлене необхідністю підвищення ефективності, точності та об’єктивності аудиторських процедур, а також адаптації аудиту до функціонування автоматизованих систем обліку й управління.

Практика показує, що інструменти аудиту набувають дедалі більшої значущості у професійній діяльності аудитора. Сучасні інформаційні середовища, прикладні програмні системи, транзакційні процеси та інші компоненти інформаційних систем характеризуються високим рівнем складності, що істотно ускладнює їх аналіз без застосування спеціалізованих засобів. У зв’язку з цим інструменти аудиту є необхідним елементом для всебічного розуміння принципів функціонування та контролю інформаційних систем. Під час планування кожної аудиторської перевірки аудитор повинен обґрунтовано визначити доцільність використання спеціальних інструментів, а також обрати їх оптимальний склад з урахуванням цілей та об’єкта перевірки.

При цьому аудитор зобов'язаний оцінити, чи здатний він охопити всі суттєві аспекти об'єкта аудиторської перевірки та виявити релевантні факти і ризики без застосування таких інструментів.

Інструменти аудиту в умовах цифрового середовища – це сукупність методів, прийомів, аудиторських процедур та комп'ютеризованих засобів аудиту (CAATs), що використовуються аудитором для автоматизованого збору, обробки та аналізу даних про фінансово-господарську діяльність суб'єкта господарювання. До таких інструментів належать електронні форми документальної та фактичної перевірки, цифрові методи тестування і аналітичних процедур, а також стандарти і спеціалізоване програмне забезпечення, призначене для оцінки відповідності, ефективності внутрішнього контролю та рівня аудиторських ризиків в інформаційному середовищі.

У науковій та професійній літературі комп'ютеризовані засоби аудиту зазвичай позначаються терміном Computer-Assisted Audit Tools and Techniques (CAATs)**.** У широкому розумінні CAATs являють собою сукупність програмних продуктів, технічних інструментів і методичних прийомів, що застосовуються аудитором з метою автоматизованого збору, обробки, аналізу та оцінки аудиторських доказів, отриманих з інформаційних систем суб'єкта господарювання.

Комп'ютеризовані засоби аудиту (Computer-Assisted Audit Tools and Techniques, CAATs) – це сукупність програмних, технічних та аналітичних інструментів і методичних прийомів, що використовуються аудитором для автоматизованого виконання аудиторських процедур з метою отримання, обробки та оцінки аудиторських доказів в електронному інформаційному середовищі.

З позицій методології аудиту комп'ютеризовані засоби аудиту розглядають як складову інструментарію аудиторської перевірки, яка забезпечує реалізацію аудиторських процедур в електронному середовищі та сприяє зниженню аудиторського ризику. Використання CAATs дає змогу аудитору аналізувати значні масиви даних, здійснювати суцільні перевірки, виявляти

викривлення та відхилення, а також підвищувати рівень професійного судження на основі об'єктивних цифрових доказів.

Використання комп'ютеризованих засобів аудиту та методик (CAATs) передбачає застосування аудитором спеціалізованих прикладних програмних засобів з метою автоматизації та підтримки процесів аудиту. Такі засоби забезпечують обробку, аналіз і відбір аудиторсько значущих даних, що зберігаються та обробляються в інформаційних системах, підвищуючи ефективність, точність і повноту аудиторських процедур.

Застосування комп'ютеризованих засобів аудиту та методик (CAATs) забезпечує належний рівень охоплення під час оцінювання заходів контролю прикладних програм, особливо в умовах обробки значних обсягів даних у межах тестового періоду, коли кількість транзакцій може сягати тисяч або мільйонів одиниць. За таких обставин отримання релевантної та придатної для аналізу інформації без використання автоматизованих інструментів є практично неможливим.

Завдяки здатності CAATs здійснювати аналіз великих масивів даних аудит, що проводиться з їх використанням, може передбачати суцільну перевірку транзакцій, що дає змогу виявляти аномалії та відхилення, зокрема дублювання операцій, а також перевіряти заздалегідь визначені контрольні параметри, такі як дотримання принципу розподілу обов'язків. За відсутності CAATs аналогічні процедури виконуються шляхом вибіркового тестування, що зумовлює підвищений рівень аудиторської невизначеності та ризику.

CAATs сприяють переорієнтації аудиторської діяльності з трудомістких ручних процедур на інтелектуальний аналіз даних, що підвищує обґрунтованість аудиторських висновків, рівень довіри користувачів аудиторської інформації та якість оцінювання аудиторських ризиків.

Основні причини застосування CAATs у процесі аудиту полягають у такому:

- *відсутність первинних документів або обмежена наявність інформації у паперовому вигляді, що зумовлює необхідність використання CAATs під час виконання процедур дотримання та процедур перевірки по суті;*
- *потреба в отриманні достатніх, належних і релевантних аудиторських доказів безпосередньо з прикладних систем і баз даних відповідно до цілей аудиту;*
- *забезпечення підтвердження аудиторських висновків шляхом системного аналізу та інтерпретації електронних доказів;*
- *необхідність доступу до інформації з інформаційних систем, що функціонують у різних апаратних і програмних середовищах, мають відмінну структуру даних, формати записів і логіку обробки, з можливістю їх уніфікації у загальноприйнятому форматі;*
- *підвищення якості аудиту та забезпечення відповідності вимогам міжнародних і національних стандартів аудиторської діяльності;*
- *визначення рівня суттєвості, аудиторського ризику та значущості контрольних процедур в IT-середовищі;*
- *підвищення ефективності та результативності аудиторського процесу;*
- *удосконалення планування аудиту та раціонального управління аудиторськими ресурсами.*

З огляду на різноманітність функціонального призначення та способів застосування комп'ютеризованих засобів аудиту, важливого значення набуває класифікація. ***Класифікація CAATs*** дозволяє систематизувати наявні інструменти, визначити напрями їх використання на різних етапах аудиторської перевірки та забезпечити методичну узгодженість між цілями аудиту й відповідними інформаційними технологіями.

У науковій практиці комп'ютеризовані засоби аудиту класифікують за низкою ознак (табл. 7.1), зокрема:

- *за функціональним призначенням*;
- *за рівнем інтеграції з обліковими системами клієнта;*

- *за ступенем автоматизації аудиторських процедур;*
- *за етапами аудиторського процесу;*
- *за характером оброблюваних даних;*
- *за типом програмного забезпечення*.

Такий підхід забезпечує комплексне розуміння ролі CAATs у сучасному аудиті та створює підґрунтя для їх ефективного впровадження в практику аудиторської діяльності.

Таблиця 7.1

Класифікація комп'ютеризованих засобів аудиту (CAATs)

Класифікаційна ознака	**Види CAATs**	**Характеристика**	**Приклади застосування**
За функціональним призначенням	Засоби аналізу даних	Забезпечують обробку, сортування, агрегацію та аналітичне дослідження великих масивів облікових даних	Аналіз журналів операцій, виявлення нетипових транзакцій, тестування повноти даних
	Засоби тестування контролів	Призначені для перевірки ефективності автоматизованих засобів внутрішнього контролю	Перевірка логічних контролів доступу, тестування автоматичних обмежень
	Засоби вибірки	Дозволяють формувати статистичні та нестатистичні аудиторські вибірки	Генерація вибірки для перевірки дебіторської заборгованості
	Засоби документування аудиту	Забезпечують автоматизоване оформлення та зберігання робочих документів аудитора	Формування електронних робочих файлів
За рівнем інтеграції з обліковими системами клієнта	Вбудовані CAATs	Інтегруються безпосередньо в облікову або управлінську систему підприємства	Вбудовані аудиторські модулі в ERP-системах
	Автономні CAATs	Функціонують незалежно від інформаційної системи клієнта	Аналіз даних після експорту з бухгалтерської програми
За ступенем автоматизації аудиторських процедур	Частково автоматизовані	Передбачають активну участь аудитора в обробці результатів	Використання е-таблиць для аналітичних процедур

	Повністю автоматизовані	Забезпечують автоматичне виконання аудиторських процедур за заданими алгоритмами	Безперервний аудит, автоматичне виявлення аномалій
За етапами аудиторського процесу	CAATs планування	Використовуються на етапі планування аудиту	Оцінка ризиків, попередній аналіз фінансової інформації
	CAATs виконання	Застосовуються під час проведення аудиторських процедур	Тестування операцій, аналіз первинних документів
	CAATs завершення	Забезпечують узагальнення результатів аудиту	Формування аналітичних звітів та висновків
За характером оброблюваних даних	Засоби роботи з структурованими даними	Обробляють формалізовані облікові дані	Дані бухгалтерських регістрів
	Засоби роботи з неструктурованими даними	Аналізують текстову, графічну та мультимедійну інформацію	Аналіз договорів, електронного листування
За типом програмного забезпечення	Універсальні програмні засоби	Програмне забезпечення загального призначення	Електронні таблиці, система управління базами даних (СУБД)
	Спеціалізовані аудиторські програми	Орієнтовані безпосередньо на потреби аудиту	Професійні аудиторські програмні продукти

Як показує таблиця 7.1, класифікація комп'ютеризованих засобів аудиту виконує системоутворюючу функцію в аудиторській діяльності, забезпечуючи впорядкування різноманітних інструментів CAATs та формуючи методичні передумови для їх цілеспрямованого й раціонального використання в процесі аудиторської перевірки. Різноманітність функціонального призначення, технічних характеристик і способів застосування комп'ютеризованих засобів аудиту зумовлює необхідність їх комплексного групування за сукупністю класифікаційних ознак, які відображають специфіку використання інформаційних технологій на окремих етапах аудиторського процесу та забезпечують методичну узгодженість між цілями аудиту, характером аудиторських процедур і відповідними цифровими інструментами. Окрім того, дані таблиці 7.1 зазначають, що значну роль у практичній діяльності аудитора

відіграють універсальні програмні засоби загального призначення, які характеризуються доступністю, гнучкістю та широкими аналітичними можливостями. Серед таких засобів особливе місце займають табличні процесори, що широко використовуються аудиторами та фахівцями з фінансової безпеки для виконання аналітичних процедур, формування аудиторських вибірок, виявлення відхилень і документування результатів перевірки.

На основі цих спостережень та практичного досвіду застосування CAATs розглянемо більш детальну класифікацію інструментів і методик за їх ключовими функціональними можливостями. Такий підхід дозволяє системно оцінити, яким чином окремі засоби підтримують доступ до даних, аналіз інформації, автоматизацію процедур та документування результатів, забезпечуючи при цьому ефективність і повноту аудиту.

Ключові функціональні можливості комп'ютеризованих засобів аудиту та методик (CAATs) класифікують за такими основними категоріями:

1. ***Доступ до файлів і даних:***

➢ *дана категорія охоплює здатність CAATs здійснювати зчитування та обробку різних форматів записів і структур файлів*.

Йдеться про роботу з поширеними форматами даних, зокрема базами даних, текстовими файлами, електронними таблицями (наприклад, Excel) та іншими структурованими й напівструктурованими джерелами. Як правило, доступ до даних реалізується за допомогою функцій імпорту та стандартних інтерфейсів взаємодії, таких як ODBC.

ODBC (Open Database Connectivity) – це відкритий програмний інтерфейс, що використовується у комп'ютеризованих засобах аудиту для підключення таких інструментів, як Excel, Power BI та інші аналітичні застосунки, до бухгалтерських і фінансових баз даних з метою автоматизованого отримання, аналізу та візуалізації аудиторських даних.

2. ***Реорганізація та інтеграція файлів:***

➢ *ця категорія включає функції індексації, сортування, агрегування, злиття та зв'язування даних з іншими ідентифікованими файлами або джерелами інформації.*

Використання зазначених функцій дає змогу аудитору оперативно аналізувати дані з різних аналітичних позицій та формувати багатовимірне уявлення про досліджувані процеси.

3. ***Відбір і фільтрація даних*:**

➢ *функції відбору даних передбачають застосування умовних та логічних критеріїв, у тому числі глобальних фільтрів, для вибору релевантної інформації відповідно до визначених параметрів аудиту.*

Це забезпечує зосередження аудиторських процедур на суттєвих елементах досліджуваної сукупності.

4. ***Статистичні функції*:**

➢ *до цієї групи належать інструменти статистичного аналізу, зокрема вибіркове тестування, стратифікація даних, частотний аналіз та інші методи кількісної оцінки.*

Застосування статистичних функцій сприяє підвищенню обґрунтованості аудиторських висновків і зниженню рівня аудиторського ризику.

5. ***Арифметичні та обчислювальні функції:***

➢ *зазначені функції передбачають використання арифметичних операторів для виконання повторних обчислень, перерахунків і перевірки коректності результатів обробки даних.*

Вони забезпечують можливість відтворення розрахунків та повторного виконання процедур з метою підтвердження отриманих результатів.

Класифікація функціональних можливостей CAATs дозволяє аудитору ефективно працювати з різнорідними джерелами даних, здійснювати їх інтеграцію, відбір, статистичний та арифметичний аналіз, що підвищує обґрунтованість аудиторських висновків і сприяє зниженню аудиторського ризику в умовах цифрового середовища.

Ураховуючи ключову роль комп'ютеризованих засобів аудиту (CAATs) у підвищенні точності, об'єктивності та ефективності аудиторських процедур, особливого значення набуває дотримання методологічних принципів та запобіжних заходів їх застосування. CAATs надають аудиторам значні переваги, забезпечуючи можливість виконання широкого спектра аналітичних та контрольних процедур, автоматизацію обробки даних і оперативне виявлення відхилень. Водночас їх застосування потребує дотримання відповідних запобіжних заходів для забезпечення достовірності, точності та повноти аудиторського аналізу.

До основних запобіжних заходів при застосуванні комп'ютеризованих засобів аудиту належать:

- *чітке визначення даних, необхідних для проведення аудиту;*
- *збір правильних та актуальних файлів даних з відповідних джерел;*
- *ідентифікація всіх суттєвих полів, до яких необхідно отримати доступ із системи;*
- *попереднє визначення формату даних та належне налаштування полів для завантаження;*
- *перевірка того, що дані повно і адекватно відображають предмет аудиту;*
- *забезпечення актуальності та повноти аналізу даних;*
- *проведення необхідного тестування для підтвердження коректності обробки та результатів;*
- *використання інформації, отриманої за допомогою CAATs, лише як індикатора можливих ризиків або відхилень, що потребують подальшої перевірки.*

Міжнародні професійні організації підкреслюють важливість дотримання цих заходів. Так, ICAI у своєму посібнику з CAATs наголошує на стандартах гарантії достовірності аудиту, а ISACA розробила відповідні стандарти та керівництва щодо використання CAATs в аудиторських процедурах. Дотримання цих рекомендацій дозволяє підвищити ефективність аудиторських

перевірок, мінімізувати ризики помилок і забезпечити надійність результатів аналізу в цифровому середовищі.

ICAI (Institute of Chartered Accountants of India) – це національна професійна організація Індії, створена у 1949 році, що здійснює регулювання бухгалтерської та аудиторської діяльності, встановлює професійні стандарти та забезпечує підготовку і сертифікацію фахівців у сфері обліку й аудиту.

У міру розширення використання інформаційних систем суб'єктами господарювання для ведення обліку, здійснення транзакцій та обробки даних зростає потреба в застосуванні аудиторами спеціалізованих інструментів для належної оцінки ризиків. Використання комп'ютеризованих засобів аудиту (CAATs) є невід'ємною складовою сучасного аудиту, оскільки сприяє збільшенню його охоплення, забезпечує більш глибокий і послідовний аналіз даних та зменшує аудиторський ризик.

ISACA (Information Systems Audit and Control Association) – це міжнародна професійна асоціація, заснована у 1969 році, яка об'єднує фахівців у сфері аудиту інформаційних систем, управління інформаційними технологіями, контролю, інформаційної безпеки, кібербезпеки та цифрової довіри. Діяльність ISACA спрямована на розроблення та поширення міжнародно визнаних стандартів і методологій (наприклад, COBIT), а також на сертифікацію авторитетних кваліфікаційних сертифікатів (зокрема, CISA, CISM, CRISC та інші).

Комп'ютеризовані засоби аудиту (CAATs) охоплюють широкий спектр інструментів і методів, які застосовуються аудиторами в практичній діяльності. До них належать універсальне аудиторське програмне забезпечення, індивідуально розроблені запити та сценарії обробки даних, службові утиліти, засоби відстеження й візуалізації програмного коду, а також експертні аудиторські системи.

У практиці аудиту CAATs використовуються під час виконання різних аудиторських процедур, зокрема:

- *для перевірки окремих транзакцій;*

- *проведення аналітичних процедур;*
- *оцінки відповідності засобів контролю інформаційних систем;*
- *тестування контролів на рівні прикладних програм.*

Застосування CAATs дає змогу аудитору отримати значну частину аудиторських доказів безпосередньо з електронних даних підприємства, підвищуючи ефективність і надійність перевірки. У зв'язку з цим аудитор повинен заздалегідь планувати використання таких інструментів, визначати їх доцільність для конкретних процедур і дотримуватися принципу належної професійної обережності під час роботи з ними.

З огляду на різноманітність комп'ютеризованих засобів аудиту, особливу практичну цінність для аудиторів становлять універсальні програмні інструменти загального призначення, які поєднують доступність, гнучкість і достатній функціональний потенціал для виконання широкого кола аудиторських завдань. У реальній практиці саме такі засоби найчастіше використовуються на початкових етапах впровадження CAATs, а також у поєднанні зі спеціалізованим аудиторським програмним забезпеченням, виконуючи допоміжну або аналітичну функцію. Серед них провідне місце посідають табличні процесори, які завдяки розвиненим можливостям обробки, аналізу та візуалізації даних стали невід'ємним інструментом сучасного аудиту.

У цьому контексті ***табличні процесори Microsoft Excel та Google Sheets*** розглядаються як базові комп'ютеризовані засоби аудиту, що належать до категорії частково автоматизованих CAATs і можуть застосовуватися на різних етапах аудиторського процесу – від планування до узагальнення результатів аудиту.

7.2. Робота з табличними процесорами (Excel, Google Sheets) для аудиторських процедур

У практиці аудиторської діяльності та забезпечення фінансової безпеки значне місце посідають універсальні програмні засоби обробки даних, які поєднують доступність використання з широкими аналітичними можливостями. Табличні процесори Microsoft Excel та Google Sheets належать до найбільш поширених інструментів, що застосовуються аудиторами для аналізу облікової інформації, виконання аналітичних процедур, формування аудиторських вибірок і документування результатів перевірки.

Табличний процесор – це програмний інструмент для створення, обробки, аналізу та візуалізації структурованих даних у вигляді таблиць.

У практиці аудиторської діяльності та забезпечення фінансової безпеки табличні процесори (зокрема Microsoft Excel і Google Sheets) відіграють вирішальну роль, оскільки дозволяють аудиторам:

- *ефективно працювати з великими масивами даних із бухгалтерських і управлінських систем;*
- *виконувати сортування, фільтрацію, групування та узагальнення інформації;*
- *обчислювати аналітичні показники та виявляти відхилення і нетипові операції;*
- *формувати аудиторські вибірки та документувати результати перевірки.*

Отже, застосування табличних процесорів в аудиторській діяльності є обґрунтованою відповіддю на зростання обсягів і складності обліково-аналітичних даних у сучасних інформаційних системах підприємств. Використання Microsoft Excel та Google Sheets забезпечує аудитору інструментальну основу для систематизації, аналітичної обробки й інтерпретації структурованих даних, що, у свою чергу, сприяє своєчасному виявленню нетипових операцій, суттєвих відхилень і потенційних фінансових ризиків. Це

підвищує обґрунтованість аудиторських суджень, ефективність процедур перевірки та рівень довіри до сформованих аудиторських висновків.

Табличні процесори позиціонуються як ***частково автоматизовані комп'ютеризовані засоби аудиту (CAATs),*** оскільки вони не замінюють професійне судження аудитора, а виконують функцію інструментальної підтримки прийняття рішень шляхом автоматизованої обробки, структурування та аналізу обліково-фінансової інформації. Водночас використання таких інструментів значно підвищує ефективність аудиторських процедур, сприяє зниженню аудиторського ризику та забезпечує прозорість і відтворюваність результатів перевірки.

У межах цього підпункту розкриємо основні напрями та інструментальні можливості використання табличних процесорів Microsoft Excel і Google Sheets для виконання типових аудиторських процедур, зокрема аналітичних перевірок, формування аудиторських вибірок, аналізу динаміки та структури фінансово-економічних показників, а також виявлення аномалій і потенційних загроз фінансовій безпеці суб'єкта господарювання.

В умовах цифровізації аудиторської діяльності табличні процесори посідають важливе місце в системі комп'ютеризованих засобів аудиту, оскільки поєднують універсальність застосування, доступність використання та значні аналітичні можливості. Програмні продукти Microsoft Excel та Google Sheets широко використовуються аудиторами та фахівцями з фінансової безпеки як інструменти первинного опрацювання облікових даних, виконання аналітичних процедур, формування аудиторських вибірок і систематизованого документування результатів аудиторської перевірки.

З позицій класифікації комп'ютеризованих засобів аудиту табличні процесори відносять до універсальних програмних засобів загального призначення, які можуть застосовуватися на різних етапах аудиторського процесу – від планування аудиту та виконання аналітичних процедур до узагальнення та оформлення його результатів.

Функціональні можливості табличних процесорів дозволяють аудитору працювати зі значними масивами структурованих даних, отриманих з бухгалтерських, фінансових і управлінських інформаційних систем суб'єкта господарювання. Використовуючи вбудовані інструменти сортування, фільтрації, агрегації та візуалізації даних, аудитор може оперативно виявляти тенденції, відхилення та нетипові операції, що мають потенційний вплив на достовірність фінансової звітності та рівень фінансових ризиків.

Вагомою перевагою табличних процесорів є їх висока гнучкість у налаштуванні аудиторських процедур з урахуванням специфіки діяльності суб'єкта господарювання (клієнта) та цілей аудиторської перевірки. Microsoft Excel і Google Sheets можуть ефективно використовуватися для реалізації як стандартних аудиторських процедур, передбачених міжнародними стандартами аудиту, так і для розроблення індивідуальних (авторських) методик аналізу, орієнтованих на виявлення ознак шахрайства, порушень фінансової дисципліни, а також потенційних загроз фінансовій безпеці.

Водночас застосування табличних процесорів у процесі аудиту потребує дотримання належного рівня методичної та професійної дисципліни, зокрема щодо перевірки повноти й коректності вхідних даних, контролю правильності використання формул, логіки алгоритмів розрахунків, а також забезпечення цілісності та конфіденційності інформації. У зв'язку з цим табличні процесори доцільно розглядати як базовий рівень комп'ютеризованих засобів аудиту, який ефективно доповнює спеціалізоване аудиторське програмне забезпечення та формує методичне підґрунтя для впровадження більш складних цифрових інструментів і аналітичних технологій в аудиторській діяльності.

Ефективність використання табличних процесорів у аудиторській діяльності значною мірою залежить від якості підготовки вихідних даних, що підлягають аналізу. Облікова та управлінська інформація, отримана з інформаційних систем суб'єкта господарювання, перед завантаженням і опрацюванням у середовищі Microsoft Excel або Google Sheets потребує попередньої перевірки, структуризації та адаптації відповідно до цілей і завдань

аудиторської перевірки. Належна організація та підготовка даних створює передумови для отримання достовірних результатів аналітичних процедур, підвищує обґрунтованість аудиторських висновків і сприяє зниженню аудиторського ризику.

На практиці аудитор найчастіше працює з даними, експортованими з бухгалтерських та управлінських інформаційних систем у поширених електронних форматах, ***зокрема CSV, XLSX, TXT або XML.*** На етапі імпорту таких даних у табличний процесор особливу увагу слід приділяти коректності відображення числових, текстових і датованих показників, правильності розподілу даних за стовпцями, а також відповідності кодування символів. Помилки, допущені на цьому етапі, можуть призвести до викривлення результатів подальшого аналізу.

Після імпорту даних аудитор переходить до їх первинної підготовки, яка включає комплексну перевірку повноти та цілісності інформації, виявлення дублікатів записів, а також некоректних або пропущених значень у ключових реквізитах. До важливих етапів підготовки належить уніфікація структури таблиці: приведення назв полів до зрозумілого та однозначного вигляду, забезпечення однорідності форматів числових показників і дат, а також виділення окремих колонок для аналітично значущих ознак (наприклад, дата операції, сума, контрагент, рахунок обліку). Такий системний підхід до підготовки даних створює основу для достовірного аналізу та знижує ризик помилкових висновків на наступних етапах аудиторської перевірки.

Після підготовки даних аудитор переходить до їх первинного аналізу з використанням базових функцій табличних процесорів, таких як сортування, фільтрація та умовне форматування.

1. Сортування. Дозволяє впорядкувати дані за критеріями, що мають аналітичне значення, наприклад за датою операції, сумою або контрагентом, що полегшує виявлення нетипових або великих транзакцій.

2. Фільтрація. Забезпечує оперативне відсіювання непотрібної інформації та фокусування на релевантних записах, відповідно до поставлених цілей аудиту.

3. Умовне форматування. Дозволяє автоматично виділяти аномалії, відхилення та ризикові показники за допомогою кольорових маркерів, індикаторів або графічних підказок, що підвищує швидкість виявлення потенційних проблемних операцій та сприяє своєчасному прийняттю аудиторських рішень.

Використання цих інструментів на ранніх етапах аналізу створює основу для глибшого статистичного та аналітичного опрацювання даних і підвищує точність подальших аудиторських висновків.

Підготовка даних для аудиторського аналізу здійснюється з урахуванням цілей конкретних аудиторських процедур. Наприклад, для аналізу динаміки показників потрібно забезпечити наявність коректного часового виміру, тоді як для формування вибірки або виявлення нетипових операцій важливим є виділення сумових показників та ідентифікаторів операцій. Таким чином, підготовка даних є не технічною, а аналітичною процедурою, що потребує професійного судження аудитора.

Правильна підготовка та первинний аналіз даних у табличних процесорах є ***визначальним етапом аудиторської перевірки***, який забезпечує достовірність подальшої аналітичної обробки та підвищує обґрунтованість аудиторських висновків. На практиці це означає, що аудитор повинен не лише імпортувати та структурувати дані, а й застосовувати базові інструменти сортування, фільтрації та умовного форматування для швидкого виявлення аномалій, відхилень і потенційно ризикових операцій. Нижче наведено приклад застосування цих принципів у середовищі Microsoft Excel.

Приклад. Аудитор отримав з облікової системи підприємства файл у форматі CSV, що містить журнал господарських операцій за звітний період із такими полями: *Дата операції, Номер документа, Контрагент, Рахунок дебету, Рахунок кредиту, Сума операції*.

Етап 1. Імпорт даних. За допомогою стандартних інструментів Excel здійснюється відкриття CSV-файлу з перевіркою правильності розмежування

полів і форматів даних. Особлива увага приділяється коректному розпізнаванню дат і числових значень сум операцій.

Етап 2. Первинна перевірка даних. Аудитор використовує сортування та фільтрацію для виявлення: 1) порожніх значень у полі *«Сума операції»*; 2) повторюваних номерів документів; 3) операцій з нульовими або від'ємними сумами.

Етап 3. Структурування даних. Для подальшого аналізу додається допоміжний стовпець *«Місяць операції»*, який формується на основі дати. Це дозволяє здійснювати подальший аналіз динаміки оборотів за періодами та виконувати групування даних за аналітично значущими показниками.

Результат. У результаті підготовки формується аналітично придатний масив даних, який може бути використаний для виконання аналітичних процедур, формування аудиторської вибірки або виявлення нетипових операцій. Використання базових інструментів Excel, таких як сортування, фільтрація та умовне форматування, дозволяє аудитору швидко виявляти відхилення, аномалії та потенційні ризики, що підвищує ефективність перевірки та обґрунтованість аудиторських висновків.

Після імпорту, первинної перевірки та структурування аудитор отримує масив, готовий до аналітичної обробки. На цьому етапі важливо не лише перевірити коректність даних, а й виявити потенційно проблемні записи, такі як дублікати, від'ємні суми або ризикові операції. Для наочності наведено приклад масиву облікових даних після імпорту, що потребує додаткової аудиторської перевірки:

Таблиця 7.2

Приклад структури облікових даних після імпорту в табличний процесор

Дата операції	№ документа	Контрагент	Рахунок Дт	Рахунок Кт	Сума операції, грн
05.01.2025	ПН-00125	ТОВ «Альфа»	361	701	125 000,00
12.01.2025	ПН-00126	ТОВ «Бета»	311	361	98 500,00
12.01.2025	ПН-00126	ТОВ «Бета»	311	361	98 500,00
28.01.2025	ПН-00140	ФОП Шевчук	685	311	–5 000,00

Цей приклад ілюструє, як після імпорту даних можна швидко виявити записи, які потребують додаткового контролю: дублікати документів (рядки 2 і 3) та від'ємні значення сум (рядок 4). Така наочна демонстрація полегшує аудитору ідентифікацію викривлень і планування подальших аналітичних процедур.

Таблиця 7.2 показує, що навіть після імпорту та базової перевірки залишаються записи, які потребують додаткової уваги. Це підкреслює, що підготовка даних є не лише технічною, а й аналітичною процедурою, спрямованою на виявлення помилок і викривлень, здатних вплинути на достовірність фінансової звітності.

Типові помилки в облікових даних, їх аудиторське значення, можливі викривлення у структурованих масивах і ризики, відображено в таблиці 7.3.

Таблиця 7.3

Типові помилки в облікових даних та їх аудиторське значення

Вид проблеми	Опис	Потенційний аудиторський ризик
Дублювання записів	Повторення одного номера документа	Завищення доходів або витрат
Пропущені значення	Відсутня сума або дата операції	Неповнота облікових даних
Невірний формат	Текстовий формат сум	Помилки в розрахунках
Від'ємні суми	Нетипові значення	Ознаки коригувальних або фіктивних операцій

Дані таблиці 7.3 підкреслюють, що навіть на етапі підготовки даних аудитору необхідно застосовувати професійне судження та методичні прийоми для виявлення і виправлення потенційно ризикових записів. Отже, підготовка даних у табличному процесорі є невід'ємною частиною аудиторської процедури, що забезпечує достовірність і надійність подальшого аналізу.

Для наочності та кращого розуміння процесу підготовки облікових даних до аудиторського аналізу доцільно представити його у вигляді послідовного алгоритму. Візуалізація логіки підготовки даних у табличному процесорі, що включає імпорт, перевірку, структурування та первинний аналіз, допомагає аудитору систематизувати свої дії та забезпечує уніфікований підхід до обробки інформації. Візуальне відображення цих етапів представлено на рисунку 7.1.

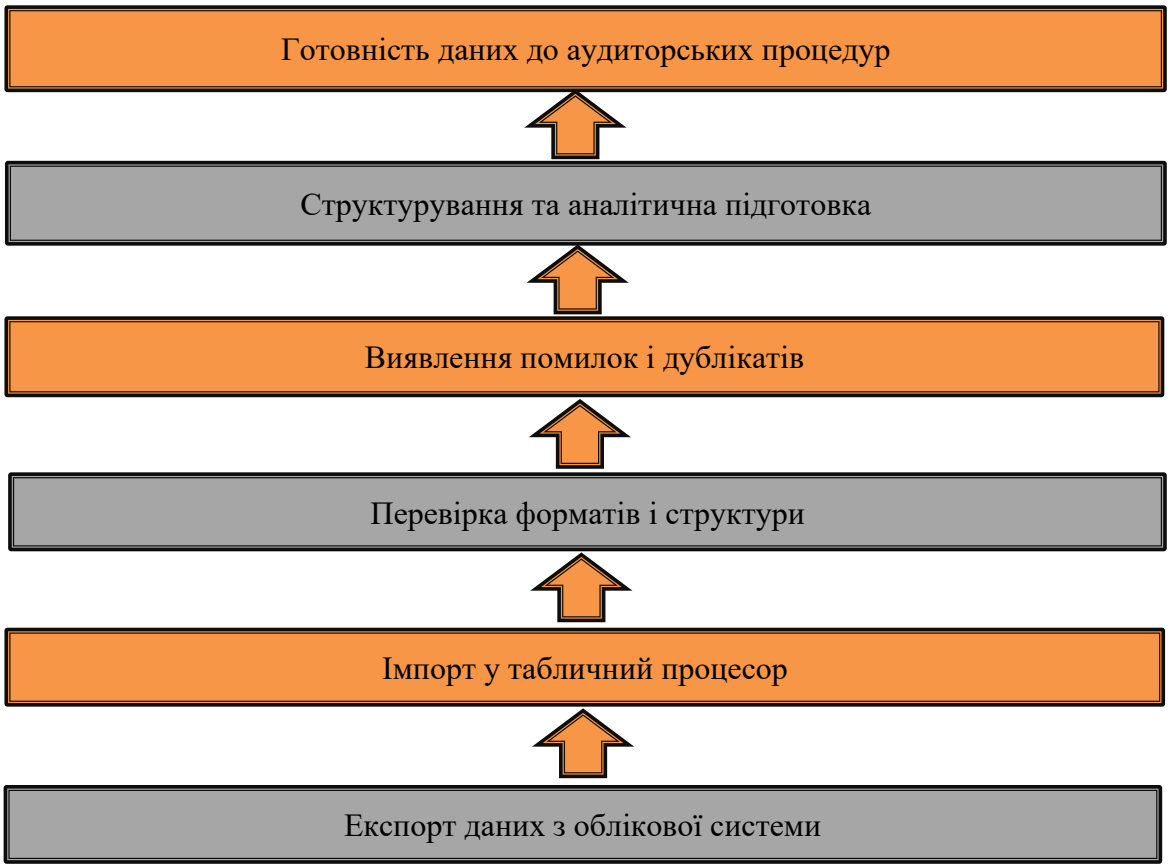


Рис. 7.1. Алгоритм підготовки облікових даних до аудиторського аналізу в Excel

Після ознайомлення з алгоритмом підготовки облікових даних, представленим на рисунку 7.1, аудитор отримує можливість перейти до виконання аналітичних процедур. Візуалізація послідовних етапів підготовки демонструє, як первинний масив даних трансформується в аналітично придатну форму, що дозволяє ефективно оцінювати тенденції фінансово-економічних показників, виявляти нетипові операції та ідентифікувати потенційні ризики.

Застосування аналітичних процедур у табличному процесорі включає:

1. ***Побудову динамічних зведень і групувань*** – систематизація інформації за періодами, контрагентами, рахунками або іншими критеріями для оцінки тенденцій оборотів, доходів і витрат.

2. ***Розрахунок ключових аналітичних показників*** – середніх величин, темпів росту, частки окремих статей у загальному обсязі, коефіцієнтів ризику тощо.

3. Виявлення нетипових та ризикових операцій – за допомогою умовного форматування, спеціальних формул або фільтрів виділяються транзакції з сумами, що перевищують задані пороги, від'ємні значення, дублікати або аномальні дати.

4. Формування аудиторських вибірок – відбір операцій для детальної перевірки на основі результатів первинного аналізу, що дозволяє сконцентрувати увагу на найбільш ризикових ділянках та підвищує ефективність аудиту.

Таким чином, правильно підготовлені дані стають основою для комплексного аналітичного опрацювання, яке забезпечує систематичний та обґрунтований підхід до аудиторської перевірки. Плавний перехід від підготовки до аналізу дозволяє поєднати методичну дисципліну та професійне судження аудитора, а також гарантує відтворюваність і прозорість процедур.

Наступним кроком після первинного аналізу та виявлення типових помилок є ***доповнення масиву даних аналітичними полями***, що дозволяє аудитору відображати додаткові ознаки ризику та формувати показники, необхідні для подальших аналітичних процедур. Такий підхід забезпечує більш глибоку оцінку фінансово-економічних процесів і підвищує ефективність виявлення нетипових операцій.

Таблиця 7.4 ілюструє, як аудитор може додавати нові аналітичні колонки до первинного масиву даних, наприклад «Місяць операції» або «Ознака ризику», на основі попередньої перевірки та умовного форматування:

Таблиця 7.4

Приклад аналітичного доповнення облікових даних

Дата операції	Сума, грн	Місяць операції	Ознака ризику
05.01.2025	125 000	Січень	Ні
12.01.2025	98 500	Січень	Дублікат
28.01.2025	–5 000	Січень	Так

Додавання таких аналітичних полів є важливою процедурою, оскільки дозволяє систематизувати потенційно проблемні записи і створює основу для подальшого детального аналізу.

Для наочності послідовність підготовки та аналітичного доповнення даних представлено у вигляді алгоритму аудиторських процедур на рисунку 7.2.

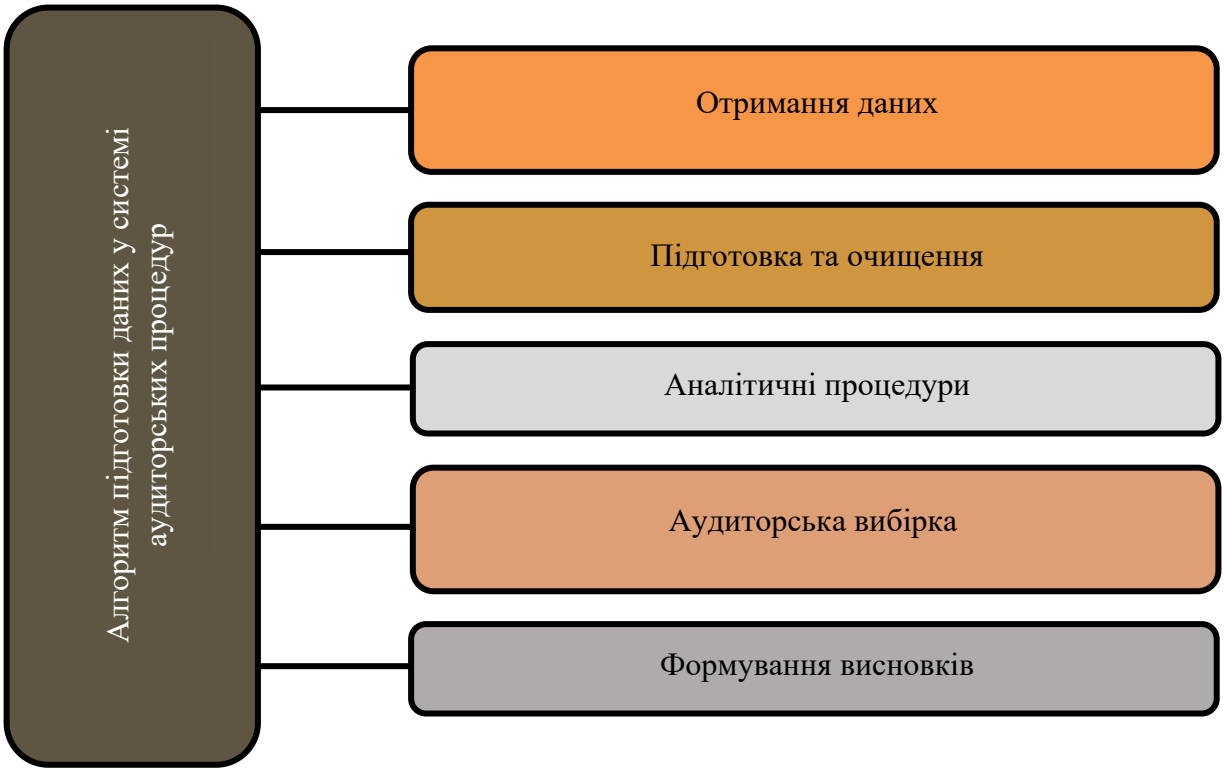


Рис. 7.2. Алгоритм підготовки даних у системі аудиторських процедур

Даний процес включає додавання допоміжних колонок (наприклад, «Місяць операції» або «Ознака ризику»), маркування потенційно проблемних записів, таких як дублікати або від'ємні суми, а також структурування даних за ключовими ознаками для подальшого аналізу та формування аудиторських вибірок. Такий системний підхід дозволяє аудитору швидко і послідовно ідентифікувати ризикові ділянки, оптимізувати роботу з даними та підвищити ефективність наступних аналітичних процедур.

Хоча Microsoft Excel є традиційним інструментом для аудиторів, Google Sheets останніми роками набув значної популярності завдяки своїй доступності та можливостям спільної роботи. Функціонально Google Sheets дозволяє виконувати ті ж базові аудиторські процедури, що і Excel: імпорт даних,

сортування, фільтрацію, умовне форматування, обчислення аналітичних показників, формування зведених таблиць та побудову графіків. Основна відмінність полягає у хмарній архітектурі, що забезпечує одночасну роботу кількох користувачів та зручне документування змін.

Використання Google Sheets у практиці аудиту дозволяє:

- *швидко імпортувати дані з CSV, XLSX та інших форматів;*
- *застосовувати базові і складні формули для обчислення аналітичних показників;*
- *використовувати умовне форматування для виділення ризикових операцій;*
- *формувати динамічні зведені таблиці та графіки;*
- *організовувати спільну роботу та коментування для командного аудиту.*

Приклад (Google Sheets): Аудитор отримав файл у форматі CSV із деталізованим журналом господарських операцій підприємства за звітний період. Для демонстрації використаємо умовну структуру даних, що включає додаткові ознаки, важливі для аналітичного аналізу та ідентифікації ризикових операцій:

Таблиця 7.5

Приклад первинного масиву даних у Google Sheets

Дата операції	№ документа	Контрагент	Сума, грн	Вид операції	Статус оплати
03.01.2025	РК-00112	ТОВ «Гамма»	45 000	Поставка	Оплачено
07.01.2025	РК-00113	ФОП Паньків	12 500	Поставка	Не оплачено
12.01.2025	РК-00114	ТОВ «Дельта»	-3 000	Повернення	Оплачено
12.01.2025	РК-00113	ФОП Паньків	12 500	Поставка	Не оплачено

На цьому етапі аудитор виконує стандартні процедури первинного аналізу:

1. Перевірка даних на дублікати та відсутні значення – за допомогою функцій UNIQUE та ISBLANK визначаються повторювані документи та порожні клітинки.

2. Додавання аналітичних колонок – для полегшення ідентифікації ризикових операцій та аналізу динаміки додаються:

- *місяць операції* (=TEXT(A2;"MMMM"));
- *ознака ризику* (=IF(OR(D2<0, COUNTIF(B:B,B2)>1, F2="Не оплачено"), "Так", "Ні")).

Таблиця 7.6

Приклад аналітичного доповнення облікових даних у Google Sheets

Дата операції	Сума, грн	Місяць операції	Ознака ризику	Контрагент	Вид операції	Статус оплати
03.01.2025	45 000	Січень	Ні	ТОВ «Гамма»	Поставка	Оплачено
07.01.2025	12 500	Січень	Дублікат	ФОП Паньків	Поставка	Не оплачено
12.01.2025	–3 000	Січень	Так	ТОВ «Дельта»	Повернення	Оплачено
12.01.2025	12 500	Січень	Дублікат	ФОП Паньків	Поставка	Не оплачено

Аудиторська оцінка даних:

- *дублікати документів* (рядки 2 і 4) сигналізують про ризик завищення оборотів або повторного обліку.
- *від'ємні суми* (рядок 3) можуть вказувати на повернення або коригування, що потребує додаткової перевірки.
- *неоплачені операції* (рядки 2 і 4) підвищують фінансовий ризик і можуть вимагати додаткового аудиторського контролю.

Застосування умовного форматування в Google Sheets дозволяє автоматично виділяти такі ризикові записи кольором, що значно прискорює процес первинного аналізу. Додатково можна використовувати зведені таблиці для оцінки оборотів за контрагентами, видами операцій або статусом оплати, що створює базу для формування аудиторських вибірок та подальшого аналітичного дослідження.

Таким чином, робота з табличними процесорами, як Microsoft Excel та Google Sheets, забезпечує аудитору інструментальну базу для імпорту, перевірки, структурування та первинного аналізу облікових даних. Використання сортування, фільтрації, умовного форматування та додаткових аналітичних колонок дозволяє швидко виявляти нетипові та потенційно ризикові операції, формувати вибірки для детальної перевірки і підвищує ефективність аудиторських процедур. Отриманий досвід роботи з універсальними табличними інструментами створює основу для переходу до більш спеціалізованого програмного забезпечення, що розширює можливості комп’ютеризованого аудиту.

7.3. Базові можливості спеціалізованого ПЗ для аудиту (огляд інструментів)

Подальший розвиток цифровізації аудиторської діяльності зумовлює поступовий перехід від використання універсальних інструментів обробки даних, таких як табличні процесори, до застосування спеціалізованого програмного забезпечення (ПЗ) для аудиту. На відміну від Microsoft Excel чи Google Sheets, спеціалізовані аудиторські системи орієнтовані безпосередньо на виконання професійних аудиторських процедур і враховують вимоги міжнародних стандартів аудиту, методологію управління ризиками та особливості роботи з великими масивами облікових даних.

Спеціалізоване ПЗ для аудиту, як правило, поєднує інструменти автоматизованого імпорту даних з облікових систем, засоби контролю їх цілісності, вбудовані аналітичні процедури, механізми формування аудиторських вибірок та функції документування результатів перевірки. Це дозволяє зменшити вплив людського фактора, підвищити відтворюваність процедур і забезпечити системний підхід до ідентифікації аудиторських ризиків.

На відміну від табличних процесорів, які потребують значної частки ручного налаштування та професійного судження на кожному етапі аналізу, спеціалізоване ПЗ пропонує аудитору заздалегідь структуроване середовище для роботи з даними. Водночас такі інструменти не замінюють аудитора, а виконують функцію розширених комп'ютеризованих засобів аудиту (CAATs), що підтримують прийняття професійних рішень.

Спеціалізоване ПЗ для аудиту охоплює широкий спектр цифрових інструментів, які відрізняються ***за функціональним призначенням, рівнем автоматизації та масштабом використання.***

Дане ПЗ класифікується за кількома визначальними ознаками, що дозволяє аудитору обґрунтовано обирати інструменти відповідно до завдань перевірки та характеристик клієнта.

За функціональним призначенням спеціалізоване аудиторське ПЗ умовно поділяють на такі групи:

- *програмні продукти для аналізу великих масивів даних (Data Analytics), які забезпечують автоматизовану перевірку суцільних вибірок і виявлення аномалій;*
- *системи управління аудиторським процесом, орієнтовані на планування аудиту, розподіл завдань, контроль виконання та формування робочої документації;*
- *комбіновані платформи, що поєднують аналітичні інструменти з функціями документування та управління аудиторськими ризиками.*

За рівнем автоматизації такі інструменти належать переважно до повністю або високорівнево автоматизованих CAATs. Вони дозволяють виконувати складні аналітичні процедури – від пошуку дублікатів і нетипових операцій до побудови моделей ризику – з мінімальним ручним втручанням, водночас залишаючи ключові рішення за аудитором.

За масштабом використання спеціалізоване ПЗ може бути орієнтоване на:

- *індивідуальних аудиторів і невеликі аудиторські фірми;*
- *середні та великі аудиторські компанії з розгалуженою структурою;*
- *внутрішній аудит і служби фінансової безпеки великих корпорацій*.

Найбільш поширеними прикладами спеціалізованого ПЗ для аудиту є ***IDEA, ACL (HighBond), CaseWare, TeamMate****, а також окремі аналітичні модулі* ***ERP-систем.*** Кожен із цих інструментів має власну спеціалізацію, однак усі вони спрямовані на підвищення якості аудиторських доказів і зниження аудиторського ризику.

Табличні процесори Microsoft Excel і Google Sheets, розглянуті у попередньому підрозділі, є універсальними інструментами обробки даних, які широко застосовуються в аудиторській практиці. Водночас із зростанням обсягів облікової інформації, складності бізнес-процесів і вимог до якості аудиторських доказів виникає потреба у використанні спеціалізованого ПЗ для аудиту. Це зумовлює доцільність порівняння можливостей зазначених інструментів.

Вони забезпечують гнучкість, доступність і універсальність аналітичних процедур, однак значною мірою залежать від ручних налаштувань, професійного судження аудитора та контролю правильності застосування формул і алгоритмів. Помилки в логіці розрахунків або структурі даних можуть залишатися непоміченими та впливати на достовірність результатів аналізу.

Спеціалізоване аудиторське ПЗ, у свою чергу, орієнтоване на системне й стандартизоване виконання аудиторських процедур. Такі інструменти забезпечують автоматизовану перевірку суцільних масивів даних, вбудовані механізми контролю цілісності інформації, а також фіксацію логіки аналізу та результатів у вигляді відтворюваних аудиторських доказів. Це суттєво знижує ризик методичних помилок і підвищує рівень надійності висновків.

Основні відмінності між табличними процесорами та спеціалізованим ПЗ для аудиту узагальнено в таблиці 7.7.

Таблиця 7.7

Порівняльна характеристика табличних процесорів і спеціалізованого аудиторського ПЗ

Критерій порівняння	Excel / Google Sheets	Спеціалізоване ПЗ для аудиту
Рівень автоматизації	Частковий	Високий або повний
Обсяг даних	Обмежений технічними ресурсами	Орієнтація на великі масиви даних
Аудиторські вибірки	Переважно ручне формування	Автоматизовані алгоритми відбору
Контроль помилок	Залежить від аудитора	Вбудовані механізми контролю
Відтворюваність процедур	Обмежена	Забезпечена системно
Документування результатів	Ручне	Інтегроване та стандартизоване

Таким чином, табличні процесори розглядаються як базовий рівень цифрових інструментів аудиту, ефективний на етапах первинної підготовки даних, виконання простих аналітичних процедур і роботи з помірними обсягами

інформації. Натомість спеціалізоване ПЗ є доцільним у випадках, коли аудитор працює з великими масивами транзакцій, потребує суцільного аналізу даних, стандартизації процедур та підвищеного рівня доказовості.

Таке порівняння підкреслює, що спеціалізоване ПЗ не замінює табличні процесори, а логічно доповнює їх у межах комплексної системи комп'ютеризованих засобів аудиту, забезпечуючи перехід від універсальних інструментів до професійних аналітичних платформ. Саме на цьому етапі в сучасній аудиторській практиці дедалі ширше застосовується спеціалізоване ПЗ для аудиту, призначене для автоматизованого аналізу великих масивів фінансово-облікової інформації, формування аудиторських доказів і систематизованого документування результатів перевірки. Аналіз сучасної аудиторської практики підтверджує, що аудитори широко використовують такі спеціалізовані програмні продукти як IDEA**,** ACL**,** CaseWare та TeamMate.

Програмні інструменти належать до спеціалізованих комп'ютеризованих засобів аудиту (CAATs), оскільки вони розроблені з урахуванням вимог міжнародних стандартів аудиту та спрямовані на автоматизовану підтримку повного циклу аудиторських процедур – від етапів планування перевірки й оцінювання аудиторських ризиків до виконання аналітичних тестів, отримання аудиторських доказів, належного документування результатів і формування обґрунтованих аудиторських висновків.

IDEA (CaseWare IDEA) – це спеціалізована аналітична платформа, орієнтована на проведення суцільного аналізу облікових даних, тобто перевірку 100 % генеральної сукупності без необхідності попереднього формування статистичної вибірки. Такий підхід істотно розширює аналітичні можливості аудитора та сприяє зниженню аудиторського ризику, пов'язаного з імовірністю невиявлення суттєвих викривлень.

Програмний продукт забезпечує імпорт даних із широкого спектра джерел, зокрема ERP-систем, бухгалтерських і управлінських програм, електронних таблиць форматів CSV та XLSX, а також реляційних баз даних. Після

завантаження інформації IDEA дозволяє виконувати стандартизовані аналітичні процедури з високим рівнем автоматизації та відтворюваності результатів.

До базових функціональних можливостей IDEA належать:

- *імпорт, перевірка та валідація великих масивів облікових і фінансових даних;*
- *автоматизований пошук дублікатів записів, пропущених реквізитів і нетипових значень показників;*
- *аналіз послідовності номерів первинних документів з метою виявлення порушень хронології або повноти обліку;*
- *тестування господарських операцій за наперед заданими правилами, алгоритмами та сценаріями аудиторського аналізу;*
- *формування відтворюваних і належним чином задокументованих аудиторських доказів.*

Сфера застосування IDEA: фінансовий аудит, внутрішній аудит, процедури виявлення ознак шахрайства, аналіз податкових розрахунків, контроль розрахункових операцій, а також виконання аналітичних процедур у межах забезпечення фінансової безпеки суб'єктів господарювання.

ACL (Audit Command Language) – спеціалізований програмний продукт для поглибленого аналітичного опрацювання даних та автоматизації аудиторських процедур. ACL дозволяє аудитору створювати складні сценарії перевірки, забезпечує систематичний підхід до аналізу даних і суттєво перевищує можливості традиційних табличних процесорів завдяки власній логіці обробки та потужним інструментам автоматизації повторюваних процедур.

До базових функціональних можливостей ACL *належать:*

- *проведення суцільного аналізу великих масивів транзакційних і облікових даних;*
- *розрахунок аналітичних показників, фінансових коефіцієнтів і індикаторів ризику;*

- *побудова правил і алгоритмів виявлення відхилень, нетипових операцій та потенційних викривлень;*
- *автоматизоване формування аудиторських вибірок для детальної перевірки;*
- *інтеграція з системами управління аудиторськими завданнями та документування результатів перевірки.*

***Сфера застосування ACL*:** внутрішній аудит, комплаєнс-контроль, управління ризиками, безперервний аудит та аналітична підтримка процедур виявлення шахрайства.

Завдяки високому рівню автоматизації та можливості налаштування сценаріїв перевірки ACL дозволяє підвищити ефективність аудиту, зменшити ручну обробку даних і забезпечити відтворюваність отриманих аудиторських доказів.

CaseWare – спеціалізоване програмне забезпечення, орієнтоване на документування аудиторського процесу та формування робочих документів аудитора відповідно до вимог міжнародних і національних стандартів аудиту. На відміну від IDEA та ACL, CaseWare менш фокусується на глибокому аналізі транзакцій, проте відіграє ключову роль у забезпеченні системності, прозорості та відтворюваності аудиторської документації.

До базових функціональних можливостей CaseWare належать:

- *ведення електронних робочих файлів аудитора з історією змін і контрольними мітками;*
- *використання шаблонів аудиторських програм і тестів для уніфікації процедур;*
- *автоматизація оформлення аудиторських висновків і звітів;*
- *інтеграція аналітичних процедур з аудиторськими доказами для забезпечення повноти перевірки;*
- *контроль виконання всіх етапів аудиторських процедур та їх документування.*

Сфера застосування CaseWare: зовнішній аудит фінансової звітності, планування аудиту, ведення робочих документів та підготовку узгоджених і стандартизованих аудиторських висновків.

Завдяки фокусуванню на структуризації даних і забезпеченні методичної дисципліни, CaseWare підвищує ефективність управління аудиторським процесом та сприяє дотриманню принципів прозорості і відтворюваності результатів перевірки.

TeamMate є інтегрованою платформою управління аудиторською діяльністю, яка поєднує аналітичні інструменти з можливостями планування, контролю та моніторингу аудиторських завдань.

До базових функціональних можливостей TeamMate належать:

- *планування аудиторських перевірок на основі ризик-орієнтованого підходу;*
- *управління аудиторськими програмами та ресурсами;*
- *централізоване зберігання результатів перевірки;*
- *моніторинг виконання рекомендацій;*
- *інтеграція з аналітичними модулями та зовнішніми джерелами даних.*

***Сфера застосування TeamMate*: внутрішній аудит, аудит державного сектору, корпоративні системи контролю.**

Завдяки інтегрованому підходу TeamMate забезпечує аудитору повний контроль над процесом перевірки, дозволяє координувати роботу команд, підвищує ефективність виконання процедур та гарантує централізоване і стандартизоване зберігання аудиторських доказів. Платформа сприяє системному виконанню аудиторських програм, підвищує відтворюваність і прозорість процедур та підтримує ризик-орієнтований підхід до аудиторських перевірок у різних секторах діяльності.

Для наочного порівняння основних характеристик і функціональних можливостей найбільш поширених спеціалізованих програмних продуктів для аудиту наведено узагальнюючу таблицю 7.8. Вона демонструє, які аналітичні, управлінські та документальні функції реалізовані в IDEA, ACL, CaseWare та

TeamMate, у яких сферах аудиторської практики вони застосовуються та які методологічні переваги забезпечують аудитору при виконанні різних процедур. Таке порівняння дозволяє швидко оцінити, який інструмент є найбільш доцільним для конкретного завдання або типу перевірки.

Таблиця 7.8

Порівняння спеціалізованого ПЗ для аудиту

ПЗ	Основні функції	Сфера застосування	Методологічні переваги
IDEA (CaseWare IDEA)	Суцільний аналіз даних, імпорт з ERP і баз даних, пошук дублікатів і нетипових значень, тестування операцій за правилами, формування відтворюваних доказів	Фінансовий аудит, внутрішній аудит, виявлення шахрайства, аналіз податкових і розрахункових операцій	Дозволяє працювати з 100 % генеральної сукупності, знижує аудиторський ризик невиявлення суттєвих викривлень, висока автоматизація аналітичних процедур
ACL (Audit Command Language)	Суцільний аналіз транзакцій, розрахунок аналітичних показників та коефіцієнтів ризику, побудова правил виявлення аномалій, формування аудиторських вибірок, інтеграція з системами управління аудитом	Внутрішній аудит, комплаєнс, управління ризиками, безперервний аудит, аналітична підтримка виявлення шахрайства	Потужна автоматизація повторюваних процедур, побудова складних сценаріїв перевірки, підвищення точності та відтворюваності доказів
CaseWare	Ведення електронних робочих файлів аудитора, шаблони аудиторських програм і тестів, автоматизація оформлення висновків, інтеграція доказів з аналітикою, контроль виконання процедур	Зовнішній аудит фінансової звітності, планування аудиту, формування робочих документів	Забезпечує системність та прозорість аудиторської документації, контроль методичної дисципліни, стандартизоване оформлення результатів

TeamMate	Планування аудиторських перевірок, управління програмами та ресурсами, централізоване зберігання результатів, моніторинг рекомендацій, інтеграція з аналітичними модулями	Внутрішній аудит, аудит державного сектору, корпоративні системи контролю	Інтегрований контроль аудиторського процесу, централізація даних, підвищення ефективності управління перевірками та відтворюваності процедур

Сучасні спеціалізовані програмні продукти для аудиту виконують взаємодоповнюючі функції та забезпечують аудитору комплексну підтримку на всіх етапах перевірки. IDEA та ACL орієнтовані на суцільний аналіз великих масивів даних, автоматизацію виявлення викривлень і формування вибірок, що підвищує точність та відтворюваність аналітичних процедур. CaseWare зосереджується на стандартизованому документуванні аудиторського процесу та інтеграції доказів із аналітичними перевірками, забезпечуючи системність і методичну дисципліну. TeamMate, у свою чергу, забезпечує централізоване управління аудиторським процесом, контроль виконання завдань і моніторинг рекомендацій, що сприяє підвищенню ефективності та прозорості внутрішнього аудиту.

Таке узагальнення демонструє, що застосування спеціалізованого ПЗ дозволяє поєднати аналітичні, управлінські та документувальні функції, забезпечуючи аудитору високу ступінь автоматизації, надійності та системності процедур. Водночас вибір конкретного інструменту має базуватися на завданнях перевірки, характеристиках облікових даних та специфіці організаційного середовища, що гарантує оптимальне поєднання ефективності аналітичної обробки та достовірності аудиторських доказів.

Ефективність спеціалізованого ПЗ для аудиту значною мірою підвищується за рахунок його інтеграції з інформаційними системами підприємства, зокрема ERP-платформами. Така інтеграція дозволяє автоматизовано імпортувати великі облікові масиви безпосередньо з джерел, що

зменшує ймовірність помилок ручного введення та забезпечує своєчасний доступ до актуальної інформації.

Крім того, ***спеціалізоване ПЗ у поєднанні з ERP-системами*** дозволяє виконувати стандартизовані аналітичні процедури у режимі суцільного аналізу даних, автоматично виявляти нетипові транзакції, дублікати, пропущені або аномальні значення, а також формувати аудиторські вибірки та відтворювані докази.

Такий підхід не лише підвищує точність і швидкість перевірок, а й забезпечує системну підтримку прийняття рішень, дозволяючи аудитору зосередитися на оцінці ризиків, інтерпретації результатів і формуванні обґрунтованих висновків.

Таким чином, спеціалізоване ПЗ для аудиту виступає ключовим елементом сучасної цифрової інфраструктури аудиторської діяльності, забезпечуючи перехід від фрагментарної обробки даних до системного, ризик-орієнтованого та відтворюваного аналізу. Інтеграція таких інструментів із ERP-системами підприємств дозволяє автоматизувати отримання та опрацювання первинної облікової інформації, здійснювати суцільний аналіз транзакцій у реальному або наближеному до реального часу режимі та формувати належні аудиторські докази з мінімальним ручним втручанням.

У практичній площині це означає ***зміну ролі аудитора – від виконавця рутинних перевірочних операцій до аналітика й експерта з оцінювання ризиків та інтерпретації результатів.*** З огляду на це, доцільним є розгляд прикладу практичного використання спеціалізованого ПЗ для аудиту в умовах інтеграції з ERP-системою підприємства, що дозволить продемонструвати прикладну цінність таких інструментів та логіку автоматизації аналітичних процедур.

Приклад. Використання IDEA чи ACL при аналізі даних з ERP-системи

У межах фінансового аудиту середнього виробничого підприємства аудитор отримує доступ до облікових даних, сформованих в ERP-системі

(наприклад, SAP, Oracle NetSuite або Microsoft Dynamics). Метою є виконання аналітичних процедур щодо перевірки повноти, коректності та економічної обґрунтованості відображення господарських операцій у фінансовій звітності.

Вихідні дані: ERP-система підприємства містить журнал господарських операцій за звітний рік, який включає такі реквізити:

- *дата операції;*
- *номер документа;*
- *рахунок дебету;*
- *рахунок кредиту;*
- *сума операції;*
- *код контрагента;*
- *тип операції;*
- *користувач, який здійснив проведення.*

Для проведення аналітичних процедур ***аудитор експортує відповідний масив даних*** із ERP-системи у форматі CSV та імпортує його до спеціалізованого програмного забезпечення IDEA або ACL.

Етап 1. Імпорт і перевірка цілісності даних. На першому етапі в IDEA / ACL виконується імпорт файлу з ERP-системи з одночасною перевіркою:

- *коректності форматів даних* (дати, числові значення, коди рахунків);
- *повноти реквізитів;*
- *відсутності технічних помилок під час експорту.*

Програмне забезпечення автоматично фіксує кількість імпортованих записів та дозволяє зіставити її з контрольними показниками ERP-системи, що забезпечує базовий контроль повноти даних.

Етап 2. Суцільний аналітичний аналіз транзакцій. Після завантаження даних аудитор застосовує вбудовані аналітичні процедури, зокрема:

- *пошук дублікатів номерів документів або ідентичних транзакцій;*
- *аналіз від'ємних і нетипових сум;*
- *перевірку послідовності номерів первинних документів;*
- *групування операцій за рахунками, контрагентами або періодами.*

На відміну від табличних процесорів, ***IDEA та ACL*** дозволяють виконувати ці процедури у режимі суцільної перевірки, охоплюючи 100 % транзакцій без формування вибірки.

Етап 3. Побудова правил виявлення ризикових операцій. На цьому етапі аудитор формує аналітичні правила, спрямовані на виявлення операцій з підвищеним рівнем ризику, наприклад:

- *операції, проведені у неробочий час або наприкінці звітного періоду;*
- *транзакції з нетиповою кореспонденцією рахунків;*
- *операції, створені або змінені користувачами з розширеними правами доступу;*
- *часті коригувальні записи з незначними сумами.*

Результати виконання таких правил формуються у вигляді ***окремих аналітичних звітів,*** які можуть використовуватися для подальшого детального тестування.

Етап 4. Формування аудиторських вибірок і доказів. На основі виявлених ризикових зон IDEA / ACL автоматично формує аудиторські вибірки для поглибленої перевірки первинних документів. При цьому програмне забезпечення:

- *зберігає логіку відбору;*
- *фіксує параметри аналізу;*
- *забезпечує відтворюваність отриманих результатів.*

Сформовані звіти та вибірки використовуються як належні ***аудиторські докази*** та можуть бути інтегровані до системи робочої документації (наприклад, CaseWare або TeamMate).

Розглянутий приклад демонструє, що застосування IDEA або ACL у поєднанні з ERP-системами дозволяє аудитору:

- *здійснювати суцільний аналіз великих масивів облікових даних;*
- *автоматизувати виявлення потенційних викривлень і аномалій;*
- *зменшити вплив людського фактору;*
- *підвищити надійність і доказовість аудиторських висновків.*

В українській аудиторській практиці поряд із міжнародними програмними продуктами застосовуються і національні спеціалізовані рішення, зокрема програмний комплекс ***Аксіома-Аудит***. Ця система орієнтована на автоматизацію планування аудиту, формування робочої документації аудитора, структурування аудиторських процедур та документування результатів перевірки відповідно до вимог Міжнародних стандартів аудиту та законодавства України.

Функціональні можливості програми передбачають формування електронного аудиторського файлу, використання шаблонів процедур, автоматизовану побудову робочих документів, контроль повноти виконання етапів аудиту, а також систематизацію доказової бази. Важливою перевагою є адаптація програмного забезпечення до української нормативно-правової бази та методичних рекомендацій професійного регулювання.

Застосування Аксіома-Аудит дозволяє:

- *стандартизувати процедури аудиту відповідно до МСА;*
- *забезпечити належне електронне документування аудиторських доказів;*
- *підвищити контроль за дотриманням внутрішніх політик якості;*
- *мінімізувати ризики пропуску обов'язкових процедур;*
- *підвищити прозорість та відтворюваність аудиторських висновків.*

Тому, використання національних програмних продуктів, таких як «Аксіома-Аудит», у поєднанні з інструментами аналізу даних (IDEA, ACL) та ERP-середовищем клієнта формує комплексну цифрову екосистему сучасного аудиту, що відповідає вимогам професійних стандартів, законодавства та системи зовнішнього контролю якості.

Поряд із програмним комплексом ***Аксіома-Аудит*** у практиці українських суб'єктів аудиторської діяльності використовується також спеціалізоване програмне забезпечення ***AuditXP***, призначене для комплексної автоматизації процесу аудиту фінансової звітності. Цей програмний продукт орієнтований на

методологічно структуровану організацію аудиторських процедур відповідно до вимог Міжнародних стандартів аудиту та чинного законодавства України, забезпечуючи формування електронного робочого файлу аудитора, систематизацію доказової бази та підтримку ризик-орієнтованого підходу до планування і виконання перевірки.

Програмний продукт AuditXP орієнтований на методологічну підтримку аудиту відповідно до вимог Міжнародних стандартів аудиту та національного законодавства. Його функціонал охоплює етапи планування, оцінки ризиків, формування програм аудиту, документування процедур, узагальнення результатів перевірки та підготовки аудиторського звіту. Система передбачає структуровану побудову електронного робочого файлу аудитора із використанням уніфікованих форм, контрольних листів і шаблонів, що забезпечує стандартизацію виконання процедур.

Важливою особливістю AuditXP є інтеграція інструментів внутрішнього контролю якості, можливість налаштування методологічних модулів відповідно до профілю клієнта, а також формування логічно пов'язаних робочих документів із фіксацією виконаних процедур і відповідальних осіб. Це сприяє забезпеченню відтворюваності аудиторських дій, прозорості професійного судження та належності доказової бази.

Застосування AuditXP дозволяє:

- *систематизувати процес ризик-орієнтованого планування аудиту;*
- *забезпечити електронне документування аудиторських доказів із дотриманням принципу достатності та належності;*
- *автоматизувати контроль повноти виконання процедур;*
- *підвищити якість внутрішнього методологічного контролю;*
- *мінімізувати операційні та методичні ризики аудиторської діяльності.*

Отже, використання програмних продуктів ***Аксіома-Аудит*** та ***AuditXP*** поряд із аналітичними платформами (IDEA, ACL) формує багаторівневу цифрову модель аудиту, в якій поєднуються інструменти аналізу даних,

управління робочою документацією та внутрішнього контролю якості, що відповідає сучасним вимогам професійного регулювання та цифровізації аудиторської діяльності в Україні.

Таким чином, спеціалізоване ПЗ виступає дієвим інструментом реалізації ризик-орієнтованого підходу та практичного застосування Міжнародних стандартів аудиту в умовах цифровізації обліку.

Поєднання табличних процесорів, аналітичних програм і спеціалізованих аудиторських систем забезпечує ефективну роботу з великими масивами даних, можливість суцільної перевірки операцій, автоматизацію контрольних та аналітичних процедур і належне електронне документування доказів. Інтеграція таких інструментів з ERP-системами підвищує якість перевірки, прозорість процедур і відтворюваність результатів, посилюючи роль аудитора та фахівця з фінансової безпеки як аналітика ризиків і суб'єкта професійного судження в цифровому середовищі.

7.4. Контрольні питання для самоперевірки

1. У чому полягає сутність комп'ютеризованих засобів аудиту (CAATs) та яке їх значення в умовах цифровізації аудиторської діяльності?
2. Які основні причини зумовлюють необхідність застосування CAATs у сучасному аудиті фінансової звітності та внутрішнього контролю?
3. Як використання CAATs впливає на рівень аудиторського ризику та якість аудиторських доказів?
4. За якими класифікаційними ознаками здійснюється групування комп'ютеризованих засобів аудиту та в чому полягає методологічне значення такої класифікації?
5. Які переваги суцільного аналізу даних, що забезпечується CAATs, порівняно з традиційним вибірковим тестуванням?
6. Яке місце табличні процесори Microsoft Excel та Google Sheets займають у системі комп'ютеризованих засобів аудиту та до якої категорії CAATs вони належать?
7. Які основні напрями використання табличних процесорів у процесі виконання аудиторських процедур та забезпечення фінансової безпеки?
8. Чому підготовка та первинна перевірка даних у табличному процесорі розглядається як аналітична, а не лише технічна аудиторська процедура?
9. Які типові помилки можуть виникати в облікових даних після їх імпорту в Excel або Google Sheets та які аудиторські ризики вони створюють?
10. У чому полягають функціональні та методичні особливості використання Google Sheets порівняно з Microsoft Excel у практиці аудиту?
11. У чому полягають принципові відмінності між табличними процесорами та спеціалізованим програмним забезпеченням для аудиту з точки зору методології та рівня автоматизації процедур?
12. Які основні функціональні можливості характерні для спеціалізованого аудиторського ПЗ та як вони підтримують повний цикл аудиторських процедур?
13. Яке практичне значення мають аналітичні платформи IDEA та ACL для виконання суцільного аналізу даних і виявлення аудиторських ризиків?

14. Яку роль у системі спеціалізованого ПЗ для аудиту відіграють CaseWare та TeamMate та в чому полягає їх відмінність від аналітичних інструментів?

15. Чому спеціалізоване програмне забезпечення для аудиту доцільно розглядати як доповнення, а не заміну універсальних табличних процесорів у межах комплексної системи CAATs?

16. У чому полягає призначення програми Аксіома-Аудит в роботі аудитора?

17. Які основні можливості має Аксіома-Аудит для створення робочих документів і збереження доказів?

18. Для чого використовується AuditXP під час планування та проведення аудиту?

19. Як AuditXP допомагає контролювати, щоб усі потрібні процедури були виконані?

20. Чому в аудиті корисно поєднувати Аксіома-Аудит і AuditXP з IDEA або ACL Analytics та даними з облікової системи клієнта?

Розділ 8

Автори:
Олена Птащенко
Ірина Осійчук

ІНТЕГРОВАНІ МОДЕЛІ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ

РОЗДІЛ 8. ІНТЕГРОВАНІ МОДЕЛІ УПРАВЛІННЯ ФІНАНСОВОЮ БЕЗПЕКОЮ

«Остерігайтеся дрібних витрат: маленький витік потопить великий корабель.»

Бенджамін Франклін

8.1. Концептуальна модель «Безпека–інклюзія–аудит»

Сучасні соціально-економічні трансформації зумовлюють необхідність переосмислення підходів до управління розвитком організацій, територій і публічних систем у цілому. Ускладнення фінансових процесів, зростання рівня невизначеності, посилення вимог до прозорості управлінських рішень та підвищення суспільного запиту на справедливість і доступність ресурсів формують нову логіку управління, у межах якої безпека, інклюзія та контроль перестають розглядатися як ізольовані елементи. Саме в цьому контексті актуалізується потреба у формуванні концептуальної моделі, що поєднує зазначені складові в єдину узгоджену систему.

Традиційні підходи до забезпечення безпеки здебільшого зосереджувалися на мінімізації ризиків та реагуванні на загрози, залишаючи поза увагою питання участі зацікавлених сторін у прийнятті рішень і механізми зворотного зв’язку. Водночас інклюзивні підходи, спрямовані на розширення доступу та залучення різних груп, не завжди супроводжувалися належним рівнем контролю й оцінювання наслідків управлінських дій. Аудит же у багатьох випадках зводився до формальної перевірки відповідності, не виконуючи

функції інтегратора між цілями безпеки та принципами інклюзії.

У цих умовах концептуальна модель «Безпека–інклюзія–аудит» розглядається як спроба подолати фрагментарність існуючих підходів шляхом формування цілісного управлінського бачення. Її логіка ґрунтується на розумінні безпеки не лише як стану захищеності, а як процесу постійного балансування інтересів; інклюзії не лише як соціального принципу, а як інструменту підвищення стійкості системи; аудиту не лише як контрольної функції, а як механізму аналітичної підтримки управлінських рішень.

Концептуальна модель «Безпека–інклюзія–аудит» – це інтегрована система управління, у межах якої запобігання ризикам, залучення зацікавлених сторін та аналітичний контроль поєднуються в єдиний контур формування, реалізації та коригування управлінських рішень.

Концептуальна модель «Безпека–інклюзія–аудит» ґрунтується на ідеї інтеграції трьох управлінських площин, які в традиційних підходах зазвичай функціонують відокремлено (рис. 8.1).

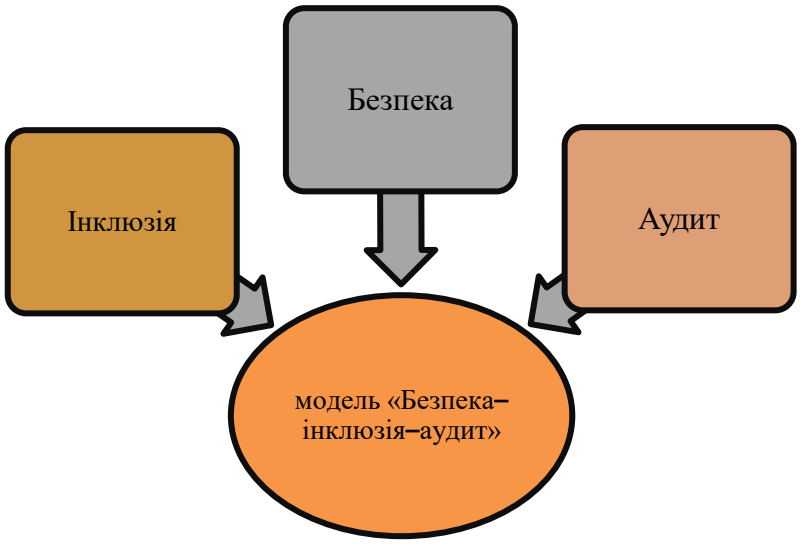


Рис. 8.1. Схематичний вигляд концептуальної моделі «Безпека–інклюзія–аудит»

Її структура передбачає не ієрархічне підпорядкування окремих елементів, а їх взаємодію у межах єдиного управлінського контуру. Кожен блок виконує самостійну функцію, водночас посилюючи ефективність інших складових моделі.

Логіка побудови моделі ґрунтується на взаємозалежності трьох компонентів:

1. Безпека розглядається не лише як технічний або фізичний захист, а як комплекс організаційних, правових та управлінських заходів, спрямованих на мінімізацію ризиків і запобігання загрозам. Формується середовище, у якому кожен учасник процесу розуміє правила та межі відповідальності.

2. Інклюзія передбачає створення умов для повноцінної участі різних груп, незалежно від їхніх соціальних, фізичних чи інших особливостей. Вона не обмежується фізичною доступністю простору, а охоплює доступ до інформації, сервісів, процедур прийняття рішень.

3. Аудит виступає інструментом об'єктивної оцінки того, наскільки перші два компоненти реалізуються на практиці. Це не лише контроль, а й механізм навчання системи, який дозволяє виявляти невідповідності та коригувати політики.

Блок безпеки формує основу концептуальної моделі та визначає її стабілізаційну функцію. У межах цієї моделі безпека розглядається не як статичний стан захищеності, а як динамічний процес управління ризиками та невизначеністю. Це здатність системи своєчасно ідентифікувати загрози, оцінювати їхній потенційний вплив та формувати превентивні управлінські рішення.

Особливістю цього блоку є орієнтація не лише на зовнішні ризики, а й на внутрішні дисбаланси, що можуть виникати внаслідок неузгодженості управлінських дій, обмеженості ресурсів або інформаційної асиметрії. Безпека в такому розумінні пов'язується з фінансовою стійкістю, інституційною спроможністю та здатністю системи зберігати функціональність у кризових умовах. Складові блоку безпеки наведено на рисунку 8.2.

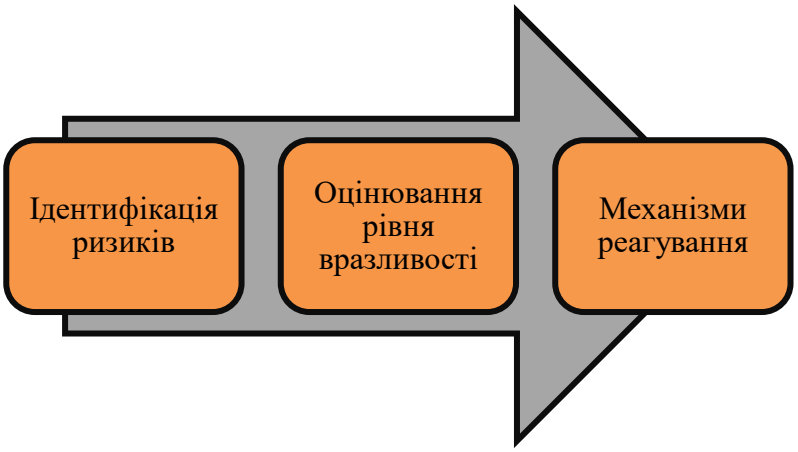


Рис. 8.2. Складові блоку безпеки

Блок безпеки в межах концептуальної моделі формується як сукупність взаємопов'язаних елементів, що забезпечують стабільність функціонування системи та її здатність протидіяти загрозам. Першою складовою цього блоку є ідентифікація ризиків, яка передбачає системне виявлення потенційних внутрішніх і зовнішніх чинників дестабілізації. Це не лише фінансові ризики, а й управлінські, інституційні та інформаційні загрози, що можуть мати відкладений або непрямий вплив.

Другою складовою виступає оцінювання рівня вразливості, яке дозволяє визначити, наскільки система здатна витримувати негативні впливи без втрати функціональної цілісності. Ця складова пов'язана з аналізом ресурсної забезпеченості, організаційної структури та якості управлінських рішень. Вона створює основу для формування пріоритетів у системі безпеки.

Третьою складовою є механізми превентивного реагування, спрямовані на запобігання реалізації загроз. Їх сутність полягає у завчасному коригуванні управлінських рішень, перерозподілі ресурсів і вдосконаленні процедур з метою мінімізації негативних наслідків.

У сукупності ці складові формують динамічний контур безпеки, орієнтований на підтримання стійкості в умовах невизначеності.

Інклюзія в межах концептуальної моделі виконує не допоміжну, а системоутворюючу роль. Вона забезпечує залучення зацікавлених сторін до процесів формування, реалізації та коригування управлінських рішень. Інклюзивний підхід передбачає вплив різних груп на управлінські процеси.

Залучення широкого кола учасників сприяє підвищенню якості інформації, що використовується в управлінні, зменшенню ризиків односторонніх рішень та формуванню довіри до управлінської системи. Крім того, інклюзія виступає чинником підвищення адаптивності, оскільки дозволяє враховувати різні точки зору та швидше реагувати на зміни зовнішнього середовища. Складові блоку інклюзії показано на рисунку 8.3.

Блок інклюзії охоплює елементи, що забезпечують відкритість управлінської системи та її здатність враховувати різноманітність інтересів. Першою складовою є залучення стейкхолдерів, яке передбачає участь зацікавлених сторін у процесах обговорення, формування та оцінювання управлінських рішень. Сприяє зниженню інформаційних перекосів і підвищенню легітимності управління.

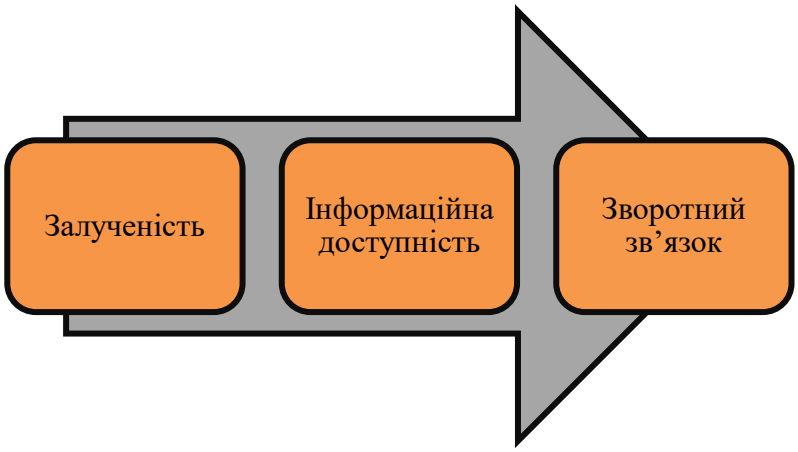


Рис. 8.3. Складові блоку інклюзії

Другою складовою виступає інформаційна доступність, що забезпечує рівний доступ до релевантної інформації та результатів управлінської діяльності. Вона формує основу для усвідомленої участі та зменшує ризики маніпулятивних рішень. Інформаційна відкритість розглядається як інструмент зміцнення довіри, а не лише як формальна вимога.

Третьою складовою блоку інклюзії є зворотний зв’язок, який дозволяє коригувати управлінські рішення з урахуванням реакції та оцінок учасників процесу. Завдяки цьому інклюзія набуває динамічного характеру й перестає бути одноразовою дією.

Сукупність зазначених складових сприяє формуванню управлінського

середовища, орієнтованого на узгодження інтересів та підвищення адаптивності системи.

Блок аудиту в концептуальній моделі «Безпека–інклюзія–аудит» виходить за межі традиційного контрольного інструментарію. Його функція полягає не лише у перевірці дотримання встановлених норм і процедур, а у формуванні аналітичної бази для прийняття обґрунтованих управлінських рішень.

Аудит у цій моделі виступає інструментом зворотного зв'язку, що дозволяє оцінити відповідність між задекларованими цілями, фактичними результатами та використаними ресурсами. Він забезпечує прозорість управлінських процесів, виявляє структурні слабкі місця та створює передумови для коригування як стратегічних, так і оперативних рішень. Складові блоку аудиту відображено на рисунку 8.4.

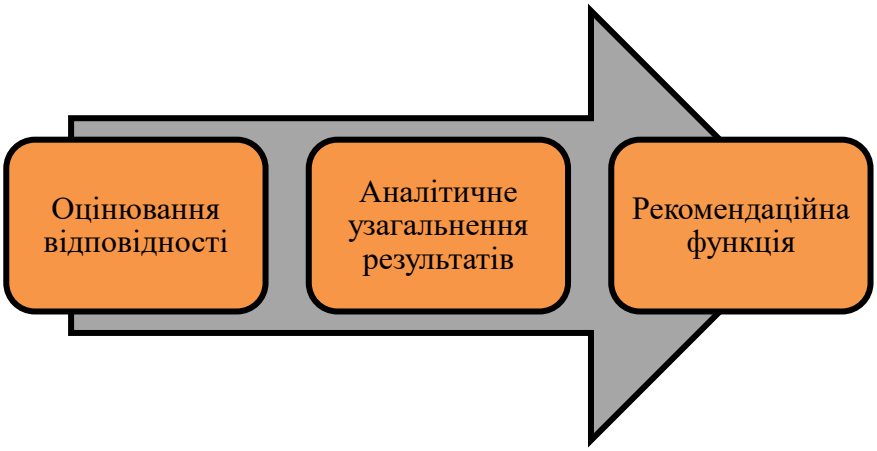


Рис. 8.4. Складові блоку аудиту

Блок аудиту у концептуальній моделі виконує функцію системного аналізу та корекції управлінських процесів. Його першою складовою є оцінювання відповідності, що передбачає зіставлення запланованих цілей із фактичними результатами. Дозволяє виявити розбіжності між стратегічними намірами та практичною реалізацією управлінських рішень.

Другою складовою є аналітичне узагальнення результатів, спрямоване на виявлення причин відхилень і структурних дисбалансів. На відміну від формального контролю, аналітичний аудит зосереджується на пошуку системних проблем, а не на фіксації окремих порушень.

Третьою складовою виступає рекомендаційна функція, що забезпечує трансформацію результатів аудиту в інструменти вдосконалення управління. Саме цей елемент надає аудиту проактивного характеру та інтегрує його у процес прийняття рішень.

У поєднанні ці складові перетворюють аудит на механізм підтримки розвитку, а не лише контролю.

Складові кожного блоку не функціонують ізольовано, а перебувають у постійній взаємодії. Результати аудиту уточнюють параметри безпеки, інклюзія впливає на якість і повноту інформації для оцінювання, а безпекові пріоритети визначають межі управлінських рішень. Така взаємодія формує цілісну концептуальну модель, здатну забезпечити баланс між стабільністю, відкритістю та контрольованістю розвитку (рис. 8.5).

Ключовою особливістю моделі є взаємозалежність її складових. Безпека без інклюзії може призводити до надмірної урегульованості та втрати довіри, інклюзія без аудиту до зниження керованості, а аудит без орієнтації на безпеку до формалізації управлінських процесів. Лише поєднання цих блоків у єдину логічну систему дозволяє досягти збалансованого управлінського ефекту.

Важливим є аудит вихідного стану, з точки зору оцінки наявних процедур, аналізу ризиків, виявлення бар'єрів для участі різних груп. На основі цього формується план дій із конкретними індикаторами результативності.

На етапі впровадження відбувається:

- *оновлення внутрішніх політик безпеки;*
- *адаптація процедур до принципів недискримінації;*
- *запровадження каналів зворотного зв'язку;*
- *визначення відповідальних осіб за моніторинг і перевірку.*

Особливого значення набуває підготовка персоналу. Навчання спрямоване не лише на дотримання інструкцій, а й на формування розуміння взаємозв'язку між захистом і відкритістю. Працівники повинні усвідомлювати, що інклюзивні практики підвищують довіру до системи, а прозорий аудит зменшує ризик формального підходу.

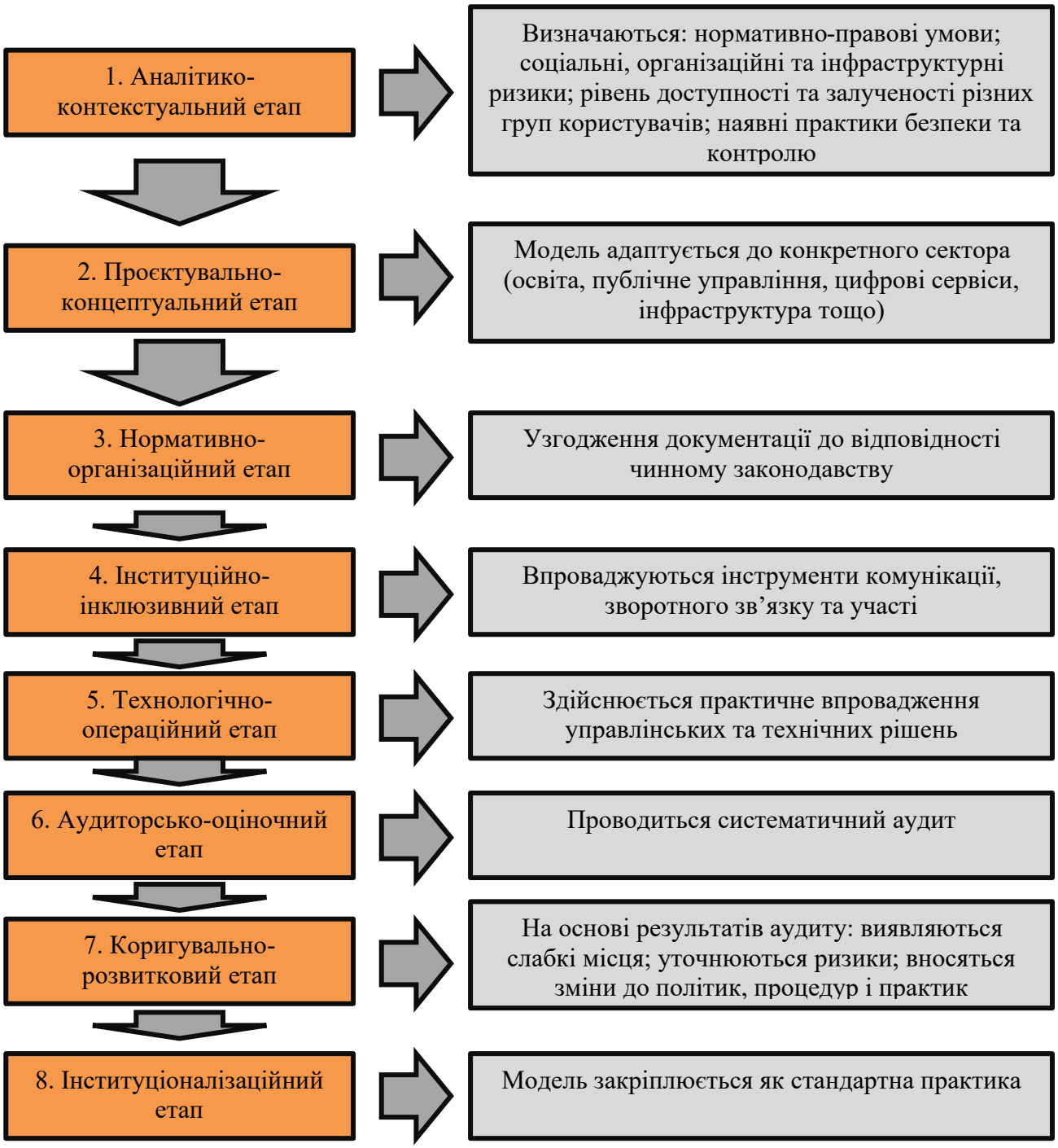


Рис. 8.5. Етапи реалізації концептуальної моделі «Безпека–інклюзія–аудит»

Таким чином, концептуальна модель «Безпека–інклюзія–аудит» створює підґрунтя для формування стійких, прозорих і адаптивних управлінських систем, здатних функціонувати в умовах підвищеної складності та невизначеності.

Реалізація моделі потребує чіткої управлінської організації та

нормативного закріплення. Насамперед визначається стратегічна мета для забезпечення збалансованого середовища, у якому захист не обмежує права, а доступність не знижує рівень контролю.

Системний аудит включає кількісні показники (відповідність стандартам, кількість інцидентів, рівень доступності) та якісні оцінки (задоволеність користувачів, ефективність комунікації). Його результати спрямовані на вдосконалення управлінських процесів (рис. 8.6).

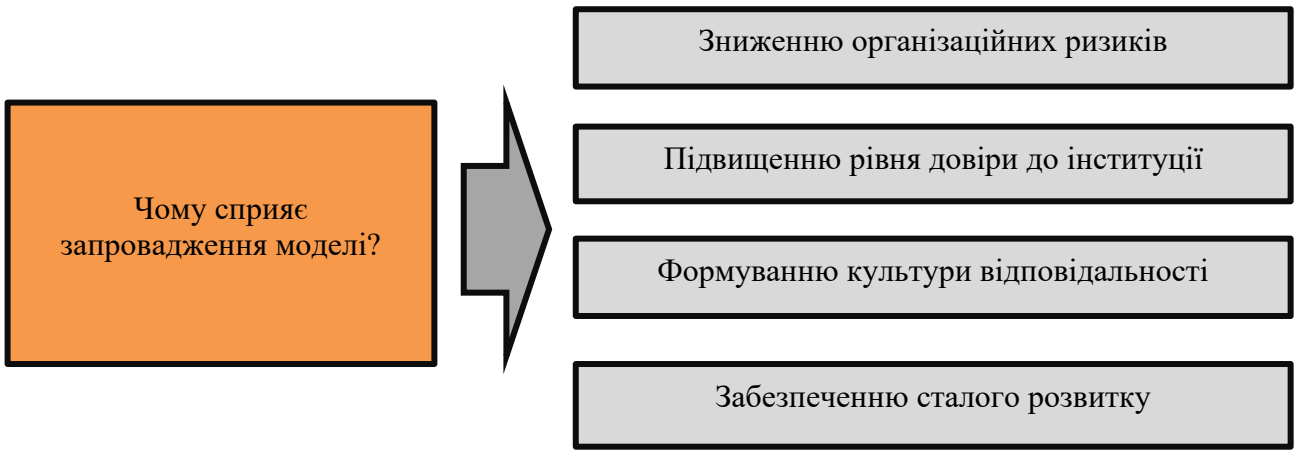


Рис. 8.6. Запровадження моделі «Безпека–інклюзія–аудит»

Інтеграція трьох складових дозволяє уникнути однобічності управлінських рішень та створює основу для довгострокової стабільності. Модель не є статичною та передбачає постійне оновлення відповідно до змін середовища, нормативної бази та суспільних очікувань.

Впровадження концептуальної моделі «Безпека–інклюзія–аудит» засвідчує необхідність переходу від ізольованих управлінських рішень до цілісної системи, у якій захист, рівний доступ і контроль розглядаються як взаємопов'язані складові єдиного процесу. Практика доводить, що орієнтація виключно на безпекові заходи без урахування принципів інклюзивності звужує соціальну базу довіри та породжує приховані конфлікти, тоді як інклюзія без належного регламентування і моніторингу може створювати додаткові організаційні ризики. Інтеграція цих компонентів через механізм регулярного аудиту формує збалансовану управлінську модель.

Сутність запропонованого підходу полягає у встановленні динамічної

рівноваги, що було представлено вище. Така триєдина конструкція мінімізує ризики, сприяє формуванню культури відповідальності, у якій контроль не сприймається як формальна процедура, а розглядається як інструмент розвитку.

Важливим наслідком реалізації моделі є підвищення інституційної стійкості. Організація, що системно аналізує власні процеси, відкрито оцінює їхню ефективність і враховує потреби різних груп, отримує здатність адаптуватися до змін зовнішнього середовища без втрати керованості.

Концептуальна модель «Безпека–інклюзія–аудит» може розглядатися як методологічна основа для формування сучасної управлінської практики, зорієнтованої на поєднання захисних механізмів, принципів рівності та прозорої підзвітності. Її впровадження створює передумови для сталого функціонування інституцій, підвищення рівня довіри та формування середовища, у якому безпека не обмежує можливості, а інклюзія не суперечить вимогам контролю.

8.2. Вплив інклюзії на навантаження системи фінансової безпеки

Питання фінансової безпеки впродовж тривалого часу розглядалося переважно через категорії стабільності, платоспроможності та протидії фінансовим правопорушенням. Однак трансформація економічних процесів, розвиток цифрових технологій і посилення соціальної орієнтації фінансової політики зумовили необхідність переосмислення традиційних підходів. Розширення фінансової інклюзії через залучення ширших верств населення та малого бізнесу до використання фінансових послуг істотно змінює параметри функціонування системи фінансової безпеки та впливає на характер її навантаження.

Інклюзія у фінансовій сфері має подвійний ефект. З одного боку, вона сприяє детінізації економіки, формуванню прозорих фінансових потоків і підвищенню рівня економічної активності. Доступ до банківських рахунків, кредитування, страхових інструментів та електронних платіжних сервісів створює умови для розширення підприємницької діяльності та соціальної мобільності. З іншого боку, збільшення кількості користувачів фінансових послуг, зростання обсягу транзакцій і поява нових цифрових каналів взаємодії підсилюють вимоги до систем моніторингу, контролю та захисту від зловживань.

Таким чином, інклюзія не лише розширює економічні можливості, а й трансформує ризиковий профіль фінансової системи. Підвищується навантаження на регуляторні органи, фінансові установи та підрозділи комплаєнсу, що відповідають за запобігання відмиванню коштів, фінансуванню незаконної діяльності та кіберзлочинності. Одночасно зростає потреба у вдосконаленні аналітичних інструментів, автоматизації контролю та підвищенні фінансової грамотності користувачів.

Особливості впливу інклюзії на навантаження системи фінансової безпеки можна представити у вигляді таблиці (табл. 8.1).

Таблиця 8.1

Особливості впливу інклюзії на навантаження системи фінансової безпеки

Аспект фінансової інклюзії	Характер впливу на систему фінансової безпеки	Тип навантаження	Потенційні ризики	Компенсаторні механізми
Розширення доступу до банківських рахунків	Зростання кількості клієнтів і транзакцій	Операційне	Підвищення складності фінансового моніторингу	Автоматизація AML-процедур, ризик-орієнтований підхід
Активізація мікрокредитування	Залучення нових позичальників із різним рівнем платоспроможності	Кредитне	Погіршення якості кредитного портфеля	Скоринг-моделі, резервування, диверсифікація ризиків
Цифровізація фінансових послуг	Зростання швидкості та обсягу електронних операцій	Технологічне	Кіберзагрози, витік персональних даних	Кіберзахист, багаторівнева аутентифікація
Залучення соціально вразливих груп	Розширення кола користувачів із низькою фінансовою грамотністю	Інформаційно-аналітичне	Шахрайство, маніпуляції, помилки користувачів	Освітні програми, консультативна підтримка
Розвиток фінтех-платформ	Поява нових посередників та небанківських інструментів	Регуляторне	Регуляторні прогалини, асиметрія інформації	Оновлення нормативної бази, ліцензування
Інтеграція віддаленої ідентифікації (e-KYC)	Спрощення доступу до фінансових сервісів	Контрольне	Використання підроблених або викрадених даних	Біометрична верифікація, централізовані реєстри
Розширення платіжної інфраструктури	Збільшення кількості точок доступу та каналів розрахунків	Інфраструктурне	Перевантаження платіжних систем	Резервні канали, масштабування серверних потужностей
Детінізація фінансових потоків	Підвищення прозорості економічних операцій	Стратегічне (позитивне)	Тимчасове зростання навантаження на органи контролю	Аналітичні платформи обробки великих даних

Аспект фінансової інклюзії	Характер впливу на систему фінансової безпеки	Тип навантаження	Потенційні ризики	Компенсаторні механізми
Розвиток програм державної підтримки через фінансові інструменти	Збільшення обсягів цільових переказів	Бюджетно-контрольне	Нецільове використання коштів	Цифрове відстеження транзакцій, аудит програм
Підвищення фінансової активності малого бізнесу	Зростання кількості суб'єктів господарювання у фінансовій системі	Системне	Локальні фінансові збої при масових неплатежах	Страхування ризиків, гарантійні фонди
Міжнародна фінансова інтеграція	Розширення транскордонних операцій	Міжнародно-правове	Відмивання коштів через складні схеми	Міждержавний обмін інформацією
Зростання обсягів безготівкових операцій	Зменшення частки готівкового обігу	Аналітичне (позитивне)	Перехід шахрайства в цифрову сферу	Антифрод-системи, поведінкова аналітика

Представлена в таблиці 8.1 систематизація дозволяє зробити узагальнений висновок про те, що фінансова інклюзія є не лише соціально-економічним пріоритетом, а й чинником глибокої трансформації архітектури фінансової безпеки. Її вплив не зводиться до механічного збільшення кількості користувачів або операцій, а змінює характер навантаження на інститути контролю, регулювання та аналітики (рис. 8.7).

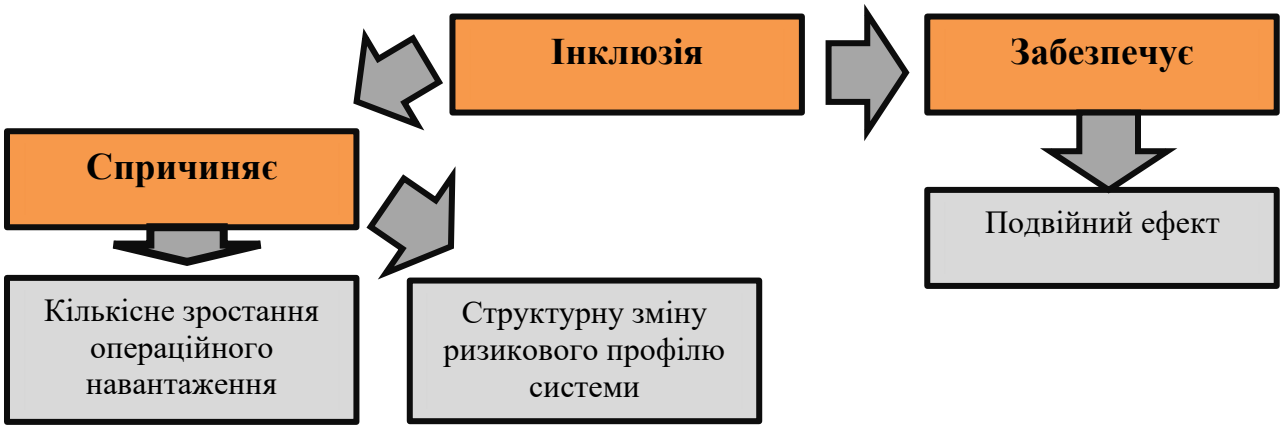


Рис. 8.7. Інклюзія як соціально-економічний пріоритет

Наведемо характеристику зазначених пріоритетів.

1. ***Інклюзія спричиняє кількісне зростання операційного навантаження.*** Розширення доступу до рахунків, цифрових платіжних сервісів і кредитних інструментів збільшує обсяг транзакцій, що потребують моніторингу. Це ускладнює роботу фінансових установ та органів нагляду, підвищуючи вимоги до швидкості обробки інформації та точності аналітичних алгоритмів.

2. ***Відбувається структурна зміна ризикового профілю системи.*** Залучення нових соціальних груп, розвиток фінтеху, дистанційна ідентифікація клієнтів і транскордонні операції створюють нові види ризиків такі, як кібернетичні, поведінкові, регуляторні. Унаслідок цього система фінансової безпеки змушена переходити від традиційних методів контролю до ризик-орієнтованих моделей управління.

3. ***Інклюзія має парадоксальний подвійний ефект.*** З одного боку, вона збільшує навантаження на механізми фінансового моніторингу та комплаєнсу, а з іншого сприяє детінізації економіки, підвищенню прозорості фінансових потоків і розширенню податкової бази. У стратегічній перспективі це може зміцнювати фінансову стійкість держави та знижувати системні загрози.

Таким чином, інклюзія не є фактором, що однозначно ускладнює або полегшує функціонування системи фінансової безпеки. Вона змінює її конфігурацію, посилюючи вимоги до гнучкості, адаптивності та технологічної оснащеності. Ефективне управління таким навантаженням можливе лише за умови комплексного підходу, який поєднує регуляторні інструменти, цифрові рішення та підвищення фінансової грамотності населення.

Розширення фінансової інклюзії означає залучення ширших верств населення та суб’єктів господарювання до використання банківських, платіжних, кредитних, страхових і цифрових фінансових інструментів. Цей процес має беззаперечний соціально-економічний потенціал, однак водночас змінює параметри функціонування системи фінансової безпеки. Це зростання обсягу операцій, трансформація конфігурації безпекового механізму та його

структурних елементів, функцій, ресурсного забезпечення (табл. 8.2).

Таблиця 8.2

Вплив розширення фінансової інклюзії на структурне, функціональне та ресурсне навантаження системи фінансової безпеки

Вимір впливу	Прояв розширення інклюзії	Зміни у системі фінансової безпеки	Характер навантаження	Потенційний ефект (коротко-довгостроковий)
Структурний	Збільшення кількості учасників фінансового ринку	Розширення кола суб'єктів контролю та нагляду	Інституційне ускладнення	Короткостроковим є зростання складності координації; довгостроковим є формування мережевої моделі управління
Структурний	Поява фінтех-компаній та небанківських сервісів	Необхідність інтеграції нових платформ у регуляторне поле	Регуляторне	Тимчасові прогалини; поступова адаптація нормативної бази
Структурний	Розвиток транскордонних фінансових послуг	Посилення міжнародної взаємодії органів фінансового контролю	Міжінституційне	Зростання складності комплаєнсу; підвищення прозорості обміну даними
Функціональний	Зростання обсягу безготівкових операцій	Розширення процедур фінансового моніторингу	Операційне	Підвищення вимог до швидкості обробки даних
Функціональний	Дистанційна ідентифікація клієнтів	Модернізація процедур KYC та верифікації	Контрольне	Ризик цифрового шахрайства; розвиток біометричних технологій
Функціональний	Залучення користувачів із низькою фінансовою грамотністю	Посилення превентивних та роз'яснювальних функцій	Превентивно-аналітичне	Зменшення шахрайства за умови освітніх програм
Функціональний	Інтеграція державних соціальних виплат у фінансові сервіси	Розширення аналітичного супроводу цільового використання коштів	Контрольно-аналітичне	Підвищення прозорості бюджетних потоків

Вимір впливу	Прояв розширення інклюзії	Зміни у системі фінансової безпеки	Характер навантаження	Потенційний ефект (коротко-довгостроковий)
Ресурсний	Зростання кількості транзакцій	Потреба у масштабуванні серверної інфраструктури	Технологічне	Збільшення витрат на IT-підтримку
Ресурсний	Ускладнення ризикових профілів клієнтів	Необхідність підготовки фахівців з аналітики та кібербезпеки	Кадрове	Підвищення вимог до професійної кваліфікації
Ресурсний	Перехід до цифрових форматів обслуговування	Інвестування в кіберзахист і захист персональних даних	Фінансове	Зростання капітальних витрат; довгострокове зниження системних втрат
Системний	Комплексне розширення фінансової участі	Трансформація моделі безпеки з реактивної у проактивну	Стратегічне	Формування адаптивної та стійкої системи

Структурний вимір впливу інклюзії проявляється у зміні складу та взаємодії інституцій, що забезпечують фінансову безпеку. Залучення нових учасників таких, як фізичні особи, малий бізнес, фінтех-компанії, небанківські установи розширює межі фінансової системи. Відповідно, система безпеки більше не може обмежуватися традиційними банківськими механізмами контролю.

Розвиток дистанційної ідентифікації, електронних гаманців, платформ кредитування та цифрових активів формує багаторівневу мережу взаємозалежностей. Це зумовлює необхідність координації між регуляторами, правоохоронними органами, кіберпідрозділами та суб'єктами фінансового ринку.

Таким чином, структурне навантаження проявляється в:

- *ускладненні інституційної архітектури;*
- *зростанні кількості точок контролю;*
- *необхідності інтеграції інформаційних систем різних органів.*

Функціональний вплив пов'язаний зі зміною характеру завдань, які виконують суб'єкти фінансової безпеки. Збільшення кількості транзакцій, поява нових фінансових продуктів і цифрових каналів взаємодії зумовлюють зростання обсягів фінансового моніторингу, перевірок та аналітичної роботи.

Розширення інклюзії означає, що до системи входять користувачі з різним рівнем фінансової грамотності та досвіду. Це підвищує ймовірність помилкових операцій, шахрайських схем або несвідомого порушення правил. У результаті функції контролю трансформуються з переважно формально-перевірочних у превентивно-аналітичні.

Функціональне навантаження також посилюється через міжнародну інтеграцію фінансових потоків. Транскордонні операції потребують обміну інформацією між юрисдикціями, що ускладнює процедури перевірки та підвищує вимоги до комплаєнсу.

Ресурсний вплив інклюзії охоплює фінансові, кадрові та технологічні ресурси, необхідні для підтримання належного рівня безпеки. Зростає потреба у фінансуванні модернізації інформаційних систем, кіберзахисту та програмного забезпечення для обробки великих масивів даних. Без відповідного технічного забезпечення збільшення кількості операцій може призвести до перевантаження інфраструктури.

Також посилюються вимоги до кваліфікації персоналу. Фахівці з фінансового моніторингу повинні володіти не лише знаннями нормативної бази, а й навичками роботи з цифровими інструментами, аналітичними платформами та алгоритмами штучного аналізу даних.

При цьому відбувається зростання витрат на навчальні та просвітницькі програми для населення. Підвищення фінансової грамотності стає елементом профілактики ризиків, оскільки інформований користувач є менш вразливим до шахрайства.

Розширення фінансової інклюзії має комплексний вплив на систему фінансової безпеки, що представимо на рисунку 8.8.

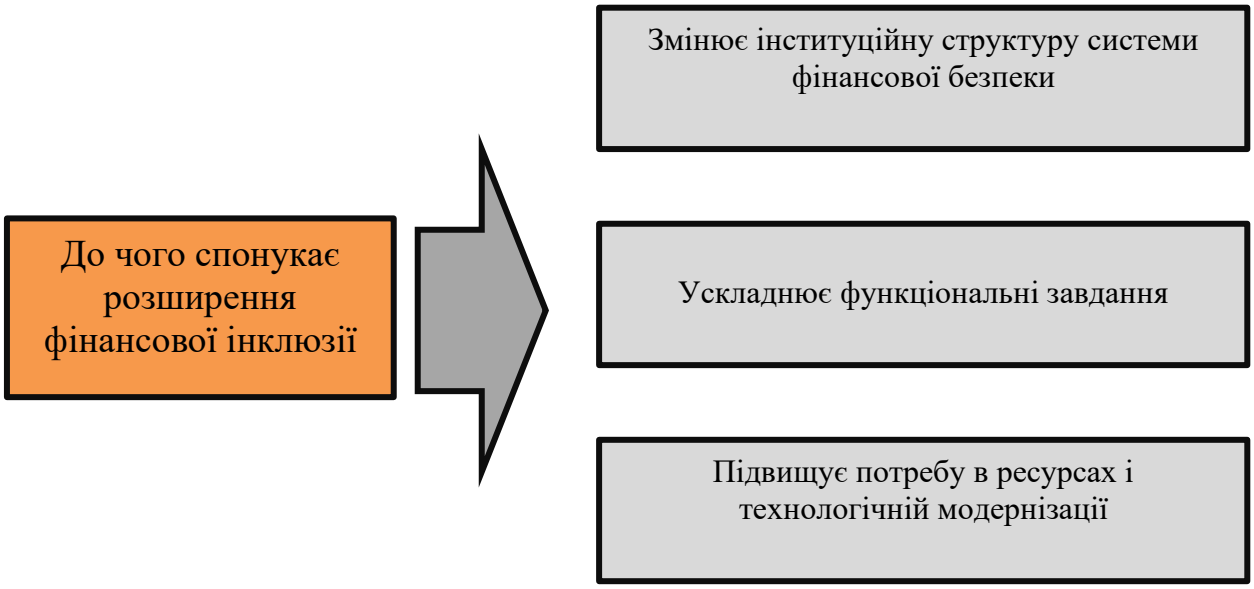


Рис. 8.8. Комплексний вплив розширення фінансової інклюзії на систему фінансової безпеки

Інклюзія сприяє підвищенню прозорості фінансових потоків, зменшенню частки готівкового обігу та детінізації економіки, що в довгостроковій перспективі може зміцнювати фінансову стійкість держави. Ключовим завданням є не обмеження інклюзивних процесів, а їх поєднання з адекватними механізмами управління ризиками.

Система фінансової безпеки в умовах розширення інклюзії повинна бути адаптивною, технологічно оснащеною та орієнтованою на превентивне реагування. Лише за таких умов можливо забезпечити баланс між відкритістю фінансового середовища та його стійкістю до внутрішніх і зовнішніх загроз.

Інклюзивна політика у фінансовій сфері дедалі частіше розглядається не лише як інструмент соціальної рівності, а як складова економічної стійкості держави. Розширення доступу до банківських рахунків, кредитних ресурсів, страхових продуктів і цифрових платіжних сервісів формує ширшу базу учасників фінансових відносин. Це впливає на структуру грошових потоків, рівень формалізації економічної діяльності та здатність фінансової системи протистояти внутрішнім і зовнішнім шокам.

Збільшення кількості користувачів, особливо тих, хто раніше перебував поза межами формального сектору, створює додаткові виклики для регуляторів і фінансових установ. Ризики пов'язані з низькою фінансовою грамотністю, недосконалістю цифрової інфраструктури, можливостями зловживань та кіберзагрозами. Отже, інклюзія виступає джерелом зміцнення фінансової стійкості та фактором, що вимагає посилення механізмів контролю й управління ризиками (табл. 8.9).

Таблиця 8.9

Позитивні наслідки інклюзивної політики для фінансової стійкості та потенційні ризики інтеграції нових учасників

Напрям впливу	**Позитивні наслідки для фінансової стійкості**	**Потенційні ризики інтеграції**	**Умови мінімізації ризиків**
Розширення доступу до банківських рахунків	Зростання обсягу офіційних грошових потоків; детінізація доходів	Використання рахунків для шахрайських операцій	Посилений фінансовий моніторинг, ідентифікація клієнтів
Залучення малого бізнесу до кредитування	Підвищення економічної активності; розширення податкової бази	Підвищений кредитний ризик через нестабільність нових позичальників	Ризик-орієнтоване кредитування, гарантійні фонди
Поширення цифрових платіжних сервісів	Зменшення частки готівки; прозорість транзакцій	Кіберзлочинність, витік персональних даних	Інвестиції в кіберзахист, цифрова грамотність
Фінансова інтеграція соціально вразливих груп	Зниження соціальної напруги; стабілізація споживчого попиту	Низький рівень розуміння фінансових продуктів	Освітні програми та консультаційна підтримка
Інклюзивні страхові та пенсійні програми	Розподіл ризиків у суспільстві; довгострокова фінансова стабільність	Неправильна оцінка страхових ризиків	Актуарний контроль, державний нагляд

Напрям впливу	Позитивні наслідки для фінансової стійкості	Потенційні ризики інтеграції	Умови мінімізації ризиків
Розвиток фінтех-сектору	Підвищення конкуренції та ефективності фінансових послуг	Регуляторні прогалини та технологічні збої	Оновлення нормативної бази, тестування інновацій
Інтеграція державних соціальних виплат у банківську систему	Підвищення прозорості бюджетних операцій	Нецільове використання коштів	Цифрове відстеження та аудит програм
Зростання безготівкових операцій	Покращення аналітики фінансових потоків	Концентрація ризиків у цифровій інфраструктурі	Резервні системи та диверсифікація каналів
Підвищення фінансової грамотності населення	Зниження рівня фінансових помилок і шахрайства	Тимчасове зростання витрат на навчальні програми	Державні та приватні освітні ініціативи

Інклюзивна політика у фінансовій сфері має багатовекторний вплив. Вона здатна посилити фінансову стійкість через розширення формального сектору економіки, зростання прозорості та диверсифікацію фінансових потоків. Інтеграція нових учасників до фінансового середовища супроводжується ризиками, які потребують системного регуляторного, технологічного та освітнього супроводу.

Ефективність інклюзивної політики визначається не лише масштабом залучення, а й якістю управління ризиками. Поєднання відкритості фінансової системи з належними механізмами контролю та захисту здатне забезпечити її довгострокову стійкість.

В наступній таблиці наведемо приклади впливу інклюзивної політики на фінансову стійкість та ризиковий профіль системи (табл. 8.10).

Таблиця 8.10

Приклади впливу інклюзивної політики на фінансову стійкість та ризиковий профіль системи

Приклад інклюзивного заходу	Конкретна ситуація / сценарій	Позитивний вплив на фінансову систему	Можливий ризик або ускладнення	Пояснення механізму впливу
Відкриття базових банківських рахунків для населення	Масове підключення громадян до безготівкових розрахунків	Зростання прозорості грошових потоків	Збільшення навантаження на фінансовий моніторинг	Формалізація доходів розширює базу контролю
Програми мікрокредитування для самозайнятих	Надання невеликих кредитів без складної застави	Активізація підприємництва	Підвищений рівень дефолтів	Нові позичальники мають нестабільний дохід
Державні соціальні виплати через банківські картки	Перехід від готівкових виплат до цифрових	Зменшення зловживань у розподілі коштів	Можливість кібератак на платіжну інфраструктуру	Централізована система потребує посиленого захисту
Запуск мобільних фінансових додатків	Спрощений доступ до фінансових послуг у віддалених регіонах	Підвищення фінансової активності населення	Шахрайство через фішингові схеми	Зростає роль цифрової грамотності
Пільгове кредитування малого бізнесу	Розширення участі підприємців у формальному секторі	Зростання податкових надходжень	Неефективне використання коштів	Потребує контролю за цільовим використанням
Страхові програми для аграрного сектору	Залучення фермерів до страхування врожаю	Зменшення фінансових втрат у кризових ситуаціях	Невірна оцінка страхових ризиків	Потребує точних актуарних розрахунків
Впровадження електронної ідентифікації (e-ID)	Дистанційне відкриття рахунків	Прискорення доступу до фінансових послуг	Використання викрадених персональних даних	Потребує багаторівневої верифікації
Підтримка фінтех-стартапів	Поява альтернативних платіжних сервісів	Зростання конкуренції та ефективності	Регуляторні прогалини	Інновації випереджають законодавство

Приклад інклюзивного заходу	Конкретна ситуація / сценарій	Позитивний вплив на фінансову систему	Можливий ризик або ускладнення	Пояснення механізму впливу
Освітні програми з фінансової грамотності	Навчання населення користуван-ню кредитними продуктами	Зменшення кількості прострочених зобов'язань	Тимчасові бюджетні витрати	Інвестиції у знання знижують ризики в майбутньому
Розвиток безготівкової інфраструктури	Поширення POS-терміналів у малих населених пунктах	Скорочення готівкового обігу	Концентрація ризиків у цифрових мережах	Необхідність резервних каналів обслуговування

Наведені приклади демонструють, що інклюзивна політика має подвійний ефект, бо зміцнює фінансову стійкість через розширення формального сектору та підвищення прозорості операцій, але одночасно трансформує ризиковий профіль системи. Характер впливу залежить від рівня регуляторної готовності, технологічного забезпечення та фінансової грамотності населення.

Структурно ***інклюзія*** змінює архітектуру системи безпеки, збільшуючи кількість учасників та точок взаємодії, що потребує вдосконалення координації між державними та приватними інститутами. Функціонально підсилює навантаження на аналітичні, контрольні та превентивні механізми, змушуючи використовувати нові методи ризик-орієнтованого моніторингу, поведінкової аналітики та кіберзахисту. Ресурсне навантаження зростає через потребу в модернізації технологічної інфраструктури, підвищенні кваліфікації персоналу та організації навчальних і просвітницьких програм для користувачів.

Також сприяє детінізації економіки, підвищенню прозорості фінансових потоків, зростанню фінансової стійкості системи та забезпечує більш стабільну податкову базу, розподіл ризиків і довгострокове зміцнення фінансового середовища. Тобто інклюзія не лише створює додаткове навантаження, а й формує умови для підвищення ефективності та стабільності фінансової системи за умови належного управління ризиками.

8.3. Інтегровані системи контролю, моніторингу та аналітики безпекових показників

Сучасні фінансові системи функціонують у складному та динамічному середовищі, де швидкість обігу коштів, різноманітність учасників та цифровізація процесів істотно підвищують вимоги до ефективного управління ризиками. У цьому контексті інтегровані системи контролю, моніторингу та аналітики набувають ключового значення. Вони дозволяють забезпечувати комплексний нагляд за фінансовими потоками, виявляти потенційні загрози та приймати обґрунтовані управлінські рішення на основі даних у режимі реального часу.

Інтегровані системи поєднують різні функціональні рівні: від контролю за операціями до стратегічного аналізу ризиків, що створює можливість не лише реагувати на проблеми, а й прогнозувати їх виникнення. Вони включають автоматизовані механізми перевірки, збору та обробки даних, аналітичні інструменти для оцінки фінансових ризиків, а також централізовані платформи для координації дій різних підрозділів і органів нагляду.

Особлива роль таких систем проявляється в умовах розширення фінансової інклюзії та цифровізації, коли збільшується кількість учасників та обсяг транзакцій. Інтегровані системи дозволяють підтримувати баланс між доступністю фінансових послуг і необхідністю забезпечення стабільності та безпеки фінансової інфраструктури. Вони створюють основу для комплексного підходу до управління ризиками, поєднуючи технологічну ефективність із аналітичним прогнозуванням та стратегічним плануванням.

Інтегровані системи контролю, моніторингу та аналітики у фінансових структурах є складними комплексами, які поєднують технологічні, організаційні та аналітичні компоненти для забезпечення стабільності, прозорості та безпеки фінансової діяльності. Їхня ефективність залежить від дотримання низки принципів побудови та повноти функціонального забезпечення (табл. 8.11).

Таблиця 8.11

Принципи побудови систем

Принцип	Характеристика
Модульності та масштабованості	Система повинна складатися з окремих функціональних модулів, що виконують специфічні завдання (контроль операцій, аналітика ризиків, моніторинг транзакцій). Дозволяє адаптувати систему до змін у масштабі фінансової діяльності або появи нових регуляторних вимог
Єдності даних та централізованого доступу	Всі дані фінансових операцій, аналітичні звіти та контрольні показники мають зберігатися у єдиному інформаційному середовищі. Централізований доступ забезпечує швидке реагування на загрози та унеможливлює дублювання інформації, що підвищує ефективність прийняття рішень
Рівнево-структурної організації	Система будується за принципом багаторівневої організації, де кожен рівень відповідає за певний спектр завдань. Така структура забезпечує узгодженість дій між різними функціональними одиницями
Інтеграції	Використання сучасних технологій збору інформації, включаючи автоматизовані платформи, сенсори, цифрові канали обміну та бази даних, забезпечує оперативність і точність контролю та аналітики
Гнучкості та адаптивності	Система повинна бути здатною адаптуватися до появи нових фінансових продуктів, змін у законодавстві, розширення фінансової інклюзії або зростання обсягу транзакцій. Гнучка архітектура дозволяє швидко інтегрувати нові модулі контролю та аналітики
Безпековості	Захист даних та цілісність інформаційних потоків є основою функціонування інтегрованих систем. Вбудовані механізми кіберзахисту, резервування даних і контроль доступу запобігають витоку, маніпуляціям та несанкціонованому доступу

Принципи побудови інтегрованих систем контролю, моніторингу та аналітики визначають їхню здатність ефективно забезпечувати фінансову безпеку та стабільність. Модульність і масштабованість дозволяють адаптувати систему до змін у обсязі та складності фінансових потоків, а централізований доступ до даних забезпечує узгодженість і швидкість прийняття рішень. Багаторівнева організація та інтеграція сучасних технологій збору й обробки інформації сприяють комплексному контролю та прогнозуванню ризиків. Гнучкість і захищеність системи гарантують її адаптацію до нових фінансових продуктів, цифрових сервісів та загроз, створюючи основу для надійного і

стабільного функціонування фінансової структури.

В наступній таблиці представимо функціональні можливості систем (табл. 8.12).

Таблиця 8.12

Функціональні можливості систем

Можливості	Характеристика
Моніторинг фінансових операцій у реальному часі	Система відстежує всі операції за рахунками, кредитами, платежами та іншими фінансовими продуктами. Дозволяє виявляти аномальні транзакції та запобігати шахрайству або незаконним діям
Контроль дотримання нормативних вимог	Інтегровані системи забезпечують автоматичну перевірку відповідності операцій регуляторним стандартам, внутрішнім політикам банків або фінансових установ. Знижує ймовірність порушень та штрафних санкцій
Аналітика ризиків та прогнозування	Використовуючи історичні дані, системи формують оцінку ризиків для окремих учасників, продуктів або напрямів діяльності. Дозволяє фінансовим установам планувати заходи для зниження ризикових факторів та підвищення стабільності
Системи раннього попередження	На основі алгоритмів виявлення аномалій та кореляцій даних система генерує сигнали для оперативного реагування на потенційні загрози, що дозволяє попереджати кризові ситуації до їх виникнення
Звітування та підтримка прийняття рішень	Інтегровані системи формують аналітичні звіти для керівництва фінансових установ і регуляторів, що спрощує стратегічне планування та прийняття обґрунтованих рішень
Інтеграція з зовнішніми джерелами інформації	Система здатна обмінюватися даними з державними органами, кредитними бюро, міжнародними платформами та іншими фінансовими інститутами, що підвищує ефективність контролю та аналітики на глобальному рівні

Функціональні можливості інтегрованих систем контролю, моніторингу та аналітики забезпечують всебічне управління фінансовими процесами та ризиками. Вони дозволяють відстежувати операції у реальному часі, контролювати відповідність нормативним вимогам, оцінювати та прогнозувати ризики, а також своєчасно реагувати на потенційні загрози. Аналітичні інструменти та системи раннього попередження сприяють обґрунтованому прийняттю рішень, підвищують прозорість і ефективність фінансової діяльності. Завдяки інтеграції з внутрішніми та зовнішніми джерелами даних, такі системи створюють комплексну основу для забезпечення стійкості та безпеки фінансової структури.

Принципи побудови та функціональні можливості інтегрованих систем контролю, моніторингу та аналітики формують фундамент для комплексного управління фінансовими ризиками. Забезпечують баланс між доступністю фінансових послуг і безпекою, дозволяють прогнозувати загрози, підвищувати ефективність внутрішніх процесів і зміцнювати фінансову стійкість установ та економічної системи в цілому.

На практиці інтегровані системи контролю реалізуються не лише як технічні платформи, а як комплекс організаційних, технологічних і аналітичних рішень, здатних підтримувати прийняття управлінських рішень у реальному часі.

Практичне застосування таких систем охоплює контроль транзакцій, моніторинг ризикових операцій, аналітику фінансових потоків і прогнозування потенційних загроз. Особлива важливість інтегрованого підходу проявляється у взаємодії між різними підрозділами установи та регуляторними органами. Така система дозволяє координувати дії контролю, аналізу та реагування, підвищуючи ефективність управління ризиками та мінімізуючи людський фактор.

У практичному аспекті інтегровані системи повинні забезпечувати баланс між доступністю фінансових послуг та їх безпекою, поєднуючи технологічні можливості з організаційною дисципліною та аналітичним потенціалом. Впровадження таких систем стає критичним елементом для стійкого розвитку фінансових структур у сучасних умовах цифровізації та розширення фінансової інклюзії.

Практичне впровадження інтегрованих систем контролю забезпечує комплексний нагляд за фінансовими процесами, дозволяє прогнозувати ризики, координувати дії різних підрозділів та підвищує прозорість діяльності фінансових установ. Ефективність таких систем визначається здатністю поєднувати технологічну інфраструктуру з організаційними механізмами та аналітичними інструментами, що забезпечує стійкість та безпеку фінансової системи (табл. 8.13).

Таблиця 8.13

Практичні аспекти сутності інтегрованих систем контролю у фінансових структурах

Напрям практичного застосування	Конкретна функція	Приклад реалізації	Практичний ефект
Контроль транзакцій	Виявлення аномальних або підозрілих операцій	Автоматичне відстеження великих переказів або транзакцій із високим ризиком	Зниження ризику шахрайства та фінансових порушень
Моніторинг ризикових профілів	Оцінка фінансового стану клієнтів та бізнесу	Системи рейтингу кредитоспроможності або ризикових сегментів	Зменшення дефолтів та втрат для установи
Аналітика фінансових потоків	Аналіз структурованих і неструктурованих даних	Побудова дашбордів для керівництва з фінансових показників	Підвищення прозорості і контрольованості операцій
Прогнозування загроз	Сценарний аналіз потенційних кризових ситуацій	Моделі ризику від коливань ринку або нестабільних партнерів	Оперативне планування заходів і запобігання втратам
Координація між підрозділами	Узгоджене реагування на інциденти	Централізована платформа для взаємодії між аналітичним, операційним та контролюючим підрозділами	Швидке локалізування і нейтралізація проблемних ситуацій
Регуляторна інтеграція	Автоматична звітність та відповідність нормативам	Передача даних до наглядових органів у стандартизованому форматі	Зменшення ризику санкцій та покарань
Підтримка прийняття рішень	Генерація аналітичних рекомендацій	Алгоритми оцінки ризиків, прогнозування доходів та оптимізації ресурсів	Підвищення ефективності стратегічного та тактичного управління
Захист і безпека даних	Контроль доступу та захист інформації	Шифрування, багаторівнева автентифікація, резервування	Зниження ймовірності витоку або компрометації фінансових даних

Стабільність сучасної економіки значною мірою визначається здатністю фінансових структур ефективно контролювати та аналізувати власну діяльність, а також відстежувати ризики на рівні окремих інститутів і ринку в цілому. Моніторинг та аналітика у фінансових структурах виступають ключовими інструментами для прийняття обґрунтованих рішень, забезпечення прозорості та оперативного реагування на загрози.

Моніторинг у фінансовому контексті охоплює відстеження транзакцій, зміни в активних портфелях, динаміку ринку та поведінку учасників. Аналітика дозволяє перетворювати зібрані дані на прогнозні моделі, оцінювати ризики, виявляти потенційні кризові сценарії та виробляти стратегії запобігання втратам. Спільне використання моніторингових і аналітичних систем дозволяє фінансовим установам поєднувати оперативний контроль із стратегічним плануванням, що стає критично важливим для підтримки стабільності та стійкості економіки в умовах швидких змін і цифровізації фінансового середовища.

Моніторинг (з точки зору фінансової сфери) – це систематичне спостереження, оцінка та контроль фінансових потоків, операцій та показників діяльності організацій чи ринку з метою своєчасного виявлення відхилень, оцінки ризиків, забезпечення фінансової стабільності та прийняття обґрунтованих управлінських рішень.

Аналітика (з точки зору фінансової сфери) – це процес збору, систематизації та оцінки фінансових даних з метою виявлення закономірностей, прогнозування фінансових результатів, оцінки ризиків та підтримки обґрунтованого прийняття управлінських рішень у межах організацій або фінансового ринку загалом.

Ефективність моніторингу та аналітики залежить не лише від технологічного забезпечення, а й від організаційної структури, кваліфікації

персоналу та інтеграції з регуляторними органами, що забезпечує комплексний підхід до управління фінансовими ризиками.

Представимо в наступній таблиці основні напрями моніторингу у фінансових структурах (табл. 8.14).

Таблиця 8.14

Основні напрями моніторингу у фінансових структурах

Напрям моніторингу	Конкретні показники	Приклад реалізації	Практичний ефект
Транзакційний моніторинг	Обсяг і частота операцій, суми переказів	Автоматичне відстеження великих або аномальних переказів	Виявлення шахрайських схем і підозрілих операцій
Моніторинг клієнтських профілів	Кредитний рейтинг, фінансова активність	Системи оцінки ризиків клієнтів та сегментація	Зменшення дефолтів та покращення управління кредитним портфелем
Ринковий моніторинг	Коливання курсів валют, ставок, цінних паперів	Аналітичні платформи для фінансових ринків	Своєчасне виявлення ризикових тенденцій і стратегічне планування
Регуляторний моніторинг	Виконання нормативів, внутрішніх політик	Автоматична генерація звітності для контролюючих органів	Зменшення ризику санкцій та підвищення прозорості діяльності
Інфраструктурний моніторинг	Доступність платіжних систем, стан IT-ресурсів	Системи контролю працездатності серверів і каналів зв’язку	Підвищення надійності фінансових операцій та зменшення технічних збоїв

Моніторинг охоплює не лише відстеження транзакцій і поведінки клієнтів, а й аналіз ринкових показників, дотримання нормативів та стан технологічної інфраструктури. Систематичне впровадження цих напрямів дозволяє фінансовим установам своєчасно виявляти відхилення від встановлених стандартів, передбачати потенційні ризики та оперативно реагувати на нестандартні ситуації. Зокрема, транзакційний та клієнтський моніторинг

забезпечують контроль за безпекою операцій і мінімізацію фінансових втрат, ринковий і регуляторний контроль забезпечує стабільність та відповідність нормативам, а інфраструктурний контроль забезпечує безперебійну роботу систем.

Таким чином, комплексний моніторинг у фінансових структурах виступає ключовим інструментом підтримки прозорості, фінансової дисципліни та стійкості системи загалом, створюючи надійну основу для ефективного управління ризиками та забезпечення стабільного розвитку економіки.

Аналітика у фінансових структурах відіграє ключову роль у забезпеченні стабільності, прозорості та ефективності фінансової діяльності. Особлива цінність аналітики полягає у її здатності перетворювати великі обсяги даних на зрозумілі показники та рекомендації, що дозволяє керівництву приймати точні та своєчасні рішення, підвищуючи стійкість і конкурентоспроможність фінансової структури в умовах швидких змін на ринку (табл. 8.15).

Таблиця 8.15

Основні напрями аналітики у фінансових структурах

Напрям аналітики	**Методи /Інструменти**	**Приклад використання**	**Практичний ефект**
Аналіз ризиків	Моделі кредитного, ринкового та операційного ризику	Оцінка потенційних втрат при зміні ринкових умов	Зменшення фінансових втрат та оптимізація резервів
Прогнозування фінансових потоків	Статистичне моделювання, сценарний аналіз	Визначення очікуваних доходів та витрат	Підвищення точності планування та управління ліквідністю
Аналітика поведінки клієнтів	Кореляційний аналіз, кластеризація	Виявлення тенденцій у споживанні фінансових продуктів	Поліпшення продуктового портфеля та маркетингових стратегій
Антикризова аналітика	Імплементація сигналів раннього попередження, стрес-тестування	Виявлення потенційних кризових сценаріїв	Своєчасне запобігання кризовим ситуаціям і збиткам

Напрям аналітики	Методи /Інструменти	Приклад використання	Практичний ефект
Регуляторна аналітика	Порівняння показників з нормативами та стандартами	Підготовка аналітичних звітів для регуляторів	Підвищення відповідності та прозорості фінансової діяльності

Аналіз ризиків, прогнозування фінансових потоків та аналітика поведінки клієнтів створюють основу для мінімізації втрат, підвищення ефективності використання ресурсів та формування стійких фінансових стратегій. Антикризова та регуляторна аналітика забезпечують своєчасне реагування на зовнішні і внутрішні загрози, сприяючи дотриманню нормативних вимог та збереженню фінансової дисципліни.

Таким чином, комплексне застосування аналітичних інструментів у фінансових структурах не лише підвищує прозорість і контрольованість діяльності, а й створює основу для стабільності та довгострокової стійкості фінансової системи в умовах динамічного ринку.

Інтегровані системи контролю, моніторингу та аналітики в сучасних фінансових структурах є критично важливими інструментами підтримки стабільності та стійкості економіки. Вони дозволяють поєднувати збір даних, оперативний контроль та аналітичну оцінку фінансових потоків, що дає змогу своєчасно виявляти ризики, прогнозувати фінансові наслідки та приймати обґрунтовані управлінські рішення.

Практичне застосування цих систем проявляється у різних сферах: від контролю великих транзакцій та оцінки ризикових профілів клієнтів до прогнозування ринкових тенденцій та інтеграції з регуляторними органами. В умовах глобалізації фінансових ринків та цифровізації послуг інтегровані системи стають ключовим елементом забезпечення прозорості, ефективності та безпеки фінансових операцій.

Нижче наведено дві таблиці, які ілюструють приклади практичного використання інтегрованих систем у світі та в Україні. Перша таблиця

демонструє міжнародний досвід (табл. 8.16), друга систематизує реальні кейси українських фінансових установ (табл. 8.17).

Таблиця 8.16

Приклади практичного застосування інтегрованих систем контролю, моніторингу та аналітики у світі

Країна / Установа	Система / Ініціатива	Практичне застосування	Джерело / Пояснення
Велика Британія, Barclays	Поведінкова аналітика та моніторинг транзакцій	Створення індивідуальних профілів клієнтів для виявлення підозрілих операцій і швидкого реагування	Використання поведінкової аналітики для профілів клієнтів та запобігання підозрілим транзакціям, що показують аномальні моделі поведінки
США, JPMorgan Chase	Аналітика та контроль транзакцій у реальному часі	Виявлення та запобігання шахрайству шляхом моніторингу великих обсягів платежів і транзакцій	У світових банках, включно з JPMorgan, системи обробки даних і аналітики дозволяють ефективно контролювати платежі та ризики
Іспанія, Banco Santander	Big Data моніторинг ризикових операцій	Аналіз великих даних для виявлення аномалій у поведінці клієнтів, що може вказувати на шахрайство чи відмивання грошей	Аналітика великих даних використовується для динамічного оцінювання ризиків у реальному часі
Німеччина, SCHUFA / Deutsche Bank	Скорингові моделі для оцінки кредитного ризику	Використання агрегованих даних із банків і реєстрів для оцінки кредитоспроможності	Моделі скорингу застосовуються у Deutsche Bank через SCHUFA та інші сервіси
Канада (RBC, TD Bank)	Різноманітні моделі ризику та поведінкова аналітика	Поєднання класичних фінансових показників та поведінкових даних для прогнозування ризиків	Банки застосовують комбіновані моделі для оцінки ризику клієнтів

Таблиця 8.17

Приклади практичного застосування інтегрованих систем контролю, моніторингу та аналітики в Україні

Установа	Система / Рішення	Практичне застосування	Пояснення та джерела
ПриватБанк	Системи фінансового моніторингу та аналітики	Застосовують автоматичні алгоритми для виявлення підозрілих транзакцій, аналіз поведінки клієнтів, виявлення ризикових операцій	Українські банки активно впроваджують технологічні системи для моніторингу фінансових операцій і виявлення ризиків
ПУМБ	Моніторинг та автоматизація банківських процесів	Аналітичні сервіси для підвищення ефективності фінмоніторингу, зниження ручної обробки даних	Українські практики включають автоматизацію фінансового моніторингу та регуляторної звітності
Ощадбанк	Аналітика фінансових показників та прогнозування	Застосовуються аналітичні модулі для оцінки руху грошових потоків, управління ліквідністю	Вибір аналітичних модулів спрямований на прогнозування і управління ресурсами
Райффайзен Банк Аваль	Кредитний моніторинг	Системи оцінки та моніторингу кредитоспроможності і для зменшення ризику невиплат	Застосування автоматизованого аналізу кредитних портфелів
Національний банк України (регулятор)	Централізовані платформи моніторингу ризиків	Збір і аналіз даних від банків для оцінки стану фінансової системи та ризиків	Системний фінансовий моніторинг є частиною регуляторного контролю за банківським сектором

Практичне застосування інтегрованих систем контролю, моніторингу та аналітики у світі та в Україні демонструє їхню ключову роль у забезпеченні фінансової стабільності. Вони дозволяють об’єднувати технології збору даних, аналітичні модулі та механізми управління ризиками, що підвищує ефективність роботи фінансових установ та зміцнює стійкість економіки в умовах динамічних

змін на ринку.

Інтегровані системи контролю, моніторингу та аналітики у фінансових структурах виступають фундаментальним інструментом забезпечення стабільності, прозорості та ефективності фінансової діяльності. Вони поєднують оперативний контроль транзакцій, аналітичну оцінку фінансових показників і прогнозування ризиків, що дозволяє своєчасно виявляти загрози та ухвалювати обґрунтовані управлінські рішення.

Практичне застосування таких систем, як показано у світових і українських прикладах, демонструє їхню здатність підвищувати ефективність управління ризиками, оптимізувати процеси прийняття рішень та підтримувати ліквідність і фінансову стійкість організацій. Автоматизація збору даних і інтеграція аналітичних модулів дозволяють значно скоротити час реакції на потенційні загрози, мінімізувати людський фактор і підвищити якість контролю фінансових потоків.

Таким чином, інтегровані системи контролю, моніторингу та аналітики не обмежуються лише внутрішнім наглядом за фінансовими операціями: вони створюють комплексний механізм підтримки стабільності фінансового середовища, забезпечують прозорість діяльності та сприяють зміцненню довіри до фінансових інститутів на національному та міжнародному рівні. Їх впровадження стає невід’ємною складовою стратегічного розвитку сучасної економіки.

8.4. Контрольні питання для самоперевірки

11. Які передумови зумовили перехід від фрагментарного до інтегрованого підходу в управлінні фінансовою безпекою?

12. У чому полягає відмінність інтегрованої моделі управління фінансовою безпекою від традиційних функціональних моделей?

13. Як взаємодіють фінансова, економічна та інституційна складові в межах інтегрованої моделі фінансової безпеки?

14. Яку роль відіграє система ризик-менеджменту в побудові інтегрованих моделей фінансової безпеки?

15. Чому узгодженість стратегічного та оперативного рівнів управління є критичною для забезпечення фінансової безпеки?

16. Яким чином інтегровані моделі управління фінансовою безпекою враховують вплив зовнішнього середовища?

17. Як цифровізація фінансових процесів змінює підходи до інтегрованого управління фінансовою безпекою?

18. Які показники доцільно використовувати для оцінювання ефективності інтегрованої моделі фінансової безпеки?

19. Які обмеження та ризики можуть виникати під час впровадження інтегрованих моделей управління фінансовою безпекою?

20. Як інтегровані моделі управління фінансовою безпекою адаптуються до умов нестабільності та кризових явищ?

Розділ 9

Автор:
Оксана Десятнюк

ЦИФРОВІ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШАХРАЙСТВА ТА ЗАГРОЗ ФІНАНСОВІЙ БЕЗПЕЦІ

РОЗДІЛ 9. ЦИФРОВІ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШАХРАЙСТВА ТА ЗАГРОЗ ФІНАНСОВІЙ БЕЗПЕЦІ

«Потрібні роки, щоб створити репутацію, і кілька хвилин, щоб її зруйнувати.»

Воррен Баффет

9.1. Поняття і види фінансового шахрайства в цифровому середовищі

Розширення використання цифрових технологій та електронних платіжних систем спричинило зростання кількості зловживань у фінансовій сфері. Сьогодні деструктивний вплив шахрайства охоплює більшість сфер суспільних відносин, виходячи за межі фінансово-кредитного та страхового секторів і поширюючись на зовнішньоекономічну діяльність та кіберпростір.

За даними міжнародних експертів, світові збитки від шахрайства та економічних злочинів щорічно сягають приблизно 6,3 трлн дол. США. На рівні окремих підприємств статистика показує, що фінансові махінації можуть зменшувати середньорічний прибуток компанії до 5 %.

Етимологічний аналіз свідчить, що категорія «фінансове шахрайство» є похідною від базового, більш широкого поняття «шахрайство». В історичній ретроспективі на українських землях цей термін мав чітко виражене негативне забарвлення. Ним позначали осіб, чия поведінка характеризувалася скритністю та недоброчесністю. Різноманіття синонімів в українській мові для позначення цього явища свідчить про те, що діяльність таких осіб базувалася на хитрості, обмані та схильності до маніпуляцій.

У Великому тлумачному словнику сучасної української мови поняття ***«шахрайство»*** визначається таким чином: «1) хитрий і спритний обман;

крутійство; ошуканство; 2) заволодіння індивідуальним майном громадян або набуття права на майно шляхом обману чи зловживання довірою».

Відповідно до тлумачення, наведеного в Юридичному словнику Мерріама-Вебстера, ***під шахрайством розуміють***: «Будь-яку дію, висловлювання, упущення або приховування, що має на меті обдурити іншу особу з метою отримання вигоди, зокрема, неправдиве представлення або приховування фактів, що мають істотне значення для угоди, з усвідомленням їх неправдивості. Або з необережним нехтуванням їх правдивості чи неправдивості та з наміром обдурити іншу особу, яка обґрунтовано покладається на ці факти і тим самим зазнає шкоди».

У сфері фінансового контролю та аудиту особливо важливо чітко розрізняти поняття «шахрайство» та «помилка». Хоч обидва явища здатні спричиняти викривлення фінансової інформації та завдавати збитків, їхня правова та психологічна природа істотно відрізняється.

Помилка – це випадкове викривлення даних, яке виникає через неуважність, хибну інтерпретацію фактів, арифметичні неточності або недосконаліть облікових процедур.

Відповідно до положень МСА 240 «Відповідальність аудитора, що стосується шахрайства, при аудиті фінансової звітності», «***шахрайство*** є навмисною дією одного або більше осіб серед керівництва, управлінського персоналу, співробітників або третіх сторін, що полягає у використанні обману для одержання неправомірної або незаконної вигоди».

На відміну від шахрайства, помилка не спрямована на обман або отримання незаконної вигоди. Ключовим критерієм розмежування цих двох понять є умисел. Розуміння цієї відмінності є фундаментом для побудови стратегії виявлення зловживань. Якщо аудитор або фахівець з безпеки знаходить ознаки системності, спроби приховування фактів та наявність мотиву, він повинен перекваліфікувати свої підозри з «можливої помилки» на «ймовірне шахрайство» і застосувати відповідні спеціалізовані процедури розслідування.

Системне порівняння цих понять за ключовими критеріями наведено у таблиці 9.1.

Таблиця 9.1

Порівняльна характеристика понять «помилка» та «шахрайство» в аудиті

Критерій порівняння	Помилка	Шахрайство
Наявність умислу	Відсутній	Є визначальною ознакою
Мотив	Відсутній (ненавмисна дія)	Особисте збагачення або інша вигода
Ризик невиявлення аудитором	Менший (порівняно з шахрайством)	Високий (через активне приховування)
Ефективність системи внутрішнього контролю	Більш ефективна для виявлення помилок	Менш ефективна (шахрайство часто передбачає змову та обхід контролю)
Вплив на фінансову звітність	Залежить від рівня суттєвості помилки	Завжди призводить до спотворення звітності

Виникнення ненавмисних помилок у фінансовому обліку та звітності зазвичай зумовлене наступними причинами:

- *кадровий фактор* (недостатній рівень професійної компетентності та кваліфікації працівників);
- *організаційний фактор* (відсутність або низька ефективність системи внутрішнього контролю);
- *особистісний (людський) фактор* (допущення неточностей через неуважність, поспіх, втому або необачність персоналу);
- *операційний фактор* (наявність складних операцій).

Відповідно до нормативних вимог, основна відповідальність за достовірність фінансової звітності та за впровадження механізмів своєчасного виявлення й запобігання як помилкам, так і шахрайству лежить безпосередньо на керівництві підприємства.

Згідно зі ст. 190 Кримінального кодексу України, ***шахрайство*** визначається як «заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою».

Хоча законодавець виокремлює обман і зловживання довірою як фундаментальні ознаки шахрайства, що дозволяють кваліфікувати його окремо від інших майнових посягань, ці способи заволодіння цінностями не є

унікальними. Зазначені способи вчинення злочину є критеріями розмежування шахрайства та інших злочинів проти власності, зокрема крадіжки. Характерною ознакою цього правопорушення є те, що передача майна або прав на нього здійснюється потерпілим добровільно, під впливом омани.

Також згідно зі ст. 190 Кримінального кодексу України встановлюється диференційована відповідальність за шахрайство, яка залежить від ступеня суспільної небезпеки діяння, розміру завданої шкоди та способу вчинення злочину (табл. 9.2).

Таблиця 9.2

Кримінальна відповідальність за шахрайство (ст. 190 КК України)

Кваліфікуючі ознаки (склад злочину)	**Санкції (види та межі покарання)**
Протиправне заволодіння чужим майном або отримання права на нього, здійснене із застосуванням обману чи зловживання довірою (за відсутності обтяжуючих обставин)	штраф: 2000–3000 неоподатковуваних мінімумів доходів громадян; громадські роботи: 200–240 год. виправні роботи: до 2 років; пробаційний нагляд: до 3 років; обмеження волі: до 3 років
Діяння, що характеризується хоча б однією з таких ознак: • повторюваність злочину; • вчинення групою осіб за попередньою змовою; • спричинення потерпілому шкоди у значному розмірі	штраф: 3000–4000 неоподатковуваних мінімумів доходів громадян; виправні роботи: 1–2 роки; обмеження волі: до 5 років; позбавлення волі: до 3 років
Шахрайство, вчинене в умовах воєнного або надзвичайного стану, яке призвело до завдання значної шкоди потерпілому	штраф: 4000–8000 неоподатковуваних мінімумів доходів громадян; позбавлення волі: 3–5 років
Діяння, вчинене: • у великих розмірах; • шляхом неправомірного втручання з використанням комп'ютерних систем та електронної техніки	позбавлення волі: 3–8 років
Діяння, що характеризується найвищим ступенем суспільної небезпеки: • вчинене в особливо великих розмірах; • здійснене у складі організованої групи	позбавлення волі: 5–12 років; обов'язкове додаткове покарання: конфіскація майна

Стаття 222 Розділу VIII Кримінального кодексу України «Кримінальні правопорушення у сфері господарської діяльності» визначає ***«шахрайство з фінансовими ресурсами»*** як «надання завідомо неправдивої інформації органам державної влади, органам влади АР Крим чи органам місцевого самоврядування,

банкам або іншим кредиторам з метою одержання субсидій, субвенцій, дотацій, кредитів чи пільг щодо податків».

Слід зауважити, що наведене законодавче трактування має обмежений характер. Воно стосується виключно посягань на ресурси держави або суб'єктів господарювання, залишаючи поза увагою фінансові інтереси окремих громадян. Крім того, це визначення не охоплює низку суміжних протиправних діянь, таких як корупція, хабарництво, привласнення майна чи використання викрадених персональних даних для збагачення.

Ключовим нормативним документом, що визначає алгоритм дій аудитора при перевірці фінансової звітності на предмет шахрайства, є Міжнародний стандарт аудиту (МСА) 240. Цей стандарт встановлює, що відповідальність за запобігання та виявлення шахрайства покладається на управлінський персонал та вище керівництво суб'єкта господарювання, тоді як завданням аудитора є «отримання обґрунтованої впевненості у тому, що фінансова звітність не містить суттєвих викривлень».

МСА 240 зобов'язує аудитора ідентифікувати та оцінювати ризики суттєвих викривлень умисного характеру. До таких порушень стандарт відносить дві категорії: викривлення, що є наслідком недобросовісної фінансової звітності, та викривлення, спричинені незаконним привласненням активів. Основні принципи яких має дотримуватися аудитор при виявленні шахрайства можна систематизувати наступним чином:

1. Принцип розмежування відповідальності. МСА 240 чітко встановлює, що первинна відповідальність за запобігання та виявлення шахрайства покладається на осіб, наділених управлінськими повноваженнями, та найвище керівництво суб'єкта господарювання. Вони зобов'язані створити середовище чесного контролю та етичної поведінки.

2. Принцип професійного скептицизму. Стандарт вимагає від аудитора підтримувати позицію професійного скептицизму протягом усього процесу аудиту. Це означає, що аудитор повинен:

- *розглядати як ймовірну наявність суттєвих викривлень через шахрайство, навіть за умови попереднього позитивного досвіду співпраці з клієнтом та довіри до доброчесності керівництва;*
- *критично оцінювати аудиторські докази, не сприймаючи їх автоматично як достовірні;*
- *уважно відстежувати ознаки, що можуть свідчити про шахрайство, і критично оцінювати надані пояснення, якщо вони суперечать наявним доказам.*

Застосування принципу професійного скептицизму передбачає, що аудитор протягом усіх етапів перевірки критично оцінює дії управлінського персоналу, враховуючи можливі кримінологічні аспекти шахрайства. Відповідно до МСА 300 «Планування аудиту фінансової звітності», аудитор має здійснити ідентифікацію та оцінку значущих факторів ще до початку виконання завдання. Це включає попереднє визначення ділянок з підвищеним ризиком суттєвих викривлень, а також оцінку того, як загальний ризик таких викривлень може вплинути на підхід керівництва, здійснення нагляду та організацію роботи аудиторської групи.

3. Ризик-орієнтований підхід (ідентифікація факторів ризику). Цей принцип зобов'язує аудитора активно виявляти та оцінювати ризики суттєвого викривлення фінансової звітності внаслідок шахрайства. Відповідно до положень МСА 315 «Ідентифікація та оцінювання ризиків суттєвого викривлення», аудитор зобов'язаний здійснювати ідентифікацію та оцінку факторів ризику шахрайства, базуючись на глибокому розумінні суб'єкта господарювання та його бізнес-середовища. У цьому контексті поняття ***«суб'єкти господарювання»*** інтерпретується як «конкретні фізичні особи, наділені повноваженнями приймати управлінські рішення щодо фінансової звітності, чиї дії детермінуються як зовнішніми обставинами, так і індивідуальними рисами характеру та ціннісними орієнтаціями».

4. Принцип обов'язкового реагування на ризики. Аудитор не може обмежуватися лише констатацією ризиків. МСА 240 вимагає розробки та впровадження загальних підходів у відповідь на оцінені ризики. Крім того, стандарт визначає обов'язкові процедури, які мають виконуватися під час кожного аудиту для протидії ризику шахрайства з боку управлінського персоналу, зокрема:

- *аналіз журнальних записів та інших коригувань з метою виявлення можливих маніпуляцій у звітності;*
- *аналіз облікових оцінок на предмет наявності упередженості керівництва;*
- *аналіз значних операцій, що виходять за межі звичайної діяльності компанії.*

Відповідно до положень МСА 240, неправдива фінансова звітність кваліфікується як умисне викривлення інформації (включно з навмисним пропуском сум або нерозкриттям обов'язкових даних), метою якого є введення в оману користувачів цієї звітності. Стандарт акцентує увагу на тому, що таке маніпулювання звітністю стає результатом конкретних неправомірних дій, перелік яких систематизовано на рисунку 9.1.

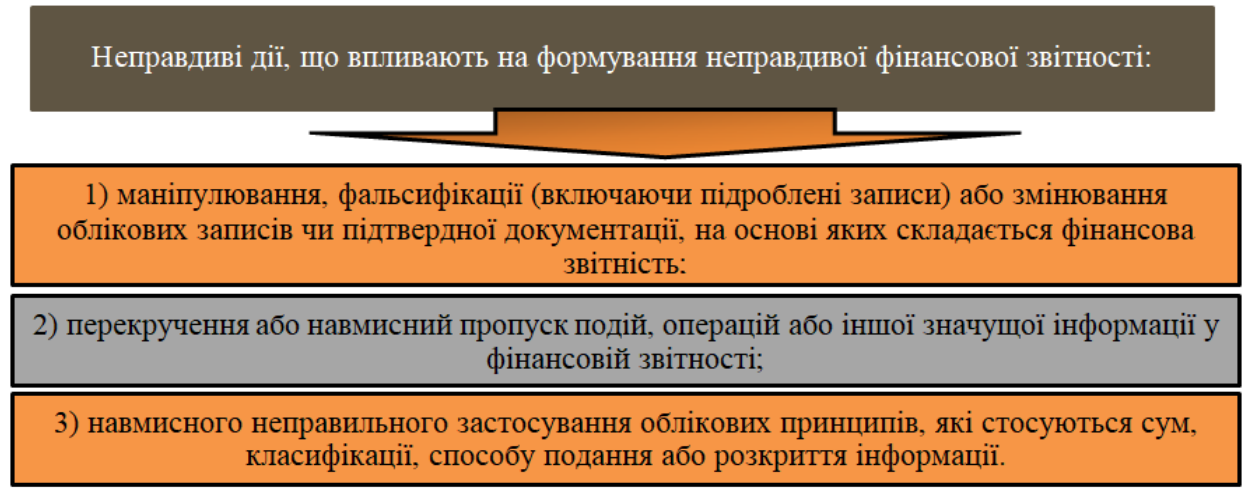


Рис. 9.1. Неправомірні дії, що призводять до викривлення показників фінансової звітності

Оскільки шахрайство належить до категорії кримінальних правопорушень, дослідження передумов його скоєння вимагає застосування спеціалізованих

підходів. Для аналізу природи корпоративних зловживань з боку персоналу загальновизнаною теоретичною конструкцією стала модель «трикутника шахрайства», яка дозволяє систематизувати фактори ризику (рис. 9.2).

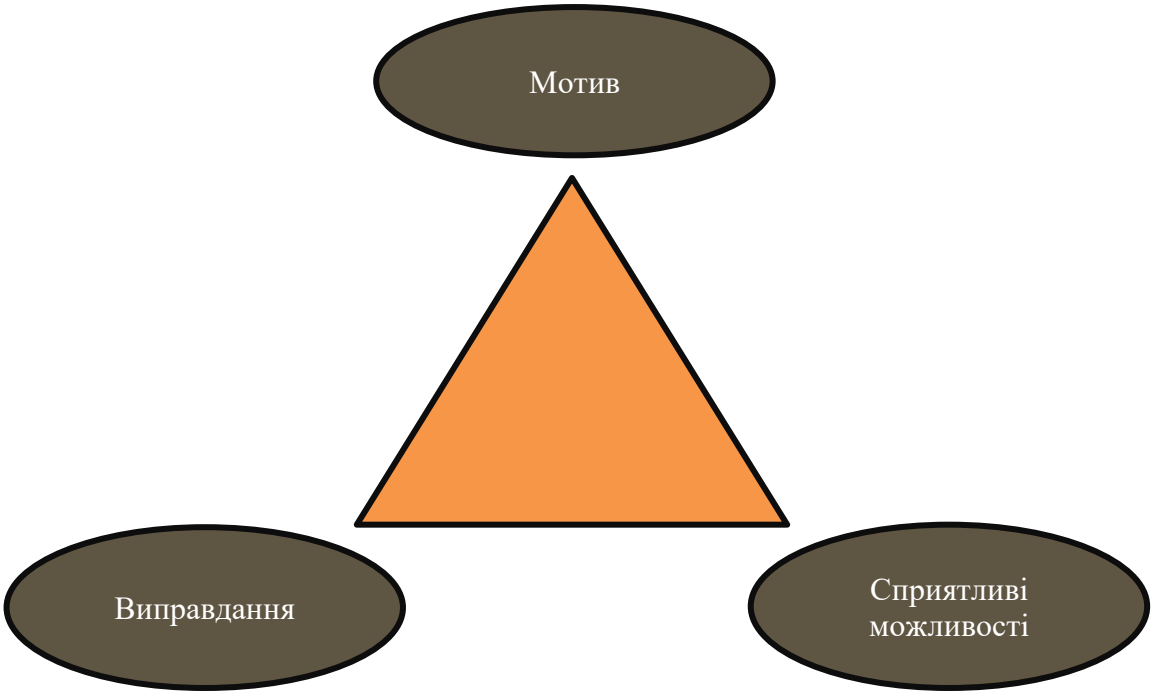


Рис. 9.2. Модель «трикутника шахрайства»

Концептуальна структура даної моделі базується на трьох взаємопов'язаних детермінантах поведінки:

1. Мотив. Це внутрішня рушійна сила, що спонукає особу до вчинення неправомірних дій. Джерелами тиску можуть виступати особисті фінансові труднощі, корисливі мотиви (наприклад, прагнення до збагачення) або фактори робочого середовища, такі як незадоволення оцінкою власної праці чи невиконання обіцянок керівництвом.

2. Виправдання. Психологічний механізм, що дозволяє особі нейтралізувати почуття провини та виправдати свої дії у власних очах. Типовими прикладами є внутрішні переконання на кшталт: «компанія мені заборгувала, я лише відновлюю справедливість» або «я тільки тимчасово позичаю ці кошти».

3. Сприятливі можливості. Об’єктивні умови, що дозволяють вчинити шахрайство та приховати його сліди. Зазвичай вони виникають внаслідок неефективності систем внутрішнього та зовнішнього контролю, а також низького рівня трудової та виконавської дисципліни на підприємстві.

Застосування цього категоріального апарату значно оптимізує процес встановлення причин шахрайських дій та ідентифікації осіб, схильних до їх вчинення. На базі «трикутника шахрайства» розроблено низку прикладних методів виявлення внутрішніх розкрадань на підприємствах.

Методологічний інструментарій виявлення фінансових зловживань на підприємстві охоплює комплекс специфічних заходів. До основних із них належать:

- *раптові перевірки* (інвентаризації, ревізії) дозволяють отримати оперативний та об’єктивний зріз фактичного стану справ на момент проведення заходу, мінімізуючи ризик підготовки з боку персоналу;
- *легендовані контрольні заходи* (наприклад, таємний покупець) дозволяють отримувати достовірну інформацію безпосередньо від джерел шляхом моделювання реальних бізнес-процесів та природної взаємодії зі співробітниками;
- *ретроспективні внутрішні розслідування* спрямовані на детальний аналіз уже вчинених випадків шахрайства для з’ясування обставин і встановлення винних осіб;
- *методи корпоративної розвідки (OSINT, HUMINT)* передбачають аналітичну обробку даних із відкритих джерел, а також інформації, отриманої шляхом опитування персоналу та вивчення службових документів і кореспонденції.

У науковій літературі загальноприйнятою є класифікація детермінант шахрайства за чотирма основними групами факторів (табл. 9.3).

Таблиця 9.3

Класифікація причин виникнення фінансового шахрайства

Група факторів	Причини виникнення
Причини економічного характеру	інтенсифікація обсягів фінансових трансакцій в умовах глобалізації світової економіки; полегшення транскордонного переміщення капіталу, товарів і послуг, що стимулює розширення транснаціональної фінансової злочинності; суттєвий дисбаланс між потенційно високими доходами від шахрайських схем та відносно низькими ризиками фінансових втрат у разі їх викриття; низький рівень життя та наявність гострих фінансових труднощів у значної частини населення, що створює економічні передумови для пошуку незаконних джерел доходу
Причини морально-психологічного характеру	домінування прагнення до швидкого незаконного збагачення та знецінення ролі права власності; індивідуальна схильність деяких осіб до ризикової девіантної поведінки та участі у шахрайських схемах; обмежені знання з фінансової грамотності серед населення, що роблять його більш вразливим до шахрайських впливів
Причини нормативно-правового характеру	наявність прогалин і суперечностей у національному законодавстві щодо протидії фінансовим зловживанням; відсутність чіткого законодавчого визначення повного переліку операцій, які мають підвищений ризик шахрайського привласнення коштів; низька ефективність механізмів юридичної відповідальності через малу ймовірність невідворотного покарання та невідповідність його розміру завданим збиткам
Причини інфраструктурно-організаційного характеру	діджиталізація економічних відносин та зростання частки безконтактних електронних угод (зокрема, в інтернет-торгівлі), що ускладнює процеси контролю та ідентифікації; прискорене удосконалення кіберзлочинних технологій на фоні загального ослаблення захисту та знецінення конфіденційності персональних даних; значна прихованість фінансових шахрайських схем у поєднанні з недостатньою ефективністю роботи правоохоронних органів у частині їх виявлення та розслідування; інституційна слабкість владних структур в організації боротьби з шахрайством, недосконаліть кадрової політики, а також відсутність дієвих механізмів превенції і контролю за поширенням злочинних схем; відсутність прозорих і доступних даних про діяльність фінансових установ та актуальні ризики на фінансовому ринку для широкого кола громадян

Значне різноманіття проявів фінансового шахрайства, що характеризується безперервним удосконаленням інструментарію та адаптацією до нових умов, робить проблематичною його всеохоплюючу класифікацію.

Узагальнену багаторівневу класифікація різновидів фінансового шахрайства, систематизовану за ключовими ознаками наведено у таблиці 9.4.

Таблиця 9.4

Класифікація видів фінансового шахрайства за характерними ознаками

Ознака класифікації	Види фінансового шахрайства
За об'єктом вчинення шахрайських дій	шахрайство з коштами юридичних осіб (корпоративне); шахрайство проти споживачів, інвесторів, вкладників; шахрайство з коштами державного бюджету та цільових фондів; шахрайство з ресурсами місцевих бюджетів та комунальних підприємств; нецільове використання коштів міжнародних донорів та організацій
За суб'єктом вчинення шахрайських дій	вище керівництво (топ-менеджмент), власники; менеджери середньої та нижчої ланки; лінійний персонал (працівники без управлінських функцій); контрагенти (постачальники, підрядники, замовники); фінансові посередники та установи; представники органів влади та контролю; організовані злочинні групи, кіберзлочинці
За сферою (сектором) реалізації здійснення	банківський сектор та небанківські фінансові установи; ринок капіталу та цінних паперів (інвестиційне шахрайство); страховий ринок; державні закупівлі та управління публічними фінансами; сфера електронної комерції (e-commerce) та фінтех (fintech); ринок нерухомості та будівництва; податкова та митна сфери
За способом (механізмом) вчинення	вчинене через пряме введення в оману шляхом свідомого надання недостовірних даних або підробки фактів і документів; вчинене шляхом зловживання довірою; вчинене з використанням службового становища; вчинене за допомогою невербального маніпулятивного впливу; вчинене із застосуванням інших специфічних методів впливу; вчинене із застосуванням комбінованих способів
За ключовим інструментом (схемою) реалізації	маніпуляції зі звітністю: фальсифікація фінансової звітності для приховування збитків або завищення прибутків; привласнення активів: крадіжка грошових коштів, товарно-матеріальних цінностей, незаконне використання активів компанії; корупційні схеми: хабарництво, «відкати», конфлікт інтересів; кібершахрайство: фішинг, вішинг, компрометація корпоративної електронної пошти, шкідливе ПЗ; фінансові піраміди та інвестиційні афери; податкові та платіжні схеми: уникнення сплати податків, інсценування банкрутства, маніпуляції з платіжними засобами
Залежно від характеру розрахунків	готівкові розрахунки; розрахунки на поточний рахунок; розрахунки пов'язані із товарообігом; розрахунки із використанням векселів або чеків; шахрайство пов'язане із кількома видами розрахунків

Однією із основних ознак класифікації шахрайства є саме суб'єкт-ініціатор протиправних дій. Відповідно до цього виокремлюють наступні основні види зловживань:

- *зловживання найманого персоналу (внутрішнє шахрайство) включає розтрати або розкрадання активів, наприклад, через реалізацію схем із закупівлі послуг за завищеними цінами з метою отримання «відкатів»;*
- *шахрайство топ-менеджменту, коли дії керівників, спрямовані, наприклад, на умисне доведення підприємства до неплатоспроможності задля виведення активів;*
- *інвестиційні афери, проведення операцій з інвестування коштів у свідомо збиткові або фіктивні структури з метою їх подальшого привласнення;*
- *шахрайство з боку постачальників, тобто постачання продукції неналежної якості або здійснення маніпуляцій із цінами на сировину та матеріали;*
- *недоброчесні дії замовників (клієнтів) проявляються в умисному невиконанні зобов'язань з оплати виконаних замовлень, зокрема через ініціювання процедури фіктивного банкрутства.*

Слід підкреслити, що незважаючи на широкий спектр зовнішніх загроз, практичний досвід показує: найбільші матеріальні збитки підприємства зазнають саме через недобросовісні дії власного персоналу.

Для систематизації видів економічних злочинів Асоціація сертифікованих фахівців з розслідування шахрайства (ACFE) розробила концептуальну модель, відому як ***«дерево шахрайства»*** (рис. 9.3).

Візуально ця схема розділяє шахрайські дії на три магістральні напрями (гілки):

- *незаконне привласнення активів;*
- *корупційні діяння;*
- *фальсифікація фінансової звітності.*

Кожен із цих напрямів деталізується на специфічні схеми зловживань.

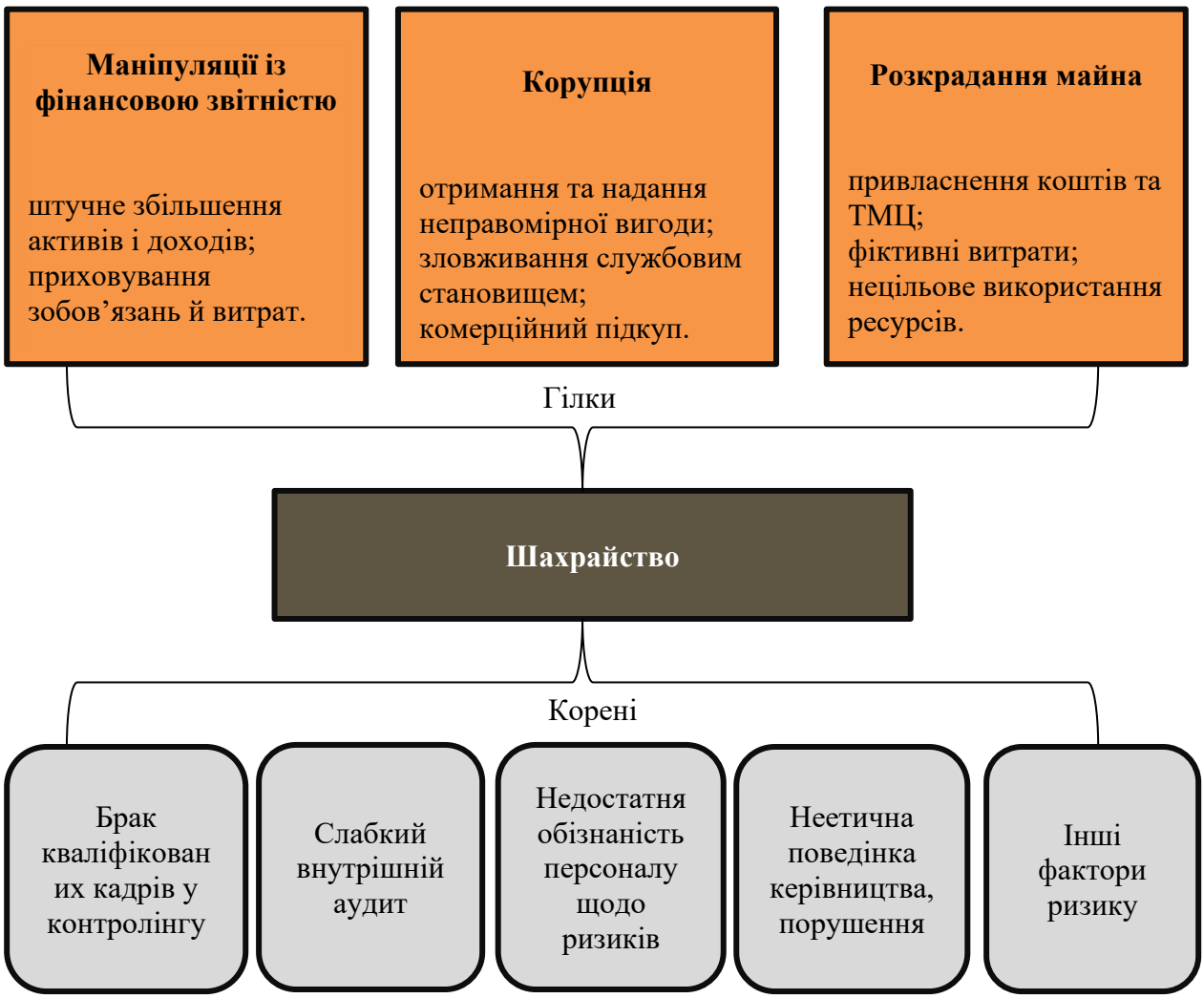


Рис. 9.3. «Дерево шахрайства»

У сучасних умовах цифровізації бізнес-процесів особливе значення набувають види шахрайства, пов'язані з кіберсередовищем та цифровими загрозами.

Згідно зі ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», «***Кіберзагроза*** – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів».

До кола цифрових загроз належать кібератаки, несанкціонований доступ до корпоративних даних, фішингові атаки, витоки конфіденційної інформації, різні форми цифрового шахрайства, а також нові вразливості, пов'язані з маніпуляціями штучним інтелектом. Реалізація цих загроз чинить як прямий, так і опосередкований негативний вплив на економічну безпеку підприємств, їх сталий розвиток та рівень конкурентоспроможності.

Розглянемо найбільш розповсюджені види фінансового шахрайства за ключовим інструментом (схемою) реалізації:

1. Соціальна інженерія. Метод протиправного впливу, що ґрунтується не на технічному втручанні в інформаційні системи, а на застосуванні психологічних прийомів маніпуляції. Її метою є спонукання особи до добровільної передачі конфіденційних відомостей. Зловмисники використовують вразливості людського фактору, зокрема довірливість, страх або неуважність, залучаючи телефонні комунікації та цифрові канали зв'язку. Результатом таких дій стає незаконне отримання персональних даних, облікових записів, паролів чи PIN-кодів безпосередньо від їх власників. Однією з модифікованих форм цього явища є ***кібербулінг***, який розглядається як різновид агресивної поведінки у цифровому середовищі, спрямованої на завдання психологічної та емоційної шкоди особі. Реалізація кібербулінгу переважно здійснюється через соціальні мережі та інші онлайн-платформи.

2. Скімінг. Поширений вид шахрайства, спрямований на компрометацію даних платіжних карток під час їх використання у банкоматах або POS-терміналах. Злочинна схема передбачає встановлення спеціального нештатного обладнання (скімерів) на картоприймач для зчитування інформації з магнітної смуги картки, а також прихованих мікрокамер або накладок на клавіатуру для фіксації PIN-коду. Отримані дані використовуються для виготовлення дублікатів карток.

3. Фішинг. Різновид інтернет-шахрайства, метою якого є несанкціоноване отримання облікових даних користувачів (логінів, паролів, номерів карток). Класична схема реалізується через масову розсилку

електронних листів, що візуально імітують офіційні повідомлення від банків або платіжних сервісів. Листи містять вимогу перейти за посиланням на підроблений веб-сайт (фішингову сторінку) та ввести конфіденційну інформацію для нібито «розблокування рахунку» чи «оновлення даних». Введені дані автоматично потрапляють до зловмисників.

4. Внутрішні кіберзагрози. Виникають у робочому середовищі та походять від людей, які легально працюють у системі. Вони можуть завдати шкоди компанії як навмисно (зливаючи дані чи влаштовуючи саботаж), так і випадково – через власну необережність, що призводить до серйозних проблем. Особливо небезпечними є ситуації, коли для прихованих атак, на кшталт SQL-ін'єкцій, використовуються акаунти з правами адміністратора, адже такі дії дуже складно помітити звичайними методами моніторингу.

SQL-ін'єкція – механізм атаки полягає у впровадженні зловмисних SQL-команд через поля введення даних, що дозволяє хакеру отримати несанкціонований доступ до бази даних. Успішна реалізація такої атаки може призвести до критичних наслідків: компрометації та витоку конфіденційної інформації, знищення даних або повного перехоплення контролю над системою.

5. Фінансові піраміди. Це специфічні псевдоінвестиційні структури, діяльність яких полягає в активному залученні коштів громадян під обіцянки отримання надвисоких прибутків. Економічна суть шахрайства полягає в тому, що виплата дивідендів першим вкладникам здійснюється виключно за рахунок грошових надходжень від нових учасників, а не внаслідок реальної прибуткової господарської діяльності. Організатори таких схем зазвичай декларують можливість швидкого отримання доходу в короткостроковій перспективі, свідомо приховуючи інформацію про критично високі ризики втрати вкладеного капіталу. Часто для надання схемі ознак легітимності вигадуються неіснуючі послуги або інноваційні проєкти. Кінцевою метою організаторів є акумуляція значного обсягу коштів та їх привласнення з подальшим зникненням.

Ефективність процесу ідентифікації осіб, причетних до системного завдання збитків підприємству, залежить від дотримання фахівцем (аудитором, спеціалістом з безпеки) чітко регламентованого алгоритму дій (рис. 9.4).

Рис. 9.4. Алгоритм проведення аудиту на виявлення шахрайства

Стандартизована методика розслідування передбачає послідовне виконання таких етапів: первинна аналітична оцінка, планування, збір доказової інформації, аналіз та перевірка зібраних даних, складання підсумкового звіту та контроль за впровадженням прийнятих рішень. Дотримання цієї логічної послідовності є критично важливим, оскільки порушення етапності може знизити ефективність розслідування.

Оскільки шахрайство є різновидом правопорушення, його ідентифікація вимагає встановлення чотирьох базових ознак:

- *наявності завданої шкоди;*
- *факту протиправної дії (бездіяльності);*
- *причинного зв'язку між ними;*
- *вини суб'єкта.*

Відповідно, при документуванні результатів дослідження перекручень фінансової звітності, спричинених шахрайством, аудитор повинен сформувати доказову базу щодо цих ознак. У звіті необхідно чітко визначити:

- *хто, яким чином і в якому розмірі зазнав матеріальної шкоди;*
- *які саме протиправні дії конкретних посадових осіб спричинили викривлення звітності;*
- *як ці дії безпосередньо призвели до завдання шкоди.*

Визначення вини здійснюється через порівняння дій осіб із їхніми посадовими обов'язками в галузі обліку та звітності. Необхідним елементом цього процесу є отримання та аналіз пояснень від усіх залучених осіб.

Окрім аудиту дієвим механізмом протидії шахрайсту є система внутрішніх перевірок. Специфіка їх проведення дозволяє не лише ідентифікувати осіб, причетних до розкрадань, але й, що важливіше, діагностувати кореневі причини виникнення можливостей для вчинення протиправних дій. На практиці такими детермінантами найчастіше виступають недосконаліть комплаєнс-процедур та неефективне функціонування служби внутрішньої безпеки. За результатами внутрішніх контрольних заходів розробляються рекомендації, спрямовані на посилення системи захисту підприємства від фінансового шахрайства та нейтралізацію процедурних вразливостей, що призвели до матеріальних втрат.

Залучення ***незалежних аудиторських компаній*** часто демонструє вищу ефективність порівняно з перевірками, проведеними державними контролюючими органами. Головною перевагою незалежного аудиту є зменшення ризику стороннього впливу на процес і результати перевірки. Крім того, такий підхід залишає за замовником (керівництвом підприємства) право самостійно обирати способи реагування на виявлені факти фінансових зловживань.

9.2. Типові «червоні прапорці» у даних бухгалтерського обліку та звітності

Передумови виникнення корпоративного шахрайства характеризуються значною багатогранністю та варіативністю, що зумовлює необхідність застосування комплексного підходу до його діагностики. Ефективність заходів із виявлення та попередження фінансових зловживань на ранніх етапах залежить не стільки від перевірки окремих транзакцій, скільки від глибокого розуміння аудитором (або фінансовим аналітиком) вразливостей системи внутрішнього контролю та всебічного оцінювання середовища, в якому функціонує підприємство.

Фінансове шахрайство характеризується низкою специфічних ознак, що вирізняють його з-поміж інших видів економічних правопорушень:

1. Сфера вчинення. Злочинні діяння реалізуються безпосередньо у площині фінансових відносин, які виникають у процесі формування, розподілу та використання грошових фондів (як централізованих, так і децентралізованих).

2. Специфічний суб'єкт. Виконавцем злочину, як правило, виступає кваліфікована особа, яка володіє спеціальними знаннями в галузі бухгалтерського обліку, фінансів чи права.

3. Складність механізму. Фінансове шахрайство належить до кримінальних діянь, що, як правило, характеризуються високим рівнем інтелектуальної організації та складними схемами реалізації задуму.

Сприятливі можливості для реалізації шахрайських схем часто детермінуються специфічними інституційними характеристиками підприємства, поточним станом його господарської діяльності та, особливо, недоліками в системі управління. Детальний аналіз саме цих параметрів дозволяє ідентифікувати ***«червоні прапорці» (red flags)*** – специфічні індикатори, наявність яких не обов'язково свідчить про вже скоєний злочин, але вказує на критично високий рівень загрози його виникнення.

Систематизований перелік таких індикаторів, згрупованих за ключовими сферами діагностики діяльності підприємства, наведено в таблиці 9.5.

Таблиця 9.5

Індикатори підвищеної загрози шахрайських дій, базовані на аналізі інституційних та операційних характеристик підприємства

Сфера ризику	Індикатори (ознаки) підвищеної загрози шахрайства
Корпоративна структура та власність	надмірна ускладненість або заплутаність організаційної структури та структури власності, що унеможливлює або суттєво ускладнює ідентифікацію кінцевих бенефіціарних власників та реальних центрів впливу; аномально висока частота реорганізаційних процедур (злиття, поділи, зміни організаційно-правової форми) або підозрілі зміни у складі власників протягом короткого проміжку часу
Географія діяльності та юрисдикція	реєстрація головного офісу або ключових відокремлених підрозділів у країнах із сприятливим податковим режимом (так званих «офшорних зонах») або у державах із низьким рівнем корпоративного та фінансового регулювання
Операційне середовище та бізнес-модель	функціонування підприємства в умовах негативної галузевої кон'юнктури або стагнації ринку; використання бізнес-моделі або здійснення специфічних видів діяльності, які за своєю природою є вразливими до зловживань (наприклад, значний обсяг операцій з готівкою, робота з високоліквідними активами); активне розширення на нові ринки збуту з високим рівнем політичних або економічних ризиків; раптові й економічно необґрунтовані зміни в налагоджених логістичних ланцюгах, наприклад, заміна ключових постачальників сировини
Фінансовий стан та облікова політика	суттєві зміни в обліковій політиці підприємства протягом звітного періоду (особливо в частині визнання доходів чи оцінки запасів), які не мають достатнього економічного обґрунтування; втрата можливості користуватися традиційним банківським кредитуванням і перехід до застосування складних та непрозорих схем залучення позикових коштів; активне застосування агресивних схем оптимізації оподаткування, що балансують на межі законності
Система управління та внутрішній контроль	відсутність або формальний характер роботи служби внутрішнього аудиту, а також її низька доведена ефективність; загострення корпоративного конфлікту між засновниками (акціонерами), що ставить під загрозу безперервність діяльності підприємства або призводить до втрати контролю над окремими бізнес-сегментами; входження підприємства до складу складних альянсів чи об'єднань з непрозорими цілями; наявність великих судових позовів з боку контрагентів, випадків притягнення керівництва до адміністративної чи кримінальної відповідальності, а також застосування регуляторних санкцій чи обмежень у діяльності підприємства

Проте фокусування лише на внутрішніх інституційних і операційних аспектах не дає змоги повністю оцінити сутність і масштаби ризиків шахрайства.

Будь-яке підприємство функціонує як відкрита система, яка постійно піддається впливу макроекономічних та глобальних факторів.

Зовнішні умови – від економічних криз до змін у законодавчому полі – часто виступають потужними каталізаторами неправомірних дій. Вони можуть створювати критичний фінансовий тиск на компанію або, навпаки, відкривати нові «вікна можливостей» для реалізації тіньових схем, які неможливо виявити, аналізуючи лише внутрішню документацію. Тому комплексний аналіз обов'язково передбачає оцінку впливу зовнішнього контексту.

Систематизований перелік індикаторів підвищеної загрози шахрайства, зумовлених впливом макро- та глобального середовища, наведено у таблиці 9.6.

Таблиця 9.6

Індикатори підвищеної загрози шахрайських дій, зумовлені впливом макроекономічного та глобального середовища

Сфера ризику	Індикатори (ознаки) підвищеної загрози шахрайства
Економічні	існування серйозної економічної кризи в державі, де зареєстроване підприємство, або в міжнародному масштабі; функціонування економіки в умовах гіперінфляції; масштабна неплатоспроможність банківських установ, наслідком якої стало значне зростання кредитних відсоткових ставок
Законодавчо-регуляторні	істотне зростання фіскального тиску на суб'єкти господарювання, що спричиняє впровадження масштабних схем податкової оптимізації; упровадження іноземними державами протекціоністських обмежень щодо українських підприємств, галузей або видів діяльності; наявність значного рівня корупційних проявів у системі державного управління та серед органів, уповноважених на здійснення контролю
Науково-технічні	активний розвиток та впровадження інноваційних рішень у закордонних державах, унаслідок чого окремі види продукції вітчизняних виробників втрачають конкурентні переваги; науково обґрунтоване визнання небезпечності окремих матеріалів і технологій, що використовуються підприємством, для людини та довкілля
Природні	виникнення ризику припинення або суттєвого обмеження функціонування підприємства під впливом пандемічних явищ чи надзвичайних природних подій; вимушений перехід на альтернативні технологічні рішення та матеріали у зв'язку з критичним погіршенням екологічного стану довкілля
Соціально-демографічні	міграція кваліфікованих кадрів з країни: трансформація соціально-демографічної структури населення

Аудитори не здійснюють юридичну кваліфікацію виявлених фактів як шахрайства. В межах своїх повноважень вони розглядають два основні типи викривлень:

➢ *викривлення, які виникають внаслідок недобросовісних дій під час формування фінансової звітності* (зазвичай ініціатором є вище керівництво);

➢ *викривлення, що виникають внаслідок незаконного привласнення або використання активів підприємства* (як правило, вчиняються працівниками всупереч інтересам компанії).

Ризик шахрайських дій істотно зменшується при чіткій персоніфікації відповідальності за конкретні ділянки роботи. Така організація процесів полегшує відстеження руху коштів і ускладнює можливість безкарного здійснення крадіжок або розтрат.

Досвід показує, що найчастіше випадки шахрайства виникають під час реалізації високоризикових проєктів, коли стандартні процедури внутрішнього контролю послаблюються або не виконуються.

Ключові ознаки, що можуть вказувати на потенційну можливість здійснення шахрайства на підприємстві, систематизовано на рисунку 9.5.

Рис. 9.5. «Червоні прапорці», що свідчать про ризик для здійснення шахрайства

Значного поширення серед облікових порушень набуло недостовірне відображення реального фінансового стану підприємства, яке реалізується через механізми так званого «управління фінансовими результатами». Така діяльність

кваліфікується як свідоме, цілеспрямоване втручання топ-менеджменту в процес формування та складання звітності, зумовлене прагненням отримати особисті економічні вигоди.

Слід підкреслити, що потенційним об'єктом викривлення може стати фактично будь-який обліковий показник. Найбільш типові та розповсюджені схеми подібного шахрайства систематизовано на рисунку 9.6.

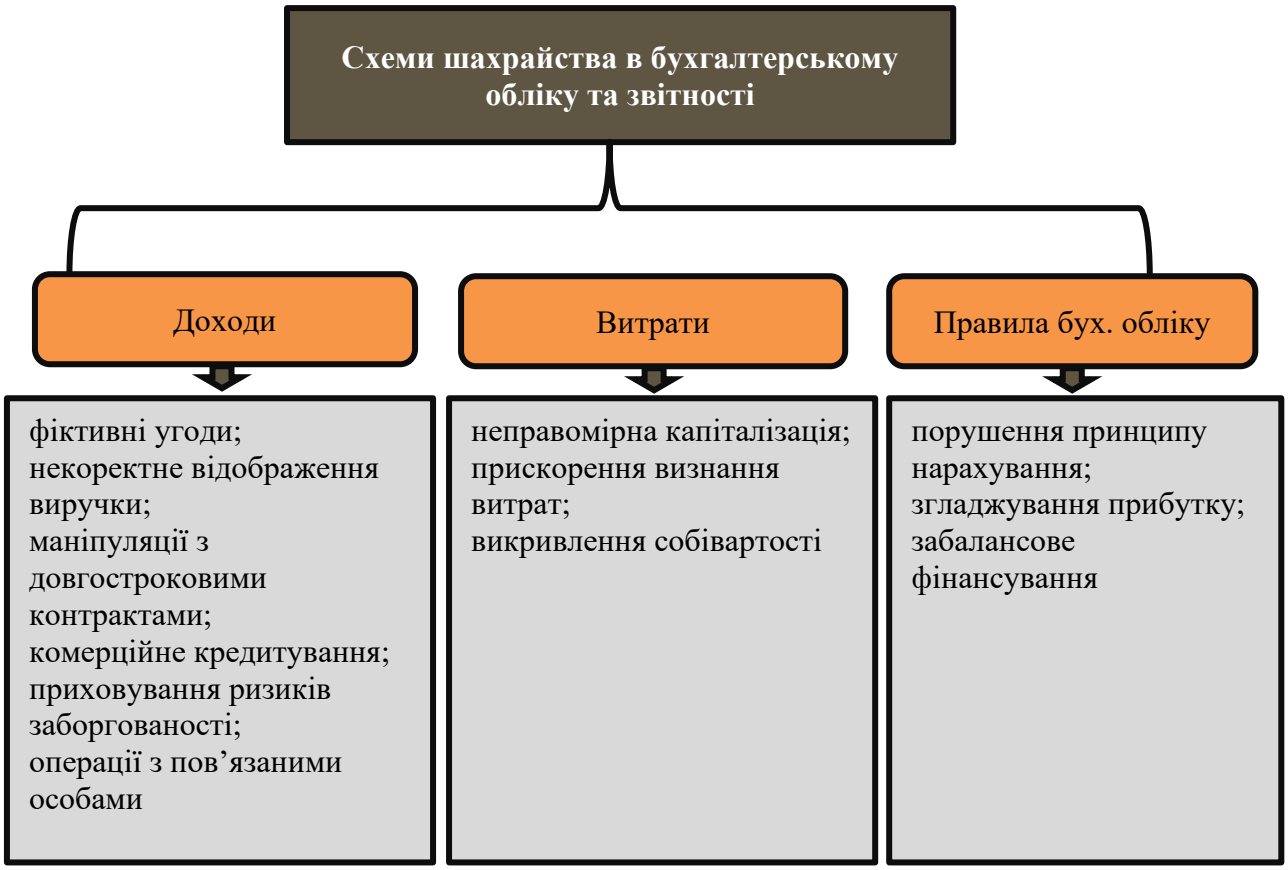


Рис. 9.6. Схеми шахрайства в бухгалтерському обліку та звітності

Схеми згруповано за трьома основними напрямами впливу на фінансовий результат:

1. Маніпуляції з доходами. Один із найбільш поширених різновидів шахрайських дій, що зумовлено визначальною роллю виручки для інвесторів. До основних способів належать, зокрема:

- *фіктивні угоди:* відображення в обліку неіснуючих продажів, як правило, із використанням підробленої первинної документації;
- *некоректне визнання виручки:* запис доходу до моменту виконання зобов'язань (наприклад, товар ще не відвантажено, а виручка вже визнана);

- *операції з пов'язаними особами:* продаж товарів «своїм» компаніям за завищеними цінами для штучного нарощування оборотів;
- *маніпуляції з довгостроковими контрактами:* штучне завищення відсотка завершеності робіт за довгостроковими договорами, що призводить до необґрунтованого збільшення доходу, визнаного в поточному звітному періоді;
- *комерційне кредитування:* відвантаження продукції з наданням значного відтермінування платежу, що дозволяє демонструвати завищені доходи у Звіті про фінансові результати та роздуту дебіторську заборгованість у Балансі.
- *приховування ризиків заборгованості:* неформування резервів за сумнівними боргами, що призводить до штучного завищення вартості активів.

2. Маніпуляції з витратами. Шахрайство може здійснюватися шляхом приховування або перенесення витрат:

- *неправомірна капіталізація:* відображення поточних витрат (наприклад, ремонтів або маркетингу) як капітальних інвестицій (активів). Це дозволяє не зменшувати поточний прибуток, а «розмазати» витрати на майбутні роки через амортизацію;
- *викривлення собівартості:* штучне зменшення витрат на реалізовану продукцію з метою завищення показника валового прибутку;
- *прискорення або відстрочення визнання витрат:* навмисне перенесення або прискорення відображення витрат між звітними періодами для досягнення запланованих бюджетних орієнтирів.

3. Зловживання обліковими правилами та оцінками. Використання гнучкості стандартів обліку для викривлення реального стану справ:

- *порушення принципу нарахування:* маніпулювання часом визнання на стику звітних періодів;
- *згладжування прибутк*у: створення надлишкових резервів у «хороші» роки, щоб використати їх для покриття збитків у «погані» роки, створюючи ілюзію стабільності бізнесу;

➢ *забалансове фінансування:* маскування боргових зобов'язань (кредитних і лізингових) поза межами балансу з метою штучного поліпшення показників ліквідності та фінансової стабільності.

Запровадження зазначених вище шахрайських практик неминуче зумовлює спотворення ключових показників фінансової звітності. Найбільш уразливими до маніпулятивних впливів є операції з визнання доходів і обліку дебіторської заборгованості, оскільки саме вони мають прямий вплив на фінансові результати діяльності та податкові зобов'язання підприємства.

Аналіз типових порушень на цій ділянці дозволяє встановити характерні взаємозв'язки між викривленнями дебіторської заборгованості, чистого доходу та бази оподаткування. Систематизацію цих впливів наведено в таблиці 9.7.

Таблиця 9.7

Вплив облікових порушень в операціях на показники звітності

Види порушень в обліку	Дебіторська заборгованість	Чистий дохід	База оподаткування
1. Визнання доходу від реалізації без одночасного відображення дебіторської заборгованості	↓	↑	↑
2. Відображення дебіторської заборгованості за відсутності факту визнання доходу від реалізації	↑	↓	↓
3. Реалізація продукції неплатоспроможним («неблагонадійним») клієнтам із наданням суттєвої відстрочки платежу	↑	↑	↑
4. Фіктивне відображення операцій з продажу, що фактично не відбулися	↑	↑	↑
5. Завищення виручки шляхом ігнорування в обліку наданих покупцям знижок	↑	↑	↑
6. Акумулювання доходів у власному обліку при перенесенні частини витрат на підконтрольні структури	↑	↑	↑
7. Неправомірна капіталізація операційних витрат (віднесення їх на збільшення вартості активів)	—	↑	↑
8. Штучне завищення витрат з метою декларування збитковості діяльності	—	↓	↓

Ефективним засобом ідентифікації умисного викривлення облікової інформації є поєднання аналітичних аудиторських процедур із поглибленим дослідженням нефінансових показників. Застосування такого інтегрованого підходу дає змогу своєчасно виявляти латентні ознаки проблем, які ще не мають

прямого відображення у звітних даних, проте свідчать про зростання ризику шахрайських дій.

Систематизацію ключових джерел та прикладів нефінансових ознак облікових викривлень наведено в таблиці 9.8.

Таблиця 9.8

Джерела та типові нефінансові ознаки облікових викривлень

Група джерел	Конкретне джерело	Нефінансові ознаки потенційних викривлень
Зовнішні джерела	Конкуренти	наявність інформації про потенційні недружні поглинання на ринку; функціонування підприємства в умовах надзвичайно жорсткої конкуренції
	Контрагенти	відсутність або неефективність налагодженої системи перевірки контрагентів; раптова поява значної кількості нових, невідомих на ринку замовників та постачальників
	Фінансові установи	систематичні відмови банків та інших установ у наданні компанії позик та кредитів; наявність критично значної суми простроченої або реструктуризованої заборгованості
	Органи ДПС України	проведення частих податкових перевірок; встановлені факти порушення компанією податкового законодавства
Внутрішні джерела	Рада директорів	звільнення членів ради директорів без належного обґрунтування причин; аномально часта ротація членів ради
	Управлінський персонал	часті зміни у складі вищого керівництва; висока плинність кадрів серед менеджерів середньої ланки
	Група компаній	наявність незвичайних або економічно необґрунтованих угод між компаніями групи; значний обсяг складних угод із пов’язаними сторонами
Специфічні джерела	Юристи	наявність складних, затяжних судових процесів, особливо з регуляторами або великими контрагентами; постійна зміна юридичних радників компанії.
	Аудит	доведена відсутність або неефективність системи внутрішнього контролю; постійна зміна зовнішнього аудитора. відмова попереднього зовнішнього аудитора від надання висновку

Аналіз нефінансової інформації надає аудитору суттєві відомості про специфіку діяльності підприємства, систему управління та власності, організаційну структуру компанії, її основних контрагентів, а також дозволяє ідентифікувати нетипові операції.

Наведені вище індикатори здебільшого орієнтовані на виявлення ***шахрайських схем*** у межах функціонуючих корпоративних структур шляхом аналізу фінансової звітності та операційного середовища. Водночас у ширшій площині забезпечення фінансової безпеки важливого значення набуває запобігання шахрайським практикам, спрямованим безпосередньо на залучення коштів широкого кола громадян та приватних інвесторів, зокрема через організацію фінансових пірамід, псевдоінвестиційних проєктів та подібних схем.

З метою мінімізації ризиків втрати капіталу та репутації, стейкхолдерам, аудиторам та фінансовим аналітикам необхідно вміти ідентифікувати типові поведінкові та управлінські «червоні прапорці», що можуть свідчити про високу ймовірність корпоративних зловживань. До найважливіших індикаторів такої загрози належать:

- *економічна необґрунтованість результатів* (декларування підприємством рівня прибутковості чи темпів зростання, що суттєво перевищують середньогалузеві показники, особливо в умовах загальної економічної стагнації, без зрозумілого пояснення джерел такого успіху);
- *нереалістичні зобов'язання менеджменту (*надмірно оптимістичні та категоричні заяви вищого керівництва перед інвесторами або аналітиками щодо досягнення завищених фінансових показників, ігноруючи об'єктивні ризики ринкового середовища);
- *авторитарний тиск та маніпуляція* (домінування одного або кількох топ-менеджерів у прийнятті рішень, ігнорування системи внутрішнього контролю, активний психологічний тиск на обліковий персонал для відображення бажаних, а не реальних результатів, агресивна поведінка щодо аудиторів);
- *агресивна облікова політика та «ексклюзивність» операцій* (застосування ризикованих методів бухгалтерського обліку, що балансують на межі стандартів, акцентування на складних, «унікальних» угодах, економічна сутність яких є незрозумілою для більшості користувачів звітності);

- *нетипові умови розрахунків* (наявність значних операцій з необґрунтованими авансовими платежами, наданням надмірних відстрочок або використанням вексельних схем, особливо з контрагентами, що мають ознаки фіктивності);
- *інформаційна непрозорість структури* (використання заплутаної мережі офшорних компаній або спеціалізованих структур без очевидної ділової мети; небажання розкривати інформацію про кінцевих бенефіціарів та реальний зміст операцій з пов'язаними особами;
- *нехтування легітимністю та комплаєнсом* (систематичне ігнорування регуляторних вимог, робота на межі фолу в правовому полі, часті конфлікти з контролюючими органами та податковою службою).

Ефективне ***виявлення «червоних прапорців»*** вимагає від фахівця інтегрованого підходу, який поєднує аналіз специфічних облікових аномалій (таких як нетипові проводки, маніпуляції з визнанням доходів чи капіталізацією витрат) із глибоким розумінням операційного контексту та нефінансових симптомів кризи корпоративного управління.

Тільки інтегрований аналіз фінансових і нефінансових показників дає змогу отримати неупереджену оцінку фактичного стану підприємства та своєчасно виявити латентні ризики на початкових етапах їх формування.

9.3. Цифрові інструменти моніторингу операцій і виявлення підозрілих транзакцій

У сучасних умовах господарювання критичного значення набуває побудова ефективної системи контролю за діяльністю підрозділів, що функціонують у зонах підвищеного ризику шахрайства. Проблема загострюється внаслідок зростання інтенсивності операцій, глибокої інтеграції цифрових технологій, автоматизації обліково-фінансових процесів та ускладнення організаційних структур. За таких обставин традиційні форми контролю втрачають ефективність, що зумовлює необхідність впровадження комплексної системи, яка інтегрує різні контрольні механізми для забезпечення надійного захисту від шахрайських посягань.

Фундаментальним елементом такої системи виступає внутрішній контроль підприємства. Відповідно до норм Бюджетного кодексу України ***внутрішнім контролем*** є «комплекс заходів, що застосовуються керівником для забезпечення дотримання законності та ефективності використання бюджетних коштів, досягнення результатів відповідно до встановленої мети, завдань, планів і вимог щодо діяльності розпорядника бюджетних коштів і підприємств, установ та організацій, що належать до сфери його управління».

Для підприємства внутрішній контроль передбачає систематичний нагляд за діяльністю структурних підрозділів, дослідження бізнес-процесів і господарських операцій, а також перевірку дотримання принципу розмежування функціональних повноважень. Результативність цієї системи визначається її спроможністю своєчасно адаптуватися до змін у бізнес-середовищі, забезпечувати прозорість операцій та формувати релевантну інформаційну базу для ухвалення управлінських рішень. Пріоритетним завданням виступає раннє виявлення відхилень у процесах для превентивного реагування на потенційні ризики. Системність і вбудованість внутрішнього контролю в повсякденну діяльність підприємства забезпечують суцільне охоплення операцій та істотно підсилюють ефективність управління ризиками.

Вагомим засобом неупередженої оцінки виступає аудит, який забезпечує об'єктивний аналіз фінансових і операційних процесів, виявлення слабких місць у системі управління та формування рекомендацій щодо їх усунення. Водночас внутрішній аудит виконує функцію первинного захисного механізму, здійснюючи безперервний контроль, тоді як зовнішній аудит забезпечує незалежне підтвердження достовірності звітної інформації, сприяючи зростанню довіри до підприємства з боку зовнішніх стейкхолдерів.

Специфічну роль у загальній системі відіграє державний фінансовий аудит. Згідно із ст. 3 Закону України «Про основні засади здійснення державного фінансового контролю в Україні», «***державний фінансовий аудит*** є різновидом державного фінансового контролю і полягає у перевірці та аналізі діяльності, фактичного стану справ щодо законного та ефективного використання державних чи комунальних коштів і майна, інших активів держави, правильності ведення бухгалтерського обліку і достовірності фінансової звітності, функціонування системи внутрішнього контролю».

Метою цього аудиту є контроль за дотриманням вимог бюджетного законодавства, а також аналіз результативного й раціонального використання державних коштів. Застосування даного контролю дозволяє виявляти порушення фінансової дисципліни та факти нецільового використання коштів, що підвищує рівень підзвітності суб'єктів з бюджетним фінансуванням.

В умовах високого ризику шахрайства система контролю має бути доповнена форензік-аудитом. У чинному законодавстві України термін «форензік-аудит» (або «форензік») прямо не визначений. Це поняття є запозиченим з міжнародної ділової практики і широко використовується в бізнес-середовищі та консалтингу, однак воно ще не імплементоване в національні нормативно-правові акти як окрема юридична дефініція.

Форензік-аудит (forensic accounting) – комплексне всебічне дослідження фінансового-сподарської діяльності економічного суб'єкта, мета якого полягає у виявленні різних фактів шахрайства, фінансових махінацій, інших неправомірних дій, як з боку управлінського апарату, так і з боку інших

співробітників, а також інших третіх осіб, крім того запропонувати систему заходів щодо їх мінімізації.

Зазначений інструмент орієнтований на ідентифікацію прихованих механізмів і схем, які не фіксуються в межах традиційних аудиторських перевірок. Методологічна база форензік-аудиту передбачає інтегроване використання спеціалізованих підходів, спрямованих на виявлення нетипових відхилень у фінансовій інформації та аналіз поведінкових характеристик. У межах цієї методології методи поділяються на три ключові групи: математичні, аналітичні (економіко-статистичні) та психофізіологічні.

1. Математичні методи. Базуються на пошуку числових закономірностей та відхилень від них.

Прикладом є застосування ***закону Бенфорда (закону першої цифри).*** Суть методу полягає в тому, що у великих масивах природних числових даних (наприклад, суми платежів, залишки товарів) частота появи певної цифри на першій позиції підпорядковується логірифмічній закономірності, де одиниця зустрічається найчастіше (близько 30 %), а дев'ятка – найрідше.

Суттєве відхилення послідовності цифр у бухгалтерських даних від розподілу Бенфорда може свідчити про фальсифікацію даних та необхідність детальної перевірки. Перевагою методу є можливість повної автоматизації процесу перевірки великих масивів даних.

2. Аналітичні методи. Включають традиційні методи економічного аналізу (порівняння взаємопов'язаних показників, виявлення алогічних зв'язків) та автоматизовані методи інтелектуального аналізу даних, спрямовані на пошук нетипових транзакцій та прихованих шаблонів.

3. Психофізіологічні методи. Застосовуються під час проведення внутрішніх розслідувань та інтерв'ю з персоналом. Вони базуються на аналізі вербальних (зміст висловлювань) та невербальних (міміка, жести, мікрорухи) реакцій для виявлення ознак нещирості.

Застосування зазначених методів потребує належного рівня професійної підготовки та виступає допоміжним елементом методологічного інструментарію форензік-аудиту.

Залежно від цілей дослідження, форензік-аудит класифікують на такі основні види:

- *розслідування фактів фінансового шахрайства та махінацій;*
- *проведення розслідувань щодо виявлення та розшуку активів;*
- *заходи з протидії легалізації (відмиванню) доходів;*
- *розробка механізмів протидії корупційним проявам;*
- *оцінка благонадійності бізнес-партнерів та контрагентів;*
- *сприяння у врегулюванні корпоративних та господарських конфліктів тощо.*

Специфіка форензік-аудиту як форми незалежного економічного розслідування полягає у використанні розширеної доказової бази, що формується з офіційних та неофіційних джерел. Аналітичні процедури при цьому виходять за межі традиційного вивчення первинної документації та бухгалтерської або управлінської звітності, обов'язково охоплюючи збір та аналіз свідчень і пояснень широкого кола осіб: чинних співробітників, контрагентів, залучених незалежних експертів, а також колишніх бізнес-партнерів.

Основні відмінності форензік-аудиту від звичайного аудиту та інших форм контролю полягають у такому:

- *спрямованість на захист економічних інтересів бізнесу зсередини;*
- *моделювання та аналіз сценаріїв потенційного шахрайства;*
- *критична перевірка фактичної достовірності інформації, а не лише документів;*
- *специфіка ініціювання, процесу проведення та форми звітування за результатами;*
- *відсутність жорсткого, заздалегідь визначеного алгоритму перевірки.*

Системне бачення ролі та функцій різних видів контролю у механізмі управління ризиками шахрайства узагальнено в таблиці 9. 9.

Таблиця 9.9

Вплив основних видів контролю на управління ризиками шахрайства в підрозділах підприємства

Види контролю	Механізм впливу	Виявлені шахрайські дії	Наслідки для системи управління підприємства
Внутрішній контроль	Постійний моніторинг операцій, розподіл функціональних обов'язків, встановлення контрольних процедур	Аномалії в операціях, порушення внутрішніх регламентів, зловживання правами доступу	Зростання рівня операційної прозорості, оперативне виявлення порушень і зменшення прямих фінансових втрат
Аудит	Незалежна перевірка фінансової та операційної діяльності, оцінка ефективності бізнес-процесів	Фальсифікація фінансової звітності, невідповідність операцій обліковим політикам	Зміцнення довіри до звітної інформації, виявлення та усунення недоліків у процесах, а також отримання рекомендацій щодо вдосконалення системи
Державний фінансовий аудит	Перевірка дотримання законодавства та фінансової дисципліни у сфері публічних фінансів	Порушення бюджетного законодавства, нецільове використання державних ресурсів	Забезпечення дотримання правових норм у діяльності, нагляд за цільовим використанням бюджетних ресурсів і підвищення рівня підзвітності
Форензік-аудит	Поглиблена аналітика даних, цифровий моніторинг транзакцій, спеціальні розслідування	Приховані схеми, маніпуляції з первинними документами, привласнення активів	Встановлення фактів і визначення масштабів шахрайських дій, мінімізація ризику подальших втрат

У процесі формування системи внутрішнього контролю вирішальне значення має спеціалізований інструментарій, орієнтований на поглиблений аналіз даних і автоматизоване виявлення аномалій. За умов, коли обсяги операцій досягають мільйонів, а шахрайські практики ускладнюються та активно використовують цифрові канали, класичні аудиторські підходи, засновані на вибірковому контролі документації, поступово втрачають свою результативність.

Далі доцільно детальніше проаналізувати ключові цифрові інструменти, що відіграють визначальну роль у виявленні підозрілих операцій і запобіганні шахрайським діям (табл. 9.10).

Таблиця 9.10

Ключові цифрові інструменти моніторингу операцій та виявлення ознак шахрайства

Цифровий інструмент	Основні функції та методи
Інтелектуальний аналіз даних та аналітика великих даних	*тестування журнальних проводок.* Автоматизований пошук нетипових бухгалтерських записів (за часом, сумою, автором), що можуть свідчити про маніпуляції; *аналіз взаємозв'язків.* Виявлення латентних зв'язків між працівниками та контрагентами з метою ідентифікації потенційних конфліктів інтересів або корупційних механізмів
Штучний інтелект та машинне навчання	*виявлення аномалій*. Автоматичне виявлення відхилень від створеного профілю «нормальної» поведінки користувача або клієнта; *предиктивна аналітика.* Прогнозування ризику шахрайських дій за окремою транзакцією на основі аналізу історичних даних ще до моменту її завершення
Технологія блокчейн	*незмінний реєстр.* Створення децентралізованої бази даних транзакцій, записи в якій неможливо змінити або видалити «заднім числом» *смарт-контракти.* Автоматизація виконання договірних зобов'язань при настанні визначених умов
Роботизована автоматизація процесів	Застосування програмних роботів для автоматизації стандартних контрольних операцій, зокрема виконання автоматизованого тристороннього звіряння документів

Серед наведених інструментів особливої уваги заслуговують системи на базі штучного інтелекту, які здатні виявляти найменші аномалії та підозрілу активність, що часто залишаються непоміченими експертами-людьми. Ефективність функціонування сучасних ШІ-систем безпеки спирається на низку інноваційних технологій та механізмів:

- *біометрична автентифікація.* Застарілі методи захисту, що базувалися виключно на паролях та PIN-кодах, виявилися вразливими до компрометації з боку шахраїв. Системи нового покоління на основі ШІ використовують персоніфіковані біометричні дані (відбитки пальців, розпізнавання обличчя чи

голосу), гарантуючи, що доступ до облікових записів та проведення транзакцій здійснюють виключно авторизовані користувачі;

- *поведінкова біометрія*. Окрім фізичних характеристик, ШІ-механізми аналізують унікальну цифрову поведінку користувача – індивідуальну манеру набору тексту, швидкість гортання сторінок, специфіку використання пристрою. Створення та відстеження таких поведінкових патернів забезпечує додатковий рівень захисту облікового запису;
- *аналіз транзакційної поведінки.* На відміну від традиційних систем, заснованих на фіксованих правилах і схильних до значної кількості хибних спрацювань, алгоритми машинного навчання самостійно формують модель типової поведінки авторизованого користувача. Це забезпечує своєчасне виявлення нетипових операцій без створення перешкод для клієнтів;
- *обробка природної мови (NLP).* За умов активного використання чат-ботів і віртуальних асистентів алгоритми NLP дають змогу аналізувати мовні особливості та контекст комунікації, що забезпечує оперативне виявлення проявів психологічного впливу, примусу або методів соціальної інженерії в режимі, наближеному до реального часу.

Поряд із рішеннями на основі штучного інтелекту, суттєву роль у цифровому інструментарії моніторингу відіграє ***роботизована автоматизація процесів (RPA).*** Даний підхід ґрунтується на застосуванні спеціалізованого програмного забезпечення – так званих програмних роботів (ботів), які відтворюють дії користувача в інформаційних системах з метою автоматизації типових, формалізованих операцій. RPA-платформи функціонують на рівні користувацького інтерфейсу, послідовно виконуючи введення даних, навігацію та інші дії аналогічно до ручної роботи співробітника.

По суті, програмний робот автоматизує виконання дій, які раніше здійснювалися за участі персоналу, що сприяє підвищенню швидкості операцій і зменшенню ризику помилок, зумовлених впливом людського чинника.

Сучасні RPA-рішення все активніше поєднуються з інструментами штучного інтелекту та машинного навчання, утворюючи концепцію

інтелектуальної автоматизації. У межах такого підходу програмні боти здатні не лише виконувати заздалегідь визначені алгоритми, а й аналізувати дані, опановувати нові шаблони поведінки, приймати базові управлінські рішення та обробляти неструктуровані інформаційні масиви.

У системі внутрішнього контролю та запобігання шахрайським діям використання RPA надає ряд ключових переваг, зокрема:

- *забезпечення безперервного моніторингу.* На відміну від традиційного підходу, за якого працівник здійснював вибірковий контроль документів із певною періодичністю (наприклад, щомісяця), RPA-боти здатні автоматично перевіряти весь масив операцій щоденно або навіть погодинно на відповідність заданим критеріям та негайно сигналізувати про відхилення. Таким чином, RPA-технології забезпечують безперервний контроль транзакцій у реальному часі та оперативне виявлення нетипових операцій замість епізодичних перевірок за вибіркою;
- *зростання точності та уніфікованості контрольних процедур.* Автоматизовані рішення забезпечують стабільне та безперервне виконання контрольних операцій за єдиними правилами, усуваючи ризик пропусків і помилок. Програмні боти можуть оперативно зіставляти великі обсяги даних з різних інформаційних систем (зокрема систем обліку замовлень і платежів), виявляти розбіжності та формувати перелік операцій, що потребують подальшого аналізу з боку контролюючих осіб;
- *розширення масштабу контрольних заходів.* Залучення програмних роботів забезпечує можливість суттєво збільшити обсяг і кількість перевірок та напрямів контролю без відповідного зростання чисельності персоналу.

RPA-боти характеризуються технологічною незалежністю та здатні функціонувати поверх різних, зокрема застарілих, IT-платформ без необхідності їх масштабного оновлення, виконуючи роль інтеграційного елемента між розрізненими обліковими системами.

Ефективними засобами цифрового контролю виступають також технології Process Mining (інтелектуальний аналіз бізнес-процесів) і Link Analysis (аналіз посилань).

Технологія ***Process Mining*** забезпечує відтворення фактичного перебігу бізнес-процесів шляхом аналізу цифрових слідів (журнальних записів), що накопичуються в інформаційних системах.

На відміну від традиційного інтерв'ювання співробітників, які описують, як процес має відбуватися, Process Mining візуалізує те, як процес відбувається фактично. Це дозволяє миттєво виявляти:

- *обхід процедур контролю (наприклад, проведення платежу без обов'язкової візи керівника);*
- *порушення часових регламентів (узгодження складного договору за 1 хвилину);*
- *дублювання функцій або несанкціоновані зміни в документах після їх затвердження.*

Link Analysis застосовується для виявлення прихованих афілійованих зв'язків. Система автоматично будує графічні мережі взаємозв'язків між контрагентами, співробітниками та третіми особами.

Цей інструмент є критично важливим у двох напрямках:

- *виявлення конфлікту інтересів;*

Якщо керівник тендерного комітету та директор компанії-переможця мають спільну адресу реєстрації, використовують одну IP-адресу або пов'язані через спільних знайомих у соціальних мережах, система ідентифікує це як ризик корупційної змови.

- *протидія відмиванню коштів (AML) у банківському секторі*.

Link Analysis дозволяє розслідувати випадки структурування транзакцій. Наприклад, якщо моніторинг фіксує активність кількох клієнтів, які здійснюють перекази сум, що знаходяться трохи нижче порогу обов'язкового фінмоніторингу (щоб уникнути уваги регулятора), аналіз зв'язків допомагає встановити істину. Інструмент перевіряє, чи є ці клієнти пов'язаними особами

(чи мають спільних бенефіціарів, чи управляються з одного пристрою тощо). Це дозволяє аналітику швидко відрізнити випадковий збіг легітимних операцій від скоординованої діяльності «конвертаційного центру» або злочинного угруповання.

Застосування зазначених вище генерує значні масиви різнорідної інформації. Для забезпечення максимальної ефективності контролю ці технології мають функціонувати не ізольовано, а як складові єдиної інтегрованої екосистеми. Саме тому критично важливим є розуміння загальної логіки побудови таких систем.

Архітектура систем запобігання шахрайству, що базуються на технологіях штучного інтелекту, являє собою складну багаторівневу модель, яка включає низку основних етапів функціонування:

1. Збір даних. Акумуляція великих масивів якісних транзакційних та поведінкових даних з різноманітних джерел, що слугують ядром системи.

2. Розуміння поведінки. Ідентифікація специфічних рис та патернів, що дозволяють диференціювати моделі поведінки легітимного користувача та шахрая.

3. Навчання моделі. Використання масивів історичних даних з метою формування здатності алгоритмів ідентифікувати шахрайські патерни під час функціонування в реальних операційних умовах.

4. Виявлення аномалій. Безпосереднє функціонування системи, спрямоване на фіксацію відхилень від нормальної поведінки на основі запрограмованих алгоритмів.

5. Безперервне оновлення. Регулярне донавчання моделей на актуальних даних з метою своєчасної адаптації до нових та змінених шахрайських практик.

6. Сповіщення та звітність. Автоматичне формування оперативних сигналів щодо підозрілих операцій і підготовка розгорнутих аналітичних звітів для подальшого опрацювання та розслідування інцидентів.

Інтегрування спеціалізованих цифрових рішень у систему внутрішнього контролю та їх систематичне застосування у процесі форензік-досліджень

забезпечує трансформацію підходу від фіксації вже здійснених порушень до превентивного контролю. Це створює можливість оперативного виявлення й зупинення потенційно ризикових операцій у режимі, максимально наближеному до реального часу. Запровадження такого підходу набуває особливої актуальності в умовах інтенсивного зростання кількості цифрових транзакцій, за яких класичні вибіркові методи контролю поступово втрачають результативність.

9.4. Контрольні питання для самоперевірки

1. У чому полягає фундаментальна різниця між поняттями «помилка» та «шахрайство» в контексті аудиту, і який критерій є ключовим для їх розмежування?

2. Розкрийте сутність та складові елементи моделі «трикутника шахрайства». Як ця модель допомагає в ідентифікації факторів ризику?

3. Назвіть та охарактеризуйте чотири основні групи причин (детермінант) виникнення фінансового шахрайства.

4. Назвіть три основні напрями маніпулювання фінансовими результатами в бухгалтерському обліку

5. У чому полягає сутність методу соціальної інженерії як інструменту реалізації шахрайських схем, і які людські фактори при цьому експлуатуються?

6. Охарактеризуйте поняття «червоні прапорці» (red flags) в бухгалтерському обліку. Наведіть приклади таких індикаторів, що можуть свідчити про ризик внутрішніх зловживань.

7. Розкрийте механізм впливу облікових порушень в операціях реалізації на ключові показники фінансової звітності.

8. Які нефінансові симптоми можуть сигналізувати аудитору про підвищений ризик свідомого маніпулювання обліковими даними з боку управлінського персоналу?

9. У чому полягають ключові відмінності форензік-аудиту від традиційного аудиту та інших форм контролю з точки зору мети, методології та доказової бази?

10. Які основні цифрові інструменти та технології використовуються для моніторингу операцій та виявлення ознак шахрайства, і в чому полягають їхні ключові функції?

Розділ 10

Автори:
Олександр Сохацький
Вадим Шухманн

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА ЗАХИСТУ ФІНАНСОВИХ ДАНИХ

РОЗДІЛ 10. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА ЗАХИСТУ ФІНАНСОВИХ ДАНИХ

«Є лише два типи компаній: тих, які вже зламали, і тих, які ще зламають.»

Роберт Мюллер

10.1. Основні загрози кібербезпеки для бізнесу та аудиторських фірм

У сучасному цифровому середовищі ***кібербезпека*** перестала бути суто технічною функцією IT-підрозділу та перетворилася на компонент управління ризиками організації. Інформаційна безпека спрямована на забезпечення конфіденційності, цілісності та доступності даних (CIA-тріада): недопущення несанкціонованого розкриття інформації, викривлення її змісту або втрати доступності для легітимних користувачів. Для аудиторських компаній ця рамка є базовою, оскільки вони концентрують чутливі фінансові та персональні дані, а також часто мають тимчасові або постійні доступи до клієнтських інформаційних систем.

Для системного опису кіберзагроз використовується тріада CIA (конфіденційність, цілісність, доступність). Ця модель чітко ідентифікує характер шкоди, розмежовуючи первинні наслідки та супутні вторинні ефекти від атаки. Перелік ключових загроз і відповідних контролів наведено в таблиці 10.1.

Таблиця 10.1.

Карта ключових загроз за тріадою CIA (Confidentiality–Integrity–Availability)

Тип загрози	Первинний вплив (C/I/A)	Типові активи	Ключовий бізнес-ефект	Контроль першої лінії
Фішинг і соціальна інженерія	C, I	Пошта, облікові записи, хмара	Компрометація доступу, витік даних	MFA, навчання, політики протидії фішингу
Масове використання викрадених паролів	C	SSO, пошта, VPN, SaaS	Несанкціонований вхід, захоплення акаунта	Унікальні паролі, MFA, умовний доступ
Шкідливе ПЗ	C, I	Робочі станції, сервери, браузери	Стійка присутність, збір даних	EDR, управління оновленнями (патчами), мінімальні права
Програми-вимагачі (ransomware)	A, C	Файлові сховища, ERP, резерви	Простій, витрати на відновлення, шантаж	Ізольовані та незмінювані резервні копії, сегментація, EDR
Експлуатація вразливостей	C, I, A	Периметр, вебсервіс, VPN, API	Проникнення, порушення процесів	Сканування, встановлення оновлень (патчів), посилення конфігурації, WAF
Ланцюг постачання та треті сторони	C, I, A	Сервіси обміну файлами, підрядники	Ланцюгові інциденти, витоки	Оцінка постачальника, ізоляція інтеграцій
Внутрішній порушник (insider)	C, I, A	Робочі документи, довідники доступів	Витік, підміна даних, саботаж	розмежування обов’язків, журналювання, DLP, політики доступу
DDoS-атака	A	Вебсервіс, портали, VPN	Недоступність сервісів, зрив операцій	захист периметра, резервні канали, CDN, захист від DDoS

Як видно з таблиці 10.1, більшість інцидентів впливають не на один елемент CIA, а на кілька одночасно (наприклад, ransomware порушує доступність і часто супроводжується ризиком витоку). Тому практичний захист має поєднувати

запобіжні та виявляючі контролі, а не обмежуватися лише антивірусом чи складними паролями.

Ключовим інструментом аналізу загроз у кібербезпеці виступає ризик-орієнтований підхід. У ньому ризик розуміють як поєднання двох складових: ймовірності настання інциденту та тяжкості наслідків для інформаційних активів (даних, систем, сервісів). Для правильного застосування цього підходу важливо чітко розрізняти базові поняття.

Загроза – це потенційне джерело небажаної події (наприклад, зловмисник, шкідливе ПЗ або помилка користувача).

Уразливість – це конкретне слабке місце в системі чи процесі, яке створює умови для реалізації загрози, наприклад відсутність багатофакторної автентифікації, помилки конфігурації, надмірні права доступу або застаріле програмне забезпечення. Така відмінність має практичне значення: вона переводить обговорення від загальних «небезпек» до керованих рішень, які саме контролі потрібно змінювати, щоб зменшити ймовірність інциденту або обмежити масштаб його наслідків.

Окремим поняттям, важливим для розуміння цифрових загроз, є ***поверхня атаки (attack surface)*** – сукупність усіх точок входу та каналів взаємодії, через які можливе порушення безпеки. До неї належать облікові записи, віддалений доступ, хмарні сервіси, інтеграції та API, робочі станції, мобільні пристрої, корпоративна пошта, платформи спільної роботи, канали обміну документами тощо. Для аудиторських фірм поверхня атаки закономірно є ширшою, ніж у багатьох інших організацій, оскільки аудит працює у багатоклієнтському режимі, використовує спільні інструменти колаборації, регулярно отримує й передає конфіденційні дані, а також взаємодіє з різними інформаційними середовищами клієнтів. У таких умовах компрометація навіть одного робочого облікового запису може швидко перетворюватися на «ланцюговий» інцидент спочатку порушується безпека всередині фірми, а далі ризик поширюється на клієнтські проєкти через спільні сховища, доступи, інтеграції та робочі канали обміну. Тому управління поверхнею атаки в

аудиторській практиці означає системну роботу з доступами, налаштуваннями, сегментацією, журналюванням і контролем взаємодій, тобто з тими елементами, які реально визначають стійкість процесів у цифровому середовищі.

У тематиці захисту цифрових ідентичностей центральним поняттям виступає ***MFA (багатофакторна автентифікація)*** – механізм, за якого підтвердження особи відбувається щонайменше двома незалежними факторами: *знання* (пароль або код), *володіння* (телефон, токен, застосунок) або *біометрія* (відбиток, FaceID тощо).

Серед загроз провідне місце посідають фішинг і соціальна інженерія – методи маніпуляції, спрямовані на те, щоб користувач сам розкрив облікові дані або виконав небезпечну дію. Однією із них є credential stuffing (автоматизовані спроби входу із застосуванням баз викрадених логінів і паролів), які стають особливо ефективними тоді, коли люди повторно використовують один і той самий пароль у різних сервісах. Саме ці сценарії пояснюють, чому захист облікового запису в аудиторській діяльності не зводиться до формули «складний пароль», а передбачає комплекс політики унікальності, MFA, рольову модель доступу та контроль привілеїв.

Окремо для аудиторських фірм критичною є група ризиків третіх сторін і ланцюга постачання (supply chain), коли атака відбувається через довірені зв'язки між організацією та її постачальниками, підрядниками або сервісами. У практиці аудиту фірма фактично стає вузлом довіри: вона працює з консолідованими даними клієнтів і нерідко має доступ до їхніх систем, тому компрометація аудитора потенційно відкриває шлях до кількох організацій одночасно. У цьому контексті доречно відразу зафіксувати стратегічний принцип ***Zero Trust*** – підхід, за якого жоден запит не вважається надійним за замовчуванням, а доступ надається лише за умови постійної верифікації та дотримання принципу мінімальних привілеїв.

Додатковий рівень ризику пов'язаний із тим, що аудиторські команди паралельно ведуть кілька клієнтських проєктів і використовують спільні робочі середовища, шаблони, репозиторії та канали обміну файлами. Якщо

корпоративний обліковий запис співробітника компрометується, зловмисник може отримати можливості для повторного використання токенів доступу, доступу до спільних каталогів, викрадення ключів API або непомітного переміщення всередині внутрішньої інфраструктури. За такої організації роботи навіть інцидент, що починається з одного користувача (фішинг або компрометація пароля), швидко масштабується до проблеми всієї фірми, впливаючи на кілька процесів і клієнтських середовищ одночасно.

Інтеграція з клієнтськими системами є найбільш чутливою. Для виконання аудиторських завдань зазвичай надається тимчасовий або гостьовий доступ до ERP або CRM, корпоративних порталів та файлових серверів, систем управління документами або аналітичних платформ. У більшості випадків, оскільки не впроваджено принципи мінімальних привілеїв разом із чіткими термінами дії прав доступу, призначені «тимчасові» привілеї легко стають постійними, крім того, множинність облікових записів у різних клієнтських доменах ускладнює контроль. Це створює саме таке середовище, де компрометація аудитора може бути використана як місток для проникнення в клієнтські середовища.

Гібридна модель роботи створює додатковий тиск у сучасних умовах:

- *віддалена робота;*
- *хмарні сервіси;*
- *спільні робочі простори;*
- *мобільні пристрої.*

Зловмисники активно використовують неправильні конфігурації в налаштуваннях безпеки хмари, помилки в управлінні сеансами, неефективні політики доступу та людський фактор під час обміну документами. Саме тому необхідний централізований захист із багатофакторною перевіркою, яка враховує контекст місця перебування користувача, надійність його пристрою та загальний рівень ризику в цей момент.

Наслідки інцидентів для аудиторських фірм посилюються нормативними та договірними зобов’язаннями, такими як обробка персональних даних та конфіденційної інформації, з урахуванням вимог щодо захисту даних. Ці

порушення можуть призвести не лише до прямих витрат на відшкодування, але й до юридичної відповідальності, розірвання договору, втрати можливостей ліцензування або акредитації, репутаційної шкоди та зниження довіри до ринку.

Кібербезпеку слід розглядати як елемент професійної придатності та як частину системи внутрішнього контролю якості аудиторських фірм, а не виключно як IT-функцію.

Бізнес будь-якого масштабу стикається з широким спектром кіберзагроз. Найпоширеніші типи атак включають шкідливе програмне забезпечення (віруси, трояни, програми-вимагачі), фішинг та інші методи соціальної інженерії, атаки типу відмова в обслуговуванні (DoS, DDoS), компрометацію облікових записів (злам паролів, викрадення облікових даних) і внутрішні загрози. У таблиці 10.2 наведено основні категорії загроз, їх характеристику та наслідки (приклади).

Таблиця 10.2.

Основні типи кіберзагроз для бізнесу

Загроза	Характеристика	Наслідки
Фішинг (в т.ч. смішинг)	Шахрайські розсилки електронною поштою або SMS з метою виманити конфіденційні дані або змусити встановити malware	Викрадення облікових даних співробітника через e-mail, що імітує лист від партнера, з подальшим зламом внутрішньої мережі
Шкідливе ПЗ (malware)	Зловмисні програми (віруси, трояни, spyware тощо), що непомітно інфікують системи, крадуть дані або порушують роботу	Масова атака вірусу-шифрувальника на ПК компанії, що паралізує бізнес-процеси і потребує відновлення систем
Програми-вимагачі (ransomware)	Тип malware, що шифрує дані жертви та вимагає викуп за відновлення доступу. Сучасні версії комбінують шифрування з викраденням даних (подвійний та навіть «потрійний» шантаж)	Атака програми-вимагача на виробничу компанію: шифрування серверів, простої виробництва, вимога викупу в біткоїнах. У 66 % організацій у 2022 році принаймні раз успішно застосовано ransomware-атаку
Компрометація ділової пошти (BEC)	Обман шляхом втручання у бізнес-листування: зловмисник отримує доступ до корпоративної пошти та видає себе за керівника чи партнера, щоб переконати співробітників здійснити несанкціонований платіж або видачу даних	Випадок Business Email Compromise: бухгалтер перераховує велику суму на рахунок шахраїв, прийнявши фальшивий лист нібито від директора (збитки BEC у 2023 р. – $2,9 млрд)

Атаки на відмову в обслуговуванні (DDoS)	Перевантаження мережевих сервісів фальшивим трафіком, що робить сервіси недоступними для користувачів. Часто здійснюється розподіленими ботнет-мережами заражених пристроїв	DDoS-атака на веб-сайт інтернет-магазину під час розпродажу, що призводить до простою сайту і втрати продажів. У 2022–2023 рр. фіксувалося зростання потужності DDoS-атак проти фінансового сектору та держорганів
Внутрішні загрози	Навмисні чи випадкові дії співробітників або контрагентів, що призводять до витоку або пошкодження даних. Можуть включати зловмисні дії інсайдерів або нехтування правилами безпеки	Системний адміністратор копіює конфіденційні дані клієнтів на особистий носій і продає на стороні; або працівник випадково відкриває шкідливий файл, запускаючи зараження мережі

За даними Держспецзв'язку, фішингові атаки залишаються наймасовішою загрозою. Це метод №1 у кібервійні росії проти України, так як понад 90 % усіх інцидентів розпочинаються саме з фішингового повідомлення.

Зловмисники використовують фішинг для:

- *викрадення облікових даних* (логінів та паролів);
- *розповсюдження шкідливого ПЗ* (шпигунських програм);
- *початкової фази диверсій* (проникнення в мережі критичних підприємств).

Приклад: У грудні 2023 року атака на «Київстар» розпочалася зі зламу облікового запису працівника. Це дозволило російським хакерам проникнути в систему та знищити віртуальну інфраструктуру компанії. Наслідком став повний блекаут зв'язку для 24 млн абонентів та мільярдні збитки. Один скомпрометований пароль став причиною найбільшої телеком-катастрофи в історії України.

Шкідливе програмне забезпечення ***(malware)*** продовжує еволюціонувати, набуваючи форм, здатних обходити традиційні захисні механізми. Зловмисники створюють його для прихованого отримання доступу (бекдори), крадіжки даних, перехоплення введених паролів. Особливо руйнівними є програми-вимагачі (ransomware), які шифрують файлові системи підприємств. За результатами щорічного дослідження Sophos «The State of Ransomware 2023» понад дві

третини опитаних організацій (66 %) повідомили, що протягом попередніх 12 місяців зазнали ransomware-атаки, що підтверджує стабільно високий рівень поширеності цього класу загроз у бізнес-середовищі. Практичні наслідки програм-вимагачів виходять за межі тимчасового шифрування файлів і включають операційні простої, витрати на відновлення та реагування, а також ризики порушення конфіденційності через поєднання шифрування з ексфільтрацією даних (типова модель «double extortion»), коли зловмисники підсилюють тиск погрозою публікації або продажу викраденої інформації.

Атаки типу ***«відмова в обслуговуванні» (DoS, DDoS)*** також загрожують бізнесу, особливо тим, хто надає онлайн-послуги. Розподілені DDoS-атаки, що використовують ботнети, можуть на тривалий час вивести з ладу веб-сайти та сервіси підприємства. Хоча прямого вилучення даних при DDoS не відбувається, фінансові та репутаційні втрати від простою є значними. У деяких випадках DDoS використовується як відволікаючий маневр, поки зловмисники здійснюють інші приховані дії. За останні роки зафіксовано збільшення кількості DDoS-атак на фінансові установи та державні структури, зокрема під час геополітичної напруги та воєнних конфліктів.

За даними Accounting Today, у 2020–2022 рр. спостерігався сплеск атак на бухгалтерські й аудиторські фірми (майже на 300 % більше інцидентів) саме внаслідок переходу на віддалену роботу і розмивання периметру безпеки.

Сьогодні в Україні кіберзагрози стали частиною бойових дій, де головна мета росії не заробити гроші, а знищити дані. На відміну від західних країн, де хакери зазвичай вимагають викуп, проти нашого бізнесу все частіше використовують ***вайпери*** – шкідливі програми, які повністю стирають фінансові бази та аудиторські звіти без можливості відновлення (рис. 10.1). Для бухгалтера чи аудитора це часто виглядає як звичайний лист про «податкову перевірку» або «оновлення звітності», але після відкриття вкладення вся документація підприємства просто зникає. Одночасно з цим російські хакери проводять масовані DDoS-атаки на великі банки, як-от Monobank чи ПриватБанк протягом 2024–2025 років. Це не просто заважає вчасно провести платежі, а часто слугує

«димовою завісою», щоб відволікти технічних спеціалістів, поки хакери приховано викрадають паролі чи бази клієнтів.

Найбільшим ризиком залишається людський фактор, а саме через віддалену роботу та постійні блекаути фахівці часто заходять у робочі системи через незахищений домашній Wi-Fi або особисті ноутбуки, що робить їхні облікові записи вразливою ціллю. Високий рівень психоемоційного напруження суттєво знижує поріг критичного сприйняття інформації, що сприяє успішній реалізації атак із використанням соціальної інженерії (соціальних виплат або оновлення КЕП). Для спецслужб росії злам комп'ютерів фінансового сектору є пріоритетом, оскільки це дозволяє не лише виводити кошти, а й викрадати конфіденційну звітність, повністю паралізуючи роботу всього підприємства.

Рис. 10.1. Ланцюг кібератаки для аудиторської компанії (модель циклу з 8 етапів).

Як показано на рисунку 10.1, компрометація облікового запису в реальних кібератаках зазвичай не є разовим епізодом і виступає стартовою подією, яка запускає послідовний ланцюг дій зловмисника. Первинний доступ у такому ланцюгу поступово перетворюється на стійку присутність у середовищі, розширення прав, контроль над ресурсами, вплив на дані й операційну безперервність. Контрольні точки вказаного ланцюга зосереджуються не лише на вході (пароль та MFA), а й розташовуються на кожному наступному кроці. Це означає, що захист облікових записів оцінюють як систему взаємопов'язаних контролів, а не як одну вимогу.

На першій фазі ***(Initial access)*** відображено типові механізми проникнення: фішинг, використання викрадених паролів, зловживання віддаленим доступом, експлуатація слабкої автентифікації.

Для аудиту цей етап безпосередньо прив'язується до якості політик управління ідентичностями:

- *наявності MFA;*
- *дисципліни паролів;*
- *правил віддаленого доступу;*
- *практик виявлення підозрілих спроб входу.*

Далі етап закріплення ***(Foothold)*** показує, як первинний доступ утримується через токени сесій, зміни налаштувань, створення прихованих облікових записів або встановлення інструментів віддаленого керування. Саме тут стає очевидним, що вимога складного паролю є недостатньою, адже нам потрібні моніторинг аномалій, контроль інтерактивних сесій, швидке відкликання доступів і кероване реагування.

Етапи ***Privilege escalation*** та ***Lateral movement*** демонструють механізм переходу від обмежених прав до привілейованих і поширення атаки по середовищу.

Зловмисник досягає цього через викрадення адміністративних облікових даних, використання помилок у розмежуванні прав або слабкі політики управління привілеями. Для навчальної практики тут ключовими є принципи

least privilege, сегментація, підхід Zero Trust і застосування PAM (керування привілейованим доступом): чим чіткіше обмежені права та ізольовані середовища, тим нижча ймовірність, що компрометація одного облікового запису переростає у масштабний інцидент. Іншими словами, зменшення «радіуса ураження» стає такою ж важливою метою, як і блокування первинного проникнення.

Наступні фази ***Discovery or Collection*** та ***Exfiltration*** у моделі фокусують увагу на переході від технічного доступу до контролю над інформацією. На цьому відрізку атакувальник ідентифікує цінні ресурси, збирає дані та намагається вивести їх за межі організації.

У контексті аудиту це підводить до практичних вимог щодо класифікації даних, обмеження доступів до чутливих масивів, журналювання, шифрування та впровадження DLP-політик. Важливо, що саме ці контролі часто визначають, чи стане інцидент локальним технічним збоєм, чи переросте у витік даних із суттєвими фінансовими й правовими наслідками.

Для аудиторських фірм важливо не тільки знати перелік загроз, а й розуміти, через які канали вони зазвичай реалізуються. З цією метою наведено матрицю «загроза–канал–вектор», яка пов’язує типову помилку з ранніми індикаторами та потрібними контролями (табл. 10.3).

Таблиця 10.3

Матриця «загроза–канал–вектор» для аудиторської фірми

Загроза	Канал атаки	Типова уразливість	Ранній індикатор	Превентивний контроль	Контроль виявлення
Фішинг	Пошта, месенджери	Відсутність MFA, слабке навчання	Нові правила пересилання, підозрілий вхід	MFA, DMARC, SPF, DKIM, тренінги	SIEM-алерти, журнал аудиту пошти
Компрометація SSO	IdP, SSO	Слабкий умовний доступ	Незвична геолокація або пристрій	Conditional Access, MFA, перевірка відповідності пристрою	Журнали IdP, UEBA-аналіз
Шкідливі вкладення	Пошта, файли	Відсутність пісочниці, EDR	Запуск макросів, підозрілий процес	EDR, блокування макросів, пісочниця	Спрацювання EDR, ізоляція кінцевого пристрою

Програми-вимагачі	Початковий доступ, мережа	Слабка сегментація	Масове перейменування файлів	Сегментація, резервне копіювання	EDR, файлові алерти, IDS
Експлуатація уразливості вебсервісу	Вебсервіс, API	Застарілі патчі, помилки конфігурації	Аномальний трафік, помилки 5xx	Встановлення патчів, WAF, посилення конфігурації	Події WAF, IDS, SIEM
Ланцюг постачання, треті сторони	Сервіс обміну, підрядник	Надмірні інтеграції, токени	Неочікувані API-запити	Оцінка постачальника, ізоляція інтеграцій	Журнали API, ревізія токенів
Внутрішній порушник	Доступи до даних	Відсутнє розмежування обов'язків, надмірні права	Нетипові масові завантаження	Розмежування обов'язків (SoD), RBAC, DLP	DLP, журнали доступу, UEBA
Зміни в системі без контролю	ERP, сервери	Відсутній контроль змін	Зміни без заявки	Управління змінами, перевірка, затвердження	Журнали змін, контрольні звіти

Таблиця 10.3 підкреслює, що один і той самий інцидент часто має різні першопричини: технічну (вразливість), організаційну (процес доступів) або поведінкову (фішинг).

Це означає, що ефективний захист має бути багаторівневим:

- *політики доступу;*
- *моніторинг;*
- *дисципліна змін.*

Аудиторські та бухгалтерські фірми зазнають усіх загальних кіберзагроз, характерних для бізнесу, однак водночас мають підвищену вразливість через специфіку діяльності. Вони постійно оперують великими масивами конфіденційної фінансової інформації, персональними даними клієнтів, робочими документами аудиту та відомостями про внутрішній контроль. Це підвищує значущість організації як цілі для атак вмотивованих фінансовою вигодою, так і доступом до інсайдерської інформації або промисловим шпигунством.

Компрометація або витік даних з аудиторської інфраструктури має подвійний ефект. По-перше, це створює прямі ризики для клієнтів (використання

інформації для нечесної конкуренції, шахрайства, маніпуляцій), по-друге завдає значної шкоди репутації самої фірми.

Для аудиторського ринку довіра є ключовим активом, а тому інциденти безпеки можуть призводити не лише до фінансових втрат, а й до судових позовів, регуляторних санкцій і втрати клієнтської бази. Окремо зростає значущість правових наслідків, коли в обігу перебувають персональні дані та інша інформація, захищена законом.

Ransomware-інциденти для аудиторських фірм особливо небезпечні через залежність від календаря звітності та жорсткі дедлайни. Зупинка IT-систем у критичний період паралізує роботу команд і може зірвати виконання контрактних зобов'язань. Зловмисники враховують цю обставину, обираючи момент атаки для максимального тиску. Отже, готовність до відновлення (резервні копії, плани BCP, DR, тестування відновлення) в аудиті має не технічний, а безпосередньо бізнесовий і фінансовий вимір.

Аудиторські фірми функціонують як вузли довіри у міжорганізаційних процесах: вони одночасно працюють з кількома клієнтськими середовищами, застосовують спільні сервіси колаборації, обмінюються файлами та використовують віддалений доступ. Унаслідок цього загальні кіберзагрози (фішинг, компрометація облікових даних, шкідливе ПЗ, ransomware) доповнюються специфічними ризиками атаками через третіх сторін, цільовими кампаніями проти високоцінної інформації та комплаєнс-наслідками у випадку витоку. Саме тому захист ідентичностей, контроль доступу, сегментація середовищ і управління взаємодіями з постачальниками мають розглядатися як базові елементи фінансової безпеки в сучасній аудиторській практиці.

Критичною особливістю аудиторської діяльності є залежність від програмних продуктів і сервісів сторонніх постачальників: від офісних пакетів і систем керування проєктами до рішень класу managed file transfer (MFT), платформ колаборації, сховищ доказів і аналітичних модулів. Це формує підвищений ризик третіх сторін (third-party risk), коли атакувальник може спрямувати зусилля не проти аудитора безпосередньо, а проти постачальника

сервісу чи конкретного програмного продукту, щоб масштабувати вплив одразу на багато організацій-користувачів.

Інциденти довкола MOVEit Transfer (2023) є показовими саме як модель ланцюгового ризику. Урядові попередження фіксували експлуатацію критичної уразливості (зокрема CVE-2023-34362) групою CL0P із фокусом на несанкціонований доступ і викрадення даних з уражених середовищ. Постачальник продукту підтверджував критичність проблеми та необхідність термінового застосування оновлень і мітигацій. У цьому прикладі важливим є не лише технічний збій, а й управлінський висновок: навіть за наявності зрілої системи внутрішніх контролів безпеки аудиторської фірми вразливість у сторонньому програмному продукті може спричинити компрометацію аудиторських матеріалів або файлів, що передаються клієнтам.

Практичну природу ланцюгового інциденту наочно демонструє ситуація, коли витік даних фіксується у клієнта як наслідок інциденту в аудиторській компанії, яка використовувала уражений сервіс передавання файлів. Офіційні повідомлення про інциденти показують, що технічна уразливість швидко переростає в репутаційні та правові ризики, а компрометація сервісу обміну документами може спричинити витік персональних даних навіть без прицільної атаки на конкретного клієнта.

Великі аудиторські компанії обслуговують провідних учасників ринку, а подекуди й державні інституції; відповідно, у їхніх інформаційних системах накопичуються значні обсяги даних, що можуть становити інтерес для конкурентів, кіберзлочинних угруповань або держав-опонентів. За таких умов зростає ймовірність цільових кібератак, зокрема з боку ***APT груп (advanced persistent threat)***, для яких характерні приховане викрадення інформації та тривала присутність у середовищі.

В APT сценаріях метою є не виведення систем із ладу, а значно частіше йдеться про встановлення контролю над інформаційними потоками та отримання доступу до корпоративного листування, робочих документів, аудиторських доказів й управлінських матеріалів.

У практиці ризик-аналізу важливо відрізняти загрозу як джерело небажаної події від уразливості як конкретного слабкого місця, що робить атаку можливою. Таке розмежування допомагає перейти від загального опису ризиків до конкретних управлінських рішень щодо того, які саме контролі слід посилити.

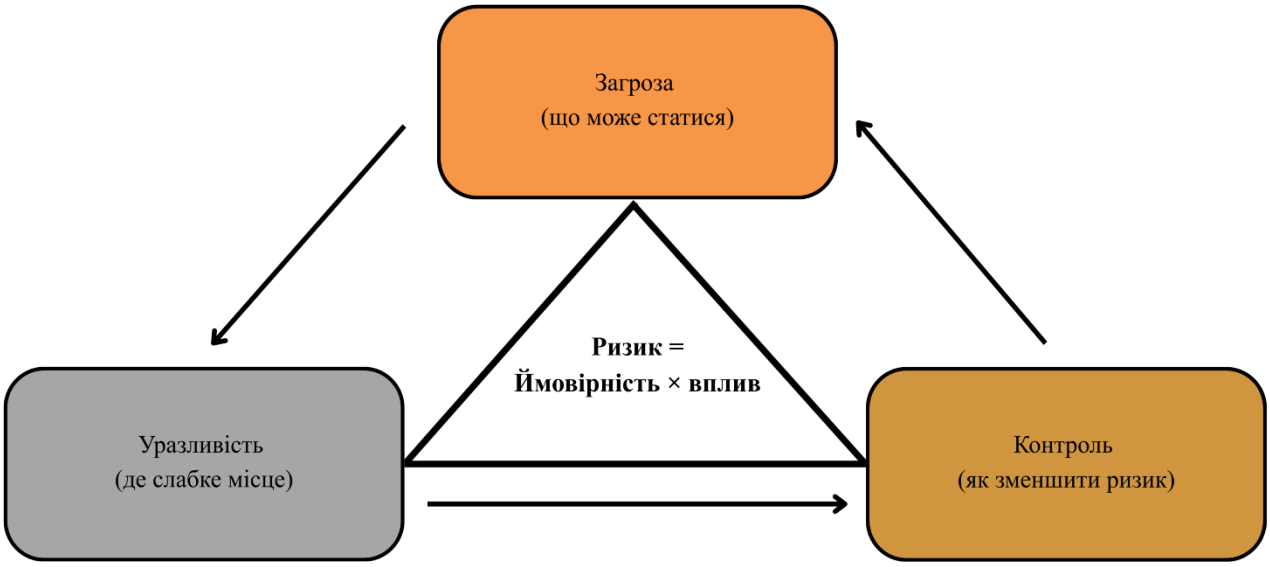


Рис. 10.2. Трикутник аналізу кіберризику: загроза–уразливість–контроль

Як показано на рисунку 10.2, контроль впливає на ризик двома способами: зменшує ймовірність реалізації загрози або обмежує масштаб наслідків. Тому оцінка кіберризику має включати не лише перелік загроз, а й аналіз вразливостей та наявних або відсутніх контролів.

Для аудиторського сектору важливо враховувати не тільки технічні загрози, а й ризики втрати конфіденційності через організаційні та управлінські проблеми. Це можуть бути помилки в управлінні доступом до даних, конфлікти інтересів або неправомірне використання інформації. Резонансні випадки, які в публічних обговореннях пов’язують із витоками податково-консультаційних даних, показують, що втрати довіри можуть бути такими ж серйозними, як і наслідки кібератаки. У відповідь клієнти зазвичай переглядають правила обміну даними, уточнюють умови договорів і висувають вищі вимоги до контролів та прозорості управління ризиками.

Посилення загроз призвело до того, що кібербезпека стала предметом постійного нагляду органів корпоративного управління. Опитування аудиторських комітетів показують, що кібербезпека стабільно залишається серед ключових пріоритетів, адже інциденти впливають на безперервність бізнесу, ризики фінансової звітності та довіру інвесторів. Для аудиторської діяльності це означає зростання очікувань клієнтів щодо підтвердженої ефективності контролів у сферах доступу, моніторингу та готовності до інцидентів.

10.2. Захист облікових записів, доступу до інформаційних систем і внутрішніх даних (резервне копіювання та відновлення)

Однією з найбільших вразливостей інформаційних систем залишаються облікові записи користувачів – логіни та паролі, що забезпечують доступ до внутрішніх ресурсів.

Зловмисники використовують дедалі складніші техніки для компрометації цих даних, включаючи фішинг на основі ШІ та атаки на обхід багатофакторної автентифікації (MFA). Згідно зі звітом ***Verizon DBIR 2024,*** використання вкрадених або слабких облікових даних залишається вектором №1 для проникнення в системи (це стосується 77 % атак на вебдодатки). Водночас, за даними ***Microsoft Digital Defense Report 2024,*** понад 99 % усіх атак на ідентифікаційні дані базуються саме на зламі паролів (через їхнє повторне використання, підбір або фішинг), що підтверджує критичну необхідність переходу до безпарольних методів захисту.

Захист облікових записів починається з розмежування типів акаунтів: звичайні користувачі, привілейовані адміністратори та сервісні облікові записи. Для кожної категорії потрібні різні вимоги до MFA, умовного доступу й моніторингу. Мінімальний стандарт таких вимог наведено в таблиці 10.4.

Таблиця 10.4.

Мінімальний стандарт політик доступу для облікових записів

Категорія акаунта	MFA	Умовний доступ	Паролі або ключі
Звичайний користувач	Обов’язково	Геолокація, ризик, пристрій	Унікальні паролі, менеджер паролів
Привілейований (адміністратор)	Обов’язково, посилена MFA	Лише керовані пристрої, доступ за потреби (JIT)	PAM, ротація, заборона спільних облікових даних
Сервісний	За можливості, ключі доступу	IP, контекст, мінімальний доступ	Сховище секретів, ротація

Таблиця 10.4 показує, що найбільший ризик виникає там, де привілейовані доступи не відокремлені й не контролюються (немає JIT або PAM, немає запису сесій). Саме тому управління привілеями є критичним елементом контролю доступу в аудиті та фінансово значущих системах.

Наслідки компрометації облікових записів можуть бути надзвичайно серйозними. Отримавши доступ під обліковим записом користувача (особливо адміністратора чи іншого з розширеними правами), зловмисник може викрасти конфіденційні дані, внести несанкціоновані зміни або розгорнути шкідливе ПЗ (наприклад, ransomware яке шифрує дані). При цьому часто залишається непоміченим тривалий час. Середній час виявлення проникнення після фактичного злому у 2024 році становив 194 дні, а окремі витоки залишаються невиявленими багато місяців. Зокрема, інциденти, в яких зловмисники використовували вкрадені облікові дані, мали найдовший життєвий цикл у середньому 292 дні від проникнення до повної ліквідації наслідків. За цей час атакувальники можуть непомітно поширити свій доступ у системі (латеральне переміщення) і завдати максимальної шкоди.

Особливо високими є ризики у разі ***компрометації привілейованих облікових записів,*** зокрема адміністраторів систем і користувачів із розширеними правами доступу до значних масивів конфіденційних даних. Такі облікові записи надають критичні повноваження в IT-середовищі, тому є пріоритетною ціллю для кіберзлочинців. Джерелом загрози можуть бути не лише зовнішні атакувальники, а й інсайдери, тобто недобросовісні або скомпрометовані працівники, які зловживають наданими правами доступу. Загалом захист облікових записів є базовим рівнем безпеки, оскільки отримання чужих автентифікаційних даних дозволяє зловмиснику обійти значну частину периметрових механізмів захисту.

Пароль традиційно є основним механізмом автентифікації користувача. Однак звичайні підходи до паролів (вимоги складності, періодична зміна тощо) із часом потребували перегляду через проблеми зручності та безпеки. Актуальні стандарти (наприклад, NIST SP 800-63B) рекомендують відмовитися від

надмірно частого примусового змінювання паролів і від застарілих вимог, наприклад обов'язкового використання спеціальних символів. Такі політики нерідко призводять до того, що користувачі створюють слабкі шаблонні паролі або змушені їх записувати. Натомість необхідно робити ставку на довжину пароля та унікальність, а саме: використовувати пасфрази (довгі парольні фрази), які легше запам'ятати, але важко зламати перебором, та не допускати повторного використання паролів для різних сервісів.

Важливо також перевіряти нові паролі на відсутність у відомих витоках. У багатьох випадках сучасні системи автентифікації можуть відхиляти пароль, якщо він присутній у базах зламаних паролів. Для зручності і безпеки рекомендується застосовувати менеджери паролів, які дозволяють генерувати стійкі випадкові паролі і зберігати їх у зашифрованому вигляді. Попри всі ці зусилля, людський фактор й надалі залишається слабкою ланкою, адже значна частка користувачів продовжує використовувати вразливі паролі або спільні між акаунтами секрети. Тому одного пароля недостатньо, щоб забезпечити необхідне додаткове підсилення автентифікації.

MFA вимагає від користувача підтвердити особу поєднанням кількох факторів:

- *знання* (пароль або PIN);
- *володіння* (пристрій або токен);
- *біометрії* (відбиток пальця, розпізнавання обличчя тощо).

Найпоширеніший варіант – ***двофакторна автентифікація (2FA),*** коли до паролю додається одноразовий код з мобільного додатку (наприклад, Google Authenticator), СМС або апаратного ключа (наприклад, YubiKey). Впровадження MFA кардинально підвищує захищеність облікових записів, навіть якщо пароль викрадено, то зловмисник не зможе увійти без другого фактора.

За оцінками Microsoft, багатофакторна автентифікація блокує 99 % атак, спрямованих на захоплення облікового запису.

Концепція ***Single Sign-On (SSO)*** передбачає, що користувач автентифікується один раз у центральній системі, після чого отримує доступ до

багатьох сервісів без повторного введення пароля. Реалізація SSO часто базується на протоколах федерації автентифікації (SAML, OAuth 2.0, OIDC), і сучасні організації широко впроваджують її через провайдерів ідентичності, таких як Azure AD, Okta, Google Workspace тощо.

Переваги SSO очевидні:

- *користувачі запам'ятовують менше паролів* (зменшується ризик використання одного пароля всюди);
- *знижується навантаження на підтримку* (менше запитів на скидання паролів);
- *централізовано застосовуються політики безпеки* (наприклад, MFA на рівні SSO поширюється на всі підключені додатки).

Однак SSO висуває підвищені вимоги до захисту центрального вузла автентифікації, а саме: компрометація SSO-акаунта відкриває двері одразу в усі пов'язані системи. Відомим інцидентом є злам постачальника SSO-послуг Okta у 2022 році, коли хакерська група LAPSUS$ отримала доступ до облікових даних інженера служби підтримки зовнішнього підрядника (Sitel), чим скомпрометувала внутрішні системи Okta та потенційно дані сотень її корпоративних клієнтів. Хоча Okta запровадила багаторівневий захист, цей випадок показав, що ланцюг довіри в SSO є настільки надійним, наскільки надійною є його найслабша ланка. Атака через стороннього підрядника дала змогу обійти основні бар'єри. Отже, при використанні SSO необхідно приділяти особливу увагу захисту ідентифікаційної інфраструктури (сувора MFA для адміністраторів і інтеграцій, моніторинг підозрілої активності, оперативне відключення скомпрометованих інтеграцій).

Традиційні підходи до кібербезпеки ґрунтувалися на периметровій моделі: вважалося, що всередині корпоративної мережі користувачам і пристроям можна довіряти більше, ніж зовні. ***Концепція Zero Trust (нульової довіри)*** докорінно змінює цю парадигму, керуючись принципом «нікому не довіряй за замовчуванням, завжди перевіряй». У рамках Zero Trust кожен запит на доступ до ресурсу має бути автентифікований, авторизований і за необхідності

додатково перевірений незалежно від того, звідки або від кого він надходить. Модель нульової довіри виходить з того, що компрометація може статися будь-де навіть всередині мережі тому мережевий периметр не може гарантувати безпеку.

Практична реалізація Zero Trust зводиться до кількох ключових принципів:

1. Неперервна верифікація. Автентифікація користувача та перевірка його прав виконується кожного разу при доступі до нового ресурсу, сесії або транзакції, а не лише при початковому вході.

2. Принцип найменших привілеїв. Користувачам і пристроям надається мінімально необхідний доступ і лише на час виконання конкретного завдання.

3. Доступ контролюється за контекстними та динамічними правилами. Політика враховує контекст запиту тип пристрою та його безпековий стан, місцезнаходження, час, поведінкові фактори і на основі цього обчислює рівень довіри та ризику.

Нарешті, здійснюється постійний моніторинг і управління ризиками, система відстежує аномалії в реальному часі і може автоматично змінювати рівні доступу або вимагати додаткову автентифікацію при зростанні ризиків.

У типовій Zero Trust-архітектурі, згідно з NIST SP 800-207, виділяють центральні логічні компоненти:

- *Policy Engine* (механізм ухвалення рішень про доступ на основі політик і даних моніторингу);
- *Policy Administrator* (компонент, що впроваджує рішення, відкриваючи або закриваючи доступ);
- *Policy Enforcement Point* (точка безпосереднього контролю, яка пропускає або блокує трафік).

Додатково залучаються джерела даних системи безперервного моніторингу стану пристроїв, аналізу поведінки користувачів, розвідки загроз, які надають Policy Engine інформацію для прийняття рішень.

На рисунку 10.3 схематично зображено таку архітектуру Zero Trust із основними взаємодіями компонентів.

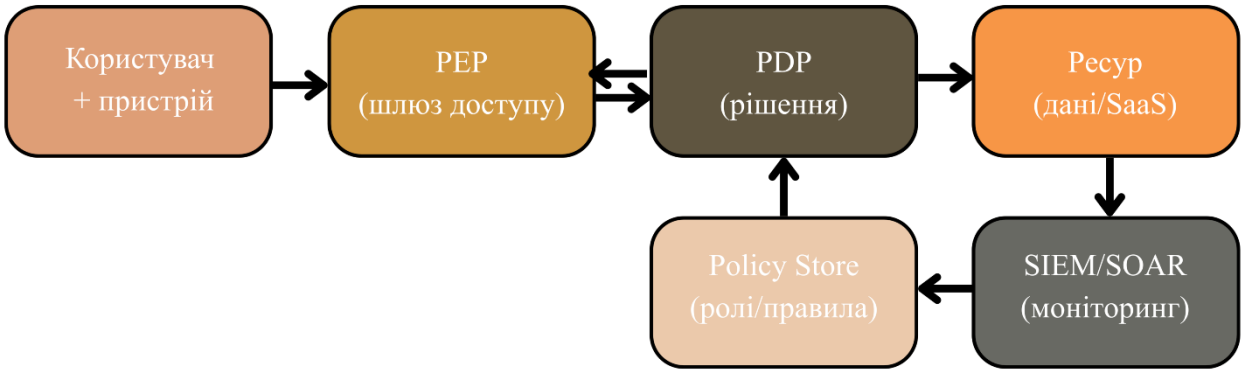


Рис. 10.3. Логічна схема Zero Trust-архітектури (основні компоненти та потоки авторизації)

Модель передбачає, що Policy Engine (двигун політик) отримує дані від моніторингових систем (стан пристрою, облікового запису, показники аномалій), на основі політик ухвалює рішення про надання або заборону доступу; Policy Administrator реалізує ці рішення шляхом налаштування точок доступу; Policy Enforcement Point є шлюзом, через який проходить трафік користувача до захищених ресурсів і який застосовує рішення Policy Engine. У Zero Trust кожен доступ є умовним і потребує повторної авторизації, навіть якщо запит надходить з внутрішньої мережі.

Впровадження Zero Trust – це поступовий процес, який вимагає перегляду багатьох аспектів інфраструктури безпеки: від сегментації мережі (розмежування ресурсів на дрібні зони з індивідуальним контролем доступу) до впровадження контролю доступу на основі ролей та атрибутів, шифрування внутрішнього трафіку та постійного аудитування дій користувачів.

Великі корпорації, такі як Google, Microsoft та інші, вже реалізували елементи Zero Trust у своїх мережах – наприклад, підхід BeyondCorp від Google дозволив співробітникам безпечно працювати з будь-якої локації без традиційного VPN, покладаючись на перевірку кожного запиту до ресурсів. Стандарти, такі як ISO/IEC 27001:2022, також враховують ці тенденції. Оновлені контрольні заходи рекомендують принцип «нульової довіри» при побудові політик доступу. Загалом, Zero Trust є сучасною відповіддю на складні атаки,

вона мінімізує потенційну шкоду від нього шляхом жорсткого контролю кожної сесії та мінімізації довіри до будь-якого елемента системи.

Захист облікових записів – це необхідна, але недостатня умова безпеки. Паралельно слід забезпечити комплексний контроль доступу до інформаційних систем і даних. Йдеться про набір організаційних і технічних заходів, спрямованих на те, щоб усі суб'єкти (користувачі або процеси) мали потрібний рівень доступу до відповідних ресурсів і лише за належних умов. Розглянемо ключові елементи такого захисту. Усі користувачі та адміністратори повинні мати доступ виключно до тих даних і систем, які потрібні їм для роботи (принцип Least Privilege).

Для цього впроваджуються моделі контролю доступу:

- *рольова* (RBAC), де ролі призначаються з певними правами користувачам;
- *дискреційна* (DAC), де власник ресурсу або уповноважений користувач визначає права доступу до об'єкта шляхом надання або відкликання дозволів конкретним суб'єктам;
- *мандатна* (MAC), де правила доступу встановлюються централізовано політикою безпеки на основі рівнів допуску та класифікації інформації, а користувачі не можуть змінювати ці правила на власний розсуд;
- *атрибутна модель* (ABAC), де рішення про доступ приймається на основі атрибутів суб'єкта, об'єкта та контексту.

Важливим є ***управління привілейованими обліковими записами (Privileged Access Management, PAM)***, адже це дуже ризиковано залишати адміністративні паролі незмінними або відомими широкому колу осіб.

Необхідно запровадити політики обмеження привілеїв, видачі адміністраторських прав лише на час виконання завдання та контролю дій адміністраторів (через журналювання, двосторонній контроль або використання ізольованих адміністративних середовищ). Існують спеціалізовані інструменти PAM, наприклад BeyondTrust Password Safe, CyberArk, які дозволяють безпечно

зберігати адміністраторські паролі, здійснювати аудит використання та регулярно змінювати їх. Підхід Zero Trust додатково передбачає перевірку контексту при наданні навіть дозволеної ролі доступу наприклад, якщо користувач з роллю «Фінансовий аналітик» раптом запитує великі обсяги даних з незвичної IP-адреси або в нестандартний час, система може вимагати повторної автентифікації або сповістити службу безпеки.

Оскільки багато внутрішніх систем доступні по мережі, критично важливими є засоби мережевої безпеки:

- *міжмережеві екрани* (фаєрволи);
- *системи виявлення* (IDS);
- *запобігання вторгненням* (IPS);
- *сегментація мережі на зони безпеки.*

Сегментація обмежує переміщення атакувальника у разі компрометації наприклад, база даних з персональними даними знаходиться у окремому сегменті, доступ до якого можливий лише через певні сервера додатків.

Мережі з нульовою довірою (ZTNA – Zero Trust Network Access) замінюють традиційні VPN. Замість повного доступу до внутрішньої мережі користувач отримує точковий захищений канал лише до конкретного сервісу, після успішної автентифікації і перевірки політик.

Такі рішення пропонують, наприклад, Cloudflare Access, Zscaler Private Access та інші. В контексті захисту даних, важливо також застосовувати шифрування: конфіденційні дані повинні зберігатися у зашифрованому вигляді (шифрування на рівні баз даних, дисків) і передаватися мережами виключно по захищених протоколах (TLS, VPN). Це гарантує, що навіть за несанкціонованого доступу до файлової системи або перехоплення трафіку, зловмисник не отримає інформацію в явному вигляді.

Система захисту доступу повинна передбачати відстеження підозрілої активності в режимі реального часу. Для цього розгортаються ***засоби моніторингу журналів і поведінки SIEM (Security Information and Event Management)*** платформи, такі як Splunk, IBM QRadar чи Microsoft Sentinel,

збирають події з різних джерел (вхід користувачів, спроби відмовленого доступу, зміни прав тощо) та аналізують їх на предмет індикаторів компрометації.

Наприклад, численні невдалі спроби логіну, а потім успішний вхід можуть свідчити про атаку перебору пароля, і система має негайно заблокувати такий обліковий запис і повідомити адміністраторів. Спеціалізовані рішення, як-от Microsoft Defender for Identity (раніше Azure ATP), відслідковують аномалії у поведінці облікових записів у корпоративних каталогах (Active Directory) – наприклад, нетипові запити LDAP, добавлення користувача до привілейованої групи і сигналізують про можливу компрометацію адміністратора або атаку типу Pass-the-Hash. В цілому, чим раніше буде виявлено спробу несанкціонованого доступу, тим менше шкоди вона завдасть.

Стратегії ***Endpoint Detection and Response (EDR) та Identity Threat Detection and Response (ITDR)*** доповнюють картину, дозволяючи автоматично реагувати на інциденти доступу. Вони здатні ізолювати кінцеві станції, відкликати маркери сесій, примусово скидати паролі тощо.

Під внутрішніми даними розуміють будь-яку інформацію компанії, доступ до якої має бути обмежений для сторонніх. Це можуть бути персональні дані клієнтів, фінансова документація, власні ноу-хау, службове листування тощо.

Для їхнього захисту використовується підхід ***Data Loss Prevention (DLP)*** – поєднання технологій і політик, що запобігають несанкціонованому винесенню або витоку інформації. DLP-системи можуть сканувати вихідний трафік, файли на кінцевих станціях та у хмарних сховищах на наявність певних типів даних (наприклад, номерів кредитних карт, паспортів) і блокувати або логувати передачу, якщо вона не відповідає політикам.

Крім цього, застосовується класифікація даних, тобто всі інформаційні ресурси маркуються відповідно до рівня чутливості (публічні, для службового користування, конфіденційні, секретні), і системи доступу враховують цю класифікацію при ухваленні рішень. Наприклад, документ з міткою «Конфіденційно» може бути доступний лише користувачам із відповідним рівнем допуску і тільки з корпоративних пристроїв.

Багато аспектів захисту доступу до систем і даних регулюються галузевими стандартами та нормативними актами. Міжнародний стандарт ISO/IEC 27001 зобов'язує організації впровадити політики керування доступом (Annex A.9) та заходи щодо забезпечення конфіденційності, цілісності й доступності інформаційних систем.

Оновлена версія ***ISO 27001:2022*** включає контроль 8.23 «Керування ідентифікацією та автентифікацією» і контроль 8.15 «Моніторинг активностей», які відповідають розглянутим підходам (вимоги використовувати належну автентифікацію, зокрема MFA, та вести журнали аудиту доступу). Окремий контроль 8.13 «Резервне копіювання» стосується захисту даних і вимагає регулярного створення та тестування резервних копій інформації.

Законодавчі акти, такі як GDPR в ЄС, також диктують суттєві вимоги: відповідно до статті 32 GDPR, компанія зобов'язана впровадити «належні технічні й організаційні заходи безпеки» для захисту персональних даних, включно з контролем доступу, шифруванням та засобами забезпечення постійної конфіденційності й доступності даних. GDPR також запровадив обов'язок повідомляти про витоки персональних даних протягом 72 годин з моменту їх виявлення. Ця норма стимулювала багато компаній посилити моніторинг доступів, аби вчасно виявляти інциденти і виконувати вимоги закону.

У США в 2023 році Комісія з цінних паперів і бірж (SEC) затвердила нові правила кібербезпеки для публічних компаній. Вони повинні розкривати у річних звітах інформацію про свою систему управління кіберризиками і контролем доступу. Крім того, суттєві кіберінциденти підлягають розкриттю у формі «Form 8-K» не пізніше ніж через 4 робочі дні після визначення їх суттєвості. Такі вимоги підсилюють значення належних контролів, у тому числі контролю доступу, оскільки недоліки в цих механізмах підвищують не лише імовірність інциденту, а й ризики регуляторних та репутаційних наслідків.

Резервне копіювання (backup) є останньою лінією оборони в кібербезпеці. Це особливо важливо перед загрозою знищення або шифрування даних внаслідок кібератаки чи технічного збою. Наявність актуальних резервних копій

дозволяє відновити системи до працездатного стану навіть після найкритичніших інцидентів. В наш час кіберзлочинці все частіше вдаються до ransomware-атак, вимагаючи викуп за розшифрування даних. Відтак, резервна копія дає шанс відновитися без сплати викупу.

Статистика підтверджує ефективність backup-стратегій. За даними Sophos, у 2023 році 97 % організацій, чиї дані були зашифровані, змогли відновити їх – здебільшого завдяки резервним копіям або іншим заходам (без або з мінімальною сплатою викупу). Показово, що серед компаній, які успішно відновилися після ransomware-атаки, 80 % невеликих підприємств покладалися саме на резервні копії, тоді як великий бізнес частіше змушений платити викупи (лише 63 % найбільших компаній змогли обійтися відновленням з backup). Таким чином, інвестиції в резервне копіювання напряму корелюють зі стійкістю до інцидентів: за оцінками, компанії, які мали напоготові ефективні резервні копії, заощадили в середньому $1 млн на витратах з ліквідації наслідків атак порівняно з тими, хто покладався на викуп.

Класичною рекомендацією для надійного резервування є правило 3-2-1, а саме: три копії даних, на двох різних носіях, одна з копій розташована поза основним майданчиком. Це означає, що окрім основної версії даних слід мати як мінімум дві резервні копії. Наприклад, одну на локальному сервері резервування, а другу у хмарному сховищі або на стрічковому носії, який зберігається в іншій локації. Такий підхід гарантує відсутність єдиної точки відмови, навіть якщо основний дата-центр буде знищено пожежею або фізичною катастрофою, одна копія залишиться неушкодженою поза ним.

Таблиця 10.5

Чек-лист 3-2-1 та ізоляція

Вимога	Як реалізовано	Доказ	Типова помилка
3 копії даних	Робоча копія, резервна копія, архів	Політика та інвентар резервних копій	Є лише одна резервна копія
2 різні носії	Диск, хмара або стрічка	Опис схеми зберігання	Усі копії на одному мережевому файловому сховищі

1 офлайн або незмінювана копія	незмінюване сховище	Налаштування незмінюваності	Резерв доступний з домену
Ізоляція доступів	Окремі облікові записи	Списки доступу, ролі, журнал доступів	Спільні акаунти з продуктивним середовищем
Перевірка виконання резервного копіювання	Щоденні звіти, сповіщення	Звіти резервного копіювання, журнал сповіщень	Помилки ігноруються
Тести відновлення	DR-тести за планом	Акти тестів, протоколи	Не тестували місяцями

Резервування без плану відновлення має обмежену цінність – необхідно заздалегідь продумати і задокументувати процес ***Disaster Recovery (DR).*** Ключовими поняттями є ***RPO (Recovery Point Objective)*** – допустимий обсяг втрати даних, тобто наскільки «старими» можуть бути дані при відновленні (наприклад, RPO=4 години означає, що при аварії можлива втрата даних за останні 4 години максимум), та ***RTO (Recovery Time Objective)*** – цільовий час відновлення, тобто як швидко після інциденту системи мають знов стати функціональними.

Виходячи з встановлених RPO та RTO, будується стратегія резервування: чим менше RPO (тобто ближче до нуля втрата даних), тим частіше слід робити копії або використовувати технології реплікації у режимі реального часу; чим жорсткіший RTO, тим більше потрібна автоматизація та відпрацьовані процедури переключення на резервні майданчики. Наприклад, для критичних фінансових систем часто RPO = 0 (жодної втрати транзакцій) – тоді застосовується синхронна реплікація даних між двома майданчиками, а на випадок відмови основного – автоматичне переключення протягом декількох хвилин. Натомість для офісних сервісів може бути прийнятним RPO = 24 год (щоденний бекап) і RTO = 48 год. В такому випадку достатньо мати щоденні копії в хмарі та протестувати план ручного відновлення протягом двох днів.

Невід'ємною частиною політики відновлення є тестування резервних копій. Стандарт ***ISO 27001*** наголошує, що «резервні копії інформації, програмного забезпечення та систем мають регулярно перевірятися шляхом відновлення, відповідно до узгодженої політики». Це означає, що компанія повинна періодично виконувати навчальні відновлення на тестових середовищах, щоб переконатися у працездатності копій і у тому, що персонал знає процедуру. Такі навчання з відновлення допомагають виявити слабкі місця та усунути їх завчасно. Наприклад, відсутність потрібних скриптів відновлення конфігурації, занадто повільне завантаження великих обсягів з хмари, конфлікти версій ПЗ. Крім того, регулярно перевірені резервні копії будуть мати юридичну силу при перевірках відповідності. Аудитор або регулятор вимагатимуть докази, що організація здатна відновити персональні дані в разі інциденту.

Сучасний ринок пропонує численні рішення для автоматизації резервного копіювання (рис. 10.5). Приклади включають Acronis Cyber Protect, Veeam Backup & Replication, Commvault, Veritas NetBackup та інші.

Ці системи зазвичай забезпечують централізоване керування резервуванням:

- *створювати копії з різних джерел* (віртуальних машин, баз даних, поштових серверів, кінцевих точок);
- *виконувати дедуплікацію;*
- *здійснювати стиснення;*
- *копіювати дані* (одночасно в локальне сховище і хмару);
- *перевіряти цілісність копій*.

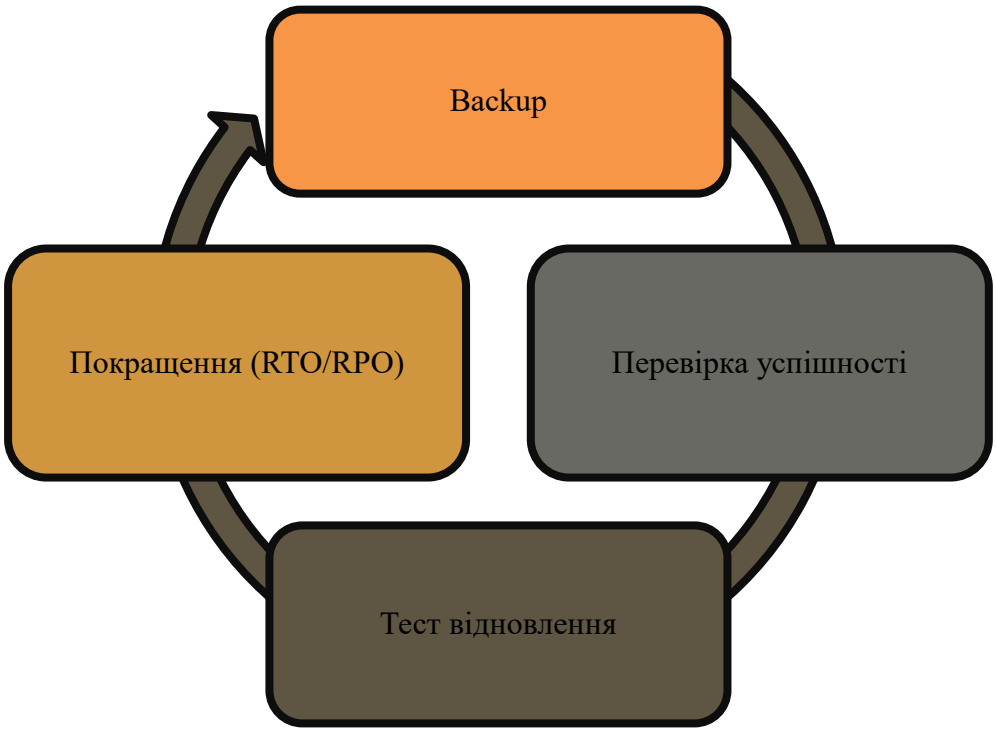


Рис. 10.5. Цикл резервного копіювання та відновлення

«Резервне копіювання – це процес регулярного створення копій критичних даних і конфігурацій з метою їх оперативного відновлення після інцидентів, що призводять до втрати, пошкодження або недоступності інформації».

Правильна стратегія резервування і відновлення перетворює потенційно руйнівний інцидент (втрату даних, зупинку сервісів) на керовану ситуацію, з якої компанія може вийти з мінімальними втратами.

У національному вимірі захист облікових записів і контроль доступу до інформаційних систем базується на двох ключових законодавчих актах. Перший із них – ***Закон України «Про основні засади забезпечення кібербезпеки України»,*** який задає організаційні засади кіберзахисту та координації дій у кіберпросторі, і другий – ***Закон України «Про захист інформації в інформаційно-комунікаційних системах»,*** який визначає вимоги до захисту інформації під час її обробки в інформаційно-комунікаційній системі (ІКС) та окреслює організаційні та технічні заходи безпеки.

Коли в обігу є персональні дані (кадрові масиви, клієнтські бази, контактні дані, ідентифікатори доступу тощо), контроль доступу набуває статусу юридично значущого: організація має забезпечувати режим обробки та захист таких даних у межах вимог ***Закону України «Про захист персональних даних».***

Це підсилює потребу в чітких правилах надання або відкликання доступів, розмежуванні ролей, журналюванні доступу до чутливих масивів і керованому обміні файлами між підрозділами та контрагентами.

В українській практиці ***контроль ідентичностей (Identity & Access Management)*** зазвичай включає не лише класичні облікові записи (логін/пароль), а й використання засобів електронної ідентифікації та довірчих послуг у ділових процесах (погодження документів, підписання, взаємодія з сервісами), що регулюється ***Законом України «Про електронну ідентифікацію та електронні довірчі послуги».*** Тому вимоги до автентифікації, керування сесіями та правами доступу потрібно узгоджувати з реальними потоками документів і повноваженнями посадових осіб.

Мінімально необхідним набором контролів облікових записів в українському контексті виступають багатофакторна та двоетапна автентифікація (MFA та 2FA). Зокрема, до них відносяться:

- *політика унікальності паролів;*
- *політика стійкості паролів;*
- *контроль віддаленого доступу;*
- *зменшення привілеїв.*

У рекомендаціях урядового сегмента кіберзахисту акцент робиться на практичному впровадженні 2FA як базового бар'єра проти компрометації облікових даних і на дисципліні налаштувань безпеки облікових записів.

Окремим важливим елементом управління кіберризиками в Україні є резервне копіювання та відновлення як інструменти стійкості до програм-вимагачів і руйнівних інцидентів. CERT-UA прямо визначає резервне копіювання як один з ефективних заходів зниження ризиків впливу ransomware, підкреслюючи регулярність створення копій і належну організацію їх зберігання.

У практичному сенсі це означає, що резерви мають бути відокремлені від робочого середовища, доступ до них мінімізований і контрольований, а відновлення процедурно перевірене.

Для українського бізнесу важливо, що вимоги до відновлення інформаційних систем і даних фактично задаються не лише кіберзагрозами, а й операційними обмеженнями (доступність зв’язку, стабільність сервісів, можливості віддаленої роботи). Тому планування резервування й відновлення необхідно прив’язувати до параметрів безперервності (цільові терміни відновлення критичних систем і допустимі втрати даних), а також до інвентаризації інформаційних активів і їх критичності в обліку і аудиту (первинні документи, робочі файли, реєстри, сховища комунікацій).

10.3. Роль аудитора у оцінці кіберризиків та їх вплив на фінансову безпеку бізнесу

У сучасній цифровій економіці ***кіберризики (cyber risk)*** стали одними з ключових факторів, що впливають на фінансову безпеку бізнесу тобто здатність підприємства захистити свої фінансові ресурси, активи та стабільність від втрат і загроз. Кіберризик визначається як ймовірність і потенційний вплив реалізації кіберзагрози, з урахуванням таких факторів, як наявні заходи безпеки та вразливості системи.

Іншими словами, це операційний ризик, що може призвести до прямих або опосередкованих фінансових збитків суб'єктів господарювання внаслідок їх діяльності у кіберпросторі. Кіберризики включають широкий спектр подій від цілеспрямованих кібератак (навмисних дій зловмисників) до випадкових кіберінцидентів, зумовлених збоями систем чи помилками персоналу.

Незалежно від джерела, наслідки таких подій можуть бути суттєвими: порушення роботи інформаційних систем, компрометація конфіденційних даних, прямі фінансові втрати, штрафи та судові витрати, погіршення репутації компанії тощо (табл. 10.6).

Таблиця 10.6

Вплив кіберподій на статті фінансової звітності

Ланка подій	Прямі витрати	Непрямі втрати	Потенційні зобов'язання	Аудиторський фокус
Інцидент (компрометація або простій)	Консалтинг з реагування на інциденти (IR), технічне відновлення	Зупинка процесів, затримки	Оціночні зобов'язання	Повнота відображення витрат
Порушення доступності (A)	Додаткові ресурси, понаднормова робота	Втрачений дохід, штрафи за SLA	Резерв під санкції	Перевірка договорів і санкцій
Витік або порушення конфіденційності (C)	Юридична підтримка, повідомлення	Втрата клієнтів і контрактів	Штрафи, позови	Оцінка розкриттів і резервів
Порушення цілісності (I)	Звірки, повторні процедури	Помилки звітності, ризик шахрайства	Коригування, перерахунки	Надійність даних і загальні

				IT-контролі (ITGC)
Відновлення та післяінцидентні зміни	Модернізація, ліцензії	Тимчасове падіння продуктивності	Ризики безперервності діяльності	Оцінка стійкості та BCP, DRP

Фінансова безпека українського бізнесу тісно пов'язана з ефективністю управління кіберризиками, адже кібератаки дедалі частіше призводять до простою сервісів, зриву операційних процесів і додаткових витрат на відновлення.

Це також підтверджується динамікою виникнення інцидентів. Урядова команда CERT-UA у 2024 році опрацювала 4 315 кіберінцидентів, тоді як у 2023 році таких випадків було 2 543. Показовим прикладом операційно-фінансового впливу є кібератака на «Укрзалізницю» у березні 2025 року, яка порушила роботу онлайн-сервісів продажу квитків і цифрових процесів у сфері вантажних перевезень, унаслідок чого компанія була змушена тимчасово перейти на паперові процедури для частини операцій. Довгостроково важливим для українського контексту залишається й урок NotPetya 2017 року, коли шкідливий код поширився через компрометоване оновлення бухгалтерського програмного забезпечення, що використовувалося значною кількістю українських організацій, а наслідки інциденту трансформувалися у масштабні збитки для бізнесу в різних країнах і секторах.

Такі приклади демонструють, що кіберризики здатні мати матеріальний вплив на фінансові результати компаній:

- *втрату виручки внаслідок простою;*
- *додаткові витрати;*
- *витрати на відновлення;*
- *санкційні витрати;*
- *судові витрати;*
- *репутаційні втрати.*

Відповідно оцінка кіберконтролів у компанії має спиратися на чіткий розподіл ролей між власниками процесів, функціями управління ризиками та інформаційної безпеки, а також внутрішнім аудитом, який забезпечує незалежну

перевірку ефективності контролів. Місце зовнішнього аудитора в цій системі та його фокус на доказовості контролів показано на рисунку 10.6.

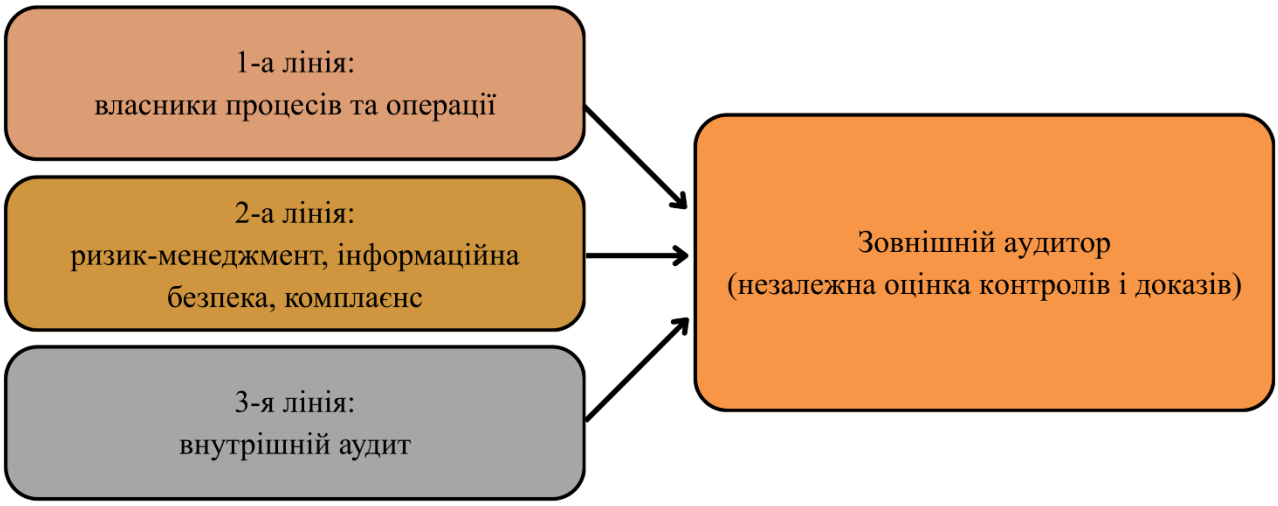


Рис. 10.6. Модель трьох ліній захисту та місце зовнішнього аудитора в оцінці кіберконтролів

Рисунок 10.6 демонструє, що зовнішній аудитор не підміняє функції кібербезпеки, а оцінює дизайн і ефективність контролів у частині, що впливає на фінансові дані та звітність. Тому ключовим стає узгодження доказів: журнали, матриці доступів, протоколи змін і результати DR-тестів.

Вразливими до кібератак є підприємства будь-якого масштабу, проте малі та середні бізнеси особливо під ризиком через обмежені ресурси на кібербезпеку. Дослідження Національного альянсу кібербезпеки США показало, що близько 60 % малих компаній не відновлюють діяльність протягом 6 місяців після серйозної кібератаки. Причиною цього є те, що прямі фінансові збитки та непрямі втрати (наприклад, відтік клієнтів, штрафні санкції, вимушені простої) можуть перевищувати фінансовий запас міцності малих підприємств. Таким чином, ефективне управління кіберризиками стало необхідною умовою забезпечення фінансової стійкості бізнесу.

Для підтримання належного рівня фінансової безпеки керівництво підприємства повинно приділяти увагу кіберризикам нарівні з традиційними видами ризиків (операційними, кредитними, ринковими тощо).

Згідно з рекомендаціями міжнародних фахівців, кіберризик слід розглядати як суттєвий бізнес-ризик, на одному рівні з ризиками невідповідності вимогам (compliance):

- *операційними;*
- *фінансовими;*
- *репутаційними.*

Це означає, що керівники компаній та власники повинні впровадити належну систему кібербезпеки, а саме: сукупність технологій, процесів і практик для захисту інформаційних систем і даних та інтегрувати управління кіберризиками в загальну систему управління ризиками підприємства. Наявність зрілого кіберризик-менеджменту (включно з політиками безпеки, процедурами реагування на інциденти, планами відновлення тощо) безпосередньо впливає на здатність бізнесу запобігати значним фінансовим втратам або швидко відновлюватися після інцидентів.

У відповідь на зростання кіберзагроз, світові професійні організації та органи стандартизації розробили низку стандартів, моделей та рекомендацій, що допомагають інтегрувати кібербезпеку в практики управління ризиками та аудиту. Аудиторам – як зовнішнім, так і внутрішнім важливо орієнтуватися в цих стандартах, щоб якісно оцінювати кіберризики та їхній вплив на фінансову безпеку бізнесу.

Міжнародна рада з аудиторських стандартів та стандартів забезпечення (IAASB) у межах ***Міжнародних стандартів аудиту (МСА)*** встановлює вимоги щодо оцінки ризиків у ході фінансового аудиту, включно з IT-аспектами. Зокрема, ***МСА 315 (Revised 2019)*** «Виявлення та оцінка ризиків суттєвого викривлення» вимагає від аудитора отримати розуміння інформаційних систем суб'єкта і відповідних заходів внутрішнього контролю. Цей стандарт прямо вказує на необхідність врахувати ризики, пов'язані з IT-середовищем, включаючи загрози для цілісності, конфіденційності та доступності даних, а також визначити та оцінити IT-загальні контролі (IT general controls), що підтримують фінансову звітність.

Комітет організацій-спонсорів Комісії Тредвея (COSO) інтегрував питання кіберризиків у свою концепцію управління ризиками підприємства (ERM). У 2020 році COSO спільно з Deloitte випустили спеціальне керівництво «Управління кіберризиком в цифрову епоху» (Managing Cyber Risk in a Digital Age), адресоване радам директорів, аудит-комітетам та менеджменту. Це керівництво показує, як п’ять компонентів та 20 принципів ERM-Framework COSO можуть бути використані для ідентифікації та управління кіберризиками. Згідно з COSO, ***кіберризик*** – це не лише технічна загроза, але й стратегічний бізнес-ризик, який повинен враховуватися при визначенні апетиту до ризику організації та впливати на стратегічні рішення.

Для аудиторів це означає, що при оцінці загальної системи внутрішнього контролю та ризик-менеджменту на підприємстві (наприклад, під час аудиту відповідності або оцінки ризиків шахрайства) слід зважати, наскільки кіберризики інтегровані у культуру ризик-менеджменту компанії. COSO рекомендує залучати до управління кіберризиком всю вертикаль корпоративного управління – від ради директорів (яка має встановити очікування і контроль за кібербезпекою) до керівників підрозділів і технічних фахівців. Для аудитора це важливий сигнал, бо саме ефективне управління кіберризиками свідчить про зрілість корпоративного управління, тоді як його відсутність може вказувати на слабкі місця у загальній системі контролю.

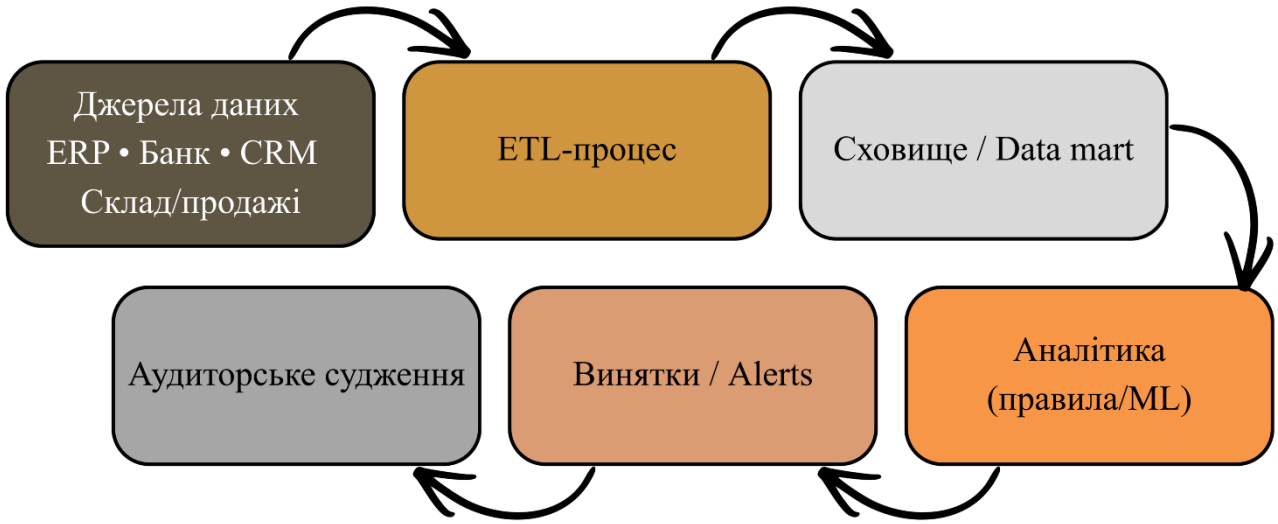


Рис. 10.7. ETL-процес у безперервному аудиті: від джерел даних до винятків і аудиторського судження

Національний інститут стандартів і технологій (NIST, США) запропонував ***Рамкову модель кібербезпеки (NIST CSF)***, що здобула міжнародне визнання. Крім неї, у 2020 році NIST випустив спеціальний документ NIST IR 8286 ***«Інтеграція кібербезпеки та управління ризиками підприємства (ERM)».*** Цей документ націлений на подолання розриву між IT-безпекою та традиційним управлінням підприємницькими ризиками, пропонуючи спільну мову для кіберфахівців і фінансових менеджерів.

У ньому, зокрема, представлено схему інформаційних потоків про ризики від рівня IT-систем до рівня керівництва підприємства, а також приклади форматів реєстрів кіберризиків і їх трансляції в портфель безпеки підприємства. Для аудиторів (особливо внутрішніх) NIST IR 8286 може бути корисним при оцінці належного процесу об'єднання інформації про кіберінциденти з бізнес-ризиками.

Наприклад, аудитор може перевірити:

- *включення суттєвих кіберризиків до корпоративного реєстру ризиків;*
- *встановлення для них відповідального власника ризику;*
- *визначення метрик толерантності до кіберінцидентів.*

Така інтеграція вказує, що компанія системно підходить до кібербезпеки, що, своєю чергою, позитивно впливає на загальний рівень фінансової безпеки.

Сучасні стандарти і моделі однозначно підкреслюють, ***що кібербезпека – це зона спільної відповідальності бізнесу та аудиту.***

Професійні стандарти аудиту (IAASB, IFAC) вимагають враховувати кіберризики при плануванні і виконанні аудиторських процедур; стандарти управління ризиками (COSO, NIST) інтегрують кіберризики у рамки ERM; а фахові IT-рамкові моделі (ISACA, NIST) надають практичні інструменти для оцінки ефективності кіберконтролів.

Зовнішній аудит (незалежний аудит) – це незалежна перевірка фінансової звітності суб'єкта господарювання, яку виконує аудитор або аудиторська фірма, що не належить до структури підприємства, з метою надання

обґрунтованої впевненості та висловлення аудиторської думки щодо достовірності звітності і її відповідності застосовній концептуальній основі фінансової звітності.

Зовнішній аудитор, що проводить незалежний аудит фінансової звітності, несе відповідальність за надання обґрунтованої впевненості, що фінансова звітність не містить суттєвих викривлень. Хоча об'єктом перевірки безпосередньо є фінансова звітність, зовнішній аудитор під час оцінки ризиків суттєвого викривлення повинен врахувати і ризики, пов'язані з ІТ та кібербезпекою. МСА 315 (Revised) прямо зобов'язує аудитора розуміти середовище ІТ і автоматизовані процедури, що використовуються для складання звітності. Це означає, що аудитор оцінює надійність інформаційних систем, з яких формуються бухгалтерські дані, а також ефективність ІТ-контролів, що забезпечують їх цілісність. Якщо системи чи контролі в сфері ІТ є слабкими, це може збільшувати ризик помилок або шахрайства у фінансовій звітності.

Зовнішній аудит фінансової звітності розглядає питання кібербезпеки у відносно вузькому обсязі. Необхідно збалансувати межі відповідальності: зовнішній аудитор фокусується тільки на тих аспектах кіберризику, що можуть призвести до суттєвих викривлень у звітності або суттєво вплинути на бізнес як діюче підприємство. Наприклад, короткочасний збій веб-сайту ритейлера, який призвів до незначної втрати виручки, аудитор віднесе до бізнес-ризиків, що не потребують прямої уваги в аудиті фінансової звітності. Натомість, якщо через кібератаку виявиться компрометованою бухгалтерська система або буде викрадено конфіденційні фінансові дані, то це вже безпосередньо зачіпає достовірність обліку та вимагатиме детального аналізу аудитором.

Внутрішній аудит – це незалежна діяльність всередині організації, що покликана надавати об'єктивні гарантії та консалтинг з метою поліпшення операцій компанії, включно з управлінням ризиками та системами контролю.

У контексті кіберризиків внутрішні аудитори відіграють провідну роль, оскільки вони мають значні повноваження на оцінку ефективності системи внутрішнього контролю і управління ризиками підприємства. На відміну від

зовнішніх аудиторів, які зосереджені переважно на фінансовій звітності, внутрішні аудитори розглядають кіберризики як частину сукупного профілю ризиків підприємства та можуть детально перевіряти ІТ-контролі, інформаційну безпеку, готовність до інцидентів тощо.

За сучасними стандартами внутрішнього аудиту (ІІА), однією із функцій якого є розвиток компетенцій у сфері ІТ та кібербезпеки. Опитування керівників внутрішнього аудиту вказують, що нестача технічних знань у команді є одним із головних бар'єрів збільшення охоплення кіберризиків у аудиторських планах. Тому багато відділів внутрішнього аудиту інвестують у навчання своїх співробітників або залучають зовнішніх експертів для складних перевірок (наприклад, етичних хакерів для тестування на проникнення). Така взаємодія важлива, адже кіберландшафт швидко змінюється, а кількість загроз постійно збільшується (наприклад, атаки на ланцюги постачання ПЗ, експлойти IoT-пристроїв тощо), і аудитори змушені підвищувати компетентності й практичний досвід, щоб належно оцінювати ризики.

Кіберризики становлять реальну загрозу фінансовій стабільності бізнесу, але при належному корпоративному управлінні та аудиторському супроводі їх негативний вплив можна суттєво зменшити. Аудитори як зовнішні, так і внутрішні відіграють ключову роль у тому, щоб кіберризики були прозоро враховані і контрольовані, а фінансова інформація залишалася достовірною та повною навіть в умовах зростаючих загроз.

Фінансова безпека бізнесу в цифрову епоху багато в чому залежить від зрілості кібербезпеки, а забезпечення цієї зрілості – спільне завдання управлінців та аудиторів. Аудитори виступають незалежними арбітрами, що оцінюють адекватність захисту та прозорості. Завдяки зовнішнім аудиторам інвестори можуть бути впевнені, що наслідки кіберінцидентів не приховані, а фінансова звітність достовірно відображає стан справ навіть після атак. Завдяки внутрішнім аудиторам рада директорів отримує впевненість, що всередині компанії постійно відслідковуються нові загрози, тестуються контролі і виправляються слабкі місця до того, як ними скористаються злочинці.

Кіберінцидент – означає реалізацію загрози у формі порушення конфіденційності, цілісності або доступності даних. Для бізнесу критично, що інцидент може мати як «видимі» прояви (зупинка сервісів), так і латентні (несанкціонована модифікація даних, приховане перебування в мережі). У фінансовому контексті це підвищує ризик викривлень у звітності через спотворення первинних даних, несанкціоновані операції або втрату доказової бази, що особливо важливо для процесів обліку, бюджетування та управлінської звітності.

Етап операційного впливу відображає перехід від суто ІТ-події до збоїв у бізнес-процесах:

- *порушення ланцюгів постачання;*
- *простою виробництва;*
- *порушення термінів реалізації;*
- *деградації сервісу;*
- *підвищення витрат на відновлення.*

У цій площині ключовою стає готовність підприємства до реагування, безперервності діяльності та відновлення, оскільки саме швидкість локалізації та відновлення визначає масштаб втрат. Для аудитора тут важливо оцінити, чи є ці механізми формальними документами, чи реально працюючими процедурами, що тестуються і мають підтверджену ефективність.

Подальша ланка – фінансові наслідки, які консолідують прямі та непрямі ефекти:

- *витрати на відновлення;*
- *додаткові закупівлі;*
- *штрафи;*
- *юридичні витрати;*
- *компенсації;*
- *втрати доходів;*
- *потенційне зростання вартості капіталу через підвищення ризиковості компанії.*

Саме на цьому етапі кіберризик переходить у категорії, що безпосередньо стосуються фінансової безпеки: ліквідності, платоспроможності, прибутковості та стійкості грошових потоків. Аудиторська оцінка фокусується на коректності визнання та оцінки таких наслідків (зокрема резервів і знецінення), а також на достатності доказів, що підтверджують управлінські оцінки.

Завершальна ланка – вплив на звітність і стійкість. Вона підкреслює, що кіберінциденти є не лише подіями витрат, а й чинниками, які можуть змінювати припущення щодо безперервності діяльності, потребувати додаткових розкриттів і впливати на довіру інвесторів та контрагентів.

10.4. Контрольні питання для самоперевірки

1. У чому полягає сутність кіберризику для бізнесу та чим він відрізняється від загальних операційних ризиків?
2. Які основні етапи «ланцюжка подій» від кіберзагрози до фінансових наслідків відображає рис. 10.3?
3. Які типи кіберінцидентів найбільш критично впливають на достовірність фінансової звітності (конфіденційність/цілісність/доступність) і чому?
4. Поясніть, як операційний вплив кіберінциденту трансформується у фінансові втрати (прямі й непрямі).
5. Які ключові контрольні точки аудитора відповідають етапу «кіберзагроза/вразливість» у моделі на рисунку 10.3?
6. Які аудиторські процедури є релевантними для оцінки контролів доступу та журналювання подій (IAM/ITGC)?
7. У чому полягає роль планів BCP/DRP у мінімізації фінансових наслідків кіберінцидентів і що має оцінити аудитор?
8. Які види фінансових наслідків кіберінцидентів підлягають відображенню у звітності (витрати, резерви, знецінення) та за якою логікою їх оцінюють?
9. Що означає «матеріальність» (суттєвість) кіберінциденту для аудиту?
10. У чому полягає різниця між роллю зовнішнього та внутрішнього аудитора в оцінці кіберризиків?
11. Які елементи Zero Trust-архітектури є ключовими для контролю доступу до фінансово значущих систем і даних?
12. Які управлінські документи й джерела доказів (політики, журнали, звіти, результати тестувань) є найбільш вагомими для аудитора при оцінці кіберконтролів?

Розділ 11

Автори:
Олена Сохацька
Роман Кулик

АУДИТОР ЯК ІНВЕСТИЦІЙНИЙ КОНСУЛЬТАНТ У ЦИФРОВОМУ СЕРЕДОВИЩІ

РОЗДІЛ 11. АУДИТОР ЯК ІНВЕСТИЦІЙНИЙ КОНСУЛЬТАНТ У ЦИФРОВОМУ СЕРЕДОВИЩІ

«Вол-стріт – це єдине місце, де люди роз'їжджають на Rolls-Royce в надії отримати поради від тих, хто їздить на метро»

Воррен Баффет

11.1. Роль аудитора в інвестиційному консалтингу та межі його відповідальності

Чітко вираженим світовим трендом є розширення спектру фінансових послуг у цифровому середовищі, особливо це стосується інвестиційного консалтингу. За останні двадцять років Україна активно розвиває цей ринок, що зростає як кількісно, так і якісно, трансформуючись та змінюючись з огляду на впровадження зарубіжних практик та цифровізації світової економіки.

Проте головною проблемою, що суттєво стримує цей процес, залишається відсутність довіри з боку бізнесу, яку так і не вдалося сформувати за усі роки незалежності. Саме відсутність довіри до інвестиційних консультантів (радників) сповільнює розвиток вітчизняного фондового ринку, що, своєю чергою не сприяє визначенню справедливих ринкових цін на об'єкти власності та обмежує обсяги ПІІ (прямих іноземних інвестицій).

Через підвищення попиту на послуги інвестиційного консалтингу, оцінювальні, юридичні та аудиторські компанії починають включати цей вид послуг до основного переліку, отримуючи додаткові ризики, підвищуючи межі відповідальності та наражаючись на законодавчі обмеження та етичні рамки їх застосування.

Зокрема зміст аудиторських послуг чітко визначено Законом України ***«Про аудит фінансової звітності та аудиторську діяльності»*** як огляд фінансової звітності, консолідованої фінансової звітності, виконання завдань з іншого надання впевненості та інші професійні послуги, що надаються суб'єктами аудиторської діяльності відповідно до міжнародних стандартів аудиту.

Зміст інших професійних послуг не визначається цим законом, натомість аудитором вважається фізична особа, яка підтвердила кваліфікаційну придатність до провадження аудиторської діяльності, має відповідний практичний досвід та зареєстрована у Реєстрі аудиторів та суб'єктів аудиторської діяльності.

Аудиторів готують в системі вищої освіти України з рамках спеціальності Д1 «Облік і оподаткування», сертифікують у професійних організаціях, обліковуючи у Реєстрі аудиторів. Щодо інвестиційного консультанта такої системи в Україні не існує.

Про інвестиційних консультантів мало знають, їхніми послугами користуються лише 10 % вітчизняних компаній, фізичні особи до них майже не звертаються. Натомість у США клієнтами інвестиційного консалтингу є 35 % населення, що свідчить про високий рівень інвестиційної грамотності. З огляду на можливість залучення в Україні до цього процесу фізичних осіб та домогосподарств, обсяги ринку інвестиційного консалтингу можуть зрости на порядок, що ще більше загострить проблему підготовки фахівців, здатних надавати кваліфіковані послуги у сучасному цифровому середовищі.

Значною проблемою в цьому аспекті є відсутність порогу входження в бізнес інвестиційного консалтингу, визначення спеціальності, в рамках якої (яких) потрібно готувати цих радників, а також відсутність професійної спілки, широко відомої на зарубіжних ринках CFA (Chartered Financial Analyst). Ця асоціація вважається однією з кращих на зарубіжних ринках в контексті підготовки фінансових та інвестиційних аналітиків, яких запрошують працювати міжнародні компанії, як на основні посади, так і користуються їхніми консалтинговими послугами.

В Україні цю організацію представляє CFA Society Ukraine, яка уже входить у міжнародну мережу спільноти сертифікованих фінансових аналітиків і є частиною глобальної асоціації інвестиційних професіоналів CFA Institute.

До спільноти входять понад 300 інвестиційних консультантів в Україні, які володіють сертифікатом CFA (Chartered Financial Analyst) або готуються його отримати. CFA є одним із найбільш авторитетних сертифікатів у галузі фінансів та інвестицій на світових ринках (Великобританія). Загалом станом на початок 2026 року у світі його отримали лише 149 000 осіб, коли щороку намагаються здати відповідні екзамени близько 200 000. Ця процедура є складною за змістом і досить коштовною.

Відтак, зарубіжний досвід свідчить, що базовими спеціальностями для інвестиційних аналітиків можуть бути облік та фінанси з додатковим формуванням компетентностей не тільки аналізу ринків власності, її розподілу між стейкхолдерами, але й нефінансових сфер діяльності бізнесу, зокрема ринку продукції, конкурентного статусу, інноваційності, технологічності, соціальної корпоративної відповідальності, екологічності, рівня цифровізації, що дозволить інвестиційному консультанту надати клієнту рекомендації щодо перспектив інвестування. Ці перспективи можуть бути описані трьома можливостями: тримати, купувати, продавати бізнес (рис. 11.1).

Рис. 11.1. Три варіанти рекомендацій інвестиційного аналітика

Відомі в Україні компанії-лідери у різних сферах бізнесу такі, як Baker Tilly, BFM Group Ukraine, Pro-Consulting, SECL Group Ukraine, Smart Capital, SV Development та інші, проблему відсутності кваліфікованих кадрів з інвестиційного консалтингу вирішують через навчання у внутрішніх корпоративних системах підвищення кваліфікації та шляхом прийняття на роботу сертифікованих CFA аналітиків (якщо можуть собі дозволити оплату їхньої праці згідно з рівнем кваліфікації).

Аналогічно працюють в Україні представництва великих світових консалтингових компаній, зокрема «Великої четвірки» (Deloitte, Ernst & Young, KPMG, PricewaterhouseCoopers). Робота у цих представництвах є високооплачуваною, має хороші перспективи для кар'єрного зростання.

У цьому контексті вітчизняні аудиторські фірми намагаються захопити частину цього ринку, особливо під час війни, коли з'явилася потреба визначення ризиків інвестування щодо розміщення виробництва дронів, іншої зброї за межами країни або прийняття ПІІ від зарубіжних інвесторів на нашій території, залучаючи юристів для аналізу відносин між власниками бізнесу клієнта («Аудитор. Консультант. Юрист.»), або надаючи консультації власникам контрольованих іноземних компаній (фірма «Аудит. Консультант» м. Львів).

Роль аудитора у інвестиційному консультуванні чітко визначена тим фактом, що він одночасно є ревізором та контролером, який за допомогою ШІ може на постійній основі аналізувати первинні документи та їх відображення у фінансових звітах, запобігаючи шахрайству та фінансовим махінаціям менеджменту.

Виконуючи вимоги Міжнародного кодексу етики для професійних бухгалтерів (IIESBA Code), ***аудитор повинен уникати ситуацій, коли сам може нести загрозу,*** особливо при оцінці власної роботи або маючи фінансовий інтерес у клієнта. У цьому випадку консультації, що прямо впливають на дані, які потім аудитуються, забороняються.

На рисунку 11.2. показано, у яких випадках аудитор може виступати інвестиційним консультантом.

Рис. 11.2. Умови надання аудитором інвестиційних консультацій

Як видно з рисунку 11.2, для клієнтів:

- *у яких фірма не проводить аудит, це цілком прийнятна діяльність* (звичайно, з дотриманням вимог ліцензування, конфіденційності та обмежень законодавства);
- *що отримують аудиторські послуги, це можливо у вузьких межах: надати загальну економічну інформацію* (аналітику ринку, біржові ціни, галузеві огляди); *допомогти у підготовці інвестиційного рішення, не впливаючи безпосередньо на нього; консультувати щодо системи внутрішнього контролю ризиків інвестицій* (а не щодо конкретних угод);
- *як частина надання альтернативних послуг у форматі консультаційної практики у межах аудиторської фірми, але за умов функціонального та організаційного розмежування команд аудиторів.*

Аудитор не може бути інвестиційним консультантом (особливо для свого клієнта) (рис. 11.3).

Згідно з Законом України «Про аудит фінансової звітності та аудиторську діяльність» (2017) та стандартами надання супутніх послуг, аудитор:

- *може надавати інші послуги, але з урахуванням вимог до незалежності;*

- *повинен розкривати клієнтам факт надання будь-яких додаткових послуг;*
- *йому забороняється брати участь у прийнятті управлінських рішень клієнта.*

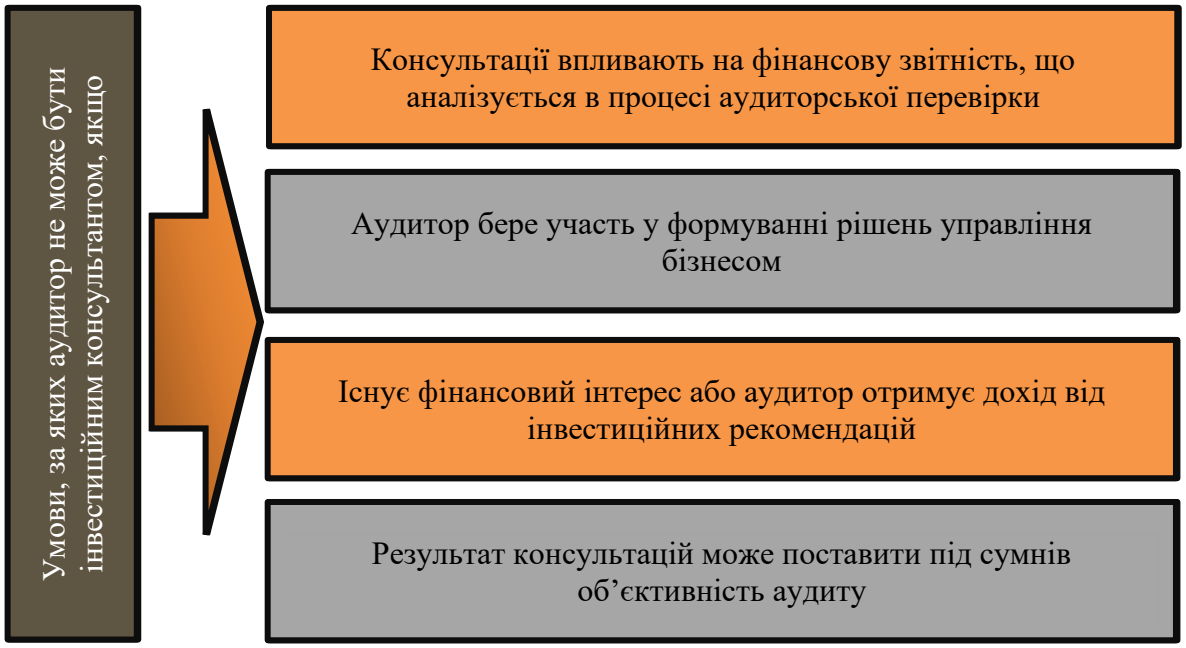


Рис. 11.3. Аудитор не може надавати інвестиційні послуги своєму клієнту

Таким чином, аудитор може бути інвестиційним консультантом лише поза межами аудиту, або в межах іншої організаційної структури фірми.

Інвестиційний консультант (радник) – професіонал з інвестування, з оцінювання об'єктів інвестицій, з вкладання капіталу з отриманням максимального прибутку при мінімальних ризиках, з розподілу фінансів як фізичних, так і юридичних осіб. Вихідною рамкою у даному випадку є його фаховість як експерта, який висловлює думку не тільки щодо достовірності фінансової звітності, але й допомагає клієнтові приймати економічні рішення, зокрема щодо структури капіталу, купівлі активів, інвестицій у цінні папери, беручи на себе частину відповідальності за наслідки цих рішень.

Відтак, для надання таких фахових інвестиційних консультацій з підготовки цих фахівців має суттєво відрізнятися від існуючих стандартів спеціальності D1 «Облік і оподаткування» та D2 «Фінанси, банківське право,

страхування і фондовий ринок», що можна здійснити в межах міждисциплінарних освітніх програм.

Порівняння змісту навчання інвестиційних радників (фінансових аналітиків, консультантів) та аудиторів на зарубіжному та вітчизняному ринках зведено в таблицю 11.1.

Таблиця 11.1

Зміст навчання	Аудит в Україні	Інвестиційний консультант на зарубіжних ринках
Інвестиційні інструменти	Акції, облігації (державні та корпоративні), похідні фінансові інструменти (загальне уявлення)	Акції; облігації (державні та корпоративні); інвестиційні фонди (etf); похідні фінансові інструменти; альтернативні інвестиції; інструменти грошового ринку, цифрові валюти та їх похідні
Основи портфельного інвестування	Переважно не вивчаються	Диверсифікація; ризик та дохідність; розподіл активів; базові принципи формування інвестиційного портфеля
Макроекономіка	Валовий внутрішній продукт; інфляція; облікова ставка центрального банку; валютні курси; економічні цикли	Валовий внутрішній продукт; Інфляція; Облікова ставка центрального банку; валютні курси; економічні цикли
Фундаментальний аналіз	Фінансова звітність підприємств; основні фінансові показники; SWOT, ABC, економічний аналіз	Загальні підходи до оцінки вартості основних активів, фінансова звітність підприємств, аналіз ринку, галузі, продукції, інновацій, конкурентного статусу, розподіл власності, визначення перспектив розвитку
Технічний аналіз	Не вивчається	Поняття ринкового тренду; рівні підтримки та опору цін; базові технічні індикатори
Управління інвестиційними ризиками	Частково вивчається	Класифікація ризиків; ризик-профіль інвестора; волатильність; ліквідність; валютний ризик
Фінансове планування інвестора	Не вивчається	Особистий бюджет; фінансові цілі; інвестиційний горизонт; довгострокові накопичення; страхування
Державне регулювання інвестиційної діяльності	Не вивчається	Функції фінансових регуляторів; правові основи інвестування; оподаткування інвестиційних доходів; валютне регулювання
Міжнародна інвестиційна діяльність	Не вивчається	Загальна характеристика міжнародних ринків капіталу, зокрема біржових,; діяльність іноземних брокерів; базові вимоги kyc/aml

Професійна етика інвестиційної діяльності	Не вивчається	Етичні принципи; конфлікт інтересів; відповідальність перед інвестором; інформаційна конфіденційність
Комунікація з інвестором	Не вивчається	Фінансова інформація та консультації; формування довіри; управління інвестиційними очікуваннями
Інформаційно-аналітичне забезпечення	Вивчається для аудиторів	Табличні процесори; базові інвестиційні розрахунки; офіційні статистичні та аналітичні джерела, ші, індивідуальні чат-боти інвестора

Як видно з таблиці 11.1, аудиторам для отримання компетентностей інвестиційного консультанта необхідно постійно підвищувати кваліфікацію, поки що, у філіях зарубіжних професійних асоціаціях. На часі до цього процесу долучитися закладам вищої освіти, а також державі (МОНУ, НАЗЯВО, НКЦПФР) для створення стандартів цієї важливої спеціальності. Для цього необхідно вивчати такі спеціальні освітні компоненти як фундаментальний та технічний аналізи.

«Фундаментальний аналіз – це всебічний ґрунтовний аналіз, що вивчає рух цін під впливом макроекономічних чинників. Головною його метою є визначення справедливої ціни досліджуваного активу.

Порівнюючи отриману оцінку із поточним станом ринку, робиться висновок – переоцінений чи недооцінений цей актив. Фундаментальний аналіз використовується стратегічними інвесторами, що розраховують на реалізацію довгострокових стратегій, заробляючи на багаторічних цінових тенденціях».

«Технічний аналіз – це метод прогнозування динаміки цін, заснований на математичних, а не на економічних теоріях.

Історично склалось так, що технічний аналіз формувався, як певна сукупність різноманітних методів, які існували окремо, один від одного, та розвивались паралельно. По суті, технічний аналіз – це накопичений досвід аналітиків, отриманий емпіричним шляхом. Основою більшості методів є спостереження практикуючих трейдерів, які досліджували ціну або курс активу і користувалися для цього спеціальними графіками».

Інвестиційні консультанти на світових ринках уже тривалий час використовують можливості цифрового простору для залучення клієнтів, зокрема фізичних осіб, а також пришвидшення аналітичних процедур для вироблення інвестиційних рекомендацій. Однак варто зазначити, що застосування інноваційних технологій та штучного інтелекту в інвестиційному консультуванні має допоміжний характер і передбачає обов'язковий професійний контроль з боку людини – інвестиційного консультанта.

До таких інновацій можна віднести аналітичні системи на основі ШІ, що дозволяють використовувати алгоритми машинного навчання в процесі обробки значного масиву даних (Big Data) як фінансових, так і не фінансових даних, а відтак визначати закономірності їх появи, тренди, ризики, що своєю чергою суттєво підвищить якість аналітичних висновків.

На зарубіжних ринках широкого застосування набули ***робо-адвайзери (robo-advisor),*** роботизований радник у формі автоматизованої платформи, що дозволяє не тільки формувати інвестиційний портфель фізичної особи, але й управляти ним. Робо-адвайзери з’явилися у США у 2008 році, уже через десять років у їхньому управлінні були активи на 200 млрд. доларів, у 2025 – більше 16 трлн.

В Україні цей інструмент використовує онлайн платформа інвестиційної та фінансової грамотності, яка розробила вдосконалений алгоритм HUG'S, що враховує реалії високої волатильності та невизначеності на світовому фондовому ринку, у інструменти якого уже активно інвестують українські фізичні особи. У даному випадку людина – інвестиційний консультант перевіряє алгоритми; адаптує рекомендації до реалій ринків; безпосередньо займається складними випадками.

Іншою технологією є система персоналізації інвестицій. У даній технології ШІ використовується для адаптації інвестиційних рішень під конкретного інвестора, його відношення до ризику, фінансових можливостей та мети інвестування. У цьому випадку формуються персональні інвестиційні портфелі, за якими складаються окремі звіти.

Популярною також є технологія прогнозної аналітики, що передбачає застосування статистичних та машинних моделей для прогнозування ринкових показників, зокрема волатильності, цін на основні активи, використання сценарного аналізу, стрес-тестування сформованих інвестиційних портфелів для різних сценаріїв.

У багатьох випадках використовується аналіз даних з альтернативних джерел, зокрема з новинних сайтів, соціальних мереж, супутникових даних, фундаментального аналізу, починаючи з макроекономічних показників, завершаючи соціальними та екологічними ініціативами об'єкту інвестування.

Важливою технологією також є автоматизація комплаєнсу та ризик-менеджменту, за допомогою якої перевіряють інвестиційну діяльність на дотримання вимог законодавства. Вона включає AML (Anti-Money Laundering) – моніторинг операцій клієнта (перекази, депозити, зняття готівки тощо) для виявлення підозрілої поведінки, яка може свідчити про наміри відмивання грошей або інші фінансові злочини.

Варто відзначити також використання ШІ для виявлення поведінкової реакції інвесторів, зокрема виявлення панічних настроїв, прийняття імпульсивних рішень тощо.

Завдяки штучному інтелекту кожен інвестор тепер може самостійно проводити аналіз ринку та відстежувати курси цінних паперів, валют, зокрема і цифрових, що раніше було доступно переважно банкам і великим інституційним гравцям.

В останні роки інвестиційні консультанти комбінують роботу з універсальними чат-ботами (найпоширенішим з яких є ChatGPT (Open AI)) з спеціалізованими фінансовими платформами. Основною вимогою до такої комбінації є доступ до закритих даних та безпека клієнтів.

Спеціалізовані чат-боти мають прямі зв'язки з відомими авторитетними інформаційними агенціями Bloomberg, Reuters, SEC filings, отримуючи реальні фінансові звіти та дані про діяльність об'єктів інвестування. До них відносять

FinChat.io, AlphaSense, HebbIA. Крім того великі банки мають свої корпоративні чат-боти.

В Україні використовують адаптовані універсальні чат-боти, в той же час Приватбанк та ICU (Investment Capital Ukraine) мають власні розробки.

Компанія ICU (Investment Capital Ukraine) успішно використовує власний ШІ – чат-бот у Телеграмі для консультування інвесторів, що купують облігації внутрішньої державної позики (ОВДП). Чат розраховує їх вартість на конкретну дату і порівнює з котируваннями, що суттєво здешевлює консультаційні послуги.

AI-сервіс у «Приват24 для бізнесу», проводить експрес-аналіз ділової репутації контрагентів. Інвестиційні консультанти зарубіжних інвесторів використовують його для швидкої перевірки ризиків роботи українських компаній.

11.2. Оцінка інвестиційної привабливості підприємства на основі цифрових даних

Інвестиційна привабливість підприємства відображає комплекс об'єктивних і суб'єктивних ознак, які формують у потенційних інвесторів уявлення про доцільність вкладення капіталу. У сучасних умовах жорсткої конкуренції і цифрової трансформації економічної діяльності підприємства змушені по-новому організовувати виробничі процеси, взаємодіяти з ринком і залучати інвестиції. У цьому процесі їм потрібні фахові консультації інвестиційних консультантів.

Інвестиційна привабливість – це багатовимірне поняття, що відображає думку інвесторів щодо перспектив подальшого успішного функціонування об'єкту інвестування та є сукупністю об'єктивних ознак, властивостей і можливостей, які визначають потенційний платіжний попит на інвестиції.

Інвестиційно привабливе підприємство спонукає інвесторів приймати рішення щодо довгострокових вкладень, що забезпечує його розвиток і підвищення конкурентоспроможності.

Інвестиційний консультант поєднує традиційні підходи до оцінювання інвестиційної привабливості підприємств, які ґрунтувалися на аналізі фінансової звітності з фундаментальним аналізом та використовує для цього цифрові технології, про які йшлося у параграфі 11.1.

Економічна нестабільність, воєнні виклики та швидкий розвиток цифрових технологій потребують нових методик, що враховують цифрові дані і цифрові компетенції підприємств. Для цього інвестиційним консультантом використовується синергетичний підхід при визначенні інвестиційної привабливості. До прикладу використання Big Data, штучного інтелекту та блокчейну дозволяє точніше здійснювати фінансове прогнозування, пропонувати зміни в управлінні ризиками та оптимізацію ресурсів підприємства. У цифрову епоху дані стають основним чинником розвитку виробництва; їхнє накопичення та використання дозволяє підприємствам виявляти можливості і підвищувати ефективність.

Інвестиційна привабливість об’єкту аналізу розглядається як відносне поняття, що характеризує співвідношення між очікуваною прибутковістю, рівнем ризику та вартістю фінансових ресурсів у певній країні, регіоні чи галузі. З іншого боку, це сукупність властивостей та можливостей економічної системи, яка визначає потенційний попит на інвестиції. Основними цілями оцінки інвестиційної привабливості є:

- *визначення поточного стану підприємства та перспектив його розвитку;*
- *розробка заходів підвищення привабливості;*
- *залучення інвестиційних ресурсів в обсягах, що відповідають рівню привабливості;*
- *отримання комплексного позитивного ефекту від використання залученого капіталу.*

Чинники, що визначають інвестиційну привабливість, поділяють на ***внутрішні та зовнішні.***

Внутрішні чинники відображають фінансово-господарську діяльність підприємства: ліквідність, рентабельність, ділову активність, фінансову залежність (частку зовнішніх запозичень), стан майна та структурні зміни у ресурсах. Зовнішні чинники охоплюють макроекономічне середовище (темпи зростання ВВП, інфляцію, валютні курси), конкурентне оточення, регуляторну політику, політичні ризики, рівень розвитку фінансового ринку та інноваційний потенціал галузі. Підвищення інвестиційної привабливості неможливе без швидкого реагування на зміни зовнішнього середовища та постійного розвитку підприємства (рис. 11.4).

Відповідно до сучасних досліджень, чинники інвестиційної привабливості можна класифікувати за такими групами:

- *фінансові показники* – ліквідність, рентабельність, ділова активність, структура капіталу, дивідендна політика. Ці показники відображають здатність підприємства генерувати достатній прибуток і забезпечувати повернення вкладених інвестицій;

- *виробничі та технологічні показники* – рівень використання потужностей, якість основних засобів, інноваційні технології, наявність патентів і ноу-хау;
- *маркетингові показники* – позиція на ринку, частка ринку, рівень задоволеності клієнтів, бренд-капітал та ефективність маркетингової стратегії. У сучасному цифровому середовищі маркетингові дані (web-аналітика, поведінка користувачів у мережі) стають важливим джерелом оцінки, дозволяючи аналізувати попит у реальному часі;
- *управлінські та кадрові чинники* – кваліфікація управлінського персоналу, корпоративна культура, наявність системи управління ризиками та знання цифрових технологій. За результатами досліджень, цифрові компетенції керівників та персоналу значно підвищують здатність підприємства адаптуватись до інноваційних викликів;
- *зовнішні фактори* – макроекономічне середовище, державне регулювання, доступність капіталу, політична стабільність, конкуренція та галузеві тенденції. Впливовим є також цифрова інфраструктура держави та законодавча база у сфері захисту даних, оскільки вони визначають можливості цифровізації бізнесу.

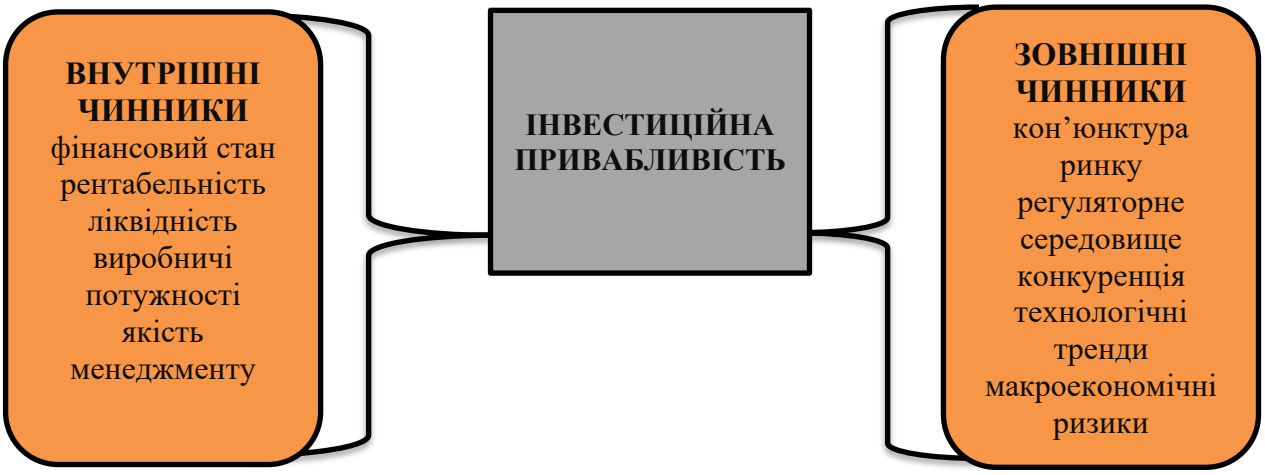


Рис. 11.4. Чинники інвестиційної привабливості

На рисунку 11.4 показано інтеграційну схему ключових чинників, що впливають на інвестиційну привабливість, що поділяє їх на внутрішні та зовнішні та демонструє взаємозв'язок між групами.

Фінансовий аналіз є основою оцінки інвестиційної привабливості. Для оцінки привабливості інвестиційний консультант розраховує ліквідність, майновий стан, ділову активність, фінансову залежність та рентабельність. Перелік основних показників подано у таблиці 11.2.

Таблиця 11.2

Показники оцінки інвестиційної привабливості підприємства за цифровими даними

Показник	Характеристика	Формула/інтерпретація
Коефіцієнти ліквідності	Показують здатність підприємства погашати поточні зобов'язання. Розрізняють поточну, швидку та абсолютну ліквідність	Поточна ліквідність = Оборотні активи / Поточні зобов'язання; швидка ліквідність відображає ліквідні активи без товарних запасів; абсолютна ліквідність – частка грошових коштів і короткострокових фінансових інвестицій
Коефіцієнти фінансової стійкості (майнового стану)	Характеризують структуру капіталу й частку власного капіталу	Коефіцієнт автономії = Власний капітал / Валюта балансу; коефіцієнт фінансової стабільності = (Власний капітал + Довгострокові зобов'язання)
Коефіцієнти ділової активності	Характеризують швидкість обороту активів, дебіторської й кредиторської заборгованості	Оборотність активів = Виручка / Середня вартість активів; оборотність запасів; середній період обороту дебіторської заборгованості
Коефіцієнти рентабельності	Відображають ефективність використання ресурсів	Рентабельність активів = Чистий прибуток / Середні активи; рентабельність власного капіталу = Чистий прибуток / Власний капітал; рентабельність реалізації = Прибуток від реалізації, Виручка
Коефіцієнти фінансової залежності	Показують залежність підприємства від зовнішнього фінансування	Коефіцієнт фінансового левериджу = Зобов'язання / Власний капітал; коефіцієнт покриття відсотків = EBIT, Витрати на відсотки

Поєднання цих показників дозволяє визначити сильні та слабкі сторони фінансового стану підприємства. Важливо враховувати динаміку показників за кілька років, порівнюючи їх із середньогалузевими значеннями.

З метою узагальнення множини показників застосовують інтегральні індекси. Інтегральний показник інвестиційної привабливості формується на основі інтегральних індикаторів фінансового стану, результативності маркетингової політики, внутрішніх бізнес-процесів та навчання персоналу.

Розрахунок таких індикаторів передбачає нормування початкових даних, визначення вагових коефіцієнтів і використання імітаційного моделювання для отримання узагальненого результату. Отриманий індикатор інтерпретується на основі шкали Харрінгтона (області «відмінний», «добрий», «задовільний», «незадовільний», «катастрофічний»).

Шкалу Харрінгтона (функцію бажаності) психофізичну шкалу, розроблену Едвіном Харрінгтоном у 1965 році використовують для перетворення різних якісних чи кількісних показників діяльності у безрозмірну шкалу наприклад від 0 до 1. Вона оцінює ступінь наближення до ідеалу, де 0 – абсолютно неприйнятно, а 1 – ідеально. Або як по областях як показано вище.

Метод інтегральної оцінки має переваги він враховує різні аспекти діяльності і дозволяє інвестиційному консультанту порівнювати підприємства. Разом з тим, він потребує значного обсягу даних і залежить від суб'єктивного вибору питомих ваг показників. У цифрову епоху доступ до великих масивів даних та можливості обробки у режимі реального часу покращують надійність таких методів.

Уже більше двадцяти років інвестиційні консультанти для визначення інвестиційної привабливості об'єктів аналізу використовують ***систему збалансованих показників (СЗП),*** запропоновану Р.Капланом і Д.Нортоном, що охоплює чотири складові: фінанси, клієнти, внутрішні бізнес-процеси, навчання й розвиток персоналу.

На відміну від традиційних фінансових індикаторів, СЗП поєднує монетарні та немонетарні показники, враховуючи стратегічні цілі підприємства. Застосування СЗП в процесі оцінки інвестиційної привабливості дає змогу інвестиційному раднику пов'язати довгострокові та короткострокові цілі, узгодити інтереси менеджменту й інвесторів. Однією з ключових переваг СЗП є взаємне доповнення фінансових показників операційними, стратегічними та якісними індикаторами.

Крім фінансових коефіцієнтів і інтегральних індикаторів, для оцінки інвестиційної привабливості використовують ***методи дисконтування***

грошових потоків (чистий приведений дохід NPV, внутрішня норма прибутковості IRR, період окупності), а також сценарний аналіз.

Ці методи дозволяють враховувати вартість грошей в часі та різні сценарії її розвитку. У контексті цифрової трансформації сценарний аналіз включає оцінку ризиків кібербезпеки, технологічної застарілості та швидких змін ринкових трендів.

У цифрову епоху дані стають основним ресурсом для прийняття рішень. Цифровізація суттєво впливає на ефективність бізнесу, хмарні обчислення, аналітика Big Data та штучний інтелект допомагають підприємствам розробляти нові продукти та послуги, оптимізувати операції і поліпшувати взаємодію з клієнтами. Саме на ці аспекти діяльності аналізованого підприємства має звертати увагу інвестиційний консультант при формування висновку щодо інвестиційної діяльності та виробленні відповідних рекомендацій.

Збір та аналіз цифрових даних включають:

- *великі масиви даних (Big Data)* – дані з внутрішніх систем ERP та CRM, сенсорні дані з виробничого обладнання, логістичні відомості. Аналіз цих даних дозволяє прогнозувати попит, оптимізувати запаси та виявляти маркетингові та логістичні ризики;
- *Web-аналітику* – інформацію про відвідування веб-сайту, конверсії, залученість користувачів у соціальних мережах. Вона відображає репутацію підприємства та ефективність маркетингових кампаній;
- *публічну інформацію та дані з відкритих джерел* – фінансові звіти, звіти державних регуляторів, реєстри судових справ, тендерів, патентів. Такі дані допомагають оцінити ступінь дотримання законодавства, наявність судових ризиків, інноваційний потенціал;
- *дані про контрагентів* – інформацію про постачальників, клієнтів, відгуки, рейтинги, що дозволяє оцінити надійність партнерів та ризик неплатежів.

Інтеграція названих вище джерел створює ***цифровий профіль підприємства,*** що дозволяє інвестиційним консультантам рекомендувати потенційним інвесторам робити більш зважені рішення.

Цифровий профіль підприємства показано на рисунку 11.5.

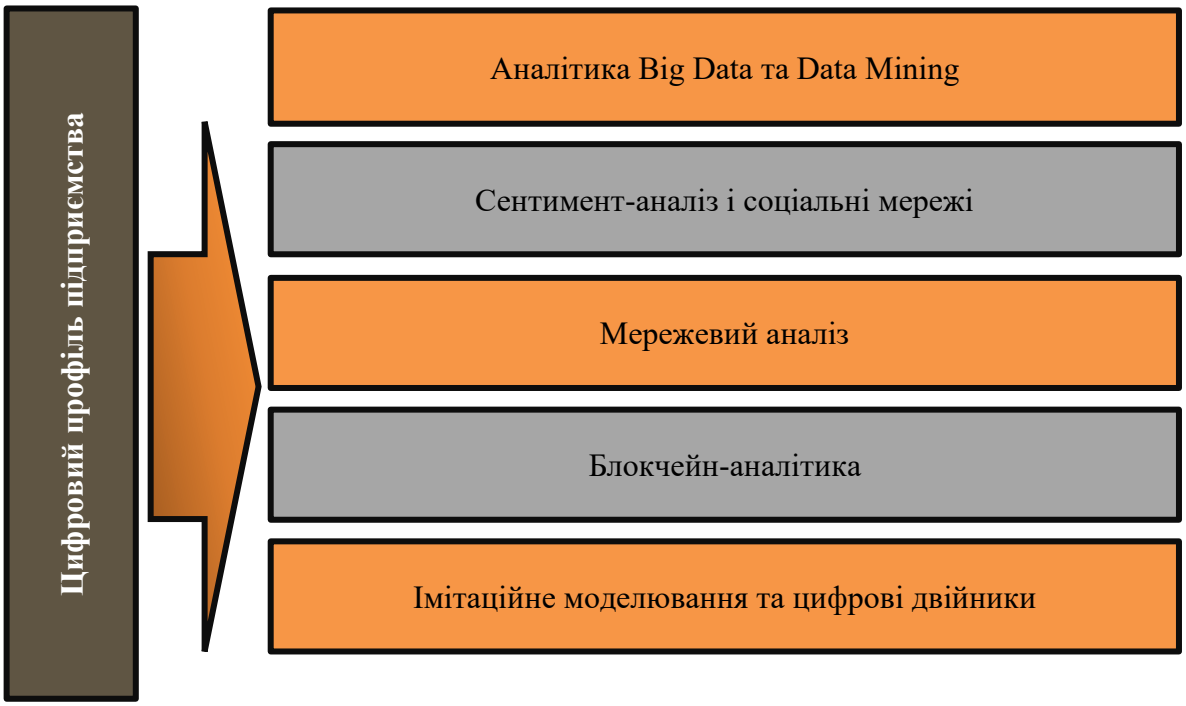


Рис. 11.5. Цифровий інвестиційний профіль аналізу об’єкта інвестування

Застосування алгоритмів машинного навчання дозволяє виявляти приховані закономірності у фінансових і нефінансових даних, прогнозувати тренди та оцінювати ризики. Наприклад, аналіз текстових даних відгуків клієнтів може свідчити про репутаційні ризики.

Аналіз змісту соціальних мереж допомагає зрозуміти ставлення громадськості до підприємства, прогнозувати поведінку споживачів та виявляти інформаційні кризи.

Дослідження взаємозв’язків між підприємством та його партнерами (через платіжні системи, логістичні ланцюги, патентні кооперації) дозволяє оцінити позицію підприємства у діловій екосистемі та виявити стратегічних контрагентів.

Завдяки прозорості блокчейн-платформ можна відстежувати історію транзакцій, перевіряти походження активів і знижувати ризик шахрайства.

Перевіряється використання смарт-контрактів у ланцюгах постачання, що підвищує довіру інвесторів.

Створення цифрових двійників підприємств, які відтворюють фізичні процеси у віртуальному середовищі, дозволяє прогнозувати вплив інвестиційних рішень і оцінювати сценарії розвитку на основі реальних даних.

Поєднання фінансових показників із цифровими технологіями, як правило, створює синергетичний ефект, що сприяє зростанню чистого доходу та підвищенню ефективності управління ресурсами. Однак основними викликами у цьому процесі є висока вартість впровадження цифрових рішень, необхідність адаптації до швидких змін на ринку та забезпечення кібербезпеки.

Можливості та потенційні ризики використання ключових цифрових технологій, що призводять до синергетичного ефекту, зведено у таблиці 11.3.

Таблиця 11.3

Можливості, виклики та загрози використання ключових цифрових технологій

Цифрова технологія	Можливості для підвищення інвестиційної привабливості	Виклики та ризики
Big Data та аналітика	Аналіз великих масивів даних дає змогу прогнозувати попит, оптимізувати виробництво й логістику, оцінювати поведінку клієнтів; підвищує точність прогнозування фінансових потоків	Висока вартість інфраструктури, потреба у кваліфікованих спеціалістах, ризики порушення конфіденційності
Штучний інтелект (AI)	Автоматизація процесів, інтелектуальний аналіз даних для підтримки прийняття управлінських рішень, моделювання інвестиційних сценаріїв	Складність інтеграції, необхідність забезпечення етичності рішень і пояснюваності моделей, ризик алгоритмічних упереджень
Блокчейн	Підвищення прозорості й довіри через використання смарт- контрактів, захист від шахрайства, спрощення перевірки активів, можливість токенізації майна	Обмежена швидкість транзакцій, регуляторна невизначеність, потреба у стандартизації
IoT і цифрові двійники	Збирання даних в реальному часі з виробничого обладнання та створення цифрових двійників для моделювання сценаріїв; підвищення надійності прогнозів	Високі вимоги до кібербезпеки, інтероперабельність пристроїв, ризики втрати даних
Цифрова технологія	Можливості для підвищення інвестиційної привабливості	Виклики та ризики

У межах інвестиційного консалтингу ***цифрові дані слід розглядати*** як багатовимірний доказовий масив, що доповнює фінансову звітність та управлінську інформацію. Їхня цінність полягає не лише у масштабі, а й у різноманітності, швидкості оновлення та достовірності, що безпосередньо впливає на якість інвестиційних висновків.

Практичне застосування Big Data-аналітики починається з побудови «карти даних» підприємства: визначення джерел, власників, прав доступу, періодичності оновлення та критичних полів, які впливають на інвестиційні рішення. Без цього етапу навіть найсильніші алгоритми машинного навчання не компенсують помилки на рівні збору та структурування даних.

Для Data Mining у інвестиційному консалтингу важливими є задачі класифікації (наприклад, імовірність фінансових ускладнень), регресії (прогноз виручки/маржі), кластеризації (виявлення типових профілів клієнтів/продуктів) та пошуку аномалій (ознаки шахрайства або управлінських викривлень). Кожен тип задачі визначає вимоги до даних і критерії валідації результатів.

Окремої уваги потребує побудова ознак, котрі займаються перетворення первинних операційних і нефінансових даних у показники, які мають економічний зміст. У контексті інвестиційної привабливості це можуть бути індикатори стабільності попиту, сезонності, надійності контрагентів, частоти рекламацій, а також показники операційної ефективності ланцюга постачання.

У прогнозуванні трендів і ризиків принципово важливо розрізняти ***короткострокові та довгострокові горизонти***. Моделі, що добре працюють на горизонті 1–3 місяці (операційні рішення), можуть бути слабкими для горизонту 2–5 років (інвестиційні рішення). Тому для консалтингу аудитора доцільно формувати «портфель моделей» для різних горизонтів і різних рівнів управління.

Текстова аналітика (NLP) у консалтингу зручна тим, що дозволяє оцифрувати якісні сигнали: відгуки клієнтів, звернення до служби підтримки, внутрішні інцидент-репорти, повідомлення медіа. Перехід від тексту до кількісних індикаторів репутаційного та операційного ризику робить ці сигнали порівнюваними в часі та між підприємствами.

Сентимент-аналіз у соціальних мережах доцільно розглядати не як оцінку настроїв, а як систему раннього попередження. Раптові зсуви тональності, зростання кількості негативних згадок або різка зміна тематичних кластерів можуть передувати падінню продажів, загостренню конфліктів із державними регуляторами або репутаційним кризам.

Водночас соціальні мережі формують ризик систематичних викривлень: голосні групи не завжди репрезентують ринок, а штучні інформаційні кампанії можуть спотворювати «цифровий образ» компанії. Отже, інвестиційному-консультанту важливо застосовувати фільтри бот-активності, географічної і демографічної репрезентативності та перевірку сигналів через альтернативні джерела даних.

Мережевий аналіз в інвестиційній оцінці дозволяє перейти від ***підприємства як одиниці – до підприємства як вузла екосистеми.*** Вузлова центральність, щільність зв'язків, залежність від критичних контрагентів, а також наявність «єдиних точок відмови» у постачанні створюють додатковий зріз ризику, який не видно зі звичайної фінансової звітності.

Особливо практичним є застосування мережевого аналізу до платіжних потоків і логістики: визначення концентрації постачальників, часу проходження замовлень, ступеня диверсифікації каналів, а також швидкості відновлення після збою. Для інвестора ці параметри перетворюються на вимірювані критерії операційної стійкості.

Разом із тим, блокчейн не є універсальною гарантією правдивості, якщо первинні дані внесені помилково або навмисно викривлено, незмінність запису лише закріплює проблему. Тому критичною залишається якість первинного введення даних та управління доступами до них, а також поєднання блокчейн-рішень із їх ретельною перевіркою (рис. 11.6).

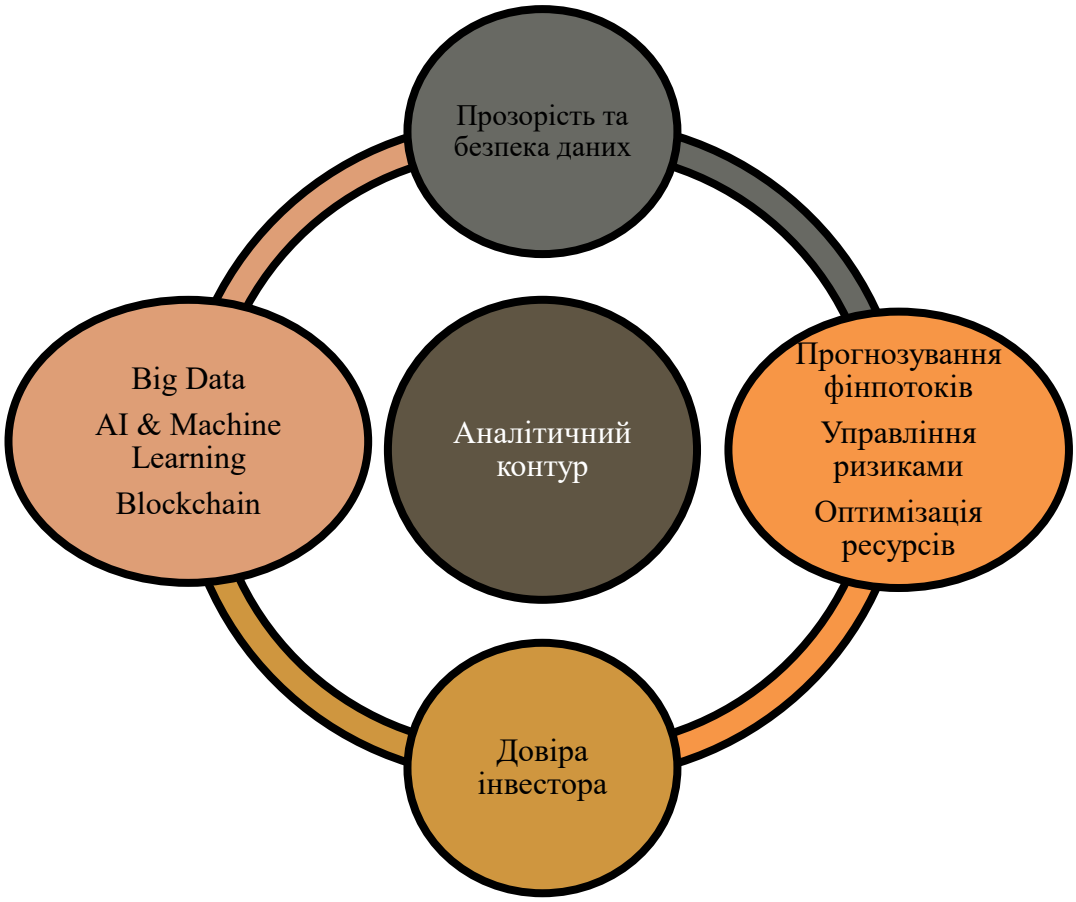


Рис. 11.6. Концептуальна схема синергії Big Data, AI і блокчейну

Імітаційне моделювання та цифрові двійники переводять оцінку інвестицій у площину сценарного аналізу «що буде, якщо». Це особливо корисно, коли підприємство планує капіталомісткі зміни: модернізацію виробництва, розширення складської інфраструктури, перехід на нові технологічні лінії або впровадження роботизації.

Цифровий двійник дозволяє тестувати сценарії без реальних втрат і простоїв, порівнюючи альтернативи за витратами, пропускною здатністю, споживанням ресурсів та ризиками. Для інвестора це означає зниження невизначеності, а для інвестиційного радника можливість аргументовано обґрунтовувати припущення, які закладені в інвестиційну модель.

Синергетичний підхід до інвестиційної привабливості фактично є переходом від «оцінки результату» до «оцінки здатності генерувати результат». Фінансові коефіцієнти фіксують наслідки рішень, тоді як цифрові технології (аналітика, AI, IoT) демонструють управлінську спроможність підтримувати ефективність і стійкість у динаміці.

У прикладній частині консалтингу важливо формалізувати синергію у вигляді карти «технологія → процес → показник → інвестиційний ефект».

Наприклад, Big Data та прогнозування попиту впливають на обсяги запасів і рівень дефіцитів, що відображається у показниках оборотності та маржинальності, а в інвестиційній логіці у зниженні потреби в оборотному капіталі.

Штучний інтелект у цьому підході трактується як інструмент підвищення якості рішень, а не просто автоматизації. Його внесок у інвестиційну привабливість проявляється через швидкість реакції на зміни, здатність до персоналізації пропозицій, зниження втрат від помилок планування та підвищення точності ризик-оцінювання.

Водночас етичність і пояснюваність моделей стають частиною інвестиційного ризику: якщо модель «чорна скринька» і породжує систематичні помилки, підприємство може отримати регуляторні, судові або репутаційні наслідки. Тому в інвестиційному консалтингу обґрунтовано вимагати протоколи валідності, контролю якості даних і моніторингу руху моделі.

IoT і цифрові двійники посилюють доказовість оцінки через доступ до даних реального часу: продуктивність обладнання, енергоефективність, стабільність технологічних режимів, рівень браку, простої. Для інвестора це зменшує «інформаційний розрив» між заявленими планами менеджменту та фактичними операційними можливостями.

Нарешті, синергія цифрових технологій у поєднанні з фінансовою аналітикою формує новий стандарт прозорості, інвестор очікує не лише звіт «як було», а й доказ «як управляється» та «як контролюється». Саме тому в цифровому середовищі інвестиційна привабливість дедалі частіше залежить від цифрової зрілості, кіберстійкості та якості управління даними поряд із традиційними фінансовими показниками.

Інтеграція Big Data, штучного інтелекту та блокчейну покращує фінансове прогнозування, оптимізує управління ресурсами і підвищує привабливість для інвесторів. При цьому ***цифрові здатності підприємств поділяються на базові,***

операційні та інтеграційні, кожна з яких позитивно впливає на ефективність і конкурентоспроможність.

Оцінка інвестиційної привабливості у цифровому середовищі – це складний, багатогранний процес, що поєднує фінансовий аналіз, інтегральні індекси, методи дисконтування та аналіз великих даних. Використання збалансованих показників та імітаційного моделювання дозволяє узгодити стратегічні і оперативні цілі, виявити слабкі місця і сформувати рекомендації для підвищення привабливості. Підприємства, які швидко адаптуються до цифрових змін, мають потенціал залучення інвестицій, зміцнення своїх позицій на ринку і забезпечувати сталий розвиток.

11.3.Ризики та етичні аспекти інвестиційного консалтингу аудитора

Інвестиційний консалтинг аудиторів відіграє важливу роль у забезпеченні ефективного руху капіталу між інвесторами та підприємствами. На відміну від традиційної функції аудиту, яка має на меті підтвердження достовірності фінансових звітів, консалтингова діяльність зорієнтована на допомогу замовнику у виборі оптимальної стратегії фінансування бізнесу або управління портфелем. Важливо розуміти, який інвестор планує вкладати кошти у компанію. Розрізняють стратегічних та портфельних інвесторів. Технології та обсяг аналізу в інвестиційному консультуванні залежать від характеристик інвестора як замовника консультацій.

Стратегічний інвестор ставить за мету встановити довгострокові відносини з об'єктом інвестування, при цьому дивіденди не є головною метою, яка може бути різною: від отримання безпосереднього впливу на управління до повного контролю; вихід на нові ринки, отримання доступу до інноваційних, в тому числі цифрових технологій, каналів збуту, бренд, управлінський досвід.

Це включає аналіз перспектив розвитку компаній, прогнозування доходності та ризиковості проєктів, а також підготовку рекомендацій щодо структури капіталу, диверсифікації активів та управління ризиками. Така діяльність тісно пов'язана з моральними та правовими викликами, оскільки інвестиційний консультант змушений балансувати між професійною незалежністю та очікуваннями клієнта. Крім того, на практиці часто виникають конфлікти інтересів, наприклад, коли консалтингова фірма одночасно рекомендує власні фінансові продукти або отримує винагороду від третіх осіб за певні інвестиційні рішення.

Портфельний інвестор вкладає кошти у цінні папери (часткові та боргові) з метою отримання доходу у вигляді дивідендів, якщо на момент їх виплати акції будуть у його власності, або різниці в цінах купівлі та продажу. Як правило, вони не втручаються в управління компанією, оскільки пакети їхніх цінних паперів є незначними , їх цікавить ліквідність цінних паперів.

Розвиток цифрових технологій значно трансформує інвестиційний консалтинг. Великі дані, штучний інтелект і блокчейн дозволяють аудиторам швидко аналізувати величезні масиви фінансової та нефінансової інформації, прогнозувати ризики та доходність із високою точністю, а також забезпечувати прозорість і незмінність записів. Однак цифровізація породжує нові ризики: порушення конфіденційності, відсутність алгоритмічної прозорості, кібербезпеку та етичні наслідки використання штучного інтелекту.

Тому важливим аспектом роботи інвестиційного консультанта є аналіз ризиків та етичних аспектів діяльності згідно міжнародних стандартів професійної етики (IIA, AICPA, IESBA). Успішне консультування щодо інвестиційних ризиків базується на їх систематизації. В основному їх розмежовують на п’ять ключових категорій: фінансові, операційні, стратегічні, комплаєнс-ризики та репутаційні. Кожна категорія має власні характеристики, джерела та інструменти управління. Узагальнення основних видів ризиків зведено у таблиці 11.4.

Таблиця 11.4

Категорії ризиків у інвестиційному консалтингу

Категорія ризику	**Основні характеристики**	**Приклади в інвестиційному консалтингу**
Фінансові	Передбачають потенційні втрати через коливання ринкових цін, неплатоспроможність контрагентів, проблеми ліквідності або зміни процентних ставок	неправильна оцінка ринкової вартості активів; концентрація портфеля в ризикових інструментах; недостатній аналіз кредитоспроможності позичальників
Операційні	Пов’язані з процесами та системами всередині організації; джерела – помилки персоналу, технічні відмови, неефективні процедури	збій автоматизованої системи ризик менеджменту; помилки при зборі та аналізі даних; недостатній контроль доступу до конфіденційної інформації
Стратегічні	Впливають на досягнення довгострокових цілей та ринкову конкурентоспроможність	обрання невірної інвестиційної стратегії; ігнорування макроекономічних трендів; недостатня диверсифікація активів
Комплаєнс ризики	Виникають внаслідок порушення законодавства або внутрішніх політик	недотримання вимог щодо незалежності та конфіденційності; порушення правил боротьби з відмиванням коштів; пропуск змін у регуляторному середовищі

Репутаційні	Стосуються втрати довіри інвесторів та суспільства через негативний імідж або етичні порушення	відкриття конфліктів інтересів; втручання у клієнтські рішення; негативні публікації у ЗМІ щодо роботи аудиторської фірми

Класифікація допомагає інвестиційним радникам концентруватися на ключових загрозах і будувати стратегії управління. Розуміння того, що технологічні ризики, наприклад кіберзагрози, можуть бути і операційними (помилки в IT- системах), і комплаєнс-ризиками (невідповідність GDPR), дозволяє точніше визначити відповідальні підрозділи та необхідні ресурси.

IIA визначає чотири базових принципи етики: інтегритет, об'єктивність, конфіденційність та компетентність.

Цілісність (integrity) – охоплює як особисту чесність, так і професійну принциповість, цілісність та правильність даних.

Цілісніть вимагає чесності та відповідальності. Об'єктивність означає неупереджену оцінку інформації й заборону діяльності, що може її скомпрометувати. Принцип конфіденційності забороняє розкривати інформацію без відповідних повноважень і використовувати її для власної вигоди. Компетентність передбачає наявність необхідних знань і досвіду та постійне їх удосконалення.

Правила поведінки конкретизують принципи. Наприклад, щодо цілісності, інвестиційний радник має діяти чесно, дотримуватися законів, не брати участь у незаконних операціях і сприяти досягненню законних цілей організації.

Об'єктивність вимагає уникнення будь-яких відносин, що можуть вплинути на неупередженість, і повідомлення про всі факти, які можуть спотворити звіт. Дотримання конфіденційності включає обережне поводження з інформацією і заборону використання її у власних інтересах. Принцип компетентності зобов'язує залучати лише ті послуги, у яких він має необхідну експертизу, та постійно підвищувати кваліфікацію.

Кодекс етики Американського інституту сертифікованих бухгалтерів (AICPA) розширює набір принципів, включаючи відповідальність, служіння

суспільним інтересам, цілісність, об’єктивність та незалежність, належну ретельність і сферу та характер послуг.

Принцип відповідальності покладає на аудиторів професійний обов’язок діяти з моральною чутливістю, зберігати довіру суспільства та сприяти розвитку професії. Служіння суспільному інтересу означає, що фахівець повинен приймати рішення, які служать добробуту всієї громади, а не лише окремих клієнтів.

Цілісність вимагає діяти чесно і відмовлятися від особистої вигоди. Принцип об’єктивності та незалежності наголошує, що член професії має уникати конфліктів інтересів та підтримувати незалежність у фактах і в зовнішньому вигляді. Належна ретельність передбачає дотримання професійних стандартів, постійне вдосконалення кваліфікації та виконання роботи на найвищому рівні. Ці принципи вимагають комплексного підходу до етики, оскільки аудитор повинен бути не лише незалежним, а й демонструвати відповідальність перед суспільством.

Проблема конфлікту інтересів стала однією з найгостріших у сучасному інвестиційному консалтингу. Аналітики CFA Institute відзначають, що багато консалтингових компаній позиціонують себе як «незалежних», хоча їхні рекомендації можуть бути упередженими через власний економічний інтерес.

Поширеною практикою є просування складних портфелів з активним управлінням, альтернативними інвестиціями та приватним капіталом, що підвищує комісійні доходи консультантів, але не обов’язково приносить користь клієнтам. Відсутність прозорості щодо вибору бенчмарків та відсутність відповідальності за результати також створює ризики для інвесторів.

Правила AICPA наголошують, що радник повинен бути об’єктивним і незалежним як фактично, так і зовні, тобто уникати будь-яких зв’язків, які можуть підірвати довіру до його суджень.

Незалежність зовнішнього вигляду означає, що навіть якщо фахівець зберігає внутрішню об’єктивність, сам факт належності до певних фінансових інститутів, отримання бонусів або інших вигод може створювати уявлення про

упередженість. У міжнародній практиці поширений підхід, коли аудиторам заборонено виконувати консалтинг для клієнта, чию звітність вони одночасно перевіряють, натомість інвестиційний консультант має таку можливість. Крім того, вони не повинні отримувати комісійну винагороду від третіх сторін за рекомендації клієнтам. У таблиці 11.5. узагальнено типові джерела конфліктів інтересів в інвестиційному консалтингу та можливі способи їх усунення.

Таблиця 11.5

Джерела конфлікту інтересів і заходи з їх мінімізації

Джерело конфлікту	Суть проблеми	Заходи запобігання
Продаж власних продуктів або афілійованих фондів	Консалтингова фірма рекомендує клієнтам інструменти, з яких отримує комісію або інші вигоди	Розділення функцій аудиту та консалтингу; розкриття клієнтам інформації про винагороди; впровадження політики «заборони продажу власних фондів»
Вибір бенчмарків та оцінка ефективності	Консультанти вибирають такі показники успішності, які сприяють позитивній оцінці їхніх власних рекомендацій	Незалежна перевірка бенчмарків; встановлення стандартизованих критеріїв оцінки; регулярний аудит результатів консультантів
Комісійна мотивація за складні портфелі	Активне управління та альтернативні інвестиції забезпечують консультанту вищі комісії, але можуть не приносити очікуваної наддоходності клієнту	Винагорода консультантів повинна залежати від довгострокових результатів клієнта; збалансована система бонусів без заохочення складних стратегій
Нерозкриття інформації про відносини з третьою стороною	Консультант може отримувати винагороду від постачальника фінансових продуктів, приховуючи цей факт	Зобов’язання до повного розкриття будь яких фінансових зв’язків; внутрішній контроль і зовнішній аудит політики розкриття

Зменшення конфліктів інтересів передбачає прозору політику щодо винагород, відкриті відносини з клієнтами, а також незалежну оцінку роботи консультанта. Не менш важливі регулярне підвищення кваліфікації та дотримання професійних стандартів.

Застосування цифрових технологій (Big Data, штучного інтелекту, блокчейну) радикально змінює роботу аудиторів. Аналітичні інструменти можуть забезпечити більш точне прогнозування грошових потоків, управління ризиками та оптимізацію використання ресурсів. Проте цифровізація породжує нові етичні ризики:

1. ***Конфіденційність та захист даних.*** Використання великих масивів клієнтських даних потребує дотримання законодавства про персональні дані (GDPR, закони про банківську таємницю тощо). Порушення конфіденційності може призвести до фінансових санкцій і втрати довіри.
2. ***Алгоритмічна упередженість.*** Системи штучного інтелекту приймають рішення на основі тренувальних даних. Якщо ці дані містять історичну упередженість (наприклад, щодо певних галузей або компаній), алгоритм може відтворювати нерівність і порушувати принцип об'єктивності.
3. ***Прозорість та пояснюваність.*** Клієнти повинні розуміти, як саме алгоритм формує рекомендації. Непрозорі моделі (black-box) можуть викликати сумніви щодо правильності рішень.
4. ***Кібербезпека.*** Витік або злам даних може вплинути на фінансову стабільність та репутацію. Операційні і репутаційні ризики цифрового середовища часто перекривають традиційні ризики.

Міжнародна рада з етики для бухгалтерів (IESBA) пропонує концептуальну рамку, що дає змогу ідентифікувати, оцінювати та усувати погрози відповідності фундаментальним принципам етики. Хоча повний текст останньої редакції 2024 р. неможливо навести через ліцензійні обмеження, видання підкреслює, що аудитор має визначити тип погрози (наприклад, саморецензування, самореклама, родинні чи фінансові інтереси), оцінити рівень ризику та запровадити заходи для його мінімізації.

Такий підхід збігається з ***принципом due care*** – професіонал повинен діяти з належною ретельністю, адаптуючи рішення до конкретної ситуації та оцінюючи суму ризиків і переваг для клієнта.

Спочатку аудитор має звернутися до фундаментальних принципів:

- *цілісності;*
- *об'єктивності;*
- *конфіденційності;*
- *компетентності;*
- *відповідальності перед суспільством;*

- *належної ретельності.*

Далі потрібно ідентифікувати тип ризику (фінансовий, операційний, стратегічний тощо) та можливі загрози для дотримання етичних принципів. Оцінивши ймовірність та вагомість ризику, аудитор розробляє наступні контрольні заходи (рис. 11.7).

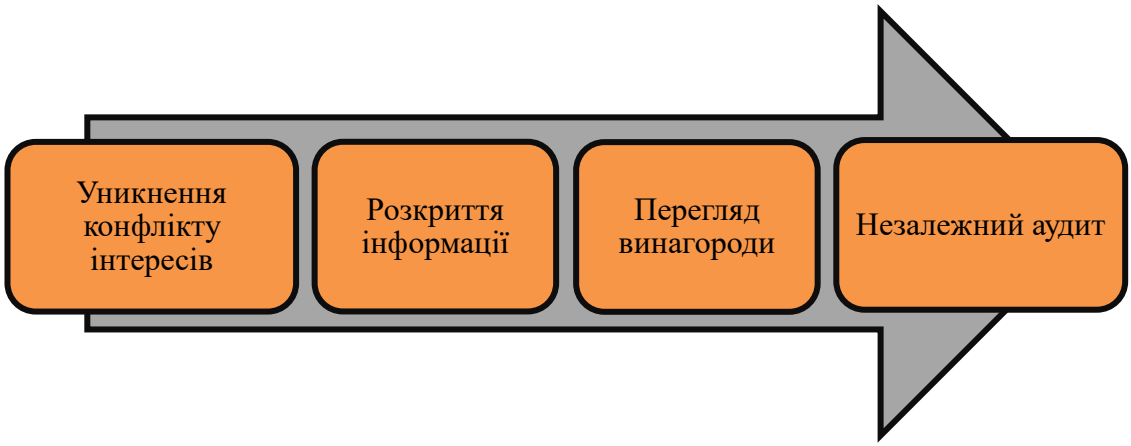


Рис. 11.7. Контрольні заходи аудитора

Лише після цього приймається рекомендація клієнту. У випадку невирішеного конфлікту аудитор може відмовитися від завдання.

Етичний консалтинг вимагає гармонійного поєднання трьох елементів: незалежності аудитора, управління конфліктами інтересів та дотримання цифрової етики. Незалежність забезпечує об'єктивність; контроль конфліктів інтересів зменшує вплив особистої вигоди; цифрова етика регулює використання технологій, підвищуючи прозорість та безпеку. У центрі перетину цих сфер інтегрований підхід до управління ризиками, де для кожної ситуації підбирають відповідні методи моніторингу, аудиту, розкриття інформації та технічного захисту.

Розглянемо ситуацію, у якій аудиторська компанія надає інвестиційні рекомендації технологічному стартапу. Компанія планує залучити венчурний капітал для розробки штучного інтелекту, що аналізує фінансові ринки. Ризики включають:

- *невизначеність щодо оцінки проєкту;*
- *можливі втрати інвесторів у випадку невдачі;*
- *коливання вартості акцій після виходу на біржу;*
- *ймовірні помилки в алгоритмах ШІ;*
- *нестача кваліфікованих фахівців;*
- *ризик кіберзагроз;*
- *конкуренцію зі світовими лідерами у сфері фінтех;*
- *швидкоплинність технологічних тенденцій;*
- *потенційну зміну регуляторного середовища;*
- *недотримання вимог щодо захисту персональних даних;*
- *уникнення маніпуляцій;*
- *сертифікацію алгоритмів;*
- *звинувачення у маніпулюванні ринком, якщо продукт викликає небажані коливання цін.*

Етична оцінка починається з визначення потенційних ***конфліктів інтересів.*** Якщо аудиторська компанія планує інвестувати у стартап або отримує винагороду від венчурних фондів за рекомендації, виникає загроза упередженості. Для вирішення конфлікту може бути запропонована незалежна експертиза або відмова аудитора від фінансової участі, натомість запрошується інвестиційний консультант.

Далі оцінюється правомірність та етичність використання даних. Аудитору необхідно забезпечити зберігання інформації відповідно до GDPR, уникати алгоритмічної дискримінації та забезпечувати пояснюваність моделі. Фінансові ризики зменшуються за допомогою диверсифікації інвестицій та стрес-тестування моделей. Важливим елементом є комунікація з інвесторами, оскільки радник повинен чесно інформувати про можливі втрати та витрати, щоб зберігати достовірність даних.

Інвестиційний консалтинг аудиторів потребує глибокого розуміння ризиків і бездоганного дотримання етичних стандартів. (рис. 1.8.) Названа вище класифікація ризиків допомагає будувати ефективну систему контролю

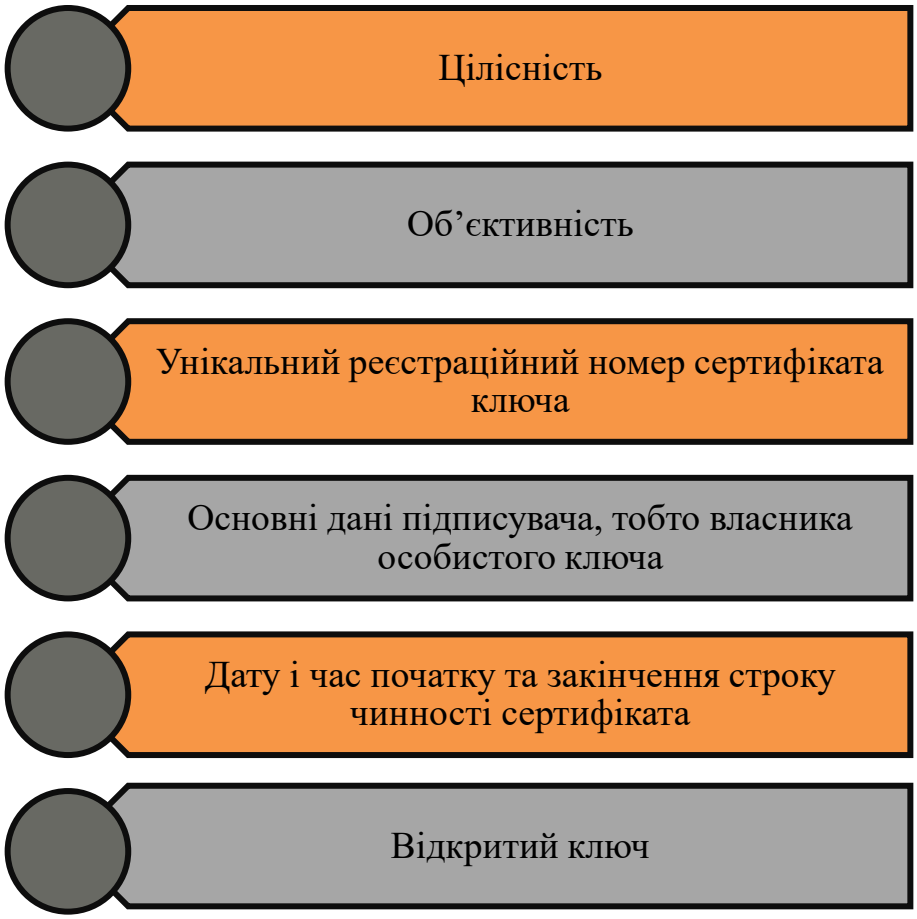


Рис. 11.8. Фундаментальні принципи професійної етики

Усі ці принципи створюють основу для прийняття правильних рішень. Конфлікти інтересів, притаманні консалтингу, необхідно виявляти та усувати за допомогою прозорих політик, незалежного аудиту та належної мотивації консультантів.

Цифрові технології відкривають нові можливості, але вимагають особливої уваги до етичних аспектів:

- *захисту даних;*
- *алгоритмічної справедливості;*
- *прозорості;*
- *кібербезпеки.*

Рекомендується з самого початку закладати в систему захист приватності, застосовувати зрозумілі й прозорі алгоритми та регулярно проводити перевірки систем штучного інтелекту.

Лише гармонійне поєднання незалежності, управління конфліктами інтересів і цифрової етики може забезпечити високий рівень довіри до

аудиторського консалтингу та сприятиме сталому розвитку ринку консультаційних послуг.

Спільна співпраця аудиторів та інвестиційних консультантів уже здійснюється в Україні, запит на цих фахівців буде зростати. Конфліктів інтересів можна уникнути через вдосконалення законодавчих регуляторних процедур та втілення в життя етичних принципів формування звітів та рекомендацій для клієнтів.

11.4 Контрольні питання для самоперевірки

1. Про який тренд на ринку фінансових послуг свідчить поява інвестиційних консультантів в аудиторських фірмах?
2. В чому полягає відмінність між аудитором та інвестиційним консультантом?
3. Які три основних варіанти рекомендацій може надавати клієнтам інвестиційний консультант?
4. Як ви розумієте сутність фундаментального аналізу об’єкта, що потребує інвестиційного консультування?
5. Коли і для яких інвесторів інвестиційний консультант використовує технічних аналіз цін на основні активу у реальному часі?
6. Наскільки відрізняються програми підготовки аудиторів та інвестиційних консультантів?
7. Як досліджують інвестиційну привабливість об’єкта аналізу інвестиційні радники?
8. Які показники аналізуються для визначення інвестиційної привабливості, крім фінансових?
9. Які технології цифрового простору використовує для аналізу та вироблення рекомендацій інвестиційний консультант?
10. Які етичні моменти має враховувати інвестиційний консультант при підготовці звіту та при комунікації з клієнтом?

Розділ 12

Автор:
Валентина Панасюк

ІНТЕГРАЦІЯ ШІ В АУДИТОРСЬКІ ПРОЦЕДУРИ

РОЗДІЛ 12. ІНТЕГРАЦІЯ ШІ В АУДИТОРСЬКІ ПРОЦЕДУРИ

«Гідність людини та права мають бути критерієм для нових технологій.»

Папа Франциск

12.1. Місце та можливості ШІ в аудиті

Відповідно до статті 1 Закону України «Про аудит фінансової звітності та аудиторську діяльність», аудит фінансової звітності визначається як «аудиторська послуга з перевірки даних бухгалтерського обліку і показників фінансової звітності та/або консолідованої фінансової звітності юридичної особи або представництва іноземного суб'єкта господарювання, або іншого суб'єкта, який подає фінансову звітність та консолідовану фінансову звітність групи, з метою висловлення незалежної думки аудитора про її відповідність в усіх суттєвих аспектах вимогам національних положень (стандартів) бухгалтерського обліку, міжнародних стандартів фінансової звітності або іншим вимогам».

Згідно з Концепцією розвитку штучного інтелекту в Україні, схваленою розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р: «***штучний інтелект*** – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також

створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань».

Інтеграція таких технологій в аудит дозволяє оптимізувати обробку значних масивів інформації та підвищити обґрунтованість аудиторських висновків. Впровадження ШІ зумовлене зростанням обсягів даних, ускладненням бізнес-процесів і підвищенням вимог до якості та оперативності аудиторських висновків.

ШІ також розширює можливості безперервного аудиту та моніторингу. Інтелектуальні системи здатні працювати в режимі реального часу, відстежуючи фінансові показники, дотримання внутрішніх контролів і комплаєнс-вимог. Такий підхід сприяє своєчасному виявленню відхилень і підвищує превентивну функцію аудиту.

Фундаментальною зміною, яку приносить ШІ в методологію аудиту, є перехід від ризик-орієнтованих вибірок до суцільного аналізу даних у реальному часі. Це, у свою чергу, зумовлює перегляд ролі аудитора, який поступово переходить від виконавця перевірочних процедур до аналітика та інтерпретатора результатів, отриманих за допомогою інтелектуальних технологій.

Історично аудитори були змушені покладатися на статистичні або нестатистичні методи вибірки, перевіряючи, наприклад, лише 20–50 операцій з кількох тисяч, щоб зробити висновок про відсутність суттєвих викривлень. Такий підхід несе в собі невід'ємний ризик вибірки – ймовірність того, що висновок аудитора, зроблений на основі вибірки, відрізнятиметься від висновку, який був би зроблений за результатами перевірки всієї сукупності.

Галузь штучного інтелекту – напрям діяльності у сфері інформаційних технологій, який забезпечує створення, впровадження та використання технологій штучного інтелекту.

Успішна імплементація технологій штучного інтелекту в аудиторські процедури неможлива без налагодження міжфункціональної взаємодії всередині організації. Провідні компанії вже реалізують комплексні стратегії

перекваліфікації персоналу, які виходять за межі суто технічного навчання. Ключовим завданням стає трансформація менталітету працівників та формування культури співпраці як з колегами, так і з цифровими системами. Для закріплення цих змін застосовують широкий спектр інструментів: від кадрових ротацій та освітніх курсів до проведення професійних змагань.

Алгоритми штучного інтелекту та аналітики даних дозволяють обробляти 100 % транзакцій клієнта, незалежно від їх кількості, що дає змогу виявляти не лише системні помилки, але й поодинокі аномалії, які могли б залишитися непоміченими при традиційній вибірці (табл. 12.1).

Таблиця 12.1

Порівняльна характеристика традиційного аудиту та аудиту з використанням ШІ

Критерій порівняння	**Традиційний аудит**	**Аудит з використанням ШІ (AI-enabled Audit)**
Обсяг перевірки	Вибіркова перевірка. Фокус на репрезентативності	Суцільний аналіз. Фокус на аномаліях
Характер процедур	Переважно ручні процедури, звірка паперових документів	Автоматизовані алгоритми, звірка цифрових слідів
Час проведення	Циклічний (раз на рік)	Безперервний аудит або наближений до реального часу
Роль аудитора	Збір, агрегація та перевірка даних	Налаштування алгоритмів, інтерпретація результатів, професійне судження
Виявлення шахрайства	Реактивне (постфактум), обмежене вибіркою	Проактивне, на основі патернів поведінки та предиктивних моделей

Економічна інформація, що аналізується під час проведення аудиторських процедур, за своєю природою, є гетерогенною: це можуть бути скани договорів, записи в регістрах бухгалтерського обліку, банківські виписки, електронні листи або логи складських програм. Для того, щоб штучний інтелект міг застосувати до цієї інформації аналітичні процедури, вона повинна пройти процес ***ETL (Extract, Transform, Load)*** – вилучення, трансформації та завантаження.

Процес перетворення економічної інформації в дані для аудиту можна представити у вигляді логічної схеми (рис. 12.1):

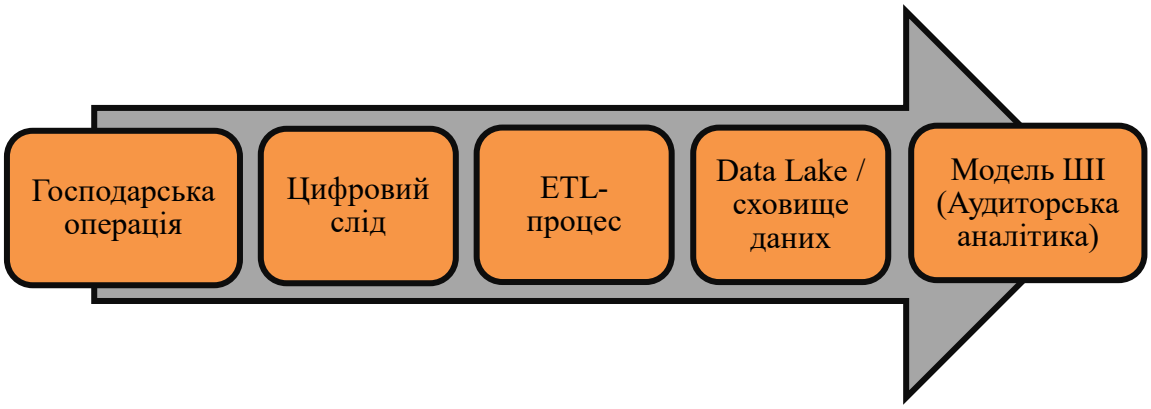


Рис. 12.1. Схема перетворення економічної інформації в дані

Цей процес включає наступні етапи, критичні для розуміння аудитором:

1. Цифровізація факту. На цьому етапі реальна господарська операція (наприклад, відвантаження товару) фіксується в обліковій системі. Важливим аспектом є автоматизація цього етапу (використання сканерів штрих-кодів, ЕДО), що мінімізує вплив людського фактора і забезпечує цілісність «цифрового сліду».

2. Структурування та класифікація. Неструктурована інформація перетворюється на впорядковані записи баз даних (рядки та стовпці). Для аудитора важливо пересвідчитися, що таксономія даних клієнта (система кодування статей, центрів витрат) дозволяє алгоритмам ШІ коректно ідентифікувати тип операції.

3. Очищення та збагачення. Перед подачею на вхід нейромережі дані очищаються від дублікатів, помилок форматування та шумів. Часто на цьому етапі внутрішні дані компанії збагачуються зовнішніми даними (курси валют, індекси цін, галузеві бенчмарки), що дозволяє проводити більш глибокий контекстний аналіз.

4. Генерація ознак. Специфічний етап для ML-моделей, де з масиву даних виділяються ключові змінні (предиктори), які найбільше впливають на результат аудиторської перевірки.

«Машинне навчання (ML) (machine learning) – процес використання обчислювальних методів, щоб надати системам здатність навчатися на даних або досвіді».

Розуміння цієї схеми є критичним для аудитора, оскільки помилка на будь-якому з етапів трансформації призводить до викривлення результатів роботи ШІ. Аудитор повинен верифікувати не лише кінцевий результат (фінансову звітність), але й саму логіку (алгоритм) перетворення даних, оцінюючи ризики втрати або спотворення інформації в процесі її обробки автоматизованими системами.

Роль ШІ в економічному секторі України посилюється та має тенденцію до постійного зростання. Аналіз динаміки зростання обсягу ринку штучного інтелекту в Україні демонструє загальну висхідну тенденцію: з $157,7 млн у 2020 році він зріс до $338,9 млн у 2021 році, після чого спостерігалося певне уповільнення у 2022 році ($211,5 млн). У подальші роки відбулося поступове відновлення та зростання – до $233,1 млн у 2023 році, $316,3 млн у 2024 році та $419,4 млн у 2025 році.

Прогнозні оцінки свідчать про суттєве прискорення розвитку галузі. Вбачається, що до 2030 року обсяг українського ШІ-ринку може досягти $1 419,9 млн, вказуючи на значний потенціал масштабування та стратегічну роль штучного інтелекту в цифровій трансформації економіки України (рис. 12.2).

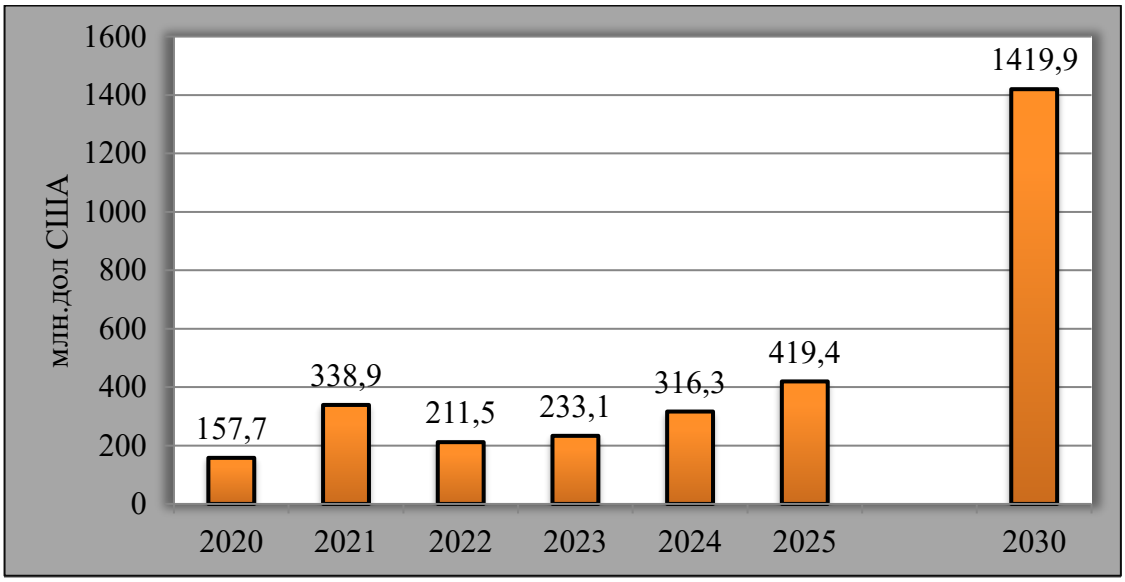


Рис. 12.2. Розмір ринку ШІ в Україні, млн дол. США

Для розуміння місця ШІ в аудиторських процедурах доцільно розглянути ієрархію аналітики даних. Згідно з моделлю Gartner, яка адаптується до

аудиторської практики, виділяють чотири рівні аналітики, кожен з яких додає більшу цінність для процесу аудиту, відповідаючи на питання (рис. 12.3).

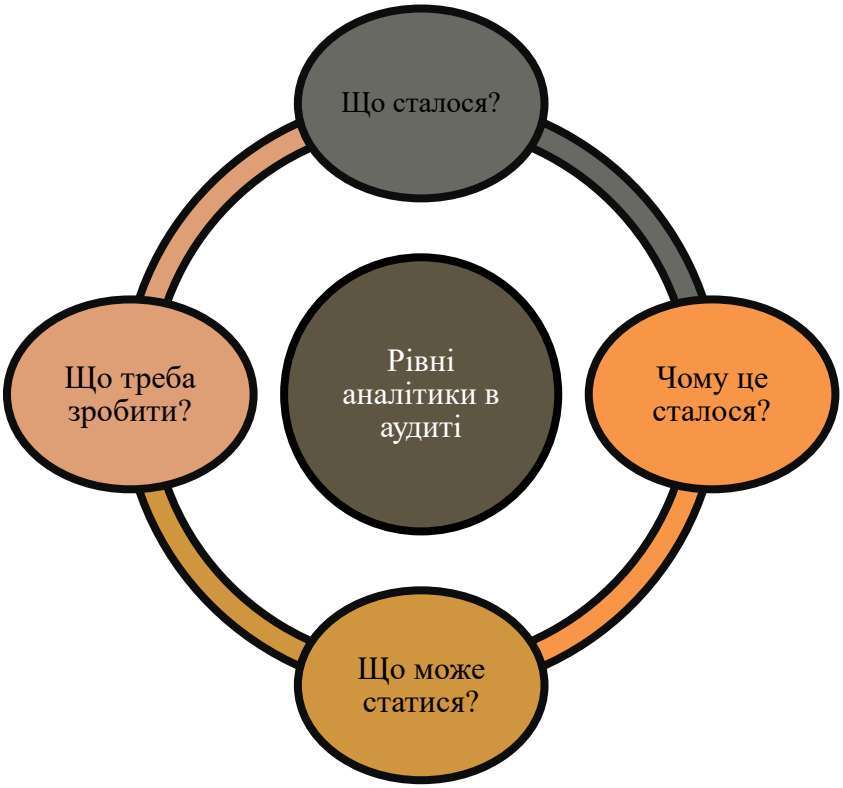


Рис. 12.3. Еволюція аналітики даних в аудиті

1. Описова аналітика – «Що сталося?» Це базовий рівень, який використовується в аудиті десятиліттями. Він включає агрегацію даних, візуалізацію (dashboarding) та розрахунок основних фінансових коефіцієнтів. На цьому етапі ШІ майже не застосовується, використовуються стандартні інструменти BI (Business Intelligence).

Приклад. Візуалізація динаміки виручки за місяцями для ідентифікації сезонності.

2. Діагностична аналітика – «Чому це сталося?» На цьому рівні аудитор намагається зрозуміти причини минулих подій. Тут починають застосовуватися елементи машинного навчання (наприклад, кластеризація), що дозволяють виявити кореляції між подіями.

Приклад. Drill-down аналіз (деталізація) витрат для з'ясування причин різкого зростання собівартості в четвертому кварталі.

3. Прогнозна аналітика – «Що може статися?» Саме тут розкривається основний потенціал ШІ. Використовуючи історичні дані, алгоритми будують

моделі майбутньої поведінки фінансових показників. Якщо фактичні дані суттєво відрізняються від прогнозу ШІ, це є сигналом для аудитора про можливі викривлення або маніпуляції з фінансовою звітністю. Функція прогнозування в аудиті виходить за межі простого планування бюджетів. Згідно з МСА 570 «Безперервність діяльності», аудитор зобов'язаний оцінити здатність підприємства продовжувати свою діяльність у майбутньому.

Приклад. Прогнозування очікуваного доходу від реалізації на основі нефінансових даних (кількість відвантажень, погодинна робота обладнання, споживання електроенергії) та порівняння з даними Головної книги.

4. Приписувальна (прескриптивна) аналітика – «Що треба зробити?» Це найвищий рівень, де системи ШІ не лише прогнозують майбутнє, але й рекомендують аудитору конкретні дії.

Приклад. Система автоматично пропонує провести інвентаризацію запасів на конкретному складі, де модель виявила високий ризик крадіжок на основі аналізу руху товарів.

Інструменти ШІ дозволяють реалізувати прогнозне моделювання банкрутства з вищою точністю. Використовуючи часові та нейронні мережі, система аналізує не лише фінансові показники, а й нефінансові сигнали:

- *динаміку звільнення ключового персоналу;*
- *тональність новин про компанію в медіа;*
- *судові позови та затримки в ланцюгах постачання.*

Такий мультифакторний аналіз дозволяє аудитору отримати раннє попередження про ризики неплатоспроможності за 6–12 місяців до настання кризи.

Важливим фактором інтеграції ШІ, поряд з аналітикою та прогнозуванням, є підтримка прийняття рішень. У сучасному аудиті утверджується концепція доповненого інтелекту. Її суть полягає в тому, що ШІ не замінює професійне судження аудитора, а підсилює його, знижуючи когнітивне навантаження та вплив людських упереджень.

Інтелектуальні системи підтримки рішень допомагають аудитору на етапах, де існує висока невизначеність:

- *визначення суттєвості* – ШІ пропонує поріг суттєвості, базуючись на бенчмарках галузі та історії помилок минулих періодів;
- *оцінка аудиторського ризику* – система агрегує фактори ризику (внутрішнього контролю, невід'ємного ризику) і пропонує аудитору карту ризиків із рекомендованими діями;
- *формування аудиторської думки* – на основі зібраних доказів система може генерувати проєкт аудиторського висновку, підсвічуючи моменти, що вимагають модифікації думки.

Взаємодію аудитора та системи підтримки рішень можна представити у вигляді ієрархічної схеми (рис. 12.4).

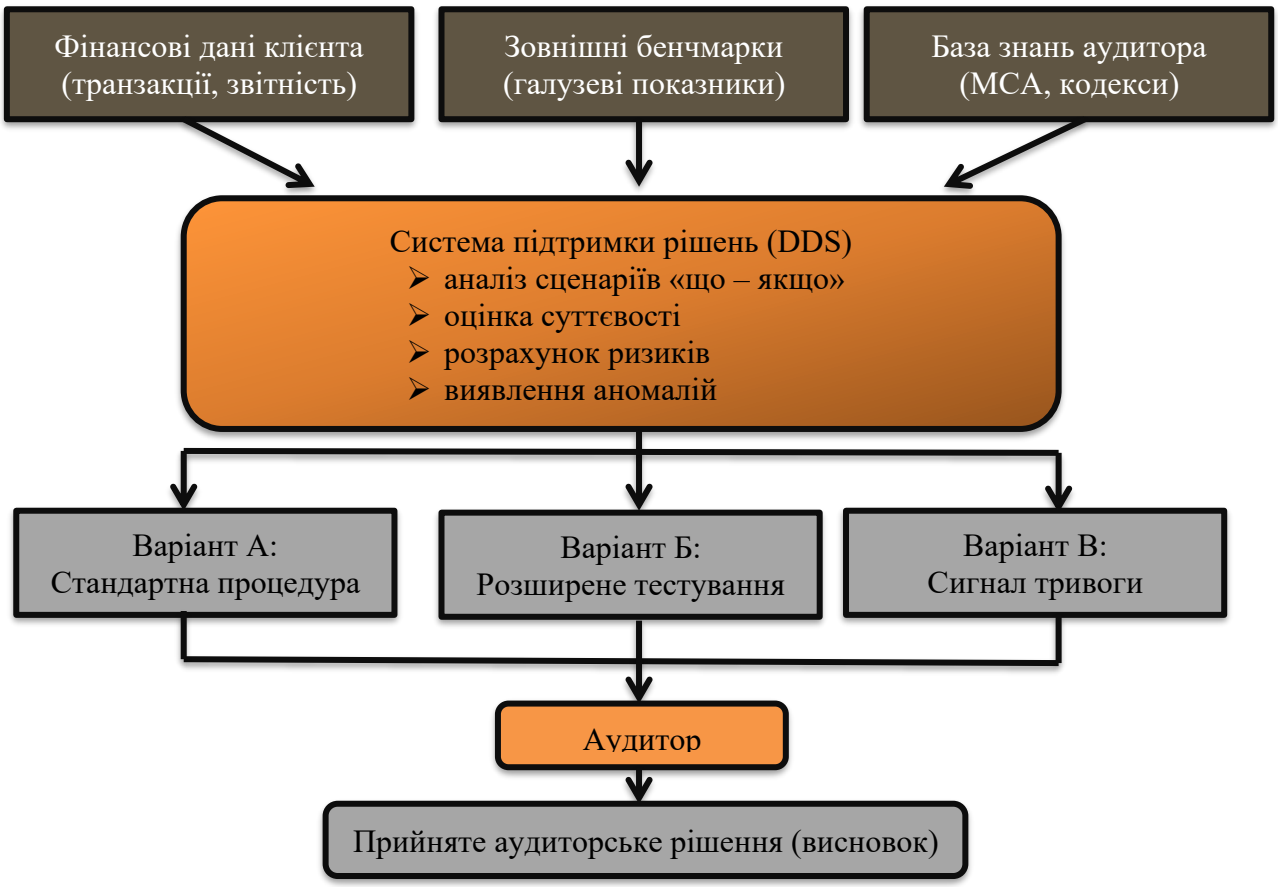


Рис. 12.4. Модель взаємодії аудитора з системою підтримки прийняття рішень

Модель описує цикл від агрегації даних до генерації сценаріїв, де роль ШІ обмежена рекомендаціями, а остаточне рішення залишається за аудитором, який

верифікує результати на основі професійного судження та етики. Таким чином, ШІ в аудиті виступає як стратегічний аналітик, що забезпечує перехід від констатації фактів до моделювання майбутнього та обґрунтування управлінських рішень.

Цифрова трансформація фінансового сектору зумовлює докорінні зміни не лише в обліку, а й у самій методології аудиту. Впровадження новітніх інструментів дозволяє відійти від класичних вибіркових методів на користь суцільного аналізу та безперервного моніторингу. Така еволюція не тільки покращує якісні показники аудиту, а й значно посилює транспарентність та довіру стейкхолдерів до фінансової звітності.

Основні напрями трансформації методології аудиту під впливом цифрових технологій узагальнено в таблиці 12.2.

Таблиця 12.2

Вплив цифрових технологій на трансформацію методології аудиту

Напрям змін у методології	**Зміст трансформаційних процесів**	**Результат цифровізації**
Автоматизація процедур	Заміщення ручної перевірки алгоритмічними обчисленнями	Миттєва обробка масивів даних у режимі реального часу
Безперервний моніторинг	Перманентний контроль бізнес-процесів замість періодичного	Оперативна ідентифікація аномалій, помилок та відхилень
Ризик-орієнтована аналітика	Детекція зон підвищеної вразливості на основі даних	Фокусування перевірки на критичних сегментах завдяки Data Analytics
Забезпечення прозорості та валідації	Цифровий трекінг усіх аудиторських дій	Впровадження електронного документообігу та фіксація журналів активності

Цифровізація докорінно змінює сутність аудиту: він еволюціонує від процедури формальної звітності до стратегічного механізму управління ризиками та зміцнення фінансової дисципліни. Використання новітніх технологій гарантує глибину та оперативність аналізу згідно з міжнародними вимогами, закладаючи фундамент для подальшого прогресу у сферах обліку та аудиту.

12.2. Інструменти ШІ для аудиторських процедур

Під інструментарієм штучного інтелекту розуміють програмне забезпечення, що базується на інтелектуальних алгоритмах і здатне виконувати когнітивні завдання, притаманні людині. Функціонал таких систем охоплює аналітику даних, ідентифікацію закономірностей, а також прийняття рішень і прогнозування. Сучасна архітектура аудиторської діяльності зазнає фундаментальних змін під впливом стрімкого зростання обсягів даних та розвитку технологій штучного інтелекту. Традиційний інструментарій, заснований на вибіркових методах та ручній перевірці, поступається місцем комплексним екосистемам, що включають алгоритми машинного навчання (Machine Learning – ML), обробку природної мови (Natural Language Processing – NLP) та інтелектуальну автоматизацію процесів.

У сфері системного аналізу застосовується широкий спектр інструментів штучного інтелекту, кожен з яких адаптований під специфічні завдання та сфери використання. Класифікація цих засобів на основі їх функціонального призначення дозволила систематизувати їх за групами (рис. 12.5).

Рис. 12.5. Способи застосування ШІ в системному аналізі

1. Аналітика даних:

- *робота з Big Data* (ШІ забезпечує глибинний аналіз масивів інформації, виявляючи кореляції та тренди, недоступні для класичних методів);
- *машинне навчання* (використання прогнозних алгоритмів дозволяє передбачати майбутні тенденції на підставі історичних даних).

2. Візуалізація інформації. Генерація інтерактивних дашбордів (панелей моніторингу) дозволяє відстежувати процеси в режимі реального часу, спрощуючи сприйняття складних даних.

3. Системи підтримки прийняття рішень:

- *імітаційне моделювання* (створення сценарних моделей для оцінки наслідків тих чи інших управлінських кроків до їх фактичного впровадження);
- *оптимізація* (застосування алгоритмів для вдосконалення операційних процесів).

4. Експертні системи. Інтеграція ШІ в бази знань для прискорення аналізу ситуацій та підвищення точності висновків.

5. Технології обробки природної мови:

- *текстовий аналіз* (обробка неструктурованого контенту (відгуків, документації) для визначення настроїв аудиторії та ключових тем);
- *генерація звітності* (автоматичне створення зведень та резюме, що мінімізує ручну працю аналітиків).

6. Прогностична аналітика та оцінка ризиків:

- *прогнозування попиту* (аналіз ринкової кон'юнктури для ефективного планування виробничих потужностей і складських запасів);
- *ранжування ризиків* (класифікація потенційних загроз залежно від ймовірності та впливу різних сценаріїв).

7. Автоматизація та контроль:

- *Robotic Process Automation* (RPA) (передача рутинних операцій алгоритмам для вивільнення інтелектуального ресурсу фахівців);
- *моніторинг загроз* (автоматичне виявлення аномалій для миттєвого реагування на збої чи небезпеки).

На відміну від традиційного програмування, де алгоритм дій задається людиною, ML-системи самостійно знаходять закономірності в масивах даних і формують правила для прийняття рішень.

Застосування машинного навчання в аудиті можна класифікувати за трьома основними напрямами:

1. Виявлення аномалій. Алгоритми аналізують великі набори даних (Big Data) для ідентифікації транзакцій, що відхиляються від стандартних патернів поведінки.

Приклад. Система вивчає типові закупівлі підприємства і автоматично сигналізує про операцію з незвичайною ціною або новим, неперевіреним постачальником.

2. Прогнозна аналітика. Використання історичних даних для моделювання майбутніх подій. В аудиті це дозволяє оцінювати безперервність діяльності підприємства, прогнозувати фінансові показники та порівнювати їх із фактичними результатами для виявлення маніпуляцій.

3. Класифікація та оцінка ризиків. Автоматичний розподіл об’єктів (транзакцій, контрагентів, договорів) за категоріями ризику.

Приклад. Алгоритми на базі дерев рішень (Decision Trees) можуть класифікувати вразливості системи безпеки за ступенем критичності, допомагаючи аудиторам встановити пріоритетність перевірки.

Важливо враховувати, що використання ML в аудиті не зводиться лише до побудови моделі. Якість результатів прямо залежить від якості даних, коректності постановки задачі та прозорості критеріїв, за якими система формує сигнали і ризик-оцінки. Тому аудитор має оцінювати не тільки вихідні сигнали, а й надійність даних, логіку інтерпретації результатів та наявність процедур валідації, щоб мінімізувати ризик помилкових індикаторів і невиявлених відхилень висновків.

Згідно з дослідженнями, життєвий цикл роботи моделі машинного навчання складається з трьох ключових етапів: підготовки даних, застосування алгоритмів (навчання) та ретротестування.

Процес реалізації ML-моделі в аудиті зображено на схемі (рис. 12.6).

Рис. 12.6. Процес реалізації ML-моделі в аудиті

Ще одним критично важливим напрямом розвитку штучного інтелекту, що забезпечує інтерфейс взаємодії між людиною та комп'ютером, є обробка природної мови. Головне завдання цієї технології – подолати бар'єр між бінарною логікою машин та багатогранною, часто неоднозначною людською мовою.

Сучасні аудиторські фірми акумулюють величезні масиви інформації, яка виходить за межі структурованих таблиць. Це електронне листування, стрічки новин, транскрипції аудіо- та відеозустрічей, текстові повідомлення в месенджерах тощо. Програмне забезпечення на базі NLP дозволяє

автоматизувати обробку цього потоку даних, аналізуючи не лише зміст, а й наміри та емоційне забарвлення (настрої) комунікації в режимі реального часу.

На глобальному ринку яскравим прикладом застосування NLP є платформа Botkeeper, яка використовує машинне навчання та мовні моделі для автоматизації бухгалтерського обліку. Про високу ефективність таких рішень свідчать емпіричні дані, згідно з якими для тисячі клієнтів компанії було автоматизовано понад 1,2 мільйона робочих годин. Автоматизація навіть 240 годин ручної праці, за оцінками експертів, може заощадити підприємству понад 9000 доларів США, що підтверджує економічну доцільність впровадження.

В Україні елементи інтелектуальної автоматизації активно впроваджуються через системи класу BAS (Business Automation Software). Ці програмні рішення дозволяють комплексно автоматизувати бізнес-процеси підприємств різних галузей та масштабів, включаючи обробку економічної інформації та документообіг, створюючи підґрунтя для подальшої інтеграції інструментів ШІ.

Процес інтелектуального аналізу текстових даних не є лінійним. Він складається з низки складних етапів перетворення «сирого» тексту на структуровану інформацію, придатну для прийняття рішень (рис. 12.7).

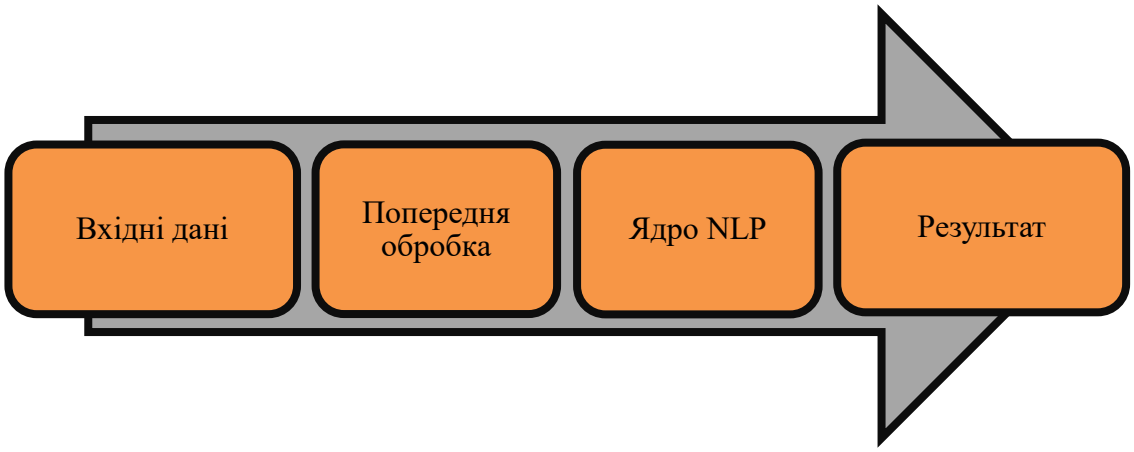


Рис. 12.7. Архітектура обробки неструктурованих даних системою NLP в аудиті

Опис етапів процесу даних системою NLP:

1. Збір даних. Система забезпечує автоматизоване отримання інформації з різнорідних джерел, зокрема шляхом оптичного розпізнавання тексту (OCR) у

відсканованих PDF-файлах, а також через аналіз корпоративної пошти, новинних ресурсів та соціальних мереж.

2. ***Попередня обробка:***

- *токенізація* – розбиття тексту на окремі слова або фрази (токени);
- *лематизація або стемінг* – приведення слів до їхньої словникової форми, що критично для української мови з її складною морфологією;
- *очищення* – видалення «стоп-слів» (прийменників, сполучників), які не несуть смислового навантаження.

3. Ядро NLP – застосування моделей (BERT, FinBERT, GPT) для визначення контексту, тональності та сутностей.

4. Результат – формування висновку: «ризиковий контракт», «негативна тональність новини», «невідповідність у звіті».

Якщо штучний інтелект та машинне навчання відповідають за «когнітивну» складову аудиту (аналіз, розуміння, прогнозування), то роботизована автоматизація процесів (Robotic Process Automation – RPA) бере на себе фізичне виконання рутинних операцій. У сучасному аудиті спостерігається еволюція від використання простих скриптів до концепції інтелектуальної автоматизації (IA), що поєднує RPA з елементами штучного інтелекту.

Технологія RPA базується на використанні програмних роботів (ботів), які імітують дії людини-користувача в цифрових системах. Боти взаємодіють з інтерфейсом програмного забезпечення так само, як аудитор: вони можуть відкривати додатки, копіювати та вставляти дані, заповнювати форми, переміщувати файли та папки, зчитувати інформацію з баз даних.

Ключовою перевагою RPA є здатність працювати з різнорідними системами, які не мають прямого програмного інтерфейсу для інтеграції. Це особливо актуально для аудиту, де часто доводиться звіряти дані між сучасними ERP-системами (наприклад, SAP) та застарілими (legacy) системами обліку або зовнішніми порталами (банківські клієнт-банки, податкові реєстри).

Основні сценарії використання RPA в аудиті:

- *збір та консолідація даних* – автоматичне вивантаження інформації з різних ERP-систем клієнта, які можуть бути несумісними між собою;
- *перехресна звірка* – порівняння даних внутрішнього обліку з зовнішніми джерелами (банківськими виписками, реєстрами податкових накладних) для виявлення розбіжностей;
- *формування робочих документів* – автоматичне заповнення стандартних аудиторських форм на основі зібраних доказів.

Процес впровадження RPA є циклічним і складається з чітко визначених етапів, кожен з яких має свою мету:

1. **Діагностика та відбір:**

- *суть* – аудит бізнес-процесів для виявлення потенційних кандидатів на автоматизацію;
- *критерії* – обираються рутинні, масові завдання, що базуються на чітких алгоритмах (правилах) і виконуються вручну. Саме тут ризик помилок персоналу є найвищим, тому цей етап є фундаментом успішного проєкту.

2. ***Проєктування:***

- *суть* – розробка архітектури майбутнього рішення;
- *дія* – детальний опис кожного кроку, який виконуватиме робот, створення логічної схеми процесу.

3. ***Технічна реалізація:***

- *суть* – написання коду та налаштування бота в середовищі RPA;
- *дія* – програмування алгоритмів для взаємодії робота з різними додатками та коректної обробки даних.

4. ***Валідація (імплементація системи):***

- *суть* – перевірка працездатності;
- *дія* – виявлення багів, тестування точності виконання операцій та фінальна оптимізація перед запуском.

Фаза розробки є критичною точкою переходу від теорії до практики. На цьому етапі відбувається конфігурація робота для забезпечення його безшовної взаємодії з корпоративним програмним забезпеченням. Розробники інтегрують

бота, використовуючи функціонал RPA-платформи, щоб гарантувати точність зчитування та запису інформації. Якість виконання цього етапу визначає стабільність подальшої роботи системи.

Запуск робота в експлуатацію не є фінальною крапкою, оскільки RPA функціонує за принципом безперервного покращення:

- *моніторинг* – регулярний контроль продуктивності дозволяє виявляти вузькі місця.
- *адаптація* – при зміні бізнес-логіки або інтерфейсів програм конфігурація робота оперативно оновлюється.
- *масштабування* – успішні кейси розширюються на інші відділи.

Тому RPA слід розглядати не просто як технічний інструмент, а як комплексну бізнес-стратегію. Її ефективність залежить від грамотного попереднього аналізу, правильного вибору інструментарію та готовності до постійної оптимізації процесів.

Ще одним інструментом, що виступає фундаментом довіри та цілісності інформації в екосистемі інтелектуального аудиту, є технологія блокчейн (Blockchain). Вона трансформує саму архітектуру обліку, перетворюючи її з ізольованої корпоративної функції на прозорий механізм взаємодії.

«***Блокчейн (blockchain)*** – це розподілений реєстр із підтвердженими блоками, організованими в послідовний ланцюжок лише для дописування, з використанням криптографічних зв'язків.»

Водночас у національному законодавчому полі, зокрема у Законі України «Про віртуальні активи», ця концепція розглядається ширше – через поняття технології розподіленого реєстру ***(Distributed Ledger Technology – DLT).*** Це технологія, яка забезпечує тотожність інформації у розподіленому реєстрі шляхом її синхронізації та перевірки (валідації) всіма учасниками мережі.

У прикладному сенсі для аудитора блокчейн – це децентралізована база даних, яка зберігає записи про всі транзакції в зашифрованому вигляді одночасно у всіх учасників мережі. Ключовою особливістю є незмінність даних: запис, одного разу внесений у блокчейн, неможливо видалити чи непомітно

відредагувати заднім числом, що створює ідеальне середовище для формування беззаперечного аудиторського сліду. Це вирішує одну з головних проблем, окреслених у контексті якості даних – проблему достовірності первинної інформації. В умовах використання блокчейну аудитор переходить від перевірки точності записів до перевірки сутності транзакцій, оскільки математична верифікація цілісності даних вже гарантована самим алгоритмом мережі.

Архітектура впливу блокчейну на обліково-аудиторську систему розглядається через концепцію «потрійного запису». Головна відмінність від традиційного подвійного запису, де кожна компанія веде свою окрему, ізольовану бухгалтерську книгу, полягає в тому, що потрійний запис передбачає створення третього, криптографічно захищеного запису в спільному реєстрі (блокчейні).

Цей спільний запис стає «єдиним джерелом істини» для всіх учасників транзакції. Для аудитора це означає можливість миттєво верифікувати транзакцію через доступ до цього реєстру, не витрачаючи час на традиційні процедури звірки даних між різними контрагентами (рис. 12.8).

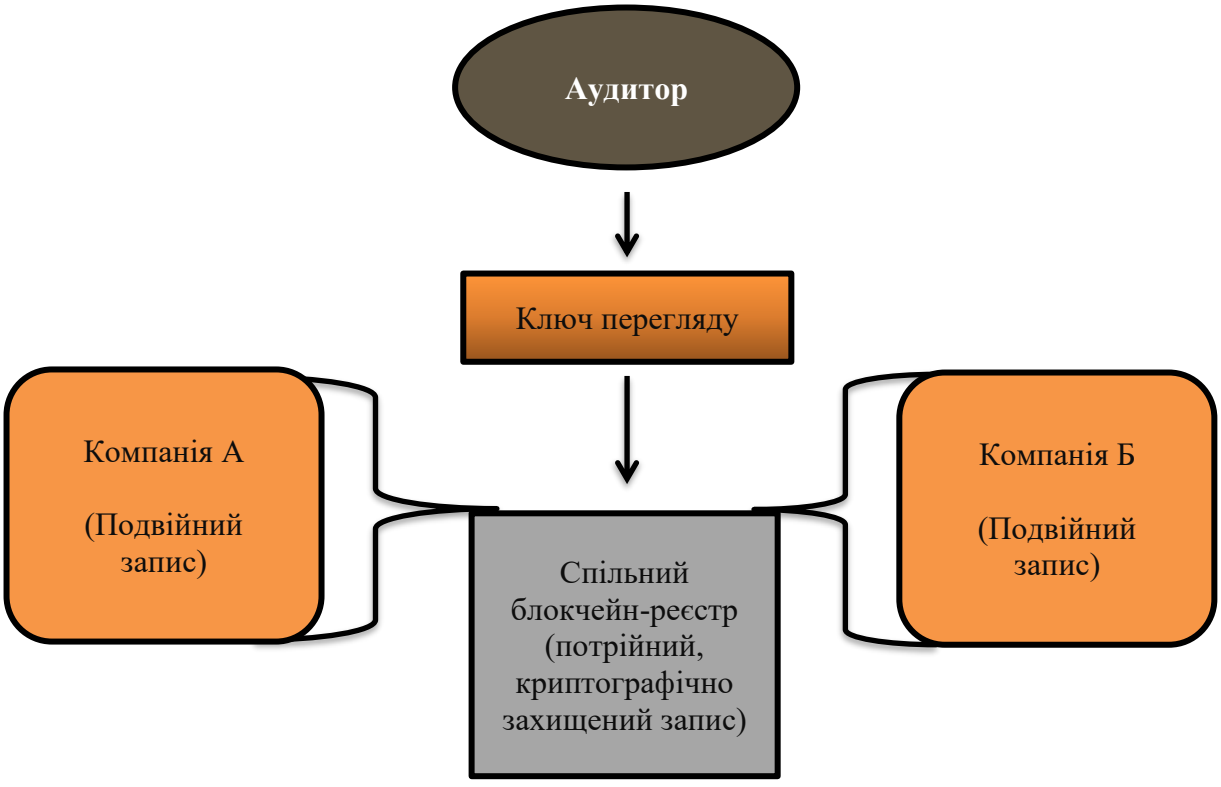


Рис. 12.8. Концепція потрійного запису в аудиті на базі блокчейну

Невіддільним елементом автоматизації на базі блокчейну є смарт-контракти. Відповідно до ДСТУ ISO 22739:2023, «***смарт-контракт (smart contract)*** – це комп'ютерна програма, що зберігається в системі розподіленого реєстру, результат виконання якої записується до розподіленого реєстру.»

У практиці аудиту це поняття трактується як автоматично виконувані угоди, де умови договору (наприклад, терміни оплати, штрафні санкції, перехід права власності) записані безпосередньо в рядки коду. По суті, це програмний код, записаний у блокчейн, який діє за логікою «Якщо... То...» (IF... THEN...).

У контексті аудиту та бухгалтерського обліку смарт-контракти виступають не просто як інструмент розрахунків, а як засіб гарантованого виконання контрольних процедур.

Практична реалізація смарт-контрактів в облікових системах часто відбувається у синергії з технологіями Інтернету речей (IoT), що дозволяє зв'язати цифровий реєстр із фізичним рухом активів.

«Інтернет речей (IoT) – це інфраструктура взаємопов'язаних сутностей, людей, систем та інформаційних ресурсів разом із послугами, які обробляють і реагують на інформацію з фізичного та віртуального світу.»

Наприклад, смарт-контракт може бути запрограмований на автоматичне перерахування оплати постачальнику виключно в той момент, коли IoT-датчик на складі підтвердить фізичне надходження товару.

Широке впровадження цієї технології створює нові виклики для професії, зміщуючи акценти в аудиторських процедурах. Оскільки умови угоди жорстко зафіксовані в програмному коді, ризик невиконання зобов'язань через людський фактор або шахрайство мінімізується, проте виникає потреба в технічному аудиті самого алгоритму.

Аудитор майбутнього повинен буде верифікувати, чи коректно програмний код відображає юридичні та комерційні домовленості сторін, а також оцінювати надійність архітектури смарт-контракту на предмет відсутності вразливостей та помилок.

Порівняльна характеристика впливу блокчейну на аудиторські процедури наведена в таблиці 12.3.

Таблиця 12.3

Трансформація аудиторських процедур під впливом технології

Критерій порівняння	Традиційна модель аудиту	Аудит у середовищі блокчейн
Джерело даних	Локальні ERP-системи клієнта, які можуть бути модифіковані адміністраторами	Розподілений реєстр, захищений криптографією, який неможливо змінити одноосібно
Процедура звірки	Трудомістка ручна або напівавтоматична звірка між контрагентами	Миттєва верифікація через спільний доступ до єдиного запису (відсутність розбіжностей)
Підтвердження	Вибіркова відправка листів-підтверджень дебіторам/кредиторам	Математична валідація всієї генеральної сукупності транзакцій
Часовий лаг	Ретроспективний аналіз (погляд у минуле)	Безперервний аудит у момент транзакції
Роль аудитора	Пошук помилок та невідповідностей у документах	Аудит смарт-контрактів, оцінка кіберризиків та архітектури системи

Технологія розподіленого реєстру фактично нівелює потребу в традиційних процедурах звірки розрахунків та запитах до третіх осіб, оскільки довіра до даних забезпечується математичними алгоритмами консенсусу, а не авторитетом контрагента. Таке середовище створює «єдину версію правди», яка є необхідною передумовою для ефективного застосування штучного інтелекту, адже навіть найдосконаліші аналітичні моделі залежать від якості та цілісності вхідної інформації.

Найвищий рівень інтелектуальної автоматизації досягається при поєднанні розглянутих технологій. Блокчейн забезпечує якість та незмінність даних, а штучний інтелект використовує ці верифіковані дані для побудови високоточних прогнозів та виявлення аномалій.

Схематично взаємодію інструментів у системі автоматизованого аудиту можна зобразити наступним чином (рис. 12.9):

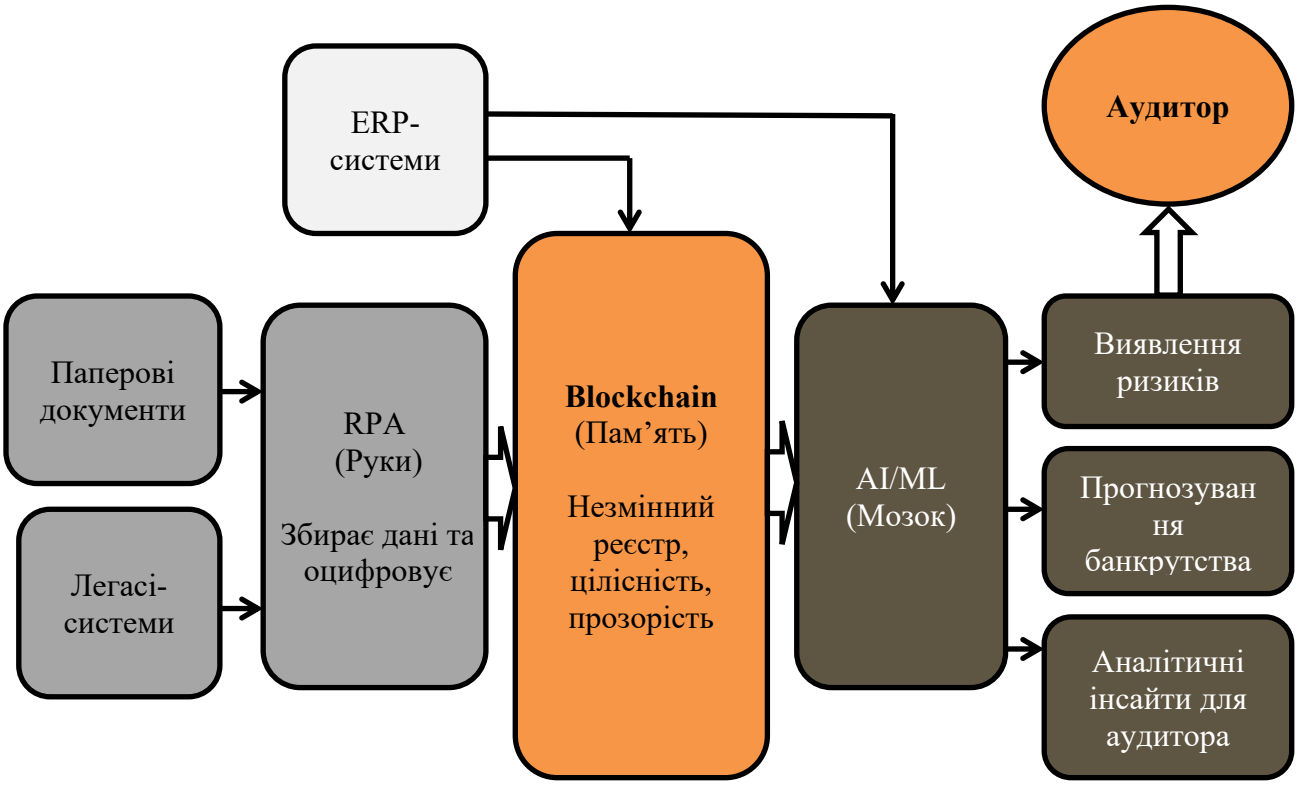


Рис. 12.9. Екосистема інтелектуальної автоматизації аудиту

Наведена архітектура демонструє концептуальну модель взаємодії технологій, однак для її практичної реалізації необхідно розуміти функціональне призначення кожного інструменту в розрізі конкретних стадій перевірки. Якщо схема ілюструє загальний потік даних від джерела до аудитора, то прикладна ефективність цієї екосистеми розкривається через синергію компонентів: «руки» (RPA) забезпечують точність збору інформації, «пам'ять» (Blockchain) гарантує її незмінність, а «мозок» (AI/ML) здійснює глибинний аналіз.

Максимальна ефективність інструментарію інтелектуальної автоматизації досягається не через ізольоване використання окремих технологій, а через їх комбінацію на різних етапах аудиту. Інтеграція RPA, машинного навчання, NLP та блокчейну дозволяє перекрити слабкі сторони одних інструментів перевагами інших, забезпечуючи повне покриття ризиків (табл. 12.4).

Таблиця 12.4

Матриця інтеграції інструментів інтелектуальної автоматизації в аудиторські процедури

Аудиторська процедура	Інструмент (Технологія)	Практичне застосування
Планування та оцінка ризиків	ML (Машинне навчання)	Кластеризація контрагентів для виявлення груп підвищеного ризику; аналіз профілів користувачів ERP для виявлення конфлікту інтересів
Тестування засобів контролю	Process Mining	Візуалізація реальних потоків документообігу для виявлення відхилень від затверджених регламентів
Перевірка договірних зобов'язань	NLP (Обробка природної мови)	Автоматичне сканування тисяч контрактів для виявлення нестандартних умов (наприклад, прихованих штрафів або неринкових термінів оплати)
Аудит доходів та витрат	ML / Прогнозна аналітика	Побудова регресійних моделей для порівняння фактичної виручки з прогнозованою (на основі нефінансових даних: трафіку, відвантажень, людино-годин)
Звірка розрахунків (Reconciliation)	RPA (Роботизація)	Автоматичне вивантаження даних із «легасі-систем», клієнт-банків та порталів контрагентів із подальшим «matching» (зіставленням) позицій
Інвентаризація та підтвердження активів	Computer Vision / IoT / Blockchain	Використання дронів для підрахунку запасів; автоматичне підтвердження права власності через записи в розподіленому реєстрі
Процедури щодо безперервності діяльності	ML (Нейромережі)	Прогнозування ймовірності банкрутства на 12 місяців вперед на основі мультифакторних моделей (фінансові показники разом із новинами та судовими реєстрами)
Формування аудиторської документації	GenAI (Генеративний ШІ)	Автоматичне створення чернеток аудиторських запитів, опис виявлених недоліків та формування попереднього тексту аудиторського звіту

Сучасний інструментарій трансформує аудит з рутинного процесу перевірки минулого на високотехнологічну процедуру гарантування довіри в реальному часі. Імплементація наведених рішень є ключовим кроком до переходу на модель інтелектуального аудиту, де швидкість та точність перевірки забезпечуються алгоритмами, а стратегічне бачення залишається прерогативою професійного аудитора.

12.3. Ризики та етика інтеграції ШІ

Інтеграція систем штучного інтелекту в аудиторську діяльність створює нові види ризиків, які підлягають ідентифікації та оцінці згідно з вимогами МСА 315 «Ідентифікація та оцінка ризиків суттєвого викривлення». Стандарт вимагає від аудитора розуміння IT-середовища клієнта та ризиків, що виникають унаслідок застосування автоматизованих інструментів. Ризики, що виникають при використанні інтелектуальних алгоритмів, не є однорідними та класифікуються за джерелами виникнення, етапами аудиту та характером впливу на кінцевий результат.

Для цілей побудови системи контролю якості ризики класифікуються за чотирма групами: технологічні, інформаційної безпеки, етичні та правові (рис. 12.10).

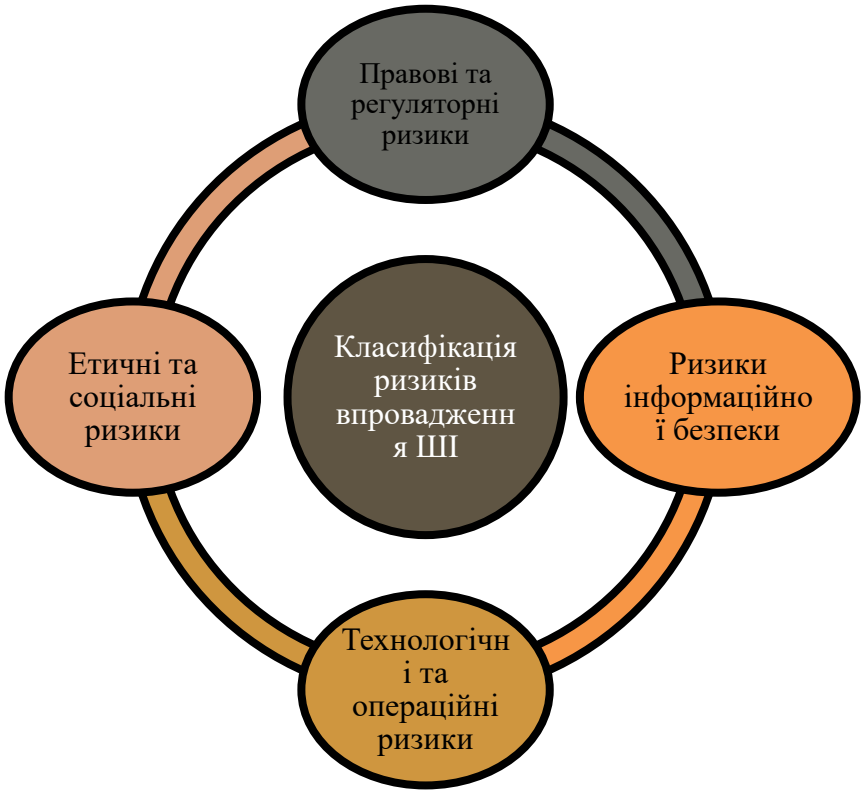


Рис. 12.10. Класифікація ризиків впровадження ШІ

Наведена класифікація дозволяє аудитору комплексно оцінити середовище контролю. Розглянемо кожну групу ризиків детальніше.

1. Технологічні та операційні ризики. Ця група охоплює технічні аспекти функціонування алгоритмів. Фундаментальною проблемою є залежність ефективності ШІ від якості даних: недостовірні або неповні вхідні дані неминуче призводять до помилкових результатів аудиту. Окремим специфічним викликом є феномен «галюцинацій» штучного інтелекту, коли генеративні моделі створюють переконливі, але фактично неправдиві дані, що вимагає впровадження додаткових процедур верифікації. Також до цієї групи належать ризики несумісності програмного забезпечення та форматів даних, що ускладнює інтеграцію автоматизованих рішень у наявну інфраструктуру підприємства.

2. Ризики інформаційної безпеки. Акумуляція великих масивів даних для навчання моделей робить аудиторські системи потенційною мішенню для кібератак. Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору».

Окремим викликом є використання хмарних сервісів ШІ. Аудитор зобов'язаний забезпечити дотримання Закону України ***«Про захист персональних даних».*** «Згідно зі статтею 2 цього Закону, обробка персональних даних включає будь-яку дію (збирання, накопичення, зберігання, використання), у тому числі з використанням автоматизованих систем.» Порушення умов конфіденційності при передачі даних третім сторонам (провайдерам ШІ) несе прямі правові ризики для аудиторської фірми.

3. Етичні та соціальні ризики. Ця категорія стосується впливу алгоритмів на справедливість та об'єктивність рішень. Ключовою проблемою є алгоритмічна упередженість, коли система відтворює або посилює соціальні стереотипи та дискримінаційні патерни, приховані в історичних даних. Це тісно пов'язано з проблемою «чорної скриньки» (алгоритмічної непрозорості), коли логіка прийняття рішення машиною залишається незрозумілою навіть для розробників, що ускладнює пояснення результатів аудиту та створює прямий

конфлікт із Міжнародним кодексом етики професійних бухгалтерів (виданим IESBA), дотримання якого є обов'язковим в Україні. Принцип професійної компетентності вимагає від аудитора розуміння інструментів, що використовуються. Якщо аудитор не може пояснити логіку, за якою ШІ виявив (або не виявив) ризик, такі результати не можуть вважатися надійними аудиторськими доказами в розумінні МСА 500 «Аудиторські докази», оскільки їх джерело не піддається верифікації.

4. Правові та регуляторні ризики. Автоматизація процесів створює «сірі зони» у сфері відповідальності. Виникають складнощі з визначенням суб'єкта відповідальності за помилкові рішення, прийняті алгоритмом: чи несе відповідальність розробник, аудитор-користувач або сама система. Додатковим викликом є необхідність забезпечення відповідності роботи алгоритмів жорстким нормативним вимогам, зокрема щодо захисту персональних даних та дотримання процедурних стандартів.

Ефективність будь-якої моделі ШІ прямо корелює з якістю інформації, на якій вона навчалася або яку вона обробляє. На рис. 12.11 відображено принцип дії «GIGO» (Garbage In, Garbage Out – «сміття на вході, сміття на виході») в професійному середовищі.

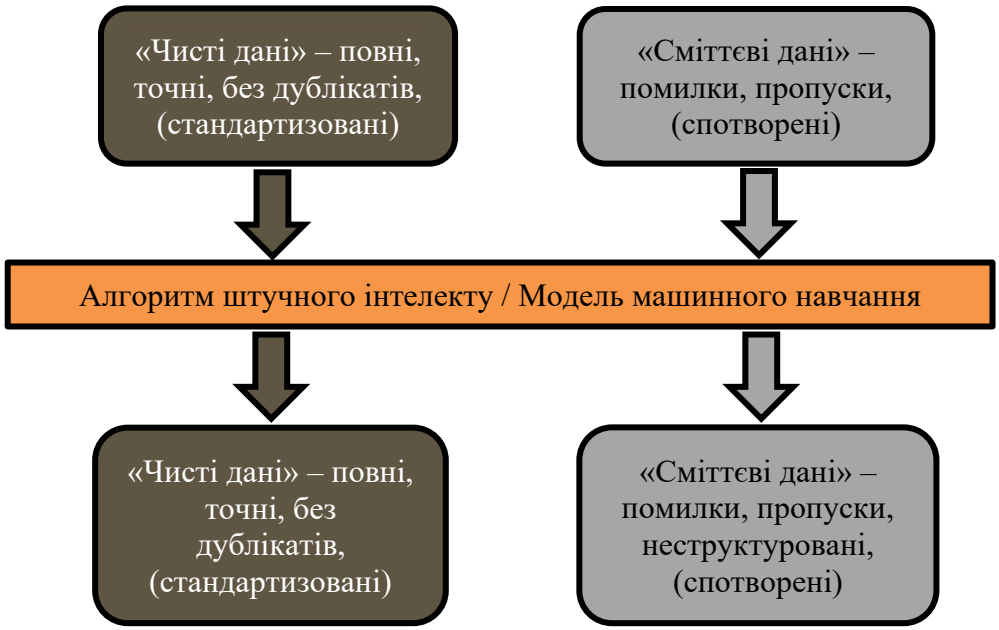


Рис. 12.11. Принцип «GIGO» (Garbage In, Garbage Out) у професійному середовищі

Отже, якщо вхідні дані є неточними, неповними або спотвореними, навіть найдосконаліший алгоритм згенерує помилкові висновки, що в контексті аудиту може призвести до невиявлення суттєвих викривлень у фінансовій звітності або надання хибних рекомендацій.

Саме тому якість інформації має найважливіше значення для забезпечення коректних результатів аудиторської перевірки. Економічна інформація, що підлягає аналізу, часто є гетерогенною. Вона надходить з різних джерел: ERP-систем клієнта, банківських виписок, зовнішніх реєстрів, електронних листів та сканованих документів.

Основні технічні проблеми, що впливають на якість даних:

- *несумісність форматів* (різні підрозділи компанії або різні контрагенти можуть використовувати відмінні стандарти кодування даних, що ускладнює їх агрегацію та порівняння);
- *фрагментарність та неповнота* (відсутність частини записів або метаданих унеможливлює коректну роботу алгоритмів кластеризації та виявлення аномалій);
- *втрата цілісності* (під час експорту, трансформації та завантаження даних (процес ETL) існує ризик технічних збоїв, що призводять до втрати частини транзакцій).

Окремим, вкрай небезпечним видом ризику є цілеспрямована маніпуляція даними, відома як «отруєння даних». Це вид кібератаки, при якій зловмисники навмисно вносять спотворення у навчальну вибірку даних на етапі тренування моделі ШІ.

Мета такої атаки – змусити алгоритм засвоїти неправильні патерни.

Приклад. У вибірку транзакцій, що маркуються як «легітимні», внести серію шахрайських операцій з певними ознаками, система в майбутньому буде ігнорувати подібні зловживання, вважаючи їх нормою. Це створює «сліпі зони» в системі внутрішнього контролю, які можуть експлуатуватися для фінансових махінацій. Аудитор повинен враховувати цей ризик і не покладатися виключно

на результати автоматизованої перевірки без верифікації цілісності вхідних баз даних.

У таблиці 12.5 узагальнено ключові виклики, пов'язані з даними, та методи їх контролю в аудиторській практиці.

Таблиця 12.5

Ключові ризики та заходи їх мінімізації та контролю.

Тип ризику	Характеристика проблеми	Заходи мінімізації та контролю
Неповнота даних	Відсутність критично важливих полів або записів, що унеможливлює коректний аналіз	- впровадження автоматизованих процедур валідації вхідних даних; - використання стандартизованих форматів (наприклад, SAF-T)
«Отруєння даних»	Навмисне внесення спотворень у навчальні вибірки для обману алгоритмів	- регулярний аудит навчальних вибірок; - захист каналів передачі даних; - використання методів виявлення аномалій у тренувальних сетах
«Галюцинації»	Генерація системою ШІ недостовірних фактів, які виглядають переконливо	- перехресна перевірка людиною; - порівняння результатів декількох моделей; - обмеження використання ШІ для розрахункових задач
Історична упередженість	Дані минулих періодів містять сліди дискримінаційних рішень або застарілих практик	- попередня підготовка даних для очищення від упереджень; - тестування алгоритмів на чутливість до змінних
Застарілість даних	Моделі навчаються на даних, що не відповідають поточним економічним умовам	- забезпечення безперервного потоку оновлення даних; - моніторинг актуальності моделей
Неповнота даних	Відсутність критично важливих полів або записів, що унеможливлює коректний аналіз	- впровадження автоматизованих процедур валідації вхідних даних; - використання стандартизованих форматів

Ще одним критичним аспектом інтеграції штучного інтелекту є етична складова, яка часто недооцінюється порівняно з технічними характеристиками. В аудиторській практиці та фінансовому контролі існує небезпечна ілюзія, що математичні алгоритми є абсолютно об'єктивними та неупередженими.

Згідно з положеннями пункту 12 МСА 540 ***«Аудит облікових оцінок та розкриття пов'язаної з ними інформації»***, під упередженістю управлінського персоналу (management bias) слід розуміти «відсутність нейтральності з боку керівництва суб'єкта господарювання під час підготовки звітності.»

Як свідчить практика, системи ШІ здатні не лише відтворювати, а й масштабувати людські упередження, приховані в історичних даних, що виявляється у виникненні алгоритмічної упередженості.

Алгоритмічна упередженість – це систематична помилка в роботі комп'ютерної системи, яка призводить до несправедливих результатів, надання необґрунтованих переваг одним групам або дискримінації інших.

Основні джерела упередженості можна розділити на три категорії:

1. Історична упередженість. Якщо модель навчається на даних за минулі періоди, де існували певні дискримінаційні практики, ШІ сприйме ці патерни як правильну норму поведінки.

2. Репрезентативна упередженість. Виникає, коли навчальна вибірка не повністю відображає генеральну сукупність.

3. Упередженість вимірювання. Пов'язана з вибором некоректних змінних-індикаторів. Алгоритм може використовувати нейтральні на перший погляд параметри, які фактично корелюють з факторами ризику, створюючи ефект дискримінації за географічною ознакою.

Для візуалізації цього процесу доцільно розглянути схему циклічного посилення упередженості (рис. 12.12).

Поряд з упередженістю, ключовим етичним викликом є непрозорість алгоритмів, відома як проблема «чорної скриньки». Сучасні методи глибокого навчання (Deep Learning) створюють настільки складні моделі, що простежити логічний шлях від вхідних даних до конкретного рішення стає неможливим навіть для розробників.

В аудиті це створює конфлікт із професійними стандартами, які вимагають наявності достатніх та прийнятних аудиторських доказів. Якщо ШІ вказує на високий ризик суттєвого викривлення, але аудитор не може пояснити чому (які саме фактори вплинули на цей висновок), такий результат не може бути повноцінною підставою для аудиторського висновку.

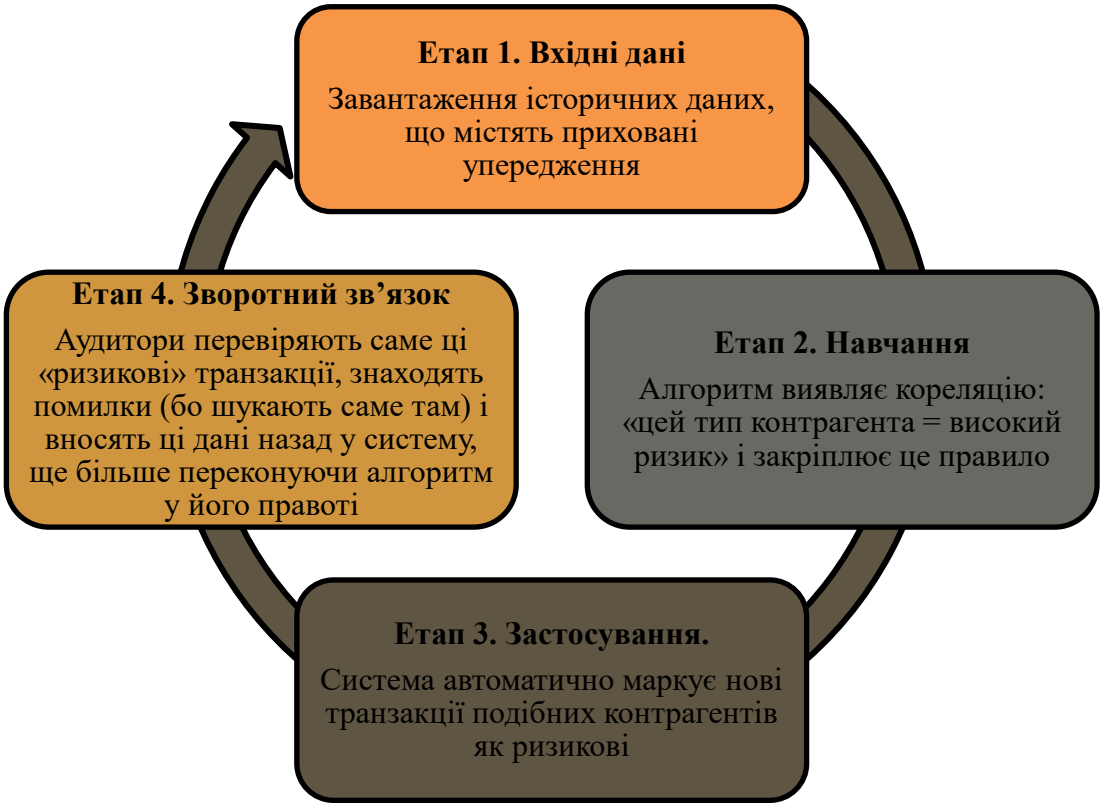


Рис. 12.12. Механізм формування та посилення алгоритмічної упередженості в інтелектуальних системах

Виділяють три рівні непрозорості, які повинен враховувати фахівець (табл. 12.6).

Таблиця 12.6

Рівні алгоритмічної непрозорості в аудиторських системах

Рівень непрозорості	Характеристика	Ризики для аудитора
Технічна непрозорість	Складність математичної моделі (наприклад, нейромережі з мільйонами параметрів), яку неможливо інтерпретувати людині.	Неможливість пояснити клієнту або регулятору причини конкретних висновків системи.
Процедурна непрозорість	Відсутність інформації про те, чи було рішення прийнято автоматично, чи за участю людини.	Розмивання відповідальності. Ризик, що аудитор сліпо підтвердив рішення машини без перевірки.
Комерційна непрозорість	Закритість коду комерційного ПЗ (комерційна таємниця розробника-вендора).	Неможливість провести незалежну валідацію алгоритму та переконатися у відсутності вразливостей.

Наведені рівні непрозорості відображають зворотну залежність між складністю структури моделі та прозорістю її логічних рішень. Це створює ризик

неможливості обґрунтування аудиторської думки перед замовником або регулятором. Для вирішення цієї проблеми необхідне застосування методів «пояснюваного штучного інтелекту» (Explainable AI – XAI), які надають зрозумілу інтерпретацію отриманих автоматизованих результатів.

Explainable AI – комплекс інструментів, процесів та методів, що забезпечують прозорість алгоритмічних рішень, дозволяючи користувачам усвідомлювати логіку отриманих результатів і формувати довіру до системи.

Завдяки інтерпретації роботи ШІ розробники можуть контролювати справність системи, забезпечувати комплаєнс (відповідність нормам) та отримують інструменти для налагодження чи перегляду логіки моделі (рис. 12.13).

Для ефективного використання методів XAI компаніям необхідно зосередитися на трьох базових принципах:

1. Забезпечення точності. Щоб гарантувати надійність прогнозів у щоденній роботі, результати роботи моделей порівнюють із вихідними навчальними даними. Популярним методом тут виступає LIME, що пояснює принципи передбачень моделі.

2. Технічна простежуваність. Цей принцип реалізується через встановлення чітких меж для правил і функцій системи. Для цього часто використовують метод DeepLIFT, який демонструє взаємозв'язки між нейронами, порівнюючи їхню активацію з еталонними показниками.

3. Інтерпретація для користувачів. На відміну від попередніх технічних аспектів, цей пункт стосується людей. Він вимагає навчання співробітників розумінню мотивації рішень ШІ. Це критично важливо для того, щоб користувачі довіряли висновкам, згенерованим системою.

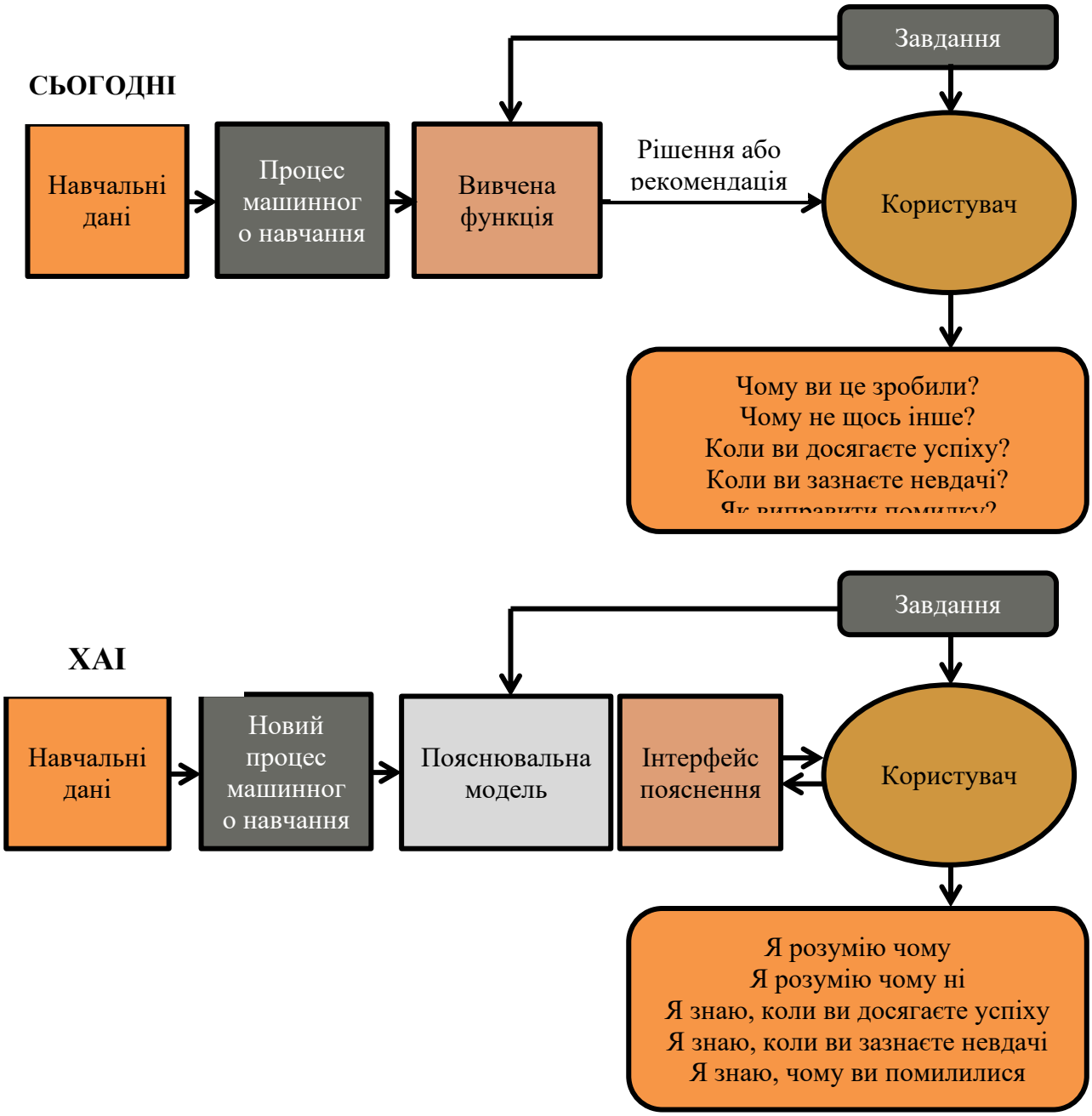


Рис. 12.13. Концептуальна модель переходу від «чорної скриньки» до пояснюваного штучного інтелекту

Автоматизація прийняття рішень несе ризики для соціальної справедливості та автономії людини. Існує загроза так званої ***«автоматизації упередженості» (automation bias)*** – психологічного феномену, коли люди схильні довіряти підказкам машини більше, ніж власному судженню або фактам, навіть коли машина помиляється.

Крім того, висока автоматизація створює ризик нівелювання відповідальності. У разі помилки алгоритму виникає невизначеність щодо винної сторони (розробник, користувач чи налаштування системи). Згідно з

професійними стандартами, відповідальність за підсумковий висновок не може бути делегована технології, тому критично важливим залишається збереження контролю з боку людини, яка верифікує критичні рішення системи. Остаточне рішення, особливо в питаннях, що стосуються етичних суджень, оціночних значень та кваліфікації шахрайства, завжди має залишатися за професійним аудитором.

Професійна етика бухгалтера та аудитора в цифрову епоху трансформується. До традиційних принципів чесності та об'єктивності додається вимога цифрової компетентності – здатності розуміти обмеження технологій та етично їх використовувати.

Для мінімізації зазначених ризиків можна виділити ряд вимог до етичного використання ШІ в аналізі даних. Дотримання цих принципів є обов'язковим для забезпечення довіри до аудиторських процедур (табл. 12.7).

Таблиця 12.7

Принципи етичного використання штучного інтелекту в аналізі даних

Принцип	Характеристика та вимоги до реалізації
Прозорість та відповідальність	Процеси та рішення ШІ мають бути доступними й зрозумілими. Розробники та користувачі (аудитори) повинні забезпечити підзвітність роботи систем. Це досягається через регулярний аудит алгоритмів, чітку політику контролю та інформування користувачів про можливості й обмеження системи
Справедливість та недискримінація	Системи мають ставитися до всіх об'єктів аналізу неупереджено. Це вимагає використання репрезентативних навчальних даних, проведення тестувань на упередженість та врахування різноманітних поглядів при розробці моделей, щоб уникнути посилення нерівності
Збалансований підхід до даних та алгоритмів	Збір та обробка даних повинні здійснюватися прозоро, з дотриманням інформованої згоди та надійним управлінням конфіденційністю. Алгоритми мають розроблятися відповідно до етичних норм, з постійним моніторингом їхнього впливу та адаптацією до нових викликів

Важливо розуміти, що ШІ не здатен приймати складні морально-етичні рішення. Тому відповідальність за наслідки використання автоматизованих систем завжди залишається за людиною. Етичні практики повинні бути інтегровані на всіх етапах – від розробки моделі до її впровадження та моніторингу. Розвиток етичної екосистеми ШІ є не просто технологічним

завданням, а необхідною умовою суспільного добробуту та професійної доброчесності.

Одним з найважливіших шляхів безпечності інтеграції ШІ в аудиторські процедури є створення комплексної системи управління ризиками штучного інтелекту. Ця система має базуватися на регуляторній політиці та внутрішніх стандартах якості аудиторської фірми.

Управління ризиками ШІ – це не одноразова дія, а циклічний процес. Він базується на класичному підході, що включає п’ять послідовних етапів (рис. 12.14).

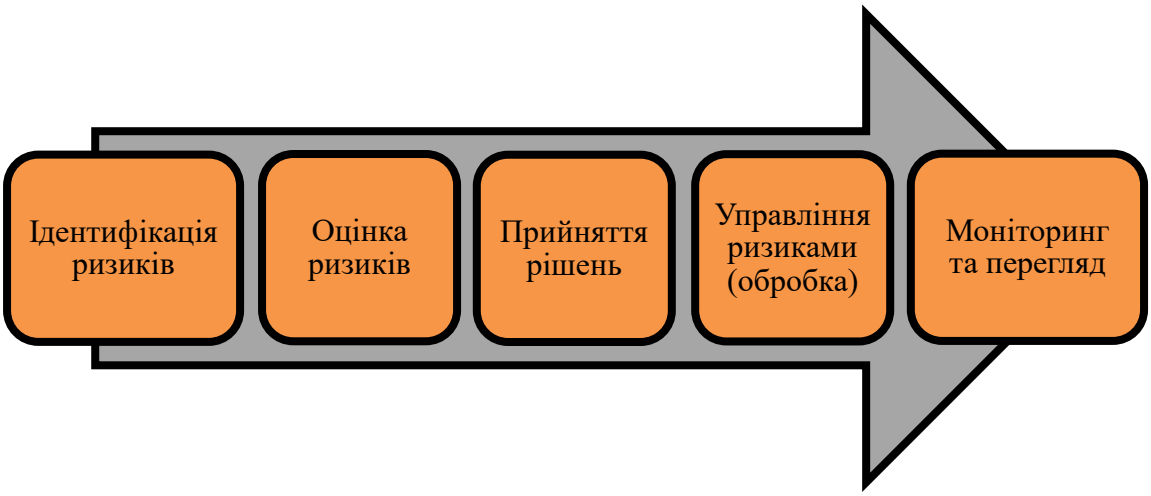


Рис. 12.14. Цикл управління ризиками штучного інтелекту

1. ***Ідентифікація ризиків.*** Це початковий і критично важливий етап, де виявляються потенційні загрози, пов’язані з ШІ. Сюди входить аналіз політик, алгоритмів, специфіки використання даних та оцінка впливу на користувачів.

2. ***Оцінка ризиків.*** Після ідентифікації кожен ризик оцінюється за двома параметрами: потенційна сила впливу (наслідки) та ймовірність виникнення. На цьому етапі застосовують аналіз чутливості, тестування на упередженість та моделювання сценаріїв.

3. ***Прийняття рішень.*** На основі оцінки менеджмент вирішує, як краще управляти виявленими ризиками (вдосконалення процесів, модифікація баз даних, зміна алгоритмів або відмова від використання конкретного інструменту).

4. Управління ризиками (обробка). Безпосереднє виконання дій: впровадження контрольних заходів, навчання персоналу, внесення змін у дизайн систем та архітектуру безпеки.

5. Моніторинг та перегляд. Оскільки алгоритми та середовище змінюються, ризики слід постійно моніторити. Це включає регулярний аудит моделей, відстеження інцидентів та збір зворотного зв'язку від аудиторів-практиків.

Зазначені процедури потребують циклічного відтворення протягом усього життєвого циклу ШІ-системи, адже з часом спостерігається природна деградація результативності моделей та з'являються нові технологічні виклики.

Для ефективної протидії загрозам необхідна реалізація заходів за трьома векторами: нормативно-правовим, технічним та організаційним.

1. ***Нормативно-правові заходи:***
   - *регуляторна політика* (чітке визначення правил використання ШІ в аудиторській діяльності на рівні стандартів фірми та державного регулювання);
   - *законодавче регулювання* (дотримання норм, які регулюють розробку та використання ШІ);
   - *міжнародне співробітництво* (врахування міжнародних норм і стандартів безпеки).
2. ***Технічні заходи:***
   - *розробка безпечних систем;*
   - *обмеження доступу* (технічні бар'єри для доступу ШІ до чутливих даних (персональні дані, комерційна таємниця) для запобігання їх витоку;
   - *аудит алгоритмів* (створення спеціальних інструментів для перевірки логіки та «знань» прикладних систем ШІ).
3. ***Організаційні заходи:***
   - *модель управління* (впровадження чіткої ієрархії відповідальності за ризики ШІ);
   - *системне підвищення цифрової грамотності персоналу* (для розуміння потенційних загроз);

- *спеціалізований контроль* (призначення відповідальних осіб або створення підрозділів, які здійснюють моніторинг та реагування).

Лише комплексне поєднання технічного захисту, етичних принципів та організаційного контролю дозволить перетворити штучний інтелект з джерела ризику на надійний інструмент аудитора.

12.4. Контрольні питання для самоперевірки

11. У чому полягає фундаментальна відмінність між традиційним аудитом на основі вибірки та аудитом з використанням ШІ?

12. Як змінюється роль аудитора в умовах використання інтелектуальних технологій?

13. Розкрийте сутність процесу ETL при підготовці економічної інформації для аналізу.

14. Назвіть та охарактеризуйте чотири рівні аналітики даних в аудиті згідно з моделлю Gartner.

15. З яких етапів складається життєвий цикл моделі машинного навчання в аудиті?

16. Наведіть класифікацію ризиків впровадження ШІ в аудиторські процедури.

17. У чому полягає принцип «GIGO» (Garbage In, Garbage Out) та як він впливає на результати аудиту?

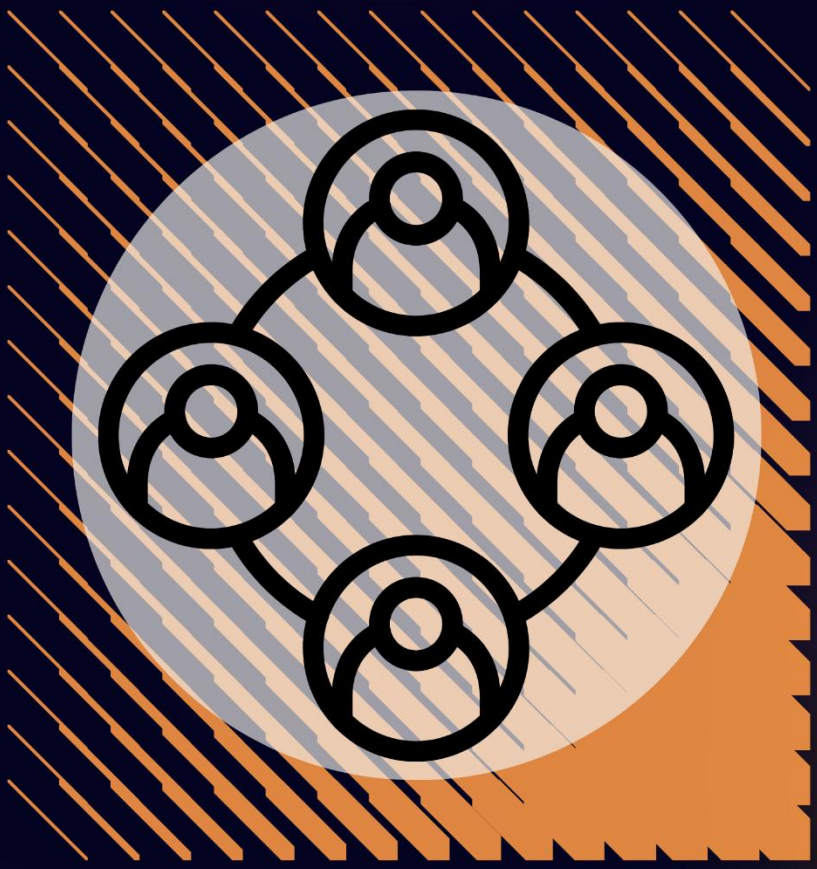
18. У чому сутність концепції «потрійного запису» на базі технології блокчейн?

19. Охарактеризуйте явище алгоритмічної упередженості та основні джерела її виникнення.

20. У чому полягає проблема «чорної скриньки» (алгоритмічної непрозорості) і чому вона є критичною для аудитора?

Розділ 13

Автори:
Аліна Жуковська
Оксана Бродовська



ЦИФРОВІ ТЕХНОЛОГІЇ ІНКЛЮЗИВНОГО АУДИТУ

РОЗДІЛ 13. ЦИФРОВІ ТЕХНОЛОГІЇ ІНКЛЮЗИВНОГО АУДИТУ

«Будую Україну для всіх і з усіма.»

Данило Скоропадський

13.1. Поняття інклюзивного аудиту та методика його проведення

Традиційні види аудиту спрямовані на перевірку правильності обліку, дотримання законодавства і внутрішніх регламентів, а також оцінювання економічної ефективності діяльності організації. Водночас навіть за високих показників фінансової дисципліни або операційної ефективності в організації можуть зберігатися бар’єри, нерівність можливостей або виключення окремих груп персоналу та стейкхолдерів із доступу до ресурсів, участі в процесах, комунікацій і професійного розвитку. Саме тому інклюзивний аудит (аудит інклюзивності) є необхідним доповненням до традиційних видів аудиту, оскільки він дозволяє виявити такі бар’єри, оцінити їх наслідки та сформувати рекомендації щодо їх усунення на рівні управлінських рішень, процесів і результатів.

Необхідність і важливість проведення інклюзивного аудиту полягає у тому, що саме він дає керівництву вимірювану відповідь на ключове управлінське питання: чи забезпечує організація однаково безпечні, доступні й справедливі умови взаємодії для персоналу, клієнтів, партнерів та інших стейкхолдерів. Фактично він виявляє бар’єри для їх повноцінної участі в діяльності організації. Невиявлені бар’єри трансформуються у приховані витрати й ризики: зниження залученості персоналу, ріст плинності кадрів,

конфліктність в колективі, падіння довіри стейкхолдерів, збільшення кількості скарг, погіршення репутації та ділового іміджу. Інклюзивний аудит забезпечує системне бачення бар'єрів, фіксує їхні причини та наслідки, а також пропонує пакет управлінських рішень щодо їх нівелювання або ліквідації, що дає змогу зберігати розумний баланс між прибутковістю, ефективністю та адаптацією діяльності до потреб людей.

Інклюзивний аудит – це комплексний інструмент діагностики, спрямований на оцінювання інклюзивності управлінських рішень, процесів і результатів діяльності організації з позиції рівності можливостей, недискримінації, доступності та залученості персоналу і зацікавлених сторін.

Інклюзивний аудит відрізняється від інших видів аудиту тим, що його предметом є не лише відповідність вимогам і правильність процедур, а вплив діяльності організації на рівність можливостей, доступ і участь різних груп персоналу та стейкхолдерів. Його унікальність полягає в орієнтації на бар'єри (виявлення конкретних точок виключення та причин їх виникнення) і в поєднанні оцінювання управлінських рішень, процесів і результатів в одній методичній логіці. Результатом інклюзивного аудиту є не лише висновок про стан інклюзивності, а пакет управлінських заходів з чіткими індикаторами контролю їх виконання та досягнутого ефекту.

Характерними рисами інклюзивного аудиту є:

1. ***Людиноцентричність і рівність можливостей.*** Полягає у врахуванні та діагностиці того, чи забезпечує організація рівний доступ і можливість участі для різних груп персоналу та стейкхолдерів у прийнятті управлінських рішень, в процесах й в розподілі результатів її діяльності;

2. ***Бар'єроорієнтований.*** Передбачає виявлення конкретних бар'єрів у рішеннях, процесах і результатах, встановлення того, де саме виникає обмеження доступу чи участі, кого воно стосується та в чому проявляється. Такий підхід обов'язково доповнюється визначенням причин і умов існування бар'єрів, а також оцінюванням їх наслідків для персоналу, стейкхолдерів і організації;

3. ***Комплексність.*** Проявляється у цілісному тривекторному проведенні

інклюзивного аудиту (аудит управлінських рішень, організаційних процесів та результатів діяльності). Комплексність дозволяє дотримуватися логіки «рішення → процес → результат» і визначати, на якому рівні закладено або відтворюється бар'єр, а отже – які управлінські зміни є необхідними для його усунення;

4. Доказовість. Забезпечується застосуванням критеріїв і системи індикаторів інклюзивності та використанням повної аудиторської інформації з різних джерел. Висновки формуються з урахуванням вимог до якості й придатності даних, що підвищує обґрунтованість оцінювання та можливість практичного застосування результатів аудиту;

5. Управлінська спрямованість. Полягає в розробці шляхів усунення виявлених бар'єрів. Результатом інклюзивного аудиту є не лише виявлення бар'єрів, ризиків і загроз, а й розробка конкретних рекомендацій щодо їх усунення із визначенням відповідальних виконавців і контрольних показників.

Тривекторна модель інклюзивного аудиту – це концептуальна модель, за якою інклюзивність в організації оцінюється у трьох взаємодоповнювальних векторах: інклюзивність управлінських рішень, інклюзивність процесів та інклюзивність результатів (рис. 13.1). Вона дає змогу комплексно діагностувати, де саме формуються або відтворюються бар'єри й нерівність можливостей, та пов'язати управлінські причини (рішення), механізми реалізації (процеси) і вимірювані наслідки (результати) в єдину логіку аудиторських висновків і рекомендацій.

Рис. 13.1. Тривекторна модель інклюзивного аудиту

Складові елементи тривекторної моделі інклюзивного аудиту:

1. Інклюзивний аудит управлінських рішень. Передбачає оцінювання процедур прийняття управлінських рішень з позиції їх інклюзивних, соціальних та управлінських наслідків для трудового колективу і зацікавлених сторін. В рамках цього вектору аудиту підлягає: участь працівників і стейкхолдерів у прийняття управлінських рішень; прозорість прийняття управлінських рішень; недискримінаційність та справедливість; соціальна відповідальність під час прийняття управлінських рішень;

2. Інклюзивний аудит процесів. Системна оцінка того, як організація вибудовує та реалізує управлінські і кадрові процеси через інклюзивність трудового колективу та масиву стейкхолдерів, інклюзивність робочих місць, реалізацію інклюзивних підходів до здійснення комунікації та участі, рівень інклюзивної культури, з метою виявлення бар'єрів та ризиків, що впливають на рівність можливостей і залученість працівників і стейкхолдерів. В рамках цього вектору аудиту підлягає: кадрова структура організації; інклюзивність робочих місць; комунікації та участь; інклюзивна культура та клімат;

3. Інклюзивний аудит результатів. Оцінювання фактичних, вимірюваних підсумків інклюзивності, які відображають, яким є реальний рівень безбар'єрності, універсального дизайну, рівності можливостей та залученості персоналу і стейкхолдерів. У межах цього вектора перевіряються не наміри та не регламенти, а підтверджені показниками наслідки: динаміка звернень і скарг, доступність каналів комунікації та сервісів, поширеність бар'єрів у взаємодії з організацією, індикатори участі й включеності, а також параметри психологічної безпеки та організаційного клімату. Результатом аудиту є узагальнена оцінка досягнутого рівня інклюзивності, визначення проблемних зон і формування доказової основи для управлінських рішень щодо усунення бар'єрів і подальшого моніторингу змін.

В рамках цього вектору аудиту підлягає: безбар'єрний простір; реалізація принципів «універсального дизайну»; соціально-відповідальна діяльність; реалізація принципів DEIB; інклюзивний розвиток організації.

Мета інклюзивного аудиту полягає у виявленні бар'єрів, що обмежують рівність можливостей, доступ і участь персоналу та стейкхолдерів у прийнятті управлінських рішень, внутрішньо-організаційних процесах та розподілі результатів діяльності організації, а також розробці конкретних шляхів їх усунення.

Поетапний алгоритм проведення інклюзивного аудиту включає (рис. 13.2):

Рис. 13.2. Поетапний алгоритм проведення інклюзивного аудиту

1. Етап 1. «Ідентифікація об'єкта інклюзивного аудиту», на якому визначаються вихідні периметри аудиту: що саме оцінюється (організація загалом або конкретний структурний підрозділ, функції чи процес) і потреби яких груп персоналу та стейкхолдерів включаються до оцінювання інклюзивності.

2. Етап 2. «Визначення критеріїв інклюзивності та системи індикаторів її оцінювання», на якому визначається за якими критеріями буде оцінюватися інклюзивність, та у закріпленні показників (індикаторів), які дозволяють зробити висновок про стан інклюзивності управлінських рішень, процесів і результатів.

В таблиці 13.1 деталізовано критерії та індикатори інклюзивного аудиту управлінських рішень, які засвідчують, наскільки активно працівники, клієнти, партнери та інші стейкхолдери приймають участь у їх виробленні.

Таблиця 13.1

Критерії оцінювання та індикатори інклюзивного аудиту управлінських рішень

Критерії	Індикатори
Участь працівників і стейкхолдерів у прийнятті управлінських рішень	1. Кількість і регулярність використання механізмів участі персоналу, клієнтів, партнерів та інших стейкхолдерів у прийнятті управлінських рішень (консультації, робочі групи, опитування) 2. Репрезентативність залучення (участь працівників із різних структурних підрозділів і рівнів посад, а не лише керівників) 3. Ефективність механізмів участі (% врахованих пропозицій персоналу, клієнтів, партнерів та іншіих стейкхолдерів)
Прозорість прийняття управлінських рішень	1. Регламентованість процедури ухвалення управлінських рішень (чітко визначена методика прийняття управлінських рішень) 2. Документоване обґрунтування (реальні дані, аргументи, альтернативи; можливість відстежити логіку рішення) 3. Комунікація та доступність інформації (своєчасне інформування; доступ до наказів, пояснень; зрозумілість рішення)
Недискримінаційність і справедливість управлінських рішень	1. Перевірка на непрямі дискримінаційні ефекти (чи «нейтральні» правила не створюють бар'єрів для окремих груп) 2. Рівність доступу до можливостей (навчання, премій, професійного розвитку, проєктів) 3. Наявність і дієвість механізму оскарження (канали подання скарг і апеляцій, чітко регламентовані строки розгляду, їх результативність)
Соціальна відповідальність під час прийняття управлінських рішень	1. Оцінка соціальних наслідків прийнятого рішення (вплив на зайнятість, добробут, безпеку, навантаження, психоемоційний стан) 2. Наявність заходів пом'якшення негативних наслідків прийнятого рішення (підтримка, перенавчання, адаптація, гнучкі рішення) 3. Довгостроковий ефект (динаміка плинності кадрів, залученості та довіри працівників і стейкхолдерів, наявність конфліктів і скарг після впровадження рішення)

У таблиці 13.2 відображено критерії та індикатори, що дозволяють перевірити,

як інклюзивні підходи реалізуються в повсякденних процедурах і комунікаціях, тобто на операційному рівні.

Таблиця 13.2

Критерії оцінювання та індикатори інклюзивного аудиту процесів

Критерії	Індикатори
Інклюзивний кадровий аудит	1. Наявність доступу до можливостей працівників, клієнтів, партнерів та інших стейкхолдерів (можливість навчатися, підвищувати кваліфікацію, брати участь у проєктах) без проявів дискримінації 2. Прозорі процедури HR (чітко регламентовані механізми відбору, оцінювання та просування персоналу) 3. Плинність кадрів і «вимивання» окремих груп працівників (плинність кадрів; звільнення за категоріями персоналу; виявлення зон ризику)
Інклюзивність робочих місць	1. Наявність процедури «розумного пристосування» (правила подання запиту, строки, відповідальні) 2. Виконання запитів на адаптацію (% виконаних та частково виконаних запитів; середній час реагування на запит) 3. Доступність середовища та інструментів (фізична, цифрова, інформаційна доступність)
Комунікації та участь	1. Ефективність системи комунікативного забезпечення (% працівників, які отримують і розуміють повідомлення) 2. Регулярність і безпечність зворотного зв'язку (наявність анонімних каналів зв'язку, частота звернень, довіра до них) 3. Ефективність зворотного зв'язку (% пропозицій, що були реально впровадженні і мали позитивні наслідки)
Інклюзивна культура та клімат	1. Психологічна безпека (індекс психологічної безпеки) 2. Реакція на випадки дискримінації (час реагування, дисциплінарні чи медіаційні заходи) 3. Залученість і довіра (лояльність, динаміка до/після змін)

У таблиці 13.3 відображено критерії та індикатори, що дозволяють оцінити фактичні, вимірювані результати інклюзивності, тобто її реальний вплив на персонал, клієнтів та інших стейкхолдерів, а також на якість управління і рівень довіри до організації.

Таблиця 13.3

Критерії оцінювання та індикатори інклюзивного аудиту результатів

Критерії	Індикатори
Безбар'єрний простір	1. Частка зон без фізичних бар'єрів (вхід, маршрути, санвузли, робочі, сервісні зони) 2. Наявність доступної навігації (зрозумілі позначення, контрастність зображення, дублювання інформації у різних формах) 3. Кількість «критичних бар'єрів» (червоних зон), що виявлені в процесі аудиту
Універсальний дизайн	1. Інтеграція принципів «універсального дизайну» у стандарти (чек-листи закупівель, ремонтних робіт, розробки документів і сервісів) 2. Рівень цифрової інклюзії (наявність та зручність внутрішньої інформаційної системи, сайту, а також форм документів, адаптованих під потреби різних користувачів) 3. Кількість індивідуальних програмах адаптації до потреб працівників, відвідувачів, стейкхолдерів (кількість «розумних пристосувань»)
Соціально відповідальна діяльність із вимірюваним ефектом	1. Наявність соціальних програм і заходів із чіткими цілями і KPI 2. Охоплення підтримкою (персонал, стейкхолдери) та підтверджений результат 3. Прозорість звітування про соціальні ініціативи (що зроблено і який ефект)
Рівність можливостей як результат	1. Доступ до навчання, підвищення кваліфікації, участі у проєктах 2. Прозорі умови кар'єрного просування та преміювання (без проявів дискримінації) 3. Зменшення розривів між групами працівників або структурними підрозділами
Позитивна динаміка ключових інклюзивних показників	1. Зниження проявів дискримінації груп працівників (диференційована плинність кадрів) 2. Залученість та психологічна безпека персоналу 3. Зменшення кількості скарг, пов'язаних з проявами дискримінації

3. Етап 3. «Визначення джерел інформації та формування інформаційної бази інклюзивного аудиту», на якому визначається перелік джерел інформації та формулюються правил використання цієї інформації в аудиті (табл. 13.4).

Таблиця 13.4

Джерела інформації для проведення інклюзивного аудиту

Джерело інформації	Особливості використання для інклюзивного аудиту
Внутрішні документи та регламенти (статут, положення, правила внутрішнього трудового розпорядку, інструкції)	Визначають принципи інклюзивності та правила взаємодії із працівниками та стейкхолдерами; права й обов'язки, стандарти поведінки, пов'язані з рівністю можливостей, доступом і участю
Управлінські рішення та документообіг (накази, протоколи, обґрунтування, службові записки)	Регламентують та документують порядок, логіку й процедури ухвалення управлінських рішень; ступінь їх прозорості та обґрунтованості; врахування потреб та інтересів персоналу, клієнтів і стейкхолдерів (зокрема через механізми залучення, консультацій і підзвітності) в управлінських рішеннях і процедурах їх ухвалення
Кадрова інформація (чисельність та структура персоналу, процедури добору кадрів та прийняття на роботу, адаптації, навчання та підвищення кваліфікації, оцінювання, кар'єрного просування)	Надає інформацію про кадровий склад і рух персоналу та про практичну реалізацію кадрових процедур; дозволяє оцінити рівність можливостей у доступі до працевлаштування, адаптації, навчання, оцінювання й кар'єрного просування, а також виявити диспропорції та бар'єри, що обмежують участь і розвиток окремих груп персоналу
Документація з охорони праці та організації робочих місць (акти або протоколи обстеження робочих місць і умов праці, матеріали оцінювання умов праці, заявки на адаптацію робочих місць)	Надає інформацію про рівень доступності та безбар'єрності робочого середовища, наявність і достатність адаптації робочих місць, відповідність умов праці потребам різних груп персоналу, а також про фактори виробничого середовища, які можуть створювати або підсилювати бар'єри участі (фізичні, організаційні, комунікаційні) у виконанні функцій
Звернення, скарги, запити (у паперовій або електронній формі, через гарячі лінії та чат-боти)	Надають інформацію про фактичні проблеми з доступом, участю та справедливістю процедур, з якими стикаються персонал, клієнти, партнери та інші стейкхолдери; дають змогу ідентифікувати типові бар'єри, їх локалізацію в управлінських рішеннях і процесах, а також ідентифікувати проблемні точки взаємодії та причини повторюваних звернень і скарг
Результати опитувань персоналу та стейкхолдерів (анонімні анкети, моніторингові опитування)	Надають узагальнену інформацію про інклюзивну культуру в організації та дає змогу виявити бар'єри, які не озвучуються відкрито через страх осуду або негативні наслідки, зокрема: щодо рівності можливостей, доступу до інформації, недискримінаційної взаємодії, залученості та психологічної безпеки
Канали та зміст комунікацій (оголошення, внутрішні канали, сайт, інформаційні повідомлення)	Надають інформацію про доступність і зрозумілість комунікацій для різних груп персоналу та стейкхолдерів; дозволяють оцінити, чи є рівний доступ до інформації (канали, формат, мова, термінологія, читабельність, наявність альтернативних форматів), а також виявляють комунікаційні бар'єри, що обмежують можливість участі

Результати тестування цифрової інклюзивності (сайти, форми, цифрові документи, сервіси)	Надають інформацію про рівень цифрової інклюзивності сайту, електронних форм документів і сервісів, тобто про наявність або відсутність цифрових бар'єрів для різних груп користувачів; дають змогу визначити проблемні елементи інтерфейсу й контенту, що ускладнюють доступ до інформації та участь у взаємодії з організацією
Аналітика цифрових каналів і сервісів (веб-аналітика, статистика використання, показники відмов)	Надає інформацію про фактичне використання цифрових каналів і сервісів та поведінкові характеристики взаємодії користувачів (переходи, завершення/переривання дій, відмови); дозволяє виявити проблемні етапи доступу й участі, на яких виникають утруднення для різних груп, а також визначити напрямки, що потребують удосконалення з позиції інклюзивності
Матеріали навчання та підвищення кваліфікації (програми, журнали участі, сертифікати)	Надають інформацію про доступність можливостей навчання та підвищення кваліфікації для різних груп персоналу; дозволяють визначити, чи забезпечується рівний доступ до розвитку компетентностей (умови участі, формати, інформування), а також виявити бар'єри, що обмежують участь у навчанні та професійному зростанні
Інформація про інциденти, конфлікти, порушення етики	Надає можливість ідентифікувати проблемні зони взаємодії в колективі та між організацією і зовнішнім середовищем, випадки порушення принципів поваги, рівного ставлення та недискримінації; дає змогу визначити рівень психологічної безпеки, наявність бар'єрів участі, а також ефективність механізмів реагування та захисту прав людей

4. Етап 4. «Перевірка якості і придатності аудиторської інформації для проведення інклюзивного аудиту», на якому відбувається перевірка повноти, актуальності, узгодженості та достовірності інформації, а також у встановленні обмежень її використання (табл. 13.5).

Таблиця 13.5

Вимоги до якості та придатності інформації для проведення інклюзивного аудиту

Вимога	Зміст вимоги
Повнота	Інформація має охоплювати ключові вектори інклюзивного аудиту (управлінські рішення, процеси, результати), а також релевантні групи персоналу і стейкхолдерів. Пропуски інформації фіксуються та враховуються у висновках
Актуальність	Інформація має відповідати чинним регламентам та умовам функціонування організації. Застарілі відомості використовуються лише як довідкові та позначаються як такі
Достовірність	Інформація має походити з надійних джерел і підлягати обов'язковій перевірці (первинні документи, реєстри, записами). Для опитувань та інтерв'ю забезпечується

	коректність збору й узгодження з іншими джерелами
Узгодженість	Інформація з різних джерел має бути логічно узгодженою. Розбіжності підлягають уточненню; у разі неможливості уточнення вони фіксуються як бар'єр для проведення аудиту
Достатність для формування висновків	Обсяг і структура інформації мають бути достатніми для проведення інклюзивного аудиту Для опитувань та інтерв'ю забезпечується достатня репрезентативність вибірок, щоб уникнути розходжень у висновках
Єдність підходів до показників	Показники (індикатори) мають визначатися та оброблятися за єдиними правилами (визначення, одиниці виміру, підхід до класифікації/кодування), що забезпечує коректність інтерпретації результатів
Однозначність інтерпретації	Категорії, ознаки та формулювання мають виключати двозначність. Для якісних даних встановлюються правила кодування та класифікації (наприклад, причин звернень), щоб забезпечити однакове трактування
Перевірюваність походження інформації	Для кожного висновку має бути визначене джерело інформації (документ, реєстр, масив даних, протокол). Має бути забезпечена можливість перевірки ланцюга «джерело → обробка → результат»
Конфіденційність та етичність використання	Інформація про персонал використовується з дотриманням принципів мінімізації даних, обмеження доступу та (за потреби) анонімізації або агрегації. Не допускається використання даних, що може спричинити стигматизацію або дискримінацію

5. Етап 5. «Інклюзивний аудит управлінських рішень організації», на якому відбувається перевірка того, чи забезпечують процедури підготовки та ухвалення управлінських рішень належне залучення, прозорість, обґрунтування та врахування наслідків для різних груп персоналу і стейкхолдерів (рис. 13.3).

Рис. 13.3. Процес інклюзивного аудиту управлінських рішень

6. Етап 6. «Інклюзивний аудит процесів організації», на якому перевіряється, як реально функціонують управлінські, кадрові, комунікаційні та інші процеси з погляду рівного доступу, можливості участі та відсутності бар'єрів для персоналу і стейкхолдерів (табл. 13.6).

Таблиця 13.6

Інклюзивний аудит процесів організації

Вид процесів	Можливі бар'єри	Умови рівного доступу та можливостей
Управлінські процеси (планування, координація, контроль, розподіл ресурсів)	Непрозорі процедури та критерії; формальне залучення; обмежений доступ до інформації; відсутність зворотного зв'язку; «ручні» рішення	Прозорі правила і критерії; чітко регламентовані процедури; доступні канали участі; підзвітність і зворотний зв'язок
Кадрові процеси (добір персоналу, прийняття на роботу, адаптація, оцінювання, просування)	Суб'єктивні критерії; упередженість; недоступні етапи відбору; нерівний доступ до розвитку; непрозорі правила оцінювання та просування	Єдині стандарти і критерії; доступні процедури; рівний доступ до навчання й професійного розвитку; прозорі правила оцінювання і кар'єрного просування
Комунікаційні процеси (внутрішнє інформування, наради, повідомлення)	Недоступні канали комунікації; складна мова; відсутність альтернативних форматів; нерівномірне поширення інформації; виключення окремих груп	Рівний доступ до інформації; зрозуміла мова; альтернативні формати; регулярність і повнота інформування; доступність комунікаційних каналів та подій
Процеси професійного розвитку персоналу (навчання, підвищення кваліфікації)	Обмеження участі через графік або формат; недоступні матеріали; нерівний доступ до інформації про можливості; непрозорий відбір учасників	Рівні можливості участі; інформування через доступні канали; гнучкі формати участі; доступні матеріали; прозорі критерії відбору
Сервісні процеси (надання послуг) (для клієнтів/користувачів)	Складні маршрути; недоступні канали; незрозумілі форми та документи; відсутність супроводу; непрозорі строки та вимоги	Безбар'єрні канали отримання послуги; універсальний дизайн; зрозумілі інструкції; доступні форми й документи; можливість супроводу; стандарти сервісу
Процеси розгляду звернень і скарг	Складність подання; недовіра до каналів; відсутність анонімності; формальний розгляд; відсутність коригувальних дій	Доступні канали звернень; можливість анонімного звернення; регламент і строки розгляду; об'єктивність і підзвітність; фіксація та контроль виконання коригувальних заходів

Процеси доступу до ресурсів і цифрових каналів (системи, сервіси, інформація)	Обмеження доступу до систем та ресурсів; цифрові бар’єри; нерівний доступ до обладнання; відсутність підтримки та адаптацій	Прозорі правила доступу; доступність цифрових ресурсів; адаптації за потреби; підтримка користувачів; стандарти цифрової доступності та безбар’єрності

7. Етап 7. «Інклюзивний аудит результатів діяльності організації», на якому визначаються фактичні, вимірювані наслідки інклюзивності на основі індикаторів: безбар’єрність середовища і комунікацій, універсальний дизайн, рівність можливостей, показники участі та залученості, динаміка звернень і скарг, показники психологічної безпеки, а також оцінюється, чи має організація підтверджувані свідчення позитивної динаміки за цими показниками та чи є відхилення, що потребують коригувальних управлінських рішень. Результати такого оцінювання слугують підставою для формування висновку про рівень інклюзивності результатів діяльності та визначення пріоритетних напрямів усунення бар’єрів (рис. 13.4).

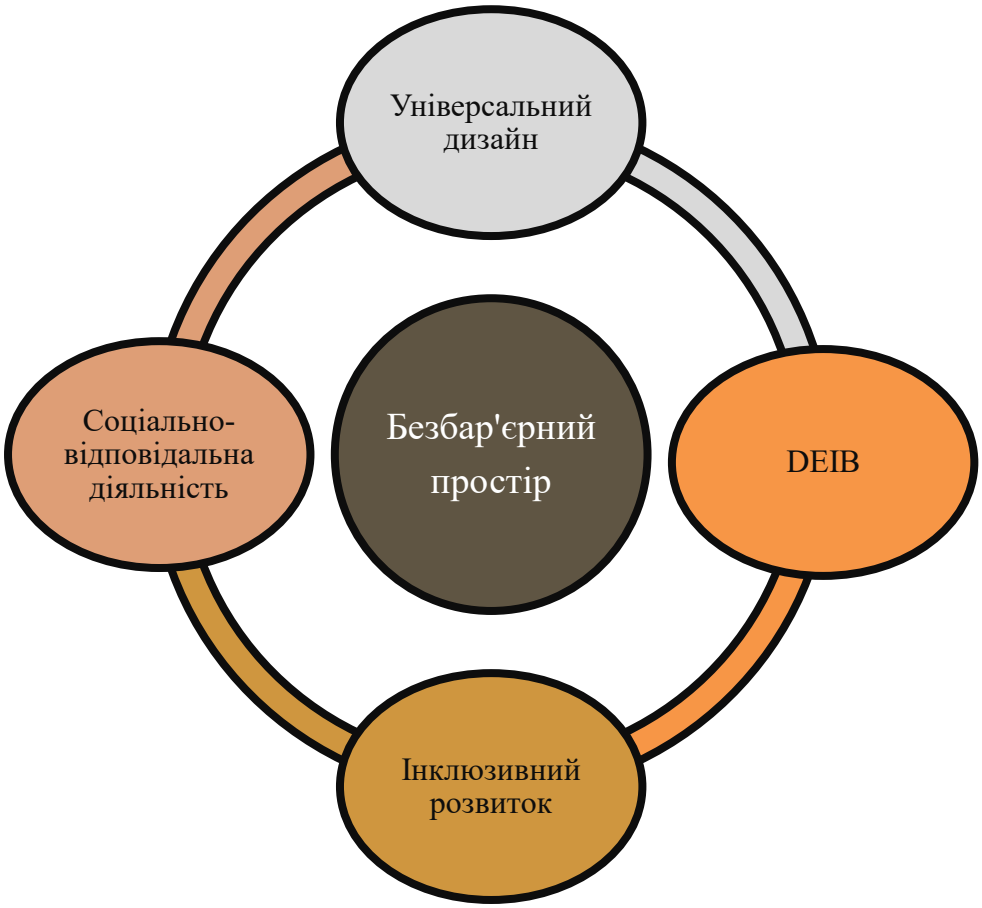


Рис. 13.4. Критерії інклюзивного аудиту результатів діяльності організації

8. Етап 8. «Ідентифікація бар'єрів та чинників, що обмежують рівність можливостей, доступ і участь», *на якому визначаються* конкретні бар'єри (фізичні, інформаційні, цифрові, освітні, економічні, суспільні) і чинників, які зумовлюють існування цих бар'єрів в практиці діяльності організації (табл. 13.7).

9. Етап 9. «Встановлення причинно-наслідкових зв'язків та оцінювання наслідків виявлених бар'єрів», на якому пояснюється чому виникає бар'єр (управлінські або процедурні причини, недоліки процесу, комунікаційний розрив тощо) та які наслідки він спричиняє для персоналу, стейкхолдерів і організації.

Таблиця 13.7

Види бар'єрів та умови їх існування

Види бар'єрів	Типові бар'єри в організації	Причини та умови існування бар'єрів
Фізичні	Недоступність приміщень і маршрутів, входів і санвузли; відсутність адаптованих робочих місць	Застаріла інфраструктура; відсутність «універсального дизайну»; недостатнє фінансування та планування адаптацій; слабкий контроль виконання
Інформаційні	Складна мова повідомлень; відсутність альтернативних форматів комунікації; нерівний доступ до інформації	Відсутність стандартів «доступної комунікації»; фрагментація каналів; нерегулярність інформування; низька культура зворотного зв'язку
Цифрові	Недоступні сайти, форми, цифрові документи; складні цифрові маршрути; неможливість виконати дію без допомоги	Відсутність стандартів цифрової доступності; недостатнє тестування; неузгоджені вимоги до розробників та постачальників; обмежені ресурси на доопрацювання
Освітні	Нерівний доступ до навчання та підвищення кваліфікації; недоступні матеріали або формати	Негнучкі формати й графіки; неадаптовані матеріали; непрозорі критерії відбору; нерівне інформування про можливості
Економічні	Нерівний доступ до ресурсів та інструментів; непрозорі механізми заохочення; фінансові «пороги» для участі	Непрозорі критерії розподілу; нерівномірне ресурсне забезпечення; відсутність бюджетування адаптацій; неформальні практики
Суспільні	Виключення з участі в обговореннях; толерування дискримінаційних практик; низька психологічна безпека	Організаційна культура «мовчання»; слабкі механізми реагування; відсутність довіри до каналів повідомлень; неефективна етична інфраструктура

10. Етап 10. «Обґрунтування управлінських заходів з усунення бар'єрів і визначення механізмів контролю результатів»**,** на якому відбувається вироблення рекомендацій і складання плану дій: які саме управлінські зміни потрібні (в рішеннях, процесах, комунікаціях, умовах праці, навчанні тощо), хто відповідальний, які строки, які показники контролю.

Практичне значення інклюзивного аудиту полягає в тому, що він дає організації можливість не лише зафіксувати рівень інклюзивності, а й виявити конкретні бар'єри доступу та участі, встановити їх причини й наслідки та обґрунтувати управлінські заходи, спрямовані на його підвищення з подальшим контролем результатів, що перетворює аудит на дієвий інструмент управління змінами. Водночас ефективність такого аудиту в реальних умовах безпосередньо залежить від того, наскільки якісно організація здатна збирати, перевіряти, систематизувати й аналізувати аудиторську інформацію, а також оперативно візуалізувати висновки та забезпечувати моніторинг виконання рекомендацій, тому виникає об'єктивна потреба у детальнішому розгляді цифрових технологій інклюзивного аудиту.

13.2. Види та призначення цифрових технологій інклюзивного аудиту

Цифрові технології інклюзивного аудиту використовуються для забезпечення доказовості та відтворюваності аудиторських висновків і становлять інструментальну основу його практичного виконання. Вони охоплюють повний цикл роботи з аудиторською інформацією: збір і фіксацію даних, їх верифікацію, інтеграцію та підготовку до аналізу, подальшу аналітику і представлення результатів. У межах інклюзивного аудиту такі технології застосовуються для оцінювання інклюзивності управлінських рішень, процесів і результатів, а також для супроводу контролю виконання наданих рекомендацій.

Застосування цифрових рішень підвищує оперативність аудиторських процедур і розширює можливості роботи з великими масивами даних. Це дає змогу швидше ідентифікувати бар'єри, виявляти повторювані закономірності, окреслювати зони ризику й формувати результати у форматі, придатному для управлінського використання та подальшого моніторингу.

Цифрові технології інклюзивного аудиту доцільно класифікувати за функціональним призначенням у межах аудиторського циклу, оскільки саме виконувана функція визначає їх роль у встановленні бар'єрів та оцінюванні інклюзивності. Такий підхід дозволяє пов'язати кожну технологію з конкретним етапом аудиту та очікуваним результатом її застосування.

До цифрових технологій інклюзивного аудиту належать: технології збору та фіксації аудиторської інформації; технології інтеграції та підготовки даних; технології аналітики процесів і виявлення «вузьких місць»; технології аналізу звернень, скарг і текстових даних; технології оцінювання цифрової доступності та безбар'єрності; технології бізнес-аналітики та візуалізації результатів; технології управління виконанням рекомендацій і моніторингу (табл. 13.8). Розглянемо їх більш детально.

Таблиця 13.8

Цифрові технології інклюзивного аудиту

Види цифрових технологій	Призначення в інклюзивному аудиті
Технології збору та фіксації аудиторської інформації	Забезпечують системне накопичення аудиторської інформації щодо управлінських рішень, виконання процесів, комунікацій, кадрових подій та взаємодії зі стейкхолдерами; створюють основу для доказового оцінювання інклюзивності та відтворюваності висновків
Технології інтеграції та підготовки даних	Забезпечують уніфікацію даних із різних джерел, усунення дублювань, стандартизацію класифікаторів і показників, підготовку даних для подальшого аналізу та розрахунку індикаторів інклюзивності
Технології аналітики процесів і виявлення «вузьких місць»	Дають змогу реконструювати фактичний перебіг процесів, оцінити відповідність регламентам, виявити відхилення, затримки, повторні кола, точки відмов і «випадання» користувачів/персоналу; локалізують бар'єри участі у процесах
Технології аналізу звернень, скарг і текстових даних	Забезпечують систематизацію звернень і скарг, класифікацію причин, виявлення повторюваних проблем, тематичний аналіз відкритих відповідей; дозволяють виявити бар'єри, що не відображені у формальних регламентах
Технології оцінювання цифрової інклюзивності	Забезпечують перевірку інклюзивності цифрових каналів комунікації (сайтів, форм, документів, сервісів), виявляють цифрові бар'єри для різних груп користувачів і формують підстави для їх усунення
Технології бізнес-аналітики та візуалізації результатів	Забезпечують інтеграцію та представлення індикаторів інклюзивності у формі, придатній для управлінського використання; підтримують інтерпретацію відхилень, порівняння за підрозділами/каналами та контроль динаміки показників
Технології управління виконанням рекомендацій і моніторингу	Забезпечують планування заходів, призначення відповідальних, контроль строків і статусів виконання, фіксацію результатів, повторні перевірки та оцінювання ефекту від змін

Технології збору та фіксації аудиторської інформації – цифрові інструменти, що забезпечують документування, накопичення та збереження аудиторської інформації про діяльність організації у формах, придатних для подальшої перевірки, аналітичної обробки та формування доказових висновків. Їх застосування створює базову умову інклюзивного аудиту – наявність відтворюваної інформаційної бази, яка дає змогу оцінювати інклюзивність не за поодинокими випадками, а на основі системних даних, зафіксованих у корпоративних системах та реєстрах.

Технології збору та фіксації аудиторської інформації охоплюють такі напрями:

- *документування управлінських рішень і їх життєвого циклу* (ініціювання, погодження, зміни, обґрунтування, затвердження, доведення до виконавців, комунікація зі стейкхолдерами) *для перевірки прозорості ухвалення рішень, належного залучення та врахування потреб різних груп;*
- *фіксація виконання процедур та операцій у процесах* (трасування заявок, запитів, операційних кроків і статусів) *для оцінювання процесів у реальних умовах і виявлення причин затримок, відмов, повторних звернень та нерівномірного доступу;*
- *облік звернень, скарг і запитів як джерела інформації про бар'єри доступу, участі та якості взаємодії, що не завжди відображені у внутрішній документації;*
- *фіксація результатів опитувань і зворотного зв'язку* (анкети, інтерв'ю, фокус-групи, електронні форми, оцінювання сервісу) *для аналізу досвіду участі, сприйняття справедливості процедур і виявлення проблем, які не озвучуються відкрито;*
- *кадрові дані та HR-аналітика* (добір, адаптація, навчання, оцінювання, кар'єрне просування, оплата праці, плинність) *для оцінювання рівності доступу до можливостей розвитку та наявності структурних диспропорцій;*
- *реєстрація інцидентів, конфліктів і порушень етики та реагування організації* (факт, канал повідомлення, розгляд, рішення, коригувальні дії) *як індикатор організаційної культури й психологічної безпеки та підтвердження фактичних практик взаємодії.*

Призначення технологій збору та фіксації аудиторської інформації в інклюзивному аудиті полягає у формуванні повної та достовірної доказової бази. Така база дозволяє встановити, хто саме був залучений до процедур і в який спосіб здійснювалася участь, чи забезпечувався рівний доступ до можливостей і каналів взаємодії, а також де виникають повторювані проблеми. На підставі зафіксованих фактів аудитор отримує змогу підтвердити або спростувати

наявність бар'єрів і окреслити їх причини. Системна фіксація інформації також є основою для подальшого моніторингу змін і перевірки фактичного ефекту управлінських заходів після завершення аудиту.

Види цифрових технологій збору та фіксації аудиторської інформації, їх призначення та конкретні приклади представлені в таблиці 13.9.

Таблиця 13.9

Технології збору та фіксації аудиторської інформації в інклюзивному аудиті

Види технологій	Призначення	Приклади
Системи електронного документообігу та управління записами	Фіксація управлінських рішень, етапів їх погодження, версій і обґрунтувань; підтвердження прозорості процедур та наявності документальних підстав; формування доказової бази щодо залучення і підзвітності	Microsoft SharePoint/365 (DMS); M-Files; OpenText; Alfresco; корпоративні DMS на базі BAS, 1C та інші внутрішні системи документообігу
Системи управління процесами та заявами (реєстри послуг та заяв)	Реєстрація проходження процедур (статуси, строки, результат); фіксація маршрутів і точок прийняття рішень у процесі; виявлення проблемних етапів, де можуть виникати обмеження доступу або участі	ServiceNow; Jira Service Management; Zendesk/Freshdesk (як реєстри запитів); внутрішні реєстри заяв і послуг; модулі BPM/Workflow у корпоративних платформах
HR-інформаційні системи (кадрові модулі)	Документування кадрових подій і параметрів кадрових процесів; підтвердження правил і практики добору, адаптації, навчання, оцінювання та просування; оцінювання рівності доступу персоналу до можливостей розвитку	SAP SuccessFactors; Workday; BambooHR; PeopleForce; Hurma; BAS «Зарплата і кадри», інші HR-модулі
CRM звернень і скарг, системи розгляду звернень	Облік звернень, скарг і запитів за каналами; фіксація причин, результатів розгляду та повторюваності проблем; виявлення «сигналів бар'єрності» у взаємодії з організацією	Salesforce Service Cloud; Microsoft Dynamics 365 Customer Service; Zendesk, Freshdesk; HelpDesk-системи; внутрішні CRM звернень і скарг
Платформи опитувань і зворотного зв'язку	Фіксація доступу й участі, сприйняття справедливості процедур та рівності можливостей; отримання анонімних сигналів щодо проблем, про які можуть не повідомляти відкрито	Google Forms; Microsoft Forms; SurveyMonkey; Qualtrics; LimeSurvey; Typeform

Системи обліку інцидентів, конфліктів і порушень етики	Формалізація повідомлень про інциденти або конфлікти; фіксація реагування та результатів розгляду; оцінювання етичних ризиків і психологічної безпеки	Whistleblowing-канали, системи повідомлень; ServiceNow Incident; внутрішні реєстри інцидентів та порушень етики
Журнали подій IT-систем (логування)	Фіксація подій цифрової взаємодії (вхід, подання, відмова, затримка тощо) у каналах і сервісах; підтвердження факту виконання/невиконання дій; основа для подальшої аналітики процесів і користувацьких сценаріїв	Журнали подій веб-сервісів, систем авторизації, CRM, HR, DMS; SIEM, лог-менеджери (за наявності) та інші засоби корпоративного логування

Технології інтеграції та підготовки даних – це цифрові інструменти, що забезпечують узгоджену уніфікацію інформації з різних джерел і її приведення до аналітично-придатного вигляду. Вони охоплюють очищення даних, уніфікацію форматів і довідників, перевірку якості, усунення дублювань і помилок, а також підготовку масивів до подальших розрахунків індикаторів інклюзивності. Саме на цьому етапі формується коректна база для обґрунтованих аудиторських висновків.

Для інклюзивного аудиту інтеграція є необхідною, оскільки оцінювання спирається на різнорідні джерела: документи і реєстри, кадрові дані, звернення і скарги, результати опитувань, аналітику цифрових каналів. Без попереднього узгодження ці масиви не забезпечують єдиного трактування показників, а отже ускладнюють порівнюваність результатів та інтерпретацію виявлених бар'єрів.

Технології інтеграції та підготовки даних охоплюють такі напрями:

- *інтеграція даних із різних систем і джерел та організація обміну даними* (конектори, API, імпорт і експорт);
- *стандартизація та очищення* даних (уніфікація форматів, усунення дублювань, помилок введення, пропусків, приведення показників до зіставного вигляду);
- *узгодження довідникової та класифікаційної бази* (підрозділи, посади, канали взаємодії, типи звернень, категорії користувачів) *і уніфікація термінів;*
- *контроль якості та придатності даних* (повнота, узгодженість, достовірність, актуальність) *із фіксацією обмежень їх використання в аудиті;*

➢ *уніфікація методики розрахунку індикаторів та формування підготовлених наборів даних для аналітики й візуалізації;*

➢ *забезпечення захисту персональних даних і режимів доступу під час обробки кадрової та іншої чутливої інформації.*

Види цифрових технологій інтеграції та підготовки даних в інклюзивному аудиті представлені в таблиці 13.10.

Таблиця 13.10

Цифрові технології інтеграції та підготовки даних в інклюзивному аудиті

Види технологій	Призначення	Приклади
Інструменти інтеграції даних (ETL або ELT)	Об'єднання даних із різних систем у єдиний масив; автоматизація завантаження, перетворення і оновлення даних для подальшої аналітики інклюзивності.	Microsoft Power Query, Power BI Dataflows; Talend; Pentaho (Kettle); Apache NiFi; SSIS; Fivetran, Stitch (за наявності).
Конектори, API та механізми обміну даними	Налаштування регулярного отримання даних із корпоративних систем (документообіг, кадрові системи, CRM, реєстри); забезпечення актуальності та повноти інформаційної бази аудиту.	API типів REST та SOAP; конектори до SharePoint і Google Workspace; інтеграції через Zapier або Make (для простих сценаріїв); корпоративні шлюзи інтеграції.
Інструменти очищення та трансформації даних	Виявлення та виправлення помилок, пропусків і дублювань; стандартизація форматів; підвищення якості та придатності даних для розрахунку індикаторів.	Power Query; OpenRefine; Trifacta, Alteryx (за наявності); вбудовані модулі очищення даних у BI та аналітичних платформах.
Управління довідниками та класифікаторами (MDM та корпоративні довідники)	Уніфікація класифікаторів (підрозділи, канали, типи звернень, категорії персоналу); забезпечення єдиного трактування показників і коректних порівнянь.	Корпоративні довідники і MDM-рішення; SAP Master Data; Microsoft Purview (у частині словників і каталогів); внутрішні довідники у BAS та ERP.
Сховища даних і дата-марти	Централізоване зберігання інтегрованих даних; забезпечення відтворюваності та аудиторської перевірюваності наборів даних, використаних для висновків.	SQL Server; PostgreSQL; MySQL; Oracle; BigQuery, Snowflake (за наявності); корпоративні дата-марти.
Технології контролю якості даних (DQ)	Перевірка повноти, узгодженості, актуальності та достовірності даних; фіксація правил валідації та журналювання помилок як елемент доказовості аудиту.	Great Expectations; Deequ; вбудовані модулі контролю якості у сховищах даних та BI; контрольні правила в ETL-процесах.

Засоби управління доступом і захисту даних	Забезпечення конфіденційності та законності обробки кадрових і чутливих даних; розмежування доступу; анонімізація або псевдонімізація за потреби.	Ролі доступу в системах документообігу, кадрових системах і CRM; Azure AD (Entra ID); DLP-політики; шифрування;

Технології аналітики процесів і виявлення «вузьких місць» – це цифрові інструменти, що на основі даних про події та дії в інформаційних системах дозволяють відтворити фактичний перебіг організаційних процесів, оцінити їх результативність і відповідність встановленим правилам, а також виявити етапи, на яких виникають затримки, повтори, відмови та інші відхилення. У контексті інклюзивного аудиту ці технології дають змогу встановити, де саме у процесі формуються бар'єри доступу й участі для персоналу та стейкхолдерів, і перейти від загальної констатації проблеми до точного визначення проблемного кроку процесу.

Технології аналітики процесів охоплюють такі напрями:

- *використання інформаційних систем як джерела подієвих даних про фактичні дії та їх послідовність;*
- *реконструкція фактичної моделі процесу та порівняння з регламентною моделлю для виявлення відхилень;*
- *часові та частотні виміри процесу* (тривалість етапів, час очікування, повторні проходження процедур);
- *ідентифікація точок відмов і «випадання» учасників процесу, а також причин накопичення черг;*
- *сегментація процесу за підрозділами, каналами та групами користувачів або персоналу для перевірки рівності доступу;*
- *виявлення аномалій і ризик-орієнтоване визначення зон поглибленої перевірки;*
- *формування доказових матеріалів для управлінських рішень щодо усунення бар'єрів у процесах.*

Види цифрових технологій аналітики процесів і виявлення «вузьких місць» в інклюзивному аудиті представлені в таблиці 13.11.

Таблиця 13.11

Цифрові технології аналітики процесів і виявлення «вузьких місць» в інклюзивному аудиті

Види технологій	Призначення	Приклади
Process mining	Реконструкція фактичного перебігу процесів за подієвими журналами, виявлення відхилень, затримок і повторів; локалізація етапів, на яких виникають бар'єри доступу й участі	Celonis; UiPath Process Mining; SAP Signavio Process Intelligence; Microsoft Process Advisor; Apromore
Аналіз подієвих журналів і трасування подій	Фіксація послідовності дій у процесі, перевірка причин відмов і збоїв, виявлення точок накопичення черг та повторних дій; підтвердження фактів проходження процедур	Журнали подій у CRM, кадрових системах і системах документообігу; системи лог-менеджменту; Elasticsearch Kibana; Splunk (за наявності)
Моделювання та картування процесів	Формування регламентної моделі процесу та її використання як бази для порівняння з фактичним виконанням; ідентифікація неузгодженостей і надмірних процедурних кроків	BPMN-моделювання; Bizagi Modeler; Camunda Modeler; SAP Signavio; ARIS
Моніторинг показників процесу та аналіз часу виконання	Оцінювання тривалості етапів, часу очікування, частоти повторних проходжень; виявлення нерівномірності доступу до проходження процедур залежно від каналу або категорії користувачів	Модулі аналітики у BPM та Service Desk; Power BI з даними процесів; інструменти аналізу черг та SLA у ServiceNow та аналогах
Аналіз шляхів користувачів у цифрових сервісах	Виявлення етапів, на яких користувачі припиняють взаємодію з сервісом; встановлення сценаріїв, що призводять до помилок та відмов; оцінювання доступності проходження цифрових процедур	Google Analytics 4; Matomo; Microsoft Clarity; системи продуктового аналізу; журналювання подій у веб-сервісах
Виявлення аномалій і ризик-індикаторів у процесі	Визначення нетипових випадків у виконанні процедур, підозрілих відхилень і нерегулярності; виділення зон підвищеної ймовірності бар'єрів або порушень рівності доступу	Інструменти виявлення аномалій у BI та аналітичних платформах; правила контролю і тригери у BPM; прості моделі машинного навчання у корпоративній аналітиці

Технології аналізу звернень, скарг і текстових даних – це цифрові інструменти, призначені для системної реєстрації, структурування та аналітичного опрацювання повідомлень, що надходять від персоналу та інших стейкхолдерів через різні канали взаємодії з організацією. Вони дозволяють узагальнювати звернення за темами і причинами, визначати повторювані

проблеми, встановлювати типові бар'єри доступу й участі та формувати доказові висновки щодо якості комунікацій і справедливості процедур. Для інклюзивного аудиту ці технології є принципово важливими, оскільки значна частина бар'єрів фіксується саме у зверненнях, скаргах і відкритих текстових відповідях, тоді як у формалізованих регламентах такі проблеми можуть не відображатися.

Технології аналізу звернень, скарг і текстових даних охоплюють такі напрями:

- *єдина реєстраційна база звернень і скарг із фіксацією каналу, теми, строків реагування та результату розгляду;*
- *кодування та класифікація причин звернень, зокрема формування типології бар'єрів за змістом повідомлень;*
- *аналіз повторюваності та концентрації звернень за підрозділами, сервісами і каналами комунікації;*
- *аналітика текстових масивів* (тематичне групування, виділення ключових мотивів, факторів незадоволеності);
- *аналіз відкритих відповідей в опитуваннях як джерела інформації про проблеми, які не завжди озвучуються у прямій комунікації;*
- *оцінювання дотримання стандартів реагування і якості зворотного зв'язку* (строки, повнота відповіді, результативність) *як елементів рівності доступу;*
- *формування аналітичних зрізів і доказових матеріалів для обґрунтування рекомендацій щодо усунення виявлених бар'єрів.*

Види цифрових технологій аналізу звернень, скарг і текстових даних в інклюзивному аудиті представлені в таблиці 13.12.

Технології оцінювання цифрової доступності та безбар'єрності – це цифрові інструменти і методи перевірки, що дозволяють встановити рівень доступності сайтів, онлайн-форм, цифрових документів і електронних сервісів організації для різних груп користувачів та ідентифікувати елементи, які формують цифрові бар'єри. У межах інклюзивного аудиту вони забезпечують доказове підтвердження проблем доступності цифрових каналів, дають підстави

для визначення пріоритетності усунення порушень і для формування рекомендацій щодо запровадження безбар'єрних рішень у цифровій взаємодії.

Таблиця 13.12

Цифрові технології аналізу звернень, скарг і текстових даних в інклюзивному аудиті

Види технологій	Призначення	Приклади
Системи обліку звернень і скарг	Фіксація звернень за каналами, темами і результатами розгляду; контроль строків реагування; формування доказової бази щодо типових проблем доступу й участі	Zendesk; Freshdesk; Jira Service Management; ServiceNow; внутрішні реєстри звернень; CRM модулі звернень
CRM звернень та сервісна аналітика	Групування звернень за категоріями, підрозділами та сервісами; аналіз повторюваності; виявлення концентрації бар'єрів у конкретних каналах або ланках	Salesforce Service Cloud; Microsoft Dynamics 365 Customer Service; SAP Customer Experience; внутрішні CRM рішення
Класифікатори причин і типологія бар'єрів	Стандартизація кодування причин звернень; забезпечення порівнюваності та відтворюваності аналітики; узгодження понятійного апарату для аудиторських висновків	Корпоративні довідники; налаштовані категорії у CRM та системах звернень; внутрішні класифікатори причин
Тематичний аналіз текстів і виділення ключових тем	Виявлення основних тем у відкритих текстах, групування повідомлень за смисловими кластерами, виділення типових бар'єрів та факторів їх виникнення	Модулі text mining у BI та аналітичних платформах; можливості Microsoft Power BI для роботи з текстами; інструменти аналізу текстів
Аналіз тональності та маркерів ризику	Виявлення повідомлень з підвищеним рівнем негативних оцінок або ознак конфлікту; ідентифікація «сигналів ризику» щодо недоступності, дискримінації або порушень етики	Вбудовані модулі аналітики тональності у корпоративних платформах; інструменти аналізу текстів з підтримкою словників ризикових маркерів
Аналітика чат-ботів і цифрових каналів звернень	Виявлення тем, з якими найчастіше звертаються; аналіз сценаріїв, на яких користувачі не отримують результату; встановлення бар'єрів у цифровій комунікації	Аналітика чат-ботів у Telegram та Viber; платформи чат-ботів з вбудованою аналітикою; модулі аналітики контакт-центрів
Аудит виконання стандартів реагування	Оцінювання дотримання строків розгляду і якості відповіді; виявлення нерівності доступу до реагування залежно від каналу або категорії звернень; підтвердження управлінської відповідальності	SLA звіти у Service Desk системах; аналітика в CRM звернень; контрольні звіти у системах документообігу

Технології оцінювання цифрової доступності та безбар'єрності охоплюють такі напрями:

- *автоматизоване сканування веб-ресурсів та інтерфейсів для виявлення типових порушень доступності;*
- *ручне тестування користувацьких сценаріїв* (проходження онлайн-процедур, заповнення форм, отримання результату);
- *перевірка доступності цифрових документів* (структура, читабельність, коректність елементів, відповідність вимогам доступності);
- *оцінювання доступності мультимедійного контенту та наявності альтернативних форматів подання інформації;*
- *перевірка сумісності з допоміжними технологіями і різними режимами користування;*
- *ідентифікація бар'єрів у навігації, сприйнятті, взаємодії та розумінні інформації, що ускладнюють отримання послуг;*
- *формування переліку порушень і пріоритезація виправлень та підготовка рекомендацій щодо усунення цифрових бар'єрів.*

Види цифрових технологій оцінювання цифрової доступності та безбар'єрності в інклюзивному аудиті представлені в таблиці 13.13.

Таблиця 13.13

Цифрові технології оцінювання цифрової доступності та безбар'єрності в інклюзивному аудиті

Види технологій	Призначення	Приклади
Автоматизовані сканери доступності веб-ресурсів	Виявлення типових порушень доступності у веб-інтерфейсах; формування первинного переліку проблем і підтвердження наявності цифрових бар'єрів	axe DevTools; WAVE; Lighthouse; Siteimprove Accessibility Checker; Tenon (за наявності)
Інструменти перевірки доступності форм і компонентів інтерфейсу	Перевірка коректності елементів взаємодії, полів введення, підказок і повідомлень про помилки; оцінювання доступності онлайн-процедур	axe DevTools; ARC Toolkit; інструменти тестування у браузерах; чек-листи перевірки форм у QA-практиках

Тестування користувацьких сценаріїв і юзабіліті з позиції безбар'єрності	Перевірка фактичної можливості виконати дію і отримати результат у цифровому сервісі; виявлення бар'єрів у навігації, сприйнятті і взаємодії	Сценарне тестування у QA; протоколи тестування; записи сесій користувачів; Microsoft Clarity (для візуалізації проблемних зон)
Перевірка доступності цифрових документів	Виявлення порушень доступності у документах, що поширюються в електронній формі; підтвердження бар'єрів у доступі до інформації та документів	Adobe Acrobat Accessibility Checker; Microsoft Office Accessibility Checker; PAC (PDF Accessibility Checker)
Оцінювання доступності мультимедійного контенту	Перевірка наявності субтитрів, альтернативних описів та інших елементів доступності; підтвердження доступності інформаційних матеріалів для різних груп	YouTube Studio для субтитрів; інструменти створення субтитрів; перевірка альтернативних описів у CMS
Моніторинг доступності та контроль виправлень	Відстеження усунення порушень у динаміці, контроль повторних перевірок і підтвердження результативності коригувальних дій	Siteimprove; Monsido; системи контролю якості контенту; повторні сканування з фіксацією змін
Чек-листи та протоколи аудиту доступності	Стандартизація процедур перевірки, забезпечення відтворюваності оцінювання та документування порушень як частини аудиторської доказової бази	Корпоративні чек-листи; протоколи аудиту доступності; шаблони звітів; внутрішні методики тестування

Технології бізнес-аналітики та візуалізації результатів – це цифрові інструменти, призначені для обробки та представлення індикаторів інклюзивності у форматі, придатному для управлінського використання. Вони забезпечують перетворення зібраних і інтегрованих даних на аналітичні висновки, порівняння показників у розрізі підрозділів, каналів взаємодії та категорій користувачів, а також виявлення відхилень від цільових орієнтирів і проблемних зон. У межах інклюзивного аудиту ці технології підвищують інтерпретованість результатів, підтримують прийняття управлінських рішень і створюють основу для моніторингу виконання рекомендацій.

Технології бізнес-аналітики та візуалізації результатів охоплюють такі напрями:

- *розрахунок та агрегування індикаторів інклюзивності на основі інтегрованих даних;*
- *порівняльний аналіз показників у розрізі підрозділів, каналів взаємодії,*

категорій персоналу і стейкхолдерів, а також у динаміці;

- *виявлення відхилень від цільових значень і порогів та формування сигналів ризику;*
- *візуалізація результатів* (панелі показників, профілі інклюзивності, карти проблемних зон, діаграми, аналітичні звіти);
- *аналітичні зрізи для обґрунтування рекомендацій і визначення пріоритетів усунення бар'єрів;*
- *стандартизація звітності через шаблони представлення результатів для забезпечення відтворюваності;*
- *моніторинг змін після впровадження заходів на основі регулярного оновлення показників.*

Види цифрових технологій бізнес-аналітики та візуалізації результатів в інклюзивному аудиті представлені в таблиці 13.14.

Таблиця 13.14

Цифрові технології бізнес-аналітики та візуалізації результатів в інклюзивному аудиті

Види технологій	Призначення	Приклади
BI-платформи для аналітики та дашбордингу	Побудова панелей показників інклюзивності, порівняння результатів за підрозділами і каналами, виявлення відхилень і тенденцій; забезпечення управлінської інтерпретації показників	Microsoft Power BI; Tableau; Qlik Sense; Looker; SAP Analytics Cloud (за наявності)
Аналітичні моделі індикаторів і KPI	Розрахунок індикаторів інклюзивності, визначення порогових значень і контрольних орієнтирів; підготовка обґрунтованих висновків щодо рівня інклюзивності	Моделі KPI у Power BI та Excel; корпоративні модулі KPI в ERP; аналітичні калькулятори показників у BI
Візуалізація проблемних зон і картування бар'єрів	Виявлення концентрації бар'єрів за процесами, каналами, підрозділами; представлення проблемних зон для визначення пріоритетів усунення бар'єрів	Карти проблемних зон у BI; теплові карти; діаграми розсіювання; інтерактивні карти сервісних маршрутів
Формування «сигналів ризику» та автоматизованих попереджень	Автоматичне виявлення відхилень від порогів, нетипових значень або погіршення динаміки; фокусування аудиту на найбільш критичних зонах	Правила та алерти у Power BI; алерти у Tableau; тригери у корпоративних аналітичних платформах; повідомлення в Teams або електронній пошті

Стандартні шаблони звітності та аналітичні довідки	Уніфікація структури подання результатів аудиту, забезпечення відтворюваності висновків і порівнянності звітів між періодами та об'єктами аудиту	Шаблони звітів у Word і PowerPoint; експорти з BI; корпоративні форми звітності; автоматизовані звіти у BI
Інструменти статистичного та порівняльного аналізу	Поглиблена оцінка відмінностей між групами, виявлення закономірностей і підтвердження аналітичних припущень щодо бар'єрів; підвищення обґрунтованості висновків	Excel; Python або R у корпоративній аналітиці; вбудована статистика у BI; SPSS (за наявності)
Моніторингові панелі для відстеження змін	Оцінювання ефекту від реалізації рекомендацій через динаміку індикаторів; контроль виконання і стабільності досягнутих результатів	Моніторингові дашборди у Power BI; регулярні звіти; автоматизовані оновлення показників у BI

Технології управління виконанням рекомендацій і моніторингу – це цифрові інструменти, призначені для планування, організації та контролю реалізації рекомендацій, сформованих за результатами інклюзивного аудиту, а також для відстеження досягнутого ефекту за індикаторами інклюзивності. Вони забезпечують фіксацію переліку заходів, відповідальних осіб, ресурсів, строків і статусів виконання, підтримують контрольні перевірки та створюють механізм підзвітності щодо впровадження змін. У межах інклюзивного аудиту ці технології є необхідними, оскільки результативність аудиту визначається не лише якістю висновків, а й керованістю усунення бар'єрів і підтвердженням позитивної динаміки після запровадження коригувальних заходів.

Технології управління виконанням рекомендацій і моніторингу охоплюють такі напрями:

- *ведення реєстру рекомендацій із фіксацією змісту, пріоритетності та очікуваного результату;*
- *планування коригувальних заходів* (відповідальні, ресурси, строки, контрольні точки);
- *управління виконанням через завдання, статуси та контроль прострочень із прозорістю прогресу;*
- *документування виконання та збереження підтверджувальних матеріалів і доказів упроваджених змін;*

➢ *моніторинг індикаторів інклюзивності після реалізації заходів і оцінювання досягнутого ефекту;*

➢ *організація повторних перевірок і контрольних вимірювань, включаючи внутрішній контроль якості виконання;*

➢ *формування управлінської звітності та підзвітності щодо виконання рекомендацій на рівні підрозділів.*

Види цифрових технологій управління виконанням рекомендацій і моніторингу в інклюзивному аудиті представлені в таблиці 13.15.

Таблиця 13.15

Цифрові технології управління виконанням рекомендацій і моніторингу в інклюзивному аудиті

Види технологій	Призначення	Приклади
Реєстр рекомендацій та база заходів	Фіксація рекомендацій і коригувальних заходів, пріоритетів, відповідальних та очікуваних результатів; забезпечення відтворюваності управлінських дій після аудиту	Внутрішні реєстри у Excel або SharePoint; модулі реєстру рекомендацій у системах управління якістю; корпоративні бази знань
Системи управління завданнями і проєктами	Планування заходів, встановлення строків і контрольних точок, розподіл відповідальності; контроль виконання та прозорість прогресу усунення бар'єрів	Jira; Trello; Asana; Microsoft Planner; Monday.com; ClickUp (за наявності)
Workflow і BPM платформи для організації виконання	Автоматизація маршрутів узгодження та виконання заходів, контроль впровадження змін; забезпечення підзвітності та документування етапів реалізації	ServiceNow Workflow; Microsoft Power Automate; Camunda; Bizagi; SAP Signavio Workflow Accelerator (за наявності)
Системи контролю виконання та дотримання строків	Виявлення прострочень, формування нагадувань, контроль виконання у розрізі підрозділів; підвищення дисципліни реалізації рекомендацій	Модулі контролю строків у Jira та Service Desk системах; автоматизовані сповіщення у Teams або електронній пошті; календарі контрольних точок
Сховища підтверджувальних матеріалів і управління документами	Накопичення доказів виконання, збереження версій документів, протоколів, актів та звітів	SharePoint; Google Drive; корпоративні DMS; системи управління файлами з контролем версій

Моніторингові панелі та звіти за індикаторами	Відстеження динаміки індикаторів інклюзивності після впровадження змін; оцінювання ефекту від заходів та підтримка повторних контрольних вимірювань	Power BI; Tableau; Qlik; регулярні моніторингові звіти; інтеграція показників у BI
Системи внутрішнього контролю і контролінгу виконання	Планування контрольних перевірок, аудит виконання заходів, фіксація результатів внутрішнього контролю; підвищення якості реалізації рекомендацій	Чек-листи контролю; модулі внутрішнього контролю у системах управління якістю; внутрішні регламенти контролю виконання

Цифрові технології забезпечують практичне виконання інклюзивного аудиту на основі системних даних і відтворюваних процедур аналізу. Вони охоплюють повний цикл роботи з аудиторською інформацією: збір і фіксацію, інтеграцію та підготовку даних, процесну і текстову аналітику, перевірку цифрової доступності, а також представлення результатів у форматі, придатному для управлінського використання. Засоби бізнес-аналітики і візуалізації підвищують зрозумілість та зіставлюваність висновків, а інструменти моніторингу забезпечують контроль виконання рекомендацій і оцінювання досягнутого ефекту. Таким чином, цифрова підтримка підсилює доказовість і зменшує суб’єктивність, переводячи інклюзивний аудит у площину керованих управлінських дій. Це створює логічну основу для подальшого розгляду методики застосування тривекторної моделі інклюзивного аудиту з цифровою підтримкою.

13.3. Цифрові інструменти здійснення аудиторських процедур та оформлення результатів інклюзивного аудиту

Інклюзивний аудит реалізується через систему аудиторських процедур, спрямованих на отримання, перевірку та узагальнення інформації про бар'єри доступу, участі та рівності можливостей для персоналу і стейкхолдерів. Використання цифрових технологій підсилює ці процедури, оскільки забезпечує повноту інформаційної бази, відтворюваність обробки даних і подання результатів у стандартизованих формах.

Аудиторські процедури інклюзивного аудиту – це сукупність дій аудитора, спрямованих на отримання та верифікацію аудиторської інформації, встановлення наявності бар'єрів і обґрунтування висновків та рекомендацій щодо їх усунення. У цьому контексті цифрові технології застосовуються як інструмент підтримки виконання процедур і документування отриманих результатів.

У практиці інклюзивного аудиту доцільно виокремлювати такі групи процедур (рис. 13.6).

Рис. 13.6. Види аудиторських процедур

1. ***Процедури планування і організації аудиту*** передбачають визначення об’єкта аудиту, критеріїв оцінювання, переліку джерел інформації, а також формування програми аудиту. Цифрова підтримка включає використання шаблонів програми аудиту, чек-листів, матриць критеріїв, електронного реєстру процедур і контрольних показників.

2. ***Процедури збору та фіксації аудиторської інформації*** передбачають отримання даних з корпоративних систем, реєстрів, опитувань, звернень, комунікаційних каналів, а також документування зібраних матеріалів. Цифрові інструменти забезпечують формування доказової інформаційної бази аудиту і збереження її структури.

3. ***Процедури перевірки якості та придатності інформації*** охоплюють оцінювання повноти, узгодженості, достовірності та актуальності даних, а також врахування обмежень використання інформації (конфіденційність, персональні дані). Цифрова підтримка включає контрольні правила якості даних, протоколи уніфікації та фіксації змін.

4. ***Процедури аналітичної обробки та виявлення бар’єрів*** передбачають аналіз процесів, звернень, скарг, текстових даних, цифрової аналітики, результатів опитувань, а також узагальнення типових бар’єрів і зон ризику. Цифрові технології забезпечують процесну аналітику, тематичне групування проблем, розрахунок показників і формування аналітичних висновків.

5. ***Процедури оцінювання цифрової доступності та безбар’єрності*** передбачають перевірку сайтів, форм, документів, сервісів на предмет наявності цифрових бар’єрів, а також документування порушень і формування рекомендацій щодо їх усунення.

6. ***Процедури формування висновків і рекомендацій*** передбачають узагальнення результатів аудиту, встановлення причин бар’єрів, визначення пріоритетності заходів і формування рекомендацій. Цифрова підтримка полягає у створенні матриці «бар’єр → причина → наслідки → рекомендації → відповідальний виконавець → індикатор контролю».

7. ***Процедури оформлення результатів і комунікації*** передбачають

підготовку звіту, аналітичних довідок, панелей показників, а також презентацію результатів керівництву. Важливим елементом є стандартність структури подання результатів та чіткість управлінських формулювань.

8. Процедури контролю виконання рекомендацій і моніторингу змін передбачають створення плану заходів, контроль виконання, повторні вимірювання індикаторів і підтвердження усунення бар'єрів. Цифрові інструменти дозволяють вести реєстр рекомендацій, статуси виконання, докази виконання та моніторингові показники (табл. 13.16).

Таблиця 13.16

Аудиторські процедури інклюзивного аудиту та їх цифрові інструменти

Процедура	Мета	Цифрові інструменти	Результат процедури
Визначення об'єкта, меж і критеріїв аудиту	Установити, що саме підлягає оцінюванню, які групи персоналу та стейкхолдерів охоплюються, які критерії і показники застосовуються	Електронні сховища документів; спільні робочі простори; шаблони критеріїв і чек-листів; електронні форми узгодження периметра аудиту	Затверджений периметр аудиту, набір критеріїв і показників інклюзивності, перелік об'єктів перевірки
Формування програми аудиту та плану процедур	Сформувати послідовність процедур, перелік доказів і відповідальних, визначити форми робочих документів аудитора	Шаблони програми аудиту; системи управління завданнями; електронні чек-листи; таблиці планування у Word або Excel	Програма інклюзивного аудиту, робочі документи аудитора, календар процедур і контрольних точок
Ідентифікація джерел інформації та формування інформаційної бази	Забезпечити повноту і системність інформації для оцінювання інклюзивності за рішеннями, процесами і результатами	Інструменти експорту і завантаження даних; конектори; реєстри звернень; платформи опитувань; журнали подій; корпоративні сховища даних	Сформований перелік джерел і наборів даних, підтверджені витяги з систем, структурована інформаційна база аудиту
Перевірка якості та придатності аудиторської інформації	Оцінити повноту, узгодженість, достовірність і актуальність даних, визначити обмеження використання та режим доступу	Правила контролю якості даних; інструменти очищення і валідації; фіксація змін; засоби розмежування доступу; маскування даних	Підтверджена придатність даних, протокол перевірки якості, перелік обмежень використання і ризиків даних

Аналіз управлінських рішень та їх процедурності	Перевірити, чи забезпечують процедури підготовки та ухвалення рішень прозорість, обґрунтування, залучення та оцінку наслідків для різних груп	Системи електронного документообігу; робочий потік; журнал версій; аналітика маршрутів погодження; реєстр рішень	Висновки щодо якості процедур прийняття рішень, перелік виявлених процедурних бар'єрів, пропозиції коригувальних заходів
Оцінювання інклюзивності процесів і виявлення «вузьких місць»	Встановити, як процеси реально функціонують, де виникають затримки, відмови і «точки випадання», що створюють бар'єри участі	Процес-майнінг; аналіз подій; моделювання процесів; аналітика часу виконання; BI для процесних показників	Карта фактичного процесу, перелік «вузьких місць», опис бар'єрних етапів та їх проявів для різних груп
Аналіз звернень, скарг і текстових даних	Виявити повторювані проблеми доступу і участі, отримати сигнали бар'єрів, що не відображені у регламентах	CRM звернень; категоризація причин; тематичний аналіз текстів; аналітика чат-ботів; BI-звіти за зверненнями	Типологія бар'єрів за зверненнями, частотність причин, перелік критичних тем та підтверджені висновки
Оцінювання цифрової доступності та безбар'єрності	Встановити наявність цифрових бар'єрів у сайтах, формах, документах і сервісах та обґрунтувати заходи їх усунення	Сканери доступності; ручне сценарне тестування; перевірка доступності документів; протоколи аудиту доступності	Перелік порушень доступності, пріоритезація виправлень, рекомендації щодо безбар'єрних цифрових рішень
Розрахунок індикаторів інклюзивності та узагальнення результатів	Систематизувати дані, розрахувати індикатори, визначити відхилення та сформувати узагальнений профіль інклюзивності	BI-платформи; аналітичні таблиці; інструменти статистичної обробки; шаблони профілю інклюзивності	Профіль інклюзивності організації або підрозділу, інтерпретація відхилень, карта проблемних зон
Формування рекомендацій та плану коригувальних заходів	Перетворити виявлені бар'єри на конкретні управлінські дії з визначенням відповідальних, строків і показників контролю	Матриця «бар'єр → причина → наслідок → рекомендація»; системи управління завданнями; процес узгодження заходів	План заходів з усунення бар'єрів, реєстр рекомендацій, визначені індикатори контролю та відповідальні
Оформлення результатів аудиту та комунікація висновків	Подати результати у стандартизованій формі та забезпечити їх зрозумілість для керівництва і відповідальних підрозділів	Шаблони звіту; дашборди; презентаційні матеріали; електронні підписи та маршрути затвердження	Звіт за результатами інклюзивного аудиту, аналітичні довідки, дашборд інклюзивності, протокол узгодження

Контроль виконання рекомендацій і моніторинг змін	Відстежити впровадження заходів і підтвердити ефект змін за індикаторами інклюзивності	Системи управління завданнями; реєстр рекомендацій; сховища доказів виконання; моніторингові панелі у BI	Звіт про виконання рекомендацій, підтвердження усунення бар'єрів, динаміка індикаторів і підстава для повторних перевірок

Результати інклюзивного аудиту оформлюються у вигляді взаємопов'язаного комплексу документів і цифрових продуктів:

- *робочі документи аудитора* (програма аудиту, чек-листи, протоколи перевірки, витяги з систем, узагальнення звернень, таблиці індикаторів);
- *матриця бар'єрів і рекомендацій* (ключовий практичний інструмент: бар'єр, групи, яких стосується, джерела підтвердження, причина, наслідки, рекомендація, пріоритет, відповідальні, індикатор контролю);
- *аналітичний звіт за результатами аудиту* (структурований текст з висновками й рекомендаціями);
- *BI-дашборд або профіль інклюзивності* (візуалізація індикаторів, зон ризику і динаміки);
- *план заходів і реєстр виконання* (дисципліна впровадження рекомендацій і підзвітність).

Цифровий формат робочих документів, які використовуються в процесі інклюзивного аудиту, представлений в таблиці 13.17.

Таблиця 13.17

Зміст та цифровий формат робочих документів, які використовуються в процесі інклюзивного аудиту

Документ	Що фіксує	Цифровий формат
Наказ або розпорядження про проведення інклюзивного аудиту	Підстави, мету, об'єкт і межі аудиту, склад групи, повноваження, строки та порядок взаємодії	Електронний документ у системі документообігу з електронним підписом; реєстраційний запис у DMS
Технічне завдання або робоче завдання на аудит	Перелік завдань, критерії, очікувані результати, обмеження доступу до даних, вимоги до звітування	Шаблон Word у спільному сховищі; картка завдання у системі управління проєктами або робочому потоці
Матриця критеріїв і показників інклюзивності	Критерії оцінювання, індикатори, джерела даних, порогові значення та правила інтерпретації	Таблиця у Excel або Google Sheets; довідник показників у BI; прикріплений файл у робочій справі аудиту

Програма інклюзивного аудиту і план процедур	Перелік процедур, послідовність виконання, джерела доказів, відповідальні, контрольні точки	Шаблон Word або Excel; календар у корпоративній системі; задачі у системі управління завданнями
Реєстр джерел аудиторської інформації та витягів з систем	Перелік джерел даних, способи отримання, дати витягів, параметри вибірки, опис наборів даних	Електронний реєстр у Excel; метадані у сховищі даних; посилання на файли у структурованій папці аудиту
Протокол перевірки якості і придатності даних	Результати перевірки повноти, узгодженості, достовірності, актуальності; обмеження використання даних; ризики даних	Форма протоколу у Word або електронна форма; журнал перевірок у системі якості даних
Чек-листи аудиторських процедур	Виконання конкретних перевірок за критеріями, фіксацію виконаних кроків, відмітки щодо відповідності та зауваження	Електронні чек-листи у Word або Forms; контрольні списки у системі задач; записи у робочій справі аудиту
Протоколи інтерв'ю, фокус-груп і спостережень	Факти і свідчення щодо практики процесів, досвіду доступу й участі, приклади бар'єрів та пояснення причин	Електронні протоколи у Word; записи з дотриманням конфіденційності у захищеному сховищі; узагальнення у базі кейсів
Зведення звернень і скарг та їх категоризація	Тематику, причини, повторюваність звернень, канали надходження, строки реагування, результати розгляду	Звіт із CRM звернень; аналітична таблиця; BI-зріз за зверненнями; експортовані витяги з системи
Результати процесної аналітики і карти «вузьких місць»	Фактичні маршрути процесів, затримки, повтори, відмови, точки «випадання»; сегментацію за групами та каналами	Звіти процес-майнінгу; схеми процесів; аналітичні файли; скріншоти або експорти графів з інструментів
Протокол оцінювання цифрової доступності	Перелік порушень доступності, докази недоступності, пріоритетність виправлень, рекомендації щодо усунення бар'єрів	Звіт сканера доступності; протокол ручного тестування; таблиця порушень; прикріплені докази
Матриця бар'єрів, причин, наслідків і рекомендацій	Виявлені бар'єри, групи, яких вони стосуються, джерела підтвердження, причини, наслідки, рекомендації, пріоритетність та індикатори контролю	Таблиця у Word або Excel; реєстр рекомендацій у системі задач; зв'язок з BI-показниками
Проєкт звіту за результатами інклюзивного аудиту	Узагальнені висновки, оцінку рівня інклюзивності, опис бар'єрів, рекомендації та план заходів	Шаблон звіту у Word; електронне погодження і версійність у DMS; контроль змін
Дашборд або профіль інклюзивності	Індикатори інклюзивності, відхилення, проблемні зони, динаміку показників і контрольні орієнтири	BI-дашборд; інтерактивний звіт; експорт у PDF для додатків до звіту

Реєстр виконання рекомендацій і план моніторингу	Заходи, відповідальних, строки, статуси виконання, підтвердження виконання та повторні вимірювання показників	Система управління завданнями; робочий потік; таблиця контролю; посилання на докази виконання у сховищі

Структура підсумкового звіту інклюзивного аудиту визначає, наскільки результати перевірки є зрозумілими, відтворюваними та придатними для управлінського використання. У навчальній і практичній площині важливо, щоб звіт не зводився до опису проблем, а містив логічний ланцюг «критерій → дані → висновок → бар'єр → причина → наслідок → рекомендація → контроль». Такий підхід забезпечує прозорість аудиторських висновків, дає змогу перевірити їх на підставі зафіксованих джерел, а також переводить результати аудиту в площину конкретних дій та моніторингу змін. Типова структура підсумкового звіту інклюзивного аудиту може бути подана у вигляді такого міні-шаблону.

Міні-шаблон підсумкового звіту інклюзивного аудиту має такий вигляд:

1. Загальні положення: назва аудиту, замовник, виконавці, підстава проведення, коротка характеристика об'єкта аудиту.

2. Мета, об'єкт і периметр аудиту: формулювання мети; опис меж аудиту; перелік охоплених процесів, підрозділів, каналів взаємодії; групи персоналу і стейкхолдерів, щодо яких здійснювалося оцінювання.

3. Критерії та методи інклюзивного аудиту: критерії інклюзивності, індикатори та логіка їх інтерпретації; перелік застосованих методів і процедур (аналіз документів і даних, інтерв'ю, опитування, процесна аналітика, аналіз звернень, оцінювання цифрової доступності тощо).

4. Джерела аудиторської інформації та обмеження даних: перелік використаних джерел (документи, реєстри, HR-дані, звернення і скарги, опитування, аналітика цифрових каналів, результати тестів доступності); оцінка придатності даних; зазначення обмежень використання і аспектів конфіденційності.

5. Ключові висновки щодо рівня інклюзивності: узагальнена оцінка результатів; основні сильні сторони; проблемні зони; короткий опис найбільш

суттєвих відхилень від цільових орієнтирів або очікуваних стандартів.

6. Ідентифіковані бар'єри та їх причини: опис виявлених бар'єрів за типами (процедурні, організаційні, кадрові, комунікаційні, культурні, інфраструктурні, цифрові); пояснення причин виникнення бар'єрів із посиланням на підтверджувальні джерела.

7. Оцінювання наслідків бар'єрів: характеристика наслідків для персоналу, стейкхолдерів і організації; ризики, які формуються внаслідок бар'єрів (втрата доступу, зниження участі, погіршення якості взаємодії, репутаційні ризики, конфлікти та інше).

8. Рекомендації та пріоритизація заходів: перелік рекомендацій із уточненням, який бар'єр усувається, який очікуваний результат, які ресурси і умови потрібні; визначення пріоритетів (критичні, першочергові, середньострокові).

9. План заходів і відповідальні виконавці: заходи, відповідальні виконавці, строки, контрольні точки, необхідні ресурси; формат контролю виконання і підтверджувальні матеріали виконання.

10. Індикатори моніторингу та порядок контролю змін: перелік індикаторів для відстеження динаміки після впровадження рекомендацій; періодичність моніторингу; відповідальні за збір і аналіз; формат представлення результатів (наприклад, дашборд, аналітична довідка).

11. Додатки: програма аудиту, чек-листи, протоколи інтерв'ю і спостережень, таблиці індикаторів, узагальнення звернень і скарг, результати процесної аналітики, результати тестів цифрової доступності, інші підтверджувальні матеріали.

Отже, застосування аудиторських процедур і належне оформлення результатів інклюзивного аудиту з використанням цифрових інструментів забезпечують перехід від фіксації окремих фактів до системного управлінського висновку. Цифрова підтримка підсилює доказовість і відтворюваність перевірки, дозволяє структурувати інформацію за об'єктами аудиту та пов'язати виявлені бар'єри з їх причинами, наслідками і відповідними рекомендаціями.

13.4. Контрольні питання для самоперевірки

1. Що розуміють під інклюзивним аудитом і в чому полягає його відмінність від інших видів аудиту?

2. Які вектори охоплює інклюзивний аудит та що саме підлягає перевірці в кожному випадку?

3. Яка мета інклюзивного аудиту організації та які основні завдання він вирішує?

4. Які вимоги висуваються до якості та придатності аудиторської інформації для проведення інклюзивного аудиту?

5. Які основні джерела аудиторської інформації використовуються в інклюзивному аудиті та яку роль відіграють цифрові канали комунікації?

6. Які групи цифрових технологій застосовуються в інклюзивному аудиті та яке їх призначення на різних етапах роботи з даними?

7. У чому полягає призначення технологій збору та фіксації аудиторської інформації для проведення інклюзивного аудиту?

8. Які завдання виконують технології інтеграції та підготовки даних і чому вони критично важливі для формування обґрунтованих висновків інклюзивного аудиту?

9. У чому полягає оцінювання цифрової інклюзивності?

10. Які аналітичні продукти можуть бути сформовані засобами бізнес-аналітики та візуалізації за результатами інклюзивного аудиту?

11. Які обов’язкові елементи має містити підсумковий звіт інклюзивного аудиту, щоб забезпечити його управлінську корисність?

12. Які робочі документи аудитора формують доказову базу інклюзивного аудиту та які вимоги до їх оформлення в цифровому середовищі?

13. Які принципи пріоритезації рекомендацій доцільно застосовувати за результатами інклюзивного аудиту?

14. Як організовується контроль виконання рекомендацій інклюзивного аудиту та які індикатори використовуються для відстеження результатів їх впровадження?

15. Які ризики виникають під час використання цифрових технологій в інклюзивному аудиті та як їх мінімізувати?

16. Як результати інклюзивного аудиту можуть бути інтегровані в систему управління організацією?

Розділ 14

ПРАКТИКУМ З ЦИФРОВИХ ТЕХНОЛОГІЙ В АУДИТІ ТА ФІНАНСОВІЙ БЕЗПЕЦІ БІЗНЕСУ (КЕЙСИ)

РОЗДІЛ 14. КЕЙСИ

14.1. Кейси з цифрової трансформації бізнес-процесів, технологічних трендів та реінжинірингу

Ситуаційне завдання 1. Погодження і оплата рахунків постачальників

Умова.

Компанія має близько 250 працівників і щотижня отримує приблизно 40-60 рахунків від постачальників. Рахунки надходять на спільну електронну пошту.

Бухгалтер роздруковує рахунки і передає їх керівникам підрозділів на погодження. Часто в рахунках немає номера договору або замовлення. Інколи підрозділ відповідає, що рахунок не стосується його, і документ повертається на уточнення.

Через затримки постачальники зупиняють поставки і нараховують пеню. Керівництво хоче оплачувати вчасно і зберегти контроль за погодженням.

Завдання.

1. Опишіть поточний процес від отримання рахунку до оплати і закриття документів.
2. Запропонуйте простий покращений процес з електронним погодженням і правилами повернення рахунку на доопрацювання.
3. Запропонуйте ліміти погодження за сумою і порядок ескалації для термінових рахунків.

Ситуаційне завдання 2. Обробка звернень клієнтів і дотримання сервісних строків

Умова.

Сервісна компанія обслуговує 120 корпоративних клієнтів. Звернення надходять через електронну пошту, телефон і месенджери.

Частина звернень дублюється або втрачається. Агенти відповідають у міру завантаження, а пріоритет часто визначається наполегливістю клієнта. Деякі заявки залишаються без відповідального, бо незрозуміло, кому їх передати.

У результаті строки обслуговування порушуються, і клієнти спрямовують свої скарги безпосередньо керівництву.

Завдання.

1. Опишіть, як зараз проходить звернення від отримання до закриття і де виникає втрата контролю.
2. Запропонуйте єдиний реєстр звернень і правила розподілу між виконавцями.
3. Визначте чотири рівні пріоритету від 1 до 4 і для кожного встановіть час першої відповіді та цільовий час вирішення.
4. Розподіліть ролі: хто приймає звернення, хто виконує, хто контролює строки і кого інформують про критичні випадки.
5. Визначте показники для моніторингу, наприклад час першої відповіді час вирішення кількість відкритих заявок і частка скарг.

Ситуаційне завдання 3. Управління запасами і поверненнями на складах

Умова.

Торгова компанія має чотири склади. Продавці скаржаться, що немає попиту на товари, а фінансовий директор вважає, що занадто багато товарно-матеріальних цінностей знаходиться на складі.

Інвентаризація раз на квартал виявляє нестачі, списання зростають. Закупівлі здійснюються без чіткого прогнозу. Частина товару повертається від клієнтів, але повернення не завжди фіксуються в системі вчасно.

Завдання.

1. Опишіть основні кроки руху товару і документів від закупівлі до відвантаження та повернення.
2. Запропонуйте просту сегментацію товарів за важливістю і передбачуваністю попиту та поясніть, як її використати для поповнення.
3. Запропонуйте правила поповнення запасів на основі точки замовлення і страхового запасу.

Ситуаційне завдання 4. Організація закупівель і контроль витрат поза процедурою

Умова.

У компанії немає набору стандартних технічних завдань для типових закупівель. Кожен підрозділ описує потребу по-своєму, тому вимоги часто неповні.

Тендери інколи запускають повторно через уточнення. Погодження контрактів затягується, юристи перевантажені дрібними правками. У підсумку підрозділи роблять термінові закупівлі напряму у знайомих постачальників, а відділ закупівель дізнається про це після оплати.

Завдання.

1. Побудуйте коротку карту процесу закупівель від заявки до оплати і визначте три вузькі місця.
2. Запропонуйте стандартизацію, шаблони технічних завдань, каталог типових позицій і спрощені закупівлі до ліміту.
3. Запропонуйте, як зменшити закупівлі поза процедурою без зупинки роботи бізнесу.
4. Назвіть ключові ризики і базові контролі.

Ситуаційне завдання 5. Вузьке місце на виробничій лінії та стабільність плану

Умова.

На дільниці є одна виробнича лінія, яка обробляє найбільший потік замовлень. Планування часто змінює пріоритети, тому лінію переналаштовують від шести до восьми разів на день.

Через поспіх зростає брак. Технічне обслуговування виконують переважно після поломок. Начальник цеху хоче стабільний план, а комерційний підрозділ просить гнучкість для клієнта.

Завдання.

1. Визначте, що є вузьким місцем і які втрати виникають через часті переналаштування і простої.
2. Запропонуйте заходи, щоб скоротити час переналаштування і перейти до планового технічного обслуговування.
3. Поясніть, як оцінити фінансовий ефект від зменшення простою і браку та які дані для цього потрібні.

Ситуаційне завдання 6. Хмарна міграція ERP і вимоги до SLA

Умова.

Для забезпечення віддаленого доступу і зменшення витрат на інфраструктуру ТОВ «Орбіта-Трейд» переносить ERP та бухгалтерський контур у хмарний сервіс (SaaS). Після запуску виявилося:

- у договорі з провайдером нечітко описані вимоги до резервного копіювання та відновлення;
- відсутній план виходу і сценарій міграції до іншого провайдера;
- під час закриття місяця стався збій доступу до сервісу на 6 годин, через що зірвано дедлайн управлінської звітності;
- аудитору надали доступ лише до вивантажень, але не до журналів змін у системі.

Завдання.

1. Визначте, що в цьому кейсі є оцифруванням, цифровізацією, а що – цифровою трансформацією.
2. Складіть карту ризиків.
3. Запропонуйте умови договору.
4. Опишіть мінімальний набір доказів, які повинен отримати аудитор для оцінки ІТ-контролів хмарної системи.
5. Запропонуйте 2 KPI цифровізації для фінансового контуру та поясніть, як їх вимірювати.

Ситуаційне завдання 7. Big Data моніторинг транзакцій і Data Governance

Умова.

Фінансова компанія «ПраймПей» запровадила аналітику Big Data для моніторингу транзакцій у режимі near real-time та виявлення аномалій. Через 2 місяці роботи системи служба комплаєнсу отримала 1 200 «червоних прапорців» за тиждень, але частина сигналів виявилася хибною. Додаткові дані:

- у різних джерелах даних різні довідники контрагентів (дублікати, різні ідентифікатори);
- немає формалізованої політики доступу до датасетів;
- аудитору не можуть пояснити походження окремих полів.

Завдання.

1. Визначте 2-5 ключових ризиків data-driven процесу.
2. Запропонуйте матрицю доказовості для аудиту: які джерела, логи чи вивантаження потрібні для підтвердження цілісності даних і коректності аналітики.
3. Сформуйте набір аналітичних тестів, які аудитор може застосувати для перевірки аномалій.
4. Запропонуйте 2 показники якості системи моніторингу.

Ситуаційне завдання 8. RPA у бухгалтерії і контроль змін

Умова.

У компанії «ЕкоЛогістик» RPA-бот обробляє рахунки постачальників, тобто зчитує реквізити, звіряє з договором, формує проведення та готує платіж на погодження. Після невеликого оновлення бота:

- з'явилися масові помилки у проведеннях (не ті рахунки обліку для частини витрат);
- журнал виконання (лог) містить лише статус «успіх чи помилка», без деталізації кроків;
- доступ до налаштувань бота має один адміністратор без незалежного погодження.

Завдання.

1. Визначте, які IT-ризики тут проявилися, і зіставте їх із відповідними контролями.
2. Запропонуйте процедуру Change Management для RPA.
3. Складіть перелік аудиторських процедур для оцінки надійності RPA-контролю.
4. Запропонуйте 3 KPI ефективності RPA-процесу.

Ситуаційне завдання 9. IoT дані в обліку і контроль достовірності

Умова.

Виробнича компанія «МеталПром» встановила IoT-датчики на обладнанні та складах. Дані сенсорів автоматично формують первинні документи (випуск

продукції, списання сировини), а інформація в режимі реального часу відображається в обліку. Під час проведення аудиту виявлено:

- різкі стрибки показників випуску продукції у вихідні дні;
- відсутній регламент калібрування та перевірки точності датчиків;
- IoT-мережа працює в тій самій мережевій зоні, що й офісні ПК.

Завдання.

1. Визначте ризики використання IoT у первинному обліку та аудиті.
2. Запропонуйте контрольні заходи для забезпечення достовірності.
3. Складіть план аудиторської перевірки IoT-даних як доказів.
4. Запропонуйте KPI, які покажуть ефект від IoT для фінансового контуру.

Ситуаційне завдання 10. Реінжиніринг процесу Order to Cash

Умова.

Компанія «МаркетХаб» вирішила перейти від функціональної моделі (продажі, логістика, бухгалтерія «окремо») до процесної моделі та реінжинірингу end-to-end процесу «від замовлення до грошей». Компанією планується:

- створити крос-функціональну команду та роль власника процесу;
- автоматизувати узгодження і документообіг;
- перейти на data-driven дашборди для контролю дебіторської заборгованості.

Частина персоналу чинить опір, а керівництво хоче швидкого ефекту без зміни регламентів.

Завдання.

1. Опишіть цільову модель процесу (AS-IS → TO-BE) на рівні кроків і контрольних точок.
2. Запропонуйте RACI або розподіл ролей та визначте ключові відповідальності.
3. Складіть план управління змінами.
4. Запропонуйте KPI для оцінки результативності реінжинірингу.

Ситуаційне завдання 11. Компрометація облікового запису і контроль доступів

Умова.

У компанії «ФінСервіс-ЮА» погодження платежів відбувається дистанційно в електронному кабінеті. Після фішингової атаки було скомпрометовано обліковий запис менеджера, і зловмисник ініціював 3 платежі на нових контрагентів. Частину операцій встигли провести, частину – заблокували. В ході службового розслідування виявлено:

- MFA увімкнено не для всіх ролей;
- права доступу надто широкі (одна роль може і створювати, і погоджувати);
- журнал аудиту подій не переглядається регулярно.

Завдання.

1. Складіть перелік термінових дій реагування (перші 24 години) і подальших дій (до 30 днів).
2. Запропонуйте пакет контролів доступу.
3. Оцініть вплив інциденту на облік і аудит, які твердження фінансової звітності стають ризиковими, та які додаткові процедури потрібні.

Ситуаційне завдання 12. API інтеграції систем і контроль цілісності даних

Умова.

Компанія використовує CRM, складську систему та бухгалтерський модуль, які інтегровані через API. Після оновлення інтеграції:

- частина продажів потрапляє в облік двічі;
- частина документів «зникає» між системами;
- немає моніторингу помилок інтеграції та регулярної звірки контрольних сум.

Завдання.

1. Визначте 4 причини збоїв інтеграції.
2. Запропонуйте контролі цілісності інтеграцій.
3. Складіть аудиторські процедури для перевірки повноти й унікальності відображення продажів у фінансовому обліку.
4. Запропонуйте KPI для моніторингу інтеграцій.

Ситуаційне завдання 13. Ефект цифровізації фінансової функції та KPI

Умова.

Керівник підприємства просить показати вимірюваний ефект цифровізації (ERP + RPA + електронний документообіг). Є дані до і після впровадження.

- Тривалість закриття звітного періоду (місяця) скоротилася з 8 до 2 днів.
- Рівень автоматизації операцій зріс із 35 % до 78 %.
- Кількість помилок на 1000 операцій зменшилася з 7 до 1,2.
- Середній час обробки рахунку постачальника скоротився з 45 до 9 хвилин.

Керівництво сумнівається, чи достатньо цього, і просить план наступних кроків.

Завдання.

1. Розрахуйте відносне покращення кожного KPI (у %), інтерпретуйте результат.
2. Визначте, які 2 додаткові KPI слід додати для балансу.
3. Сформулюйте короткий управлінський висновок (що вдалося, де залишилися ризики, які пріоритети наступного кварталу).
4. Запропонуйте план дій для переходу до більш зрілої моделі.

14.2. Кейси з моделювання та оптимізації бізнес-процесів в обліку та аудиті

Ситуаційне завдання 1. Аналіз процесу формування первинних документів

Умова.

На підприємстві ТОВ «АгроПак» процес оформлення первинних документів з постачальниками побудований за функціональним принципом. Закупівлі, склад, бухгалтерія та фінансовий відділ працюють окремо. Аудитор виявив часті затримки в оформленні актів і накладних, дублювання інформації та розбіжності між даними складу і бухгалтерського обліку.

Завдання.

1. Опишіть недоліки функціонального підходу в організації цього процесу.
2. Визначте ключові етапи процесу, які доцільно відобразити в процесній моделі.
3. Поясніть, як процесно-орієнтована модель допоможе аудитору систематизувати інформацію.
4. Запропонуйте, яку методологію моделювання доцільно використати (BPMN, IDEF0 або EPC) і чому.

Ситуаційне завдання 2. Моделювання процесу обліку витрат

Умова.

Підприємство «ЕнергоСервіс» веде облік витрат за центрами відповідальності, однак відсутній єдиний опис процесу формування витрат – від ініціювання до відображення у звітності. Це ускладнює аудит та аналіз відхилень.

Завдання.

1. Обґрунтуйте доцільність процесного опису обліку витрат.
2. Визначте елементи процесної моделі, які мають бути включені.
3. Поясніть роль процесної моделі у виявленні неефективних етапів.
4. Запропонуйте, на якому рівні деталізації модель буде найбільш корисною для аудитора.

Ситуаційне завдання 3. Процес внутрішнього контролю як об'єкт моделювання

Умова.

На підприємстві внутрішній контроль існує формально: затвердження операцій і перевірки виконуються, але не задокументовані як процес. Через це аудитор не може чітко визначити контрольні точки.

Завдання.

1. Поясніть, чому внутрішній контроль доцільно розглядати як процес.
2. Визначте, які контрольні точки слід відобразити в процесній моделі.
3. Опишіть, як процесна модель впливає на формування аудиторського судження.

Ситуаційне завдання 4. Використання BPMN у роботі аудитора

Умова.

Аудиторська фірма планує стандартизувати підхід до опису типових процесів клієнтів (облік доходів, витрат, розрахунків). Розглядається використання BPMN.

Завдання.

1. Поясніть, у чому переваги BPMN для моделювання обліково-аудиторських процесів.
2. Які елементи BPMN є найбільш корисними для аудитора?
3. Наведіть приклади управлінських рішень, які можуть ґрунтуватися на BPMN-моделях.

Ситуаційне завдання 5. Аналіз вузьких місць у процесі обліку

Умова.

Процес обробки первинних документів у ТОВ «ЛайтПро» займає в середньому 18 днів, що негативно впливає на управлінську звітність. Керівництво очікує рекомендацій від аудитора.

Завдання.

1. Поясніть, як процесний аналіз допомагає виявити вузькі місця.
2. Які дані необхідні для такого аналізу?

3. Опишіть, як результати моделювання можуть бути використані для оптимізації процесу.

Ситуаційне завдання 6. Рівні опису процесів у аудиті

Умова.

Аудитор отримав загальну карту процесів підприємства, але вона не дозволяє визначити конкретні аудиторські процедури.

Завдання.

1. Поясніть різницю між загальним, аналітичним і операційним рівнями процесного опису.
2. Визначте, який рівень є критичним для планування аудиторських процедур.
3. Обґрунтуйте необхідність переходу між рівнями моделювання.

Ситуаційне завдання 7. Інтеграція процесних результатів в управлінські рішення

Умова.

За результатами процесного аналізу аудитор виявив надмірну кількість погоджень у процесі закупівель, що збільшує строки та витрати.

Завдання.

1. Поясніть, як результати процесного моделювання трансформуються в управлінські рішення.
2. Яка роль аудитора у цьому процесі?
3. Наведіть приклади можливих управлінських змін.

Ситуаційне завдання 8. Обмеження процесного підходу

Умова.

Керівництво підприємства вимагає «формально описати всі процеси», не плануючи змінювати практику роботи.

Завдання.

1. Визначте ризики формального застосування процесних моделей.
2. Поясніть умови, за яких процесне моделювання буде ефективним.
3. Яку роль відіграє організаційна культура?

Ситуаційне завдання 9. Вибір програмного засобу для моделювання

Умова.

Аудиторська фірма обирає програмний засіб для моделювання процесів клієнтів між універсальним BPMN-редактором і корпоративною BPM-платформою.

Завдання.

1. Визначте критерії вибору програмного засобу для аудитора.
2. Поясніть, коли достатньо простого BPMN-інструмента.
3. Обґрунтуйте, у яких випадках доцільні інтегровані платформи.

Ситуаційне завдання 10. Узагальнення процесного підходу в аудиті

Умова.

Аудитор готує підсумковий звіт для керівництва клієнта щодо впровадження процесно-орієнтованого підходу.

Завдання.

1. Сформулюйте ключові переваги процесного підходу для обліку та аудиту.
2. Поясніть його значення для якості управлінських рішень.
3. Обґрунтуйте логічний зв’язок між моделюванням і оптимізацією процесів.

14.3. Кейси з цифрової трансформації аудиту

Ситуаційне завдання 1. Електронні документи, КЕП та доказовість операцій

Умова.

Підприємство перейшло на електронний документообіг. Договори і акти підписують кваліфікованим електронним підписом. Документи зберігають у хмарному архіві.

Під час аудиту з'ясувалося, що частина документів має лише 1 підпис. У системі немає зрозумілої історії версій. Журнали подій зберігаються 60 днів. Частину актів сформували із запізненням і завантажили заднім числом.

Завдання.

1. Визначте ризики для аудиторських доказів, пов'язаних із автентичністю та незмінністю електронних документів.
2. Складіть перелік доказів, які аудитор має отримати для підтвердження юридичної значущості і простежуваності.
3. Запропонуйте вимоги до архівування і зберігання електронних доказів.
4. Складіть план аудиторських процедур для перевірки електронних документів як джерела доказів.

Ситуаційне завдання 2. Перехід від перевірки результату до перевірки процесу

Умова.

Керівництво клієнта очікує, що аудитор підтвердить не лише фінансову звітність, а й надійність цифрових процесів, які формують показники. У компанії діють автоматичні правила, маршрути погодження, системні блокування та контрольні звіти.

Аудитор бачить, що частина контролів працює автоматично, але описів контролів немає. Власники процесів не можуть пояснити, які саме правила в системі блокують помилки.

Завдання.

1. Поясніть, як змінюється фокус аудиту у цифровому середовищі, коли зростає роль IT-контролів і контрольних звітів.
2. Складіть перелік елементів внутрішнього контролю і IT-контролів, які треба оцінити першочергово.

3. Запропонуйте, які докази має зібрати аудитор, щоб підтвердити роботу автоматичних контролів.
4. Складіть приклад структури робочого документа, який фіксує оцінювання цифрового процесу як джерела доказів.\

Ситуаційне завдання 3. Інтеграції між системами і ризик втрати або дублювання даних

Умова.

Компанія продає через сайт і маркетплейс. Оплати приймає через платіжного провайдера. Дані потрапляють у бухгалтерський модуль через інтеграцію.

Після оновлення інтеграції частина продажів відображається двічі. Частина оплат є у провайдера, але не потрапила в облік. Немає регулярної звірки контрольних сум і немає сповіщень про помилки інтеграції.

Завдання.

1. Визначте причини збоїв інтеграції на рівні даних і процесу.
2. Запропонуйте контролі цілісності інтеграцій і моніторингу помилок.
3. Складіть аудиторські процедури для перевірки повноти й унікальності відображення продажів і оплат у фінансовому обліку.
4. Запропонуйте 2 KPI для постійного контролю стабільності інтеграції.

Ситуаційне завдання 4. Якість даних як умова суцільного аналізу

Умова.

Аудитор отримав вивантаження з ERP, банку і складської системи для суцільного аналізу транзакцій за рік.

Під час первинного огляду виявлено, що частина контрагентів дублюється через різні назви. У частині записів відсутній код підрозділу. У довідниках різні коди номенклатури. Є повторні завантаження, через які дублюються рядки.

Завдання.

1. Розподіліть виявлені проблеми за критеріями якості даних, зокрема повнота, точність, своєчасність, узгодженість, унікальність.
2. Запропонуйте процедури перевірки якості даних перед аналізом.
3. Сформулюйте критерії прийнятності масиву для старту суцільного аналізу.

4. Запропонуйте, як задокументувати підготовку даних так, щоб аналіз можна було відтворити і перевірити.

Ситуаційне завдання 5. Контроль доступів і журналювання змін у хмарній ERP з оцінкою впливу

Умова.

Підприємство веде облік у хмарній ERP. У системі 52 активні користувачі та 12 ролей.

Під час попереднього огляду доступів встановлено:

- 8 користувачів мають роль, що дозволяє створювати і затверджувати платіжні доручення;
- 15 користувачів входять без MFA;
- 4 звільнені співробітники залишаються активними 21, 24, 33 і 46 днів після дати звільнення;
- За квартал у довіднику контрагентів виконано 1 240 змін. Із них 310 змін не мають заявки або погодження.

Окремо зафіксовано 45 змін банківських реквізитів постачальників. Із цих 45 змін 7 виконані без другого погодження.

За квартал проведено 1 980 платежів на суму 86 400 000 грн. Платежі, які створили і затвердили ті самі 8 користувачів, становлять 126 платежів на суму 9 600 000 грн.

Завдання.

1. Порахуйте % частку користувачів з конфліктом повноважень, % частку користувачів без MFA, та % частку змін довідника без заявки.
2. Визначте потенційний вплив на фінансову звітність, якщо 7 змін реквізитів без другого погодження призвели б до помилки оплати на 100% суми таких платежів. Врахуйте, що за цими 7 постачальниками було 18 платежів на суму 1 260 000 грн.
3. Порівняйте отриманий потенційний вплив з порогом суттєвості 1 200 000 грн і зробіть висновок, чи потрібно розширювати тестування деталей.

Ситуаційне завдання 6. Обмежений доступ до даних і віддалений перегляд

Умова.

Аудитор планує застосувати цифрові процедури, але політика клієнта забороняє копіювання даних на носії аудитора. Клієнт готовий надати лише віддалений перегляд екрану.

Частина звітів доступна лише як скріншоти. Вивантаження з ERP можна отримати лише у форматі PDF. Клієнт не дає доступ до журналів подій і журналу змін.

Завдання.

1. Складіть програму дій аудитора на етапі планування за таких обмежень.
2. Запропонуйте, як забезпечити відтворюваність і контрольованість цифрових процедур, якщо дані не можна експортувати.
3. Визначте, які альтернативні джерела доказів може використати аудитор замість повних вивантажень.
4. Запропонуйте, коли і як аудитор має розширити тестування деталей через обмеження доступу.

Ситуаційне завдання 7. Робочі документи аудитора і цифровий слід процедур

Умова.

Команда аудитора застосовує аналітику даних і формує робочі файли з запитами, правилами відбору та контрольними звітами.

Під час внутрішнього огляду якості виявлено, що в робочих файлах немає опису джерел даних і параметрів відбору. Версії запитів не збережені. Результати неможливо відтворити. Немає зв’язку між відхиленням і конкретними рядками у регістрах.

Завдання.

1. Запропонуйте правила документування цифрових процедур і збереження цифрового сліду.
2. Складіть перелік обов’язкових реквізитів робочого документа для аналітичної процедури.
3. Запропонуйте, як забезпечити простежуваність від транзакції до показника звітності в робочих документах.

4. Визначте, які перевірки якості має виконувати керівник завдання перед завершенням етапу цифрових процедур.

Ситуаційне завдання 8. Обхід маршруту погодження, аналіз журналів подій і розрахунок рівня порушень

Умова.

У модулі закупівель діє маршрут погодження з 4 подіями в журналі:

- створення заявки;
- фінансовий контроль;
- затвердження керівником;
- оплата.

За квартал оформлено 3 200 заявок на закупівлю на суму 96 000 000 грн.

Аналіз журналу подій показав 220 заявок на суму 12 400 000 грн мають оплату до затвердження керівником.

Аналіз журналу подій показав 100 заявок на суму 4 700 000 грн не містять події фінансового контролю.

Аналіз журналу подій показав 40 заявок на суму 1 150 000 грн мають пропуски в журналі подій, немає 1 або 2 подій.

Внутрішній контроль визначив цільовий ліміт порушень маршруту 2 % за кількістю заявок.

Завдання.

1. Визначте % частку заявок з оплатою до затвердження та частку заявок без фінансового контролю.
2. Порахуйте відхилення від цільового ліміту 2 % у процентних пунктах для загальної частки порушень.
3. Обчисліть частку сум за порушеннями, окремо для 12 400 000 грн, 4 700 000 грн і 1 150 000 грн від загальної суми 96 000 000 грн.
4. Запропонуйте 6 дій для 3 ліній захисту, які мають знизити частку порушень до 2 % у наступному кварталі.

Ситуаційне завдання 9. Незалежність аудитора у цифрових проєктах і конфлікт інтересів

Умова.

Аудиторська фірма проводить обов'язковий аудит клієнта. Паралельно клієнт просить цю ж фірму налаштувати хмарну ERP, інтеграцію з банком і електронний документообіг.

Клієнт аргументує це тим, що команда швидше отримає потрібні дані і краще розумітиме процеси. Керівник завдання хвилюється, що після впровадження систем аудитору доведеться перевіряти власну роботу.

Завдання.

1. Поясніть, які загрози незалежності можуть виникнути, якщо аудитор бере участь у впровадженні систем, які потім перевіряє.
2. Запропонуйте запобіжні заходи для управління конфліктом інтересів.
3. Складіть приклад рішення керівника завдання щодо допустимості додаткових послуг і умов їх надання.
4. Визначте, які розкриття і внутрішні погодження потрібні в аудиторській фірмі до початку таких робіт.

Ситуаційне завдання 10. RPA-звірка банківських виписок з обліком і розрахунок рівня покриття контролю

Умова.

У клієнта працює програмний робот RPA, який щодня завантажує банківські виписки та звіряє їх із даними головної книги. За місяць було 22 робочі дні.

Фактичний стан за журналами виконання:

- робот коректно виконав звірку у 18 з 22 днів;
- у 4 дні звірка не виконалася, але у звіті стоїть статус «виконано».

Обороти за 4 дні, коли звірка не виконалася:

- день 1: 3 850 000 грн;
- день 2: 4 120 000 грн;
- день 3: 2 940 000 грн;
- день 4: 3 090 000 грн.

У ці 4 дні банк відобразив 36 комісій на суму 48 600 грн, які у головній книзі не проведені. Поріг суттєвості 400 000 грн.

Завдання.

1. Обчисліть у % рівень покриття RPA контролю за місяць як частку днів, коли звірка виконана коректно.
2. Визначте суму оборотів за дні, коли звірка не виконалась, та частку цієї суми від місячних оборотів 68 400 000 грн.
3. Розрахуйте суму невідображених у головній книзі банківських комісій 48 600 грн як частку від порогу суттєвості 400 000 грн.
4. Запропонуйте 8 аудиторських процедур для оцінки надійності RPA контролю і для перевірки повноти відображення банківських операцій за 4 дні.

Ситуаційне завдання 11. Конфіденційність робочих файлів аудитора і розрахунок рівня порушень політики

Умова.

Команда аудиту з 7 осіб працює віддалено. За 3 тижні створено 140 робочих файлів, із них 65 містять персональні дані.

Перевірка дотримання політики захисту даних показала:

- 3 з 7 ноутбуків без шифрування диска;
- 2 з 7 ноутбуків без MFA для корпоративного облікового запису;
- 18 з 140 файлів були передані через публічний файлообмінник;
- 9 з 65 файлів з персональними даними зберігалися на особистому диску співробітника.

Облікова політика фірми встановлює ліміти:

- 0 ноутбуків без шифрування;
- 0 ноутбуків без MFA;
- не більше 2% файлів через публічний файлообмінник;
- 0 файлів з персональними даними на особистих дисках.

Завдання.

1. Визначте % частку ноутбуків без шифрування та частку ноутбуків без MFA.
2. Обчисліть частку файлів, переданих через публічний файлообмінник, та порівняйте з лімітом 2%.

3. Складіть план реагування з 6 дій, який знижує порушення до лімітів, та визначте 5 постійних контролів для запобігання повторенню.

14.4. Кейси з нормативно-правового забезпечення цифрового аудиту

Ситуаційне завдання 1. Чинність КЕП і відкликаний сертифікат підписувача

Умова.

Підприємство перейшло на електронний обмін договорами та актами з постачальниками. Документи підписують кваліфікованим електронним підписом і зберігають у хмарному архіві.

За рік укладено 480 договорів. Під час попереднього огляду аудитори виявили такі обставини:

- 36 договорів підписані сертифікатом, який був відкликаний за 2 дні до дати підписання;
- 12 договорів підписані з одного носія ключа, який використовували кілька співробітників відділу постачання;
- у системі зберігаються журнали подій лише 90 днів, історія версій договорів не відображається.

Завдання.

1. Визначте ризики для доказовості електронних договорів за наведених умов.
2. Запропонуйте перелік доказів, які аудитор має отримати для підтвердження чинності підписів і незмінності документів.
3. Складіть план аудиторських процедур для перевірки таких договорів як джерел доказів.
4. Запропонуйте вимоги до управління ключами та доступами, які мають знизити ризик підписання чужим ключем.

Ситуаційне завдання 2. Обов’язкові реквізити електронних первинних документів

Умова.

Компанія формує первинні документи в системі електронного документообігу, а далі автоматично передає їх у бухгалтерську систему.

За квартал сформовано 1 200 актів виконаних робіт. Під час тестування вибірки виявлено такі проблеми:

- 84 акти не містять номера документа;

- 55 актів не містять дати складання;
- 43 акти містять лише ПІБ підписанта без посади і без зазначення підстав повноважень;
- 18 актів завантажені в архів із запізненням 20, 31, 45, 62 і 70 днів після фактичного виконання робіт.

Завдання.

1. Визначте, які з наведених недоліків прямо впливають на юридичну значущість та належність документа як аудиторського доказу.
2. Запропонуйте контрольні процедури в системі електронного документообігу, які мають запобігати відсутності обов'язкових реквізитів.
3. Складіть аудит-процедури, які підтверджують факт надання послуг і правильність визнання витрат, якщо частина актів сформована із запізненням.

Ситуаційне завдання 3. Архівування електронних доказів і короткий строк зберігання журналів

Умова.

Підприємство зберігає електронні документи в хмарному архіві. У договорі з провайдером архівування встановлено зберігання журналів подій 60 днів, а резервні копії формуються 1 раз на тиждень.

Аудитор перевіряє фінансову звітність за 2025 рік і потребує даних про погодження та підписання документів за період з 01.01.2024 до 31.12.2025.

Клієнт повідомив, що частина доступів до архіву змінювалася протягом року, але звіти про зміни ролей не зберігалися.

Завдання.

1. Визначте ризики для збереженості та відтворюваності електронних доказів за такого підходу до журналювання і резервного копіювання.
2. Запропонуйте вимоги до архівування і зберігання електронних доказів.
3. Запропонуйте, як аудитор має задокументувати обмеження доступу до журналів і як це впливає на оцінку ризиків та обсяг процедур.

Ситуаційне завдання 4. Автоматичні контролі без опису і перевірка процесу

Умова.

У клієнта діє автоматизований процес закупівель. Система блокує проведення рахунків, якщо відсутні ліміти бюджету або не пройдено маршрут погодження.

Під час інтерв'ю аудитори з'ясували такі обставини:

➢ описів контролів немає, власники процесів не можуть назвати правила блокувань;

➢ протягом року змінювали налаштування 7 правил погодження, але реєстру змін немає;

➢ звіти контролю формуються автоматично, але їх не підписують і не зберігають у робочих файлах процесу.

Завдання.

1. Поясніть, як змінюється фокус аудиту, коли ключові контролі є автоматичними, а описи контролів відсутні.

2. Складіть перелік елементів внутрішнього контролю та ІТ-контролів, які треба оцінити першочергово.

3. Запропонуйте докази, які аудитор має зібрати для підтвердження роботи автоматичних контролів.

4. Складіть приклад структури робочого документа аудитора для опису та тестування автоматичного контролю.

Ситуаційне завдання 5. Незалежність аудитора при участі у цифровому проєкті клієнта

Умова.

Аудиторська фірма проводить обов'язковий аудит клієнта. Паралельно клієнт пропонує додаткове завдання з налаштування електронного документообігу, шаблонів первинних документів і маршруту погодження.

Вартість додаткових робіт становить 280 000 грн, вартість аудиту становить 620 000 грн. Проєкт планують виконати ті самі спеціалісти, які працюють в аудиті.

Клієнт пояснює, що це пришвидшить отримання даних і зменшить кількість помилок у документах.

Завдання.

1. Визначте загрози незалежності та об’єктивності аудитора за такої ситуації.

2. Визначте, які внутрішні погодження та розкриття інформації мають бути виконані в аудиторській фірмі до початку робіт.

Ситуаційне завдання 6. Доступ аудитора до електронних даних і вимоги конфіденційності

Умова.

Клієнт надає аудитору віддалений доступ до системи електронного документообігу і бухгалтерської системи. Дані містять персональну інформацію працівників і реквізити контрагентів.

У системі 62 активні користувачі. Двофакторну автентифікацію не ввімкнено для 14 користувачів. Доступи надають за ролями, але журнал змін ролей зберігається лише 30 днів.

Клієнт дозволяє аудитору перегляд і вивантаження PDF, але забороняє копіювання баз даних і журналів подій.

Завдання.

1. Визначте ризики для конфіденційності, цілісності та доступності даних за наведених обмежень доступу і журналювання.

2. Запропонуйте вимоги до доступу аудитора і захисту даних, які мають бути зафіксовані в листі узгодження умов завдання або додатках до нього.

3. Запропонуйте альтернативні процедури для отримання достатніх доказів, якщо журнали подій і бази даних не надають.

Ситуаційне завдання 7. Розбіжності часових міток і простежуваність подій

Умова.

Компанія використовує електронні накладні та акти. У документах фіксується дата створення, дата підписання і часова мітка сервера.

Під час звірки з банківською випискою аудитор виявив, що для 24 документів дата підписання відрізняється від дати оплати на 1 день, хоча платіж виконували в той самий робочий день.

ІТ-служба пояснила, що платіжний сервіс працює в іншому часовому поясі, а конвертація часу в системі не налаштована.

Завдання.

1. Поясніть можливі причини розбіжностей дат і часових міток у цифрових системах.

2. Запропонуйте перелік доказів, які підтверджують правильність хронології подій.

3. Складіть аудиторські процедури для перевірки повноти та своєчасності відображення операцій.

Ситуаційне завдання 8. Контроль якості цифрових робочих документів перед аудиторською перевіркою

Умова.

Аудиторська група використовує електронні робочі файли, аналітичні таблиці та запити до бази даних клієнта. Наприкінці завдання керівник виконує внутрішній огляд якості.

У файлі завдання виявлено такі недоліки:

- 22 робочі таблиці не містять опису джерела даних і періоду вивантаження;
- 9 запитів до бази даних збережені без версії та без параметрів відбору;
- 5 підсумкових розрахунків не мають посилання на вхідні файли, які використали для аналізу.

Загалом у файлі завдання є 150 робочих документів, які стосуються цифрових процедур.

Завдання.

1. Запропонуйте правила документування цифрових процедур і збереження цифрового сліду в робочих файлах.

2. Складіть перелік обов’язкових реквізитів робочого документа для аналітичної процедури.

3. Запропонуйте декілька варіантів перевірки якості, які має виконати керівник завдання перед завершенням цифрових процедур.

Ситуаційне завдання 9. Оцінка ризиків з урахуванням ІТ-середовища і автоматизації процесів

Умова.

Підприємство веде облік у системі, де значна частина проведень формується автоматично через інтеграції.

За місяць система створює 1 600 автоматичних проведень на підставі продажів і оплат. Бухгалтерія додатково вносить 120 ручних коригувань наприкінці місяця.

Аудитор планує оцінити ризики суттєвого викривлення з урахуванням того, що дані формуються автоматизовано, а контролі описані лише частково.

Завдання.

1. Складіть перелік інформації про ІТ-середовище і процеси, яку аудитор має отримати для оцінки ризиків.

2. Визначте ризики суттєвого викривлення, які можуть виникати через автоматизацію, інтеграції та ручні коригування.

3. Запропонуйте процедури для перевірки повноти і точності автоматично сформованих проведень.

Ситуаційне завдання 10. Суцільний аналіз даних як аудиторська процедура і перевірка надійності даних

Умова.

Аудитор застосовує суцільний аналіз продажів за рік. Масив містить 85 000 рядків і формується шляхом вивантаження з системи продажів.

Під час попередньої перевірки якості даних виявлено такі факти:

- у 2 550 рядках відсутній код складу;
- у 1 120 рядках відсутній код менеджера;
- у 340 рядках ціна дорівнює 0, хоча це не передбачено політикою продажів.

Загальна сума продажів за даними фінансової звітності становить 412 800 000 грн, за вивантаженням сума становить 409 650 000 грн.

Завдання.

1. Поясніть, які перевірки надійності і повноти масиву даних має виконати аудитор перед суцільним аналізом.

2. Запропонуйте декілька аудиторських процедур щодо рядків із ціною 0 і сформулюйте можливі причини такої аномалії.

Ситуаційне завдання 11. Аудиторська документація при використанні цифрових інструментів і скриптів

Умова.

Команда аудитора використовує цифрові інструменти для відбору вибірок і тестування операцій. Для цього застосовано скрипт, який формує список транзакцій за критеріями ризику.

Скрипт запускали 5 разів з різними параметрами. Вхідні файли з даними зберігаються на спільному диску, але правила іменування файлів не стандартизовані. Частина результатів збережена лише як знімки екрана.

Керівник завдання готує файл до внутрішнього огляду якості і перевіряє, чи можна відтворити результати процедур.

Завдання.

1. Окресліть вимоги до документування цифрових процедур, щоб забезпечити відтворюваність результатів і простежуваність рішень.

2. Складіть перелік того, що має бути зафіксовано в робочих документах про скрипт, його версію, параметри запуску і джерела даних.

3. Запропонуйте список перевірок, які має виконати керівник завдання для контролю якості цифрових робочих документів.

4. Складіть короткий план дій, якщо частину результатів неможливо відтворити, і визначте, як це вплине на висновки аудитора.

14.5. Кейси з організації цифрового аудиту та моніторингу фінансової безпеки

Ситуаційне завдання 1. Показники моніторингу фінансової безпеки

Умова.

Підприємство проводить щомісячний моніторинг фінансової безпеки та відстежує три показники.

1) Рентабельність продажів = чистий прибуток / виручка × 100 %.

2) Виручка на 1 працівника = виручка / середньооблікова чисельність працівників.

3) Коефіцієнт автономії = власний капітал / активи.

Дані за IV квартал 2025 року:

- виручка – 48 000 000 грн;
- чистий прибуток – 2 400 000 грн;
- працівників – 320;
- активи – 90 000 000 грн;
- власний капітал – 36 000 000 грн.

Дані за I квартал 2026 року:

- виручка – 52 000 000 грн;
- чистий прибуток – 1 040 000 грн;
- працівників – 310;
- активи – 92 000 000 грн;
- власний капітал – 33 000 000 грн.

Завдання.

1. Розрахуйте 3 показники для кожного кварталу та порівняйте динаміку.

2. Визначте, який із показників сигналізує про найбільше погіршення фінансової безпеки та що це може означати для ризику викривлення звітності.

3. Запропонуйте, які ділянки аудиту слід посилити з урахуванням результатів моніторингу.

Ситуаційне завдання 2. Порогові значення моніторингу та сигнали ризику

Умова.

У внутрішній політиці компанії встановлено пороги моніторингу:

- коефіцієнт автономії не нижче 0,35;
- рентабельність продажів не нижче 4 %;
- середній строк погашення дебіторської заборгованості не більше 45 днів;
- частка простроченої кредиторської заборгованості не більше 3 %.

За підсумками місяця отримано значення:

- коефіцієнт автономії 0,33;
- рентабельність продажів 3,1 %;
- строк погашення дебіторської заборгованості 58 днів;
- прострочена кредиторська заборгованість 4,2 %.

Завдання.

1. Визначте, які пороги порушено, та сформулюйте ключові сигнали ризику для фінансової безпеки.

2. Прокласифікуйте виявлені сигнали за напрямами ризику: ліквідність, платоспроможність, прибутковість, управління оборотним капіталом.

3. Складіть перелік дій аудитора на етапі планування після отримання таких сигналів.

Ситуаційне завдання 3. Регламент моніторингу та відповідальні особи

Умова.

У компанії моніторинг фінансової безпеки виконує фінансовий відділ. Дані беруть із бухгалтерського модуля, казначейства та банківських виписок.

Показники розраховують вручну в електронній таблиці. Звіт формується із затримкою на 10 днів після закінчення місяця.

Не визначено відповідальних за перевірку якості даних, а результати моніторингу не мають журналу рішень і дій.

Завдання.

1. Складіть схему процесу моніторингу від джерел даних до управлінського рішення.

2. Визначте ролі та відповідальність учасників моніторингу на 3 рівнях: виконавці, контроль, керівний орган.

3. Запропонуйте, як фіксувати результати моніторингу та наступні дії так, щоб аудитор міг перевірити простежуваність рішень.

Ситуаційне завдання 4. IT-ризики у плануванні аудиту

Умова.

Підприємство веде облік у хмарній ERP. У системі 80 активних користувачів та 14 ролей.

За результатами попереднього огляду встановлено:

- 20 користувачів входять без багатофакторної автентифікації;
- 6 користувачів мають право створювати та затверджувати платежі.

Журнали подій зберігаються 30 днів. У попередньому місяці стався інцидент фішингу, після якого змінювалися права доступу.

Завдання.

1. Визначте IT-ризики, які можуть вплинути на достовірність фінансової звітності та формування аудиторських доказів.

2. Складіть перелік інформації, яку аудитор має отримати щодо доступів і змін у системі, щоб оцінити ризики.

3. Запропонуйте зміни до стратегії аудиту з урахуванням короткого строку зберігання журналів подій.

Ситуаційне завдання 5. Фінансова стійкість та оцінка безперервності діяльності

Умова.

Компанія має кредитну угоду з ковенантом, при цьому коефіцієнт покриття боргу грошовим потоком має бути не нижче 1,20.

За попередні 12 місяців фактичне значення становило 1,05. Грошові кошти на кінець періоду – 3 000 000 грн, невикористана кредитна лінія – 2 000 000 грн.

Протягом наступних 60 днів необхідно погасити 6 000 000 грн за графіком боргу.

Завдання.

1. Оцініть, які ризики для фінансової безпеки та безперервності діяльності виникають за наведених умов.

2. Визначте, які напрями тестування та які джерела доказів аудитору слід посилити у зв'язку з ризиком порушення договірних зобов'язань.

3. Запропонуйте, які розкриття у фінансовій звітності варто перевірити аудитору, у зв'язку з такою ситуацією.

Ситуаційне завдання 6. Інтеграція даних для моніторингу та звірка залишків

Умова.

Для моніторингу фінансової безпеки компанія інтегрувала дані ERP та банку. Після оновлення інтеграції виявлено розбіжності.

За даними ERP залишок грошових коштів на кінець дня – 12 800 000 грн, за банківськими виписками – 12 100 000 грн.

За місяць проведено 2 400 платежів. Із них 45 платежів не потрапили в ERP, а 12 платежів відобразилися двічі.

Завдання.

1. Поясніть можливі причини розбіжностей між ERP і банком за наведених умов.

2. Визначте % частку платежів, що не потрапили в ERP, та % частку платежів із дублюванням.

3. Запропонуйте аудиторські процедури, які забезпечать повноту й унікальність відображення платежів.

Ситуаційне завдання 7. Електронні документи та надійність аудиторських доказів

Умова.

Підприємство перейшло на електронний документообіг. Договори й акти підписують кваліфікованим електронним підписом та зберігають у хмарному архіві.

Під час аудиту з'ясувалося, що частина актів має лише 1 підпис. У системі немає зрозумілої історії версій документів.

Журнали подій зберігаються 60 днів. Частину актів сформували із запізненням і завантажили заднім числом.

Завдання.

1. Визначте ризики для автентичності та незмінності електронних документів як джерела аудиторських доказів.

2. Складіть перелік доказів, які аудитор має отримати, щоб підтвердити юридичну значимість і простежуваність документів.

3. Запропонуйте вимоги до архівування та зберігання електронних документів, які підвищать надійність доказів.

Ситуаційне завдання 8. Робочі документи аудитора та відтворюваність аналітики

Умова.

Команда аудитора застосовує аналітику даних і формує робочі файли з запитами та правилами відбору.

Під час внутрішнього огляду якості виявлено, що у робочих файлах не описані джерела даних і параметри відбору. Версії запитів не збережені.

Результати неможливо відтворити. Немає зв’язку між відхиленнями та конкретними рядками у регістрах.

Завдання.

1. Визначте, що саме має бути зафіксовано в робочих документах, щоб аналітичні процедури можна було відтворити та перевірити.

2. Запропонуйте підхід до збереження версій запитів і контрольних звітів з урахуванням вимог конфіденційності.

3. Опишіть, як забезпечити простежуваність від транзакції до показника фінансової звітності в робочих документах аудитора.

Ситуаційне завдання 9. Хмарні сервіси у роботі аудитора та контроль доступів

Умова.

Аудиторська група використовує хмарні платформи для спільної роботи та обміну файлами з клієнтом.

Під час роботи виявлено, що частина папок із даними клієнта відкрита за посиланням без обмеження доменом. Окремі файли не мають контрольованої історії версій.

Клієнт надсилає додаткові документи через різні канали, що ускладнює облік отриманих доказів.

Завдання.

1. Визначте ризики для конфіденційності та цілісності аудиторських доказів у такій організації роботи.

2. Складіть правила доступів і обміну файлами, які мають бути погоджені з клієнтом на старті завдання.

3. Запропонуйте, як організувати реєстр отриманих документів і версій так, щоб аудит мав чіткий цифровий слід.

Ситуаційне завдання 10. Електронні підтвердження та альтернативні процедури

Умова.

Для підтвердження дебіторської заборгованості аудитор ініціював електронні підтвердження через сервіс підписання документів.

Із 15 запитів отримано 12 підтверджень у сервісі; 2 контрагенти не відповіли; 1 контрагент надіслав відповідь електронною поштою без електронного підпису.

У двох отриманих підтвердженнях суми відрізняються від обліку клієнта на 180 000 грн і 260 000 грн.

Завдання.

1. Оцініть надійність отриманих підтверджень та визначте, які відповіді потребують додаткової перевірки.

2. Запропонуйте дії аудитора щодо неотриманих підтверджень та відповіді без електронного підпису.

3. Визначте, як задокументувати розбіжності у робочих документах і які додаткові докази потрібні для їх пояснення.

14.6. Кейси з інформаційних систем підприємства як об’єкта обліку

Ситуаційне завдання 1. Надмірні права доступу

Умова.

У невеликій компанії один бухгалтер веде майже всі ділянки обліку в BAS. Йому надали роль і він може створювати, редагувати контрагентів і договори, вводити первинні документи стосовно купівлі, продажу, банківські операції, проводити їх, а також виконувати ручні операції і коригування. Керівник пояснює це тим, що IT-адміністратора немає. При цьому періодично виникають спірні ситуації і постачальник заперечує суму боргу, клієнт не визнає акт, з’являються дивні проводки в кінці місяця. Відсутнє формалізоване погодження нових контрагентів і зміни реквізитів.

Завдання.

1. Визначте ризики у цій ситуації.

2. Запропонуйте розподіл ролей і перелік доказів контролю.

Ситуаційне завдання 2. Документи датою, що минула, після закриття місяця

Умова.

Місяць у BAS «закрили», сформували звітність і передали дані керівництву. Через 2 тижні аудитору стає відомо, що деякі документи були перепроведені або створені датою, що минула попереднього місяця. Це були документи про реалізацію і списання товарів зі складу. У результаті змінилися обороти й залишки на рахунках. Працівники пояснюють це виявленням документів, які забули внести.

Завдання.

1. Опишіть контроль закриття періоду.

2. Перевірте журнал змін.

3. Сформуйте висновок щодо впливу на звітність та запропонуйте процедуру здійснення коригувань.

Ситуаційне завдання 3. Неповнота обліку та «непроведені» документи

Умова.

У BAS накопичилися документи зі статусом не проведено. Частина – це чернетки, але частина містить реальні суми з надходження, реалізації, непроведені платежі. В оборотно-сальдовій відомості не збігаються дані зі складом і випискою банку. Бухгалтер пояснює, що документи проведуть згодом, адже програма «не дає провести через помилку», бо не заповнений склад, рахунок, договір, не вистачає залишків. Наприкінці місяця це створює ризик, що операції не потрапили в регістри та звітність.

Завдання.

1. Розробіть порядок регулярної перевірки непроведених документів.
2. Встановіть причини виникнення такої ситуації.
3. Визначте докази.

Ситуаційне завдання 4. Звірка банківської виписки з BAS

Умова.

Компанія отримує банківську виписку щоденно. Під час звірки виявляється, що у виписці є платежі, яких немає в BAS, а також є на інші суми та інших контрагентів. Також, навпаки, в BAS проведені платежі, які не підтверджуються випискою. Додатково є комісії банку, валютні різниці, переміщення між рахунками, повернення платежів. Частина платежів відображається як незакриті аванси або неправильно прив’язалася до договорів.

Завдання.

1. Опишіть алгоритм звірки.
2. Встановіть типові причини розбіжностей і контрольні точки.

Ситуаційне завдання 5. Дублювання документів реалізації

Умова.

Під час аналізу доходів виявили, що один продаж відображений двома документами, а саме дві реалізації з однаковим клієнтом, датою, сумою і номенклатурою. Це могло статися через повторне завантаження з Excel, помилку оператора або відсутність контролю унікальності. Наслідком є завищений дохід, ПДВ, дебіторська заборгованість, а клієнт бачить «подвійну» заборгованість.

Завдання.

1.Запропонуйте автоматизовані ознаки «дублів».

2. Оцініть вплив на дохід і ПДВ.

3. Сформуйте рекомендації, а саме контроль унікальності, регламент повторного імпорту, звіт або перевірка перед закриттям.

Ситуаційне завдання 6. Невірні довідники і повторення контрагентів

Умова.

У довіднику контрагентів є повторення:

- ТОВ Альфа;
- ТОВ Альфа (нов.);
- Альфа ТОВ.

На одному записі заведений договір і рахунки, на іншого – акти та платежі. У результаті звіт про розрахунки показує борги, яких не повинно бути, а звірка з контрагентом не збігається. Причиною є відсутність правил заведення довідників, немає контролю за кодом ЄДРПОУ або ІПН, різні бухгалтери створювали записи паралельно.

Завдання.

1. Визначте ризики для розрахунків і звітності, запропонуйте процедуру погодження створення контрагентів

Ситуаційне завдання 7. Від'ємні залишки на складі

Умова.

У звіті залишків і руху запасів є від'ємні значення по позиціях, хоча фактично товар був на складі. Це призводить до некоректної собівартості, помилок у фінансовому результаті, проблем у інвентаризації. Працівники кажуть, що «спочатку продали, а потім оприбуткували», або переміщення не провели та помилково списали на інший склад. Часто причина – порушення хронології документів або відсутність заборони від'ємних залишків.

Завдання.

1. З'ясуйте можливі причини.
2. Запропонуйте контроль перед закриттям місяця.

Ситуаційне завдання 8. Помилки списання/переміщення між складами

Умова.

Товар помилково перемістили на інший склад. Через це один склад відображає документально завеликий обсяг товарів, а інший – порожній, і звіти за відповідальними особами викривлені. Це виявляється під час інвентаризації, коли фактичні залишки не збігаються з BAS.

Завдання.

1. Запропонуйте контрольні звіти.
2. Перевірте первинні документи про фактичне надходження товарів.
3. Опишіть коригувальні дії та запобіжні заходи.

Ситуаційне завдання 9. Помилка класифікації витрат

Умова.

Витрати на доставку, ремонт або маркетинг віднесли на неправильний рахунок. Це може суттєво змінити фінансовий результат за напрямами, спотворити управлінські звіти і розподіл собівартості. Причиною є проводки, які вносили вручну, відсутність шаблонів, некоректні налаштування в довідниках.

Завдання.

1. Визначте ризик викривлення фінансового результату і запропонуйте обмеження на проводки, які вносили вручну.
2. Вкажіть, як можна стандартизувати внесення рахунків і контролювати нетипові облікові проведення.

Ситуаційне завдання 10. ПДВ-ризики через невірні реквізити первинних документів

Умова.

Частина документів купівлі оформлена без важливих реквізитів, а саме дата, номер, ставка ПДВ, номенклатура, податкові параметри, або дані не узгоджуються з первинними документами і податковими накладними. Через це виникають ризики неправильного податкового кредиту, зобов’язань і штрафів.

Завдання.

1. Розробіть прикладні контролі.
2. Визначте перелік звітів для контролю ПДВ та порядок звірок.

Ситуаційне завдання 11. Ризик заміни банківських реквізитів контрагента

Умова.

Перед оплатою в довіднику контрагента хтось змінив IBAN. Платіж проходить, але кошти йдуть на інший рахунок. Потім з'ясовується, що постачальник не отримав коштів. Це може бути як помилка, так і шахрайство.

Завдання.

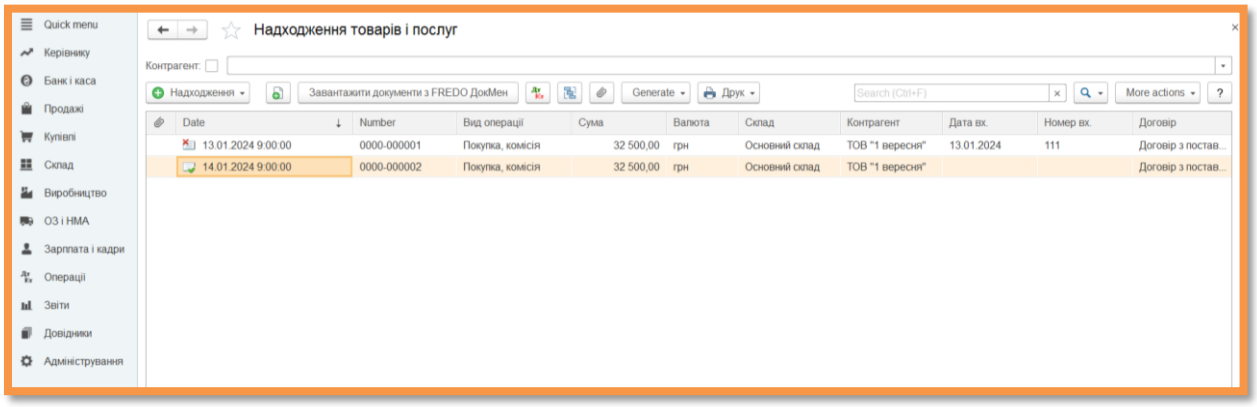
1. Запропонуйте поетапне погодження змін реквізитів.
2. Вкажіть умови обмеження прав і контроль змін.
3. Встановіть правила підтвердження реквізитів.

Ситуаційне завдання 12. Контроль надходжень товарів і послуг у BAS та виявлення ризиків

Умова.

Під час підготовки до закриття місяця головний бухгалтер помітив, що за одним постачальником у короткий проміжок часу проведено два надходження з однаковою сумою та однаковим видом операції.

Це відображення у BAS подано на рисунку.



Завдання.

1. Опишіть ключові ризики цієї ситуації для обліку та звітності.
2. Запропонуйте алгоритм перевірки.

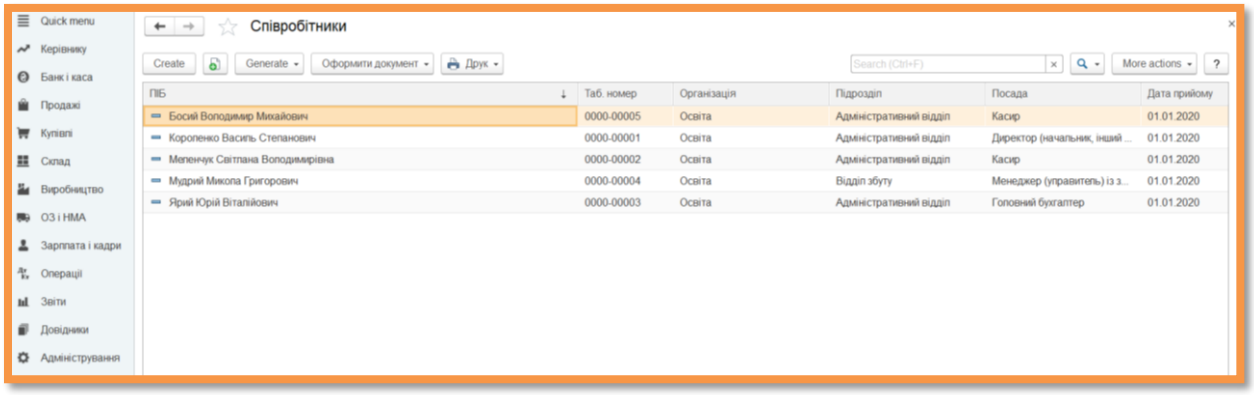
3. Визначте ознаки дублювання.
4. Запропонуйте коригувальні дії залежно від результату.

Ситуаційне завдання 13. Співробітники, доступи і контроль ризиків

Умова.

На підприємстві «Освіта» облік ведеться в BAS Бухгалтерія. Керівник просить налагодити внутрішній контроль в IT-середовищі та підготуватися до аудиту.

Виявлено, що частина користувачів має повні може створювати та редагувати довідники, вводити й проводити документи, а також вносити ручні коригування. Перелік співробітників подано на рисунку.



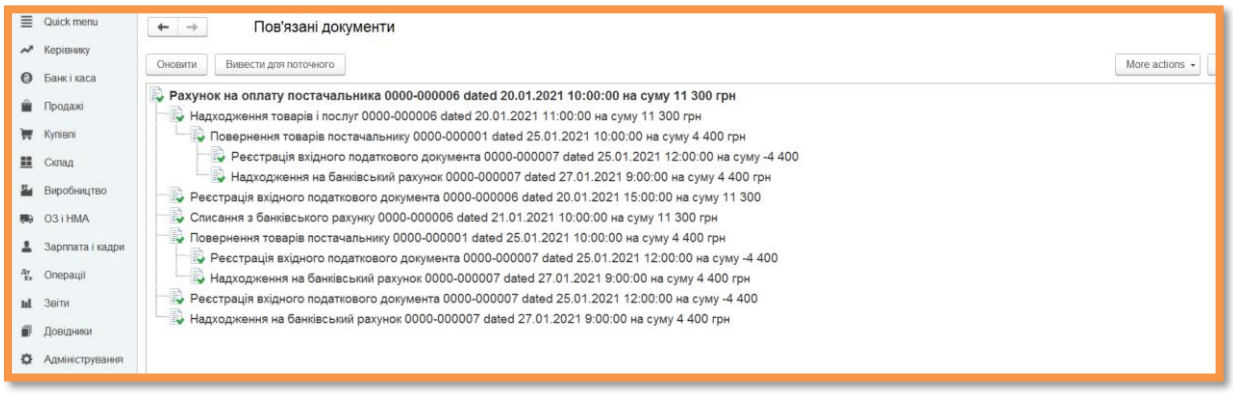
Завдання.

1. Розгляньте рисунок та оцініть правильність введення даних про співробітників.
2. Визначте ризики для достовірності обліку і звітності.
3. Опишіть перелік контрольних процедур.

Ситуаційне завдання 14. Повернення товарів постачальнику

Умова.

На підприємстві виконували закупівлю товарів у постачальника. Бухгалтер сформував документи в BAS, а аудитору або внутрішньому контролеру потрібно перевірити повноту, узгодженість і правильність відображення операцій за ланцюгом пов’язаних документів. Відображення купівлі і повернення в BAS подано на рисунку.



Завдання.

1. Перевірте узгодженість сум і правильність повернення.
2. Оцініть коригування зобов’язань ПДВ.
3. Перевірте ризик дублювання та зайвих документів у ланцюгу повернення.
4. Чи є ланцюг повернення повним?
5. Сформуйте перелік аудиторських доказів.

14.7. Кейси з цифрових інструментів аудитора та фахівця з фінансової безпеки

Ситуаційне завдання 1. Застосування табличного процесора для первинного аналізу облікових даних

Умова.

Аудитор отримав з ERP-системи підприємства файл із даними про реалізацію продукції за 2025 рік (понад 120 000 рядків). Дані містять дати операцій, номери документів, коди клієнтів, суми без ПДВ, суми ПДВ та загальні суми. Під час відкриття файлу у Microsoft Excel виявлено, що частина дат імпортована у текстовому форматі, а суми відображаються з різною кількістю знаків після коми.

Завдання.

1. Визначте, до якої категорії CAATs належить використання Excel у цій ситуації.

2. Опишіть алгоритм підготовки та очищення даних у табличному процесорі перед проведенням аналітичних процедур.

3. Які аудиторські ризики можуть виникнути у разі ігнорування проблем формату даних?

4. Запропонуйте аналітичні процедури, які доцільно виконати на цьому етапі.

5. Обґрунтуйте, чому етап підготовки даних є аналітично значущим з погляду методології аудиту.

Ситуаційне завдання 2. Порівняння можливостей Excel та спеціалізованого ПЗ при роботі з великими масивами даних

Умова.

Аудиторська фірма проводить перевірку торговельної компанії з обсягом транзакцій понад 2 млн записів на рік. Частина аудиторів пропонує виконувати аналітичні процедури в Excel шляхом розбиття файлів, інша – використати IDEA для суцільного аналізу даних.

Завдання.

1. Порівняйте методологічні обмеження Excel і можливості спеціалізованого ПЗ в цій ситуації.

2. Які процедури доцільно виконувати в Excel, а які – в IDEA або ACL?

3. Оцініть вплив обраного інструменту на аудиторський ризик невиявлення.

4. Запропонуйте комбінований підхід до використання цифрових інструментів.

5. Зробіть висновок щодо доцільності використання спеціалізованого ПЗ.

Ситуаційне завдання 3. Суцільний аналіз транзакцій у IDEA та ACL на основі ERP-даних

Умова.

Аудитор імпортував із ERP-системи дані про всі платежі постачальникам за рік до системи IDEA. Після перевірки цілісності даних він планує виконати суцільний аналіз з метою виявлення нетипових операцій.

Завдання.

1. Опишіть послідовність дій аудитора після імпорту даних до IDEA.

2. Які типи тестів і правил доцільно застосувати для виявлення аномалій?

3. Які показники можуть слугувати індикаторами підвищеного ризику?

4. Як результати суцільного аналізу трансформуються в аудиторські докази?

5. Поясніть, у чому полягає методологічна перевага суцільного аналізу порівняно з вибірковим.

Ситуаційне завдання 4. Документування цифрових аудиторських процедур у CaseWare

Умова.

Після виконання аналітичних процедур у Excel та IDEA аудитор повинен задокументувати результати перевірки відповідно до вимог стандартів аудиту. Для цього використовується система CaseWare.

Завдання.

1. Які результати цифрового аналізу підлягають обов'язковому документуванню?

2. Як забезпечується зв'язок між аналітичними процедурами та аудиторськими доказами в CaseWare?

3. Які ризики виникають у разі неналежного документування цифрових процедур?

4. Опишіть переваги використання шаблонів і стандартних форм.

5. Обґрунтуйте роль CaseWare у забезпеченні якості аудиторського завдання.

Ситуаційне завдання 5. Управління аудиторським процесом у TeamMate

Умова.

Служба внутрішнього аудиту великої корпорації використовує TeamMate для планування та контролю виконання перевірок у кількох філіях. Частина процедур виконується із застосуванням аналітичних інструментів.

Завдання.

1. Які функції TeamMate підтримують ризик-орієнтований підхід до аудиту?

2. Як система забезпечує контроль виконання процедур і рекомендацій?

3. Яким чином інтеграція з аналітичними модулями підвищує ефективність аудиту?

4. Оцініть роль централізованого зберігання даних для внутрішнього контролю.

5. Зробіть висновок щодо значення TeamMate у корпоративних системах фінансової безпеки.

Ситуаційне завдання 6. Вибір цифрових інструментів для планування та виконання аудиту

Умова.

Аудитор планує перевірку компанії, яка веде облік у цифровій системі. Під час попередньої зустрічі клієнт повідомив, що може надати дані у вигляді вивантажень регістрів, журналів подій та довідників. Обсяг операцій за рік становить 1 850 000 рядків, частина даних має лише електронний вигляд.

Команда аудитора має доступ до табличного процесора та до окремого програмного інструменту для аналізу великих масивів даних, але не має готового переліку процедур, які доцільно автоматизувати.

Завдання.

1. Визначте, які категорії комп’ютеризованих засобів аудиту доцільно застосувати на етапі планування, на етапі виконання та на етапі завершення перевірки. Наведіть щонайменше 2 приклади для кожного етапу.

2. Складіть перелік даних, які треба запросити у клієнта для автоматизованого аналізу.

3. Запропонуйте критерії вибору між табличним процесором і спеціалізованим інструментом аналізу даних для процедур по суті.

4. Визначте запобіжні заходи, які мають забезпечити повноту і достовірність результатів цифрових процедур.

Ситуаційне завдання 7. Підключення до бази даних клієнта та контроль повноти вивантаження

Умова.

Клієнт погодився надати аудитору доступ лише для читання до бухгалтерської бази даних через стандартний інтерфейс підключення. Пряме копіювання бази заборонене. Дані дозволено отримувати лише у вигляді запитів і результатів у файлах.

Аудитору потрібно отримати журнал операцій за період 01.01.2025-31.12.2025. Очікувана кількість записів у журналі за даними клієнта становить 2 460 000.

Завдання.

1. Складіть покроковий план отримання даних з бази так, щоб забезпечити принцип лише читання та мінімізувати ризик зміни даних.

2. Визначте обов'язкові поля журналу операцій для аудиторського аналізу.

3. Запропонуйте процедури контролю повноти вивантаження та узгодження кількості записів.

4. Поясніть, як аудитор має задокументувати параметри запиту та версії даних, щоб результати можна було відтворити.

Ситуаційне завдання 8. Імпорт і стандартизація даних у табличному процесорі

Умова.

Аудитор отримав від клієнта файл із журналом господарських операцій за квартал. У файлі 64 300 рядків. Під час відкриття в табличному процесорі виявлено такі проблеми:

- дати відображаються як текст;
- частина сум має текстовий формат з пробілами;
- у полі «Контрагент» є різні варіанти написання однієї і тієї самої назви;
- у 120 рядках відсутній номер документа.

Завдання.

1. Розподіліть виявлені проблеми за критеріями якості даних, зокрема повнота, точність, узгодженість, унікальність, своєчасність.

2. Складіть перелік дій для підготовки даних перед аналізом.

3. Запропонуйте правила стандартизації поля «Контрагент» для уникнення дублікатів.

4. Сформулюйте критерії, за яких масив даних можна вважати придатним для подальших аналітичних процедур.

Ситуаційне завдання 9. Виявлення дублікатів та нетипових сум з розрахунком часток

Умова.

За результатами первинної перевірки журналу операцій за рік (214 800 рядків) аудитор зафіксував такі відхилення:

- виявлено 860 дублікатів номерів документів;
- виявлено 145 операцій з від'ємною сумою;
- виявлено 320 рядків з порожнім полем «Сума».

Загальна сума оборотів у журналі становить 1 280 000 000 грн, сума операцій з від'ємними значеннями становить 3 900 000 грн.

Завдання.

1. Визначте % частку дублікатів номерів документів, частку операцій з від'ємними сумами та частку рядків з порожньою сумою.

2. Визначте % частку суми операцій з від'ємними значеннями від загальної суми оборотів.

3. Запропонуйте гіпотези причин появи дублікатів і від'ємних сум та які документи або записи це можуть підтвердити.

4. Складіть план детальної перевірки для цих відхилень.

Ситуаційне завдання 10. Аналіз платежів через сортування і фільтрацію з оцінкою ризику

Умова.

Аудитор аналізує реєстр платежів постачальникам за півріччя. У реєстрі 18 400 платежів на суму 640 000 000 грн.

Після сортування за сумою і фільтрації за ознаками часу виявлено:

- 260 платежів на суму 52 000 000 грн проведено у вихідні дні;
- 95 платежів на суму 18 700 000 грн проведено між 22:00 і 06:00;

- 140 платежів на суму 33 600 000 грн мають призначення «аванс» без договору в реєстрі договорів.

Завдання.

1. Визначте % частку платежів, проведених у вихідні, частку платежів у нічний час та частку платежів з призначенням «аванс» без договору.

2. Визначте % частку сум за кожною з 3 груп від загальної суми 640 000 000 грн.

3. Запропонуйте контрольні запитання до керівника фінансової служби щодо причин таких операцій.

4. Складіть перелік аудиторських процедур для перевірки суті цих платежів.

Ситуаційне завдання 11. Маркування ризикових операцій та формування ознаки ризику

Умова.

Аудитор готує масив продажів для аналітичних процедур. У масиві 52 000 рядків. Для кожного рядка є поля «Дата», «Номер документа», «Контрагент», «Сума», «Статус оплати», «Тип операції».

Команда домовилася маркувати рядок як ризиковий, якщо виконується хоча б одна умова:

- сума менша за 0;
- номер документа повторюється;
- статус оплати «Не оплачено» понад 30 днів;
- тип операції «Повернення» без посилання на первинний документ.

Завдання.

1. Складіть точний опис логіки ознаки ризику, включаючи необхідні додаткові поля або довідники.

2. Запропонуйте правила умовного виділення ризикових рядків та окремих типів ризику.

3. Визначте, як аудитор має перевірити правильність розрахунку ознаки ризику на тестовій підмножині даних.

4. Поясніть, як результати маркування використовувати для формування аудиторської вибірки та для оцінки ризиків.

Ситуаційне завдання 12. Аналітика оборотів за допомогою зведень та оцінка концентрації

Умова.

Аудитор аналізує продажі за рік з метою оцінки концентрації доходу за контрагентами. Загальна сума продажів становить 480 000 000 грн.

За результатами групування за контрагентами визначено, що 3 найбільші контрагенти мають такі суми:

- контрагент А - 92 000 000 грн;
- контрагент Б - 71 500 000 грн;
- контрагент В - 58 300 000 грн.

Сума продажів іншим контрагентам становить 258 200 000 грн.

Завдання.

1. Визначте % частку кожного з 3 найбільших контрагентів у загальній сумі продажів.

2. Обчисліть сумарну частку 3 найбільших контрагентів у загальній сумі продажів та зробіть висновок про рівень концентрації.

3. Запропонуйте аудиторські процедури, які мають підтвердити реальність і повноту продажів за трьома найбільшими контрагентами.

4. Складіть приклад структури робочого документа для цієї аналітичної процедури з фіксацією вихідних даних, параметрів групування та висновків.

Ситуаційне завдання 13. Стратифікація операцій та формування вибірки з розрахунками

Умова.

Для перевірки витрат на послуги аудитор має сукупність 9 600 операцій на загальну суму 96 000 000 грн. Команда вирішила застосувати стратифікацію за сумою операції.

Стратифікація дала такі групи:

- група 1 до 10 000 грн включно - 8 400 операцій на суму 36 000 000 грн;
- група 2 від 10 001 до 50 000 грн - 1 080 операцій на суму 34 200 000 грн;
- група 3 понад 50 000 грн - 120 операцій на суму 25 800 000 грн.

Завдання.

1. Визначте % частку кількості операцій та частку суми для кожної з 3 груп.

2. Запропонуйте підхід до формування вибірки так, щоб покрити не менше 70% суми сукупності. Вкажіть, які групи і яку частину операцій доцільно перевіряти.

3. Якщо команда вирішила перевірити всі 120 операцій групи 3 та 15% операцій групи 2, обчисліть, скільки операцій буде у вибірці та яку суму це покриє. Подайте покриття у відсотках від 96 000 000 грн.

4. Складіть перелік документів і цифрових доказів, які потрібно отримати для перевірки операцій у вибірці.

Ситуаційне завдання 14. Зіставлення реєстру продажів і реєстру оплат та оцінка розбіжностей

Умова.

Аудитор отримав 2 масиви даних за 2025 рік. Перший масив - реєстр продажів (156 200 рядків), другий масив - реєстр оплат від клієнтів (152 900 рядків). Масиви мають спільні поля «Номер документа», «Дата», «Контрагент», «Сума».

Після зіставлення за номером документа встановлено:

- 3 480 продажів на суму 18 600 000 грн не мають відповідної оплати у реєстрі оплат;
- 2 150 оплат на суму 9 400 000 грн не мають відповідного продажу у реєстрі продажів.

Загальна сума продажів становить 480 000 000 грн, загальна сума оплат становить 470 000 000 грн.

Завдання.

1. Визначте частку продажів без оплати за кількістю та за сумою. Подайте результат у відсотках від загальної кількості продажів і від суми продажів 480 000 000 грн.

2. Обчисліть частку оплат без продажу за кількістю та за сумою. Подайте результат у відсотках від загальної кількості оплат і від суми оплат 470 000 000 грн.

3. Запропонуйте можливі причини розбіжностей між масивами та для кожної причини вкажіть, які дані або документи треба перевірити.

4. Складіть план процедур для підтвердження повноти доходу та правильності відображення дебіторської заборгованості.

Ситуаційне завдання 15. Суцільні тести у спеціалізованому інструменті аналізу даних

Умова.

Під час перевірки торговельної мережі аудитор отримав журнал касових операцій за рік. Масив містить 3 200 000 рядків і 12 полів, включаючи час операції, номер зміни, касира, суму, спосіб оплати, номер чека.

Клієнт наполягає на суцільному аналізі ризиків без вибіркового тестування. Команда має спеціалізований інструмент, який дозволяє імпортувати великі масиви, виконувати тести та формувати протоколи виконання процедур.

Завдання.

1. Складіть перелік суцільних тестів, які доцільно виконати для касових операцій, з коротким поясненням мети кожного тесту.

2. Запропонуйте процедури контролю цілісності масиву перед початком тестів.

3. Визначте, які результати та метадані виконання тестів треба зберегти для робочих документів.

4. Поясніть, як аудитор має перейти від результатів суцільних тестів до тестування деталей та формування висновків.

Ситуаційне завдання 16. Документування цифрових процедур і відтворюваність результатів

Умова.

Команда аудитора виконала аналіз даних у табличному процесорі та у спеціалізованому інструменті. Під час внутрішнього огляду якості виявлено, що частина файлів не містить опису джерел даних, параметрів відбору та версій запитів.

Окремі розрахунки виконані вручну без фіксації формул. У протоколах немає зв’язку між виявленими відхиленнями та конкретними рядками у регістрах.

Завдання.

1. Запропонуйте правила документування цифрових процедур і збереження цифрового сліду.

2. Складіть перелік обов’язкових реквізитів робочого документа для цифрової аналітичної процедури.

3. Опишіть механізм версіонування файлів і запитів у команді аудитора так, щоб мінімізувати ризик втрати відтворюваності.

4. Запропонуйте перевірки якості, які має виконати керівник завдання перед завершенням етапу цифрових процедур.

14.8. Кейси з інтегрованих моделей управління фінансовою безпекою

Ситуаційне завдання 1. Впровадження моделі «Безпека-інклюзія-аудит» у фінансовій установі

Умова.

Фінансова установа запускає новий дистанційний сервіс для клієнтів. За 3 місяці кількість активних користувачів зросла з 18 000 до 26 500. Частина клієнтів користується сервісом через допоміжні технології, а частина потребує спрощених каналів підтвердження операцій.

Керівництво затвердило концептуальну модель «Безпека-інклюзія-аудит», але межі відповідальності між підрозділами визначені нечітко. За квартал зафіксовано 14 інцидентів інформаційної безпеки, 6 скарг на недоступність сервісів і 9 випадків помилкових блокувань операцій.

Планується внутрішній аудит впровадження моделі з фокусом на узгодженість політик, процедур і цифрових контролів.

Завдання.

1. Сформулюйте, які ключові ролі виконують компоненти «безпека», «інклюзія» та «аудит» у цій моделі.
2. Запропонуйте перелік показників для моніторингу моделі, третина з них має відображати інклюзивність процесів.
3. Складіть програму аудиторських процедур для оцінювання впровадження моделі.

Ситуаційне завдання 2. Побудова карти ризиків та пріоритизація заходів у системі фінансової безпеки

Умова.

Підприємство має інтегровану систему управління фінансовою безпекою, яка охоплює контроль ліквідності, платіжної дисципліни, контрагентських ризиків, доступів до облікових даних та реагування на інциденти.

За пів року виявлено 38 подій:

- 12 прострочень платежів постачальникам;
- 9 випадків зміни реквізитів без належного погодження;
- 7 збоїв у платіжному каналі;

- 6 помилок у довідниках;
- 4 інциденти інформаційної безпеки.

Керівництво просить внутрішнього аудитора визначити пріоритетні ризики для першочергового посилення контролів.

Завдання.

1. Згрупуйте події за категоріями ризиків та загроз.

2. Запропонуйте запобіжні заходи для кожного з пріоритетних ризиків, укажіть, які підрозділи відповідають за реалізацію.

3. Складіть перелік аудиторських доказів для підтвердження ефективності запропонованих заходів.

Ситуаційне завдання 3. Інклюзивні канали участі та зворотний зв'язок як елемент фінансової безпеки

Умова.

Організація впровадила 4 канали звернень клієнтів щодо операцій та безпеки: контакт-центр, чат у застосунку, електронна форма звернення, особистий прийом. За місяць отримано 2 400 звернень, з них 1 560 через чат, 620 через контакт-центр, 180 через форму та 40 особисто.

Час першої відповіді становить 6 годин у чаті, 18 хвилин у контакт-центрі, 2 дні у формі звернення. Частина клієнтів скаржиться на складність проходження перевірок і на повторні запити тих самих документів.

Керівництво хоче оцінити, чи підтримують канали звернень принципи інклюзії та чи не створюють вони додаткових ризиків для безпеки.

Завдання.

1. Обчисліть % частку звернень за кожним каналом.

2. Визначте ризики, які можуть виникати через неузгоджені канали звернень.

3. Запропонуйте заходи, які одночасно посилять безпеку та інклюзивність обслуговування.

4. Складіть структуру робочого документа аудитора для перевірки каналів звернень.

Ситуаційне завдання 4. Узгодження стратегічних і оперативних цілей інтегрованої моделі фінансової безпеки

Умова.

Підприємство окреслило стратегічні напрями розвитку на рік.

До цих напрямів належать:

- знизити кількість інцидентів фінансового шахрайства на 20%;
- скоротити середній час реагування на інцидент до 4 годин;
- підвищити доступність критичних сервісів до 99,5%.

Оприлюднено фактичні дані за 6 місяців:

- інцидентів фінансового шахрайства було 60, стало 58;
- середній час реагування 9 годин;
- доступність сервісів 98,9%.

Операційні підрозділи виконують локальні плани, але не можуть пояснити вплив на стратегічні цілі.

Внутрішній аудит має оцінити узгодженість стратегічного та оперативного рівнів управління.

Завдання.

1. Визначте відхилення від цілей за 6 місяців, подайте у відсотках для інцидентів і в абсолютних величинах для часу та доступності.

2. Поясніть причини, через які операційні дії можуть не призводити до досягнення стратегічних цілей у системі фінансової безпеки.

3. Складіть перелік аудиторських процедур для перевірки узгодженості цілей і фактичних результатів, зазначте очікувані докази.

Ситуаційне завдання 5. Розширення доступу до фінансових послуг і навантаження на систему контролю

Умова.

Фінансова установа запровадила програму розширення доступу до послуг у регіонах. За квартал кількість нових клієнтів становила 18 000. Кількість операцій зросла з 120 000 на місяць до 168 000 на місяць.

Підрозділ фінансового моніторингу отримував у середньому 1 200 сигналів ризику на місяць, після запуску програми отримує 2 850 сигналів. Команда аналітиків складається з 9 осіб. Середній час опрацювання 1 сигналу 12 хвилин.

Керівництво просить оцінити навантаження і запропонувати рішення, які не знизять рівень безпеки та не створять бар'єрів для клієнтів.

Завдання.

1. Визначте приріст кількості операцій і приріст кількості сигналів ризику.

2. Оцініть, скільки годин на місяць у середньому припадає на 1 аналітика за нового навантаження, якщо робочий фонд 1 аналітика 160 годин.

3. Запропонуйте рішення, які знизять навантаження і водночас підтримають інклюзивність.

Ситуаційне завдання 6. Дистанційна ідентифікація клієнтів і ризик використання викрадених даних

Умова.

Установа проводить дистанційну ідентифікацію клієнтів через відеоперевірку та підтвердження документів. За місяць виконано 9 600 реєстрацій. Система виявила 180 підозрілих реєстрацій. За результатами перевірки підтверджено 45 випадків використання викрадених документів.

Через посилення перевірок частка відмов у реєстрації зросла з 3,2% до 6,8%. Паралельно зросла кількість скарг на недоступність альтернативних каналів для осіб із порушеннями зору та слуху.

Аудитор має запропонувати підхід, що збалансує безпеку та інклюзію.

Завдання.

1. Обчисліть % частку підозрілих реєстрацій та частку підтверджених випадків від загальної кількості реєстрацій.

2. Обчисліть % частку підтверджених випадків серед підозрілих реєстрацій.

3. Складіть перелік основних аудиторських процедур для перевірки процесу дистанційної ідентифікації.

Ситуаційне завдання 7. Контроль доступів і журналювання змін в інтегрованій системі моніторингу показників безпеки

Умова.

Підприємство створило інтегровану систему контролю та аналітики показників фінансової безпеки. У системі 64 активні користувачі та 9 ролей. Під час огляду доступів встановлено:

- 14 користувачів мають роль із повним доступом до налаштувань;
- 11 користувачів входять без двофакторної автентифікації.

За місяць у довіднику показників виконано 780 змін. Із них 96 змін не мають заявки або погодження. Журнали подій зберігаються 30 днів.

Внутрішній аудит має оцінити ризики незмінності даних і можливість відтворити зміни.

Завдання.

1. Обчисліть % частку користувачів із повним доступом та частку користувачів без двофакторної автентифікації.

2. Обчисліть % частку змін без заявки або погодження.

3. Запропонуйте основні вимоги до управління доступами і журналюванням змін.

Ситуаційне завдання 8. Проєктування інтегрованої системи контролю, моніторингу та аналітики показників фінансової безпеки

Умова.

Керівництво підприємства ухвалило створити інтегровану систему контролю та моніторингу показників фінансової безпеки.

До джерел даних було віднесено:

- бухгалтерський облік;
- казначейство;
- закупівлі;
- продажі;
- кадрові дані;
- журнали доступів.

Система має забезпечувати модульність, централізоване зберігання даних, розмежування доступів, аналіз у розрізі підрозділів, гнучке налаштування порогів та формування автоматичних повідомлень.

Аудитор залучений як незалежний експерт для оцінки проєктного рішення і контрольних механізмів.

Завдання.

1. Складіть перелік показників фінансової безпеки для моніторингу.

2. Запропонуйте правила контролю якості даних для централізованого сховища.

3. Складіть перелік аудит-перевірок, які доцільно передбачити до запуску системи в експлуатацію.

Ситуаційне завдання 9. Система раннього попередження і пороги індикаторів

Умова.

Для раннього попередження інтегрована система моніторингу відстежує чотири ключові індикатори, а саме: частку простроченої дебіторської заборгованості, частку відхилених платежів, кількість змін реквізитів постачальників без погодження і кількість інцидентів доступу.

На тижневому горизонті реагування здійснюється за такими порогами: прострочена дебіторська заборгованість перевищує 8,0% від загальної дебіторської заборгованості; частка відхилених платежів перевищує 0,9% від усіх платежів; кількість змін реквізитів без погодження перевищує 10 випадків; кількість інцидентів доступу перевищує 6 подій.

Фактичні дані за тиждень:

- загальна дебіторська заборгованість 24 500 000 грн;
- прострочена дебіторська заборгованість 2 205 000 грн;
- платежів 3 600;
- відхилених 42;
- змін реквізитів без погодження 14;
- інцидентів доступу 5.

Завдання.

1. Обчисліть фактичну % частку простроченої дебіторської заборгованості та фактичну частку відхилених платежів.

2. Запропонуйте перелік дій реагування з розподілом за 3 лініями захисту, включіть заходи контролю, моніторингу і аудиту.

3. Складіть приклад короткого звіту для керівництва за результатами тижневого моніторингу.

Ситуаційне завдання 10. Оцінювання ефективності інтегрованої моделі фінансової безпеки та план удосконалення

Умова.

Підприємство працює за інтегрованою моделлю фінансової безпеки 1 рік. Порівняльні дані:

- кількість критичних інцидентів за рік була 22, стала 15;
- середній час закриття інциденту був 5,6 доби, став 3,8 доби;
- кількість порушень процедур погодження була 180, стала 96.

Рівень задоволеності користувачів сервісами за результатами опитування був 72%, став 79%. Водночас зросла кількість сигналів ризику в моніторингу з 14 400 на рік до 21 600 на рік.

Аудитор має оцінити результативність моделі та запропонувати план її адаптації з урахуванням інклюзії.

Завдання.

1. Визначте зміну показників у % для 22 → 15, 5,6 → 3,8, 180 → 96 та 72 → 79.

2. Поясніть 5 причин, чому зростання кількості сигналів ризику може бути як позитивним, так і негативним явищем для фінансової безпеки.

3. Запропонуйте основні показники для щоквартального оцінювання ефективності моделі, включіть показники інклюзивності та якості контролів.

14.9. Кейси з виявлення шахрайства та загроз фінансовій безпеці на основі цифрових даних

Ситуаційне завдання 1. Аудит виручки: ризики неправомірного визнання доходу за відсутності транспортних документів

Умова.

ТОВ «Кварц Трейдінг» (платник ПДВ) готує фінансову звітність за IV квартал 2025 року. За даними бухгалтерії, дохід від реалізації у звітному кварталі зріс на 20 % порівняно з IV кварталом 2024 року. Водночас служба логістики повідомляє, що кількість фактичних відвантажень залишалася майже незмінною, а частина поставок здійснювалася через «самовивіз».

На дату балансу обліковується дебіторська заборгованість покупців у сумі 6 240 000 грн, із якої 3 950 000 грн припадає на двох нових контрагентів, зареєстрованих приблизно 3 місяці тому. Під час внутрішньої перевірки документів з'ясовано, що видаткові накладні оформлено, проте товарно-транспортні накладні відсутні. Акти приймання-передачі підписані «представником за довіреністю», але копії довіреностей та підтвердження повноважень не надані.

Фінансовий директор пояснює ситуацію «збоєм у документообігу» та тим, що частина документів «не повернулася від контрагентів».

Завдання.

1. Визначте, чи має ситуація ознаки фінансового правопорушення, чи йдеться про помилку, порушення правил обліку та документування (обґрунтуйте).
2. Класифікуйте можливе порушення за елементами складу: об'єкт, суб'єкт, об'єктивна сторона, суб'єктивна сторона.
3. Окресліть ключові ризики суттєвого викривлення у фінансовій звітності, які у цій ситуації має ідентифікувати аудитор.
4. Сформуйте план первинних аудиторських процедур із використанням:
   - запитів і підтверджень третіх сторін;
   - аналітичних процедур;
   - цифрового тестування внутрішніх контролів.
5. Наведіть основні нормативні акти, що підлягають застосуванню (не менше 4), зокрема щодо обліку, аудиту та оподаткування.

Ситуаційне завдання 2. Аудит бюджетних операцій: нецільове використання коштів та конфлікт інтересів

Умова.

Комунальна установа «Центр сервісів громади «Пульс» отримала бюджетні асигнування на поточний ремонт приміщень у 2025 році в сумі 3 800 000 грн. Під час аналізу касових та фактичних видатків встановлено, що частину коштів було використано не за цільовим призначенням: придбано ноутбуки та смартфони для адміністративного персоналу на загальну суму 1 120 000 грн, а також оплачено «консультаційні послуги з управління проєктами» на суму 420 000 грн.

Постачальником консультацій виступає ФОП, який перебуває у родинних стосунках із керівником відділу закупівель установи. Зміни до кошторису та їх затвердження у встановленому порядку відсутні. Технічні завдання до закупівель сформовані загальним чином, а порівняльний аналіз показує, що ціни на техніку та послуги перевищують ринкові орієнтири приблизно на 25 %.

Завдання.

1. Визначте, чи є описана ситуація бюджетним порушенням, фінансовим правопорушенням, корупційним ризиком або їх сукупністю (з аргументацією).
2. Розкладіть ситуацію за елементами складу правопорушення: об’єкт, суб’єкт, об’єктивна сторона, суб’єктивна сторона.
3. Запропонуйте класифікацію можливої відповідальності: фінансова, адміністративна, кримінальна (що саме можливе та за яких умов).
4. Визначте повноваження органу державного фінансового контролю в такій ситуації: перелік потенційних дій, рішень і документів реагування.
5. Складіть перелік доказів, які необхідно зібрати аудитору.

Ситуаційне завдання 3. Аудит податкових розрахунків: податковий кредит з ПДВ за маркетинговими послугами без належного підтвердження

Умова.

ТОВ «Дельта-Медіа» протягом січня-червня 2025 року формувало податковий кредит з ПДВ на підставі придбання «маркетингових послуг» у трьох контрагентів. Загальна сума ПДВ, включена до податкового кредиту за цими операціями, становить 980 000 грн. В актах наданих послуг зазначено загальні формулювання («просування бренду», «інформаційна підтримка»), але відсутні

медіаплани, звіти, первинні матеріали, статистика охоплення, посилання на розміщення та будь-які докази фактичного надання послуг.

За результатами зустрічних звірок один із контрагентів не встановлений за місцезнаходженням, другий має нульові показники господарської діяльності, а третій перебуває у процедурі припинення. Підприємство подало уточнюючу декларацію лише після отримання письмового запиту контролюючого органу.

Завдання.

1. Визначте можливі види порушень та їх характерні ознаки в наведеній ситуації.
2. Розмежуйте порушення податкового законодавства та можливі ознаки злочину. Опишіть критерії, за яких ситуація може перейти межу адміністративно-фінансової відповідальності у площину кримінально-правової оцінки.
3. Опишіть логіку застосування штрафних санкцій.
4. Складіть алгоритм дій аудитора у цифровому підході, від постановки гіпотез до збору доказів та документування висновків.
5. Визначте нормативні блоки, які необхідно проаналізувати.

Ситуаційне завдання 4. Внутрішній аудит витрат: оплата рахунків без погодження та відсутність первинних документів

Умова.

У ТОВ «СкайПак Сервіс» (виробництво пакувальних матеріалів) у вересні 2025 року служба внутрішнього аудиту провела вибіркову перевірку адміністративних витрат за липень-серпень 2025 року. За даними бухгалтерії, адміністративні витрати за серпень зросли на 18 % порівняно з липнем.

Під час перевірки встановлено, що за два місяці було здійснено 9 платежів на користь постачальника ТОВ «Альфа-Консалт Груп» на загальну суму 1 260 000 грн із призначенням платежу «консультаційні послуги». Водночас:

- письмовий договір із постачальником відсутній (є лише рахунки на оплату);
- акти наданих послуг наявні не за всіма оплатами: підтверджено актами лише 720 000 грн, а на 540 000 грн акти відсутні;
- частина актів має однаковий опис («консультації з оптимізації процесів») без конкретизації результатів;
- виявлено дублювання оплати: рахунок на 140 000 грн був оплачений двічі з різницею у 6 днів;

- платіжні доручення готував і підписував до відправки в клієнт-банк один і той самий бухгалтер (він же веде облік цих витрат), а підтвердження погодження керівником підрозділу або фінансовим директором у документах відсутнє.

Керівник підприємства пояснює, що послуги були термінові, а документи донесуть пізніше, і просить внутрішнього аудитора не робити із цього проблеми.

Завдання.

1. Визначте основні слабкі місця внутрішнього контролю і поясніть, до яких ризиків вони призводять.
2. Назвіть можливі порушення та які статті фінансової звітності можуть бути викривлені.
3. Складіть перелік аудиторських процедур для перевірки цих операцій на основі цифрових даних:

- цифрові тести контролів;
- аудиторські процедури на основі цифрових даних, включно з перевіркою дублювань оплат, підтвердженням реальності послуг, аналізом подальших подій.

4. Опишіть, як внутрішній аудитор має задокументувати результати та з ким комунікувати щодо висновків.

Ситуаційне завдання 5. Форензик-аудит витрат: підозра у зловживаннях у транспортно-експедиторських операціях

Умова.

Власник ТОВ «Логістик Хаб» звернувся до аудиторської фірми із запитом на форензик-перевірку через підозру у зловживаннях у сфері транспортно-експедиторських витрат. За період жовтень-грудень 2025 року витрати за статтею «послуги експедиторів» зросли з 2 100 000 грн до 3 045 000 грн, тобто на 45 %, хоча обсяги перевезень за управлінськими звітами істотно не змінилися.

Протягом цього ж періоду підприємство почало працювати з 7 новими контрагентами-експедиторами; щонайменше 3 з них використовують однакові контактні дані (телефони, електронні адреси). Бухгалтерія відмовляється оперативно надавати частину договорів та підтвердних документів, посилаючись на «комерційну таємницю». Власник очікує отримати «прізвища винних» у строк 14 календарних днів.

Завдання.

1. Визначте мету та конкретні завдання форензик-аудиту в цьому кейсі.
2. Окресліть етапи виконання завдання у форензик-сценарії: від прийняття завдання та оцінки загроз незалежності до оформлення звіту.
3. Складіть перелік документів, необхідних для старту перевірки.
4. Визначте ключові ризики виконання завдання (включно з ризиком обмеження обсягу та ризиком тиску на аудитора).

Ситуаційне завдання 6. Державний фінансовий аудит: організація контрольного заходу за умов обмеження доступу до документів

Умова.

Комунальна установа «Офіс розвитку громад «Горизонт» отримала направлення на проведення контрольного заходу. Попередньо встановлено, що частина видатків за кодами економічної класифікації (КЕКВ) не відповідає затвердженому кошторису та плану асигнувань.

Під час підготовки до перевірки з'ясовано, що частину первинних документів (акти, накладні, підтвердження виконання робіт) зберігає підрядник і установі їх «не повернули». Керівник установи наполягає, щоб перевірка проводилася лише у присутності юриста, та забороняє копіювання матеріалів, посилаючись на внутрішні правила.

Завдання.

1. Визначте організаційні кроки аудитора у перші 1-2 дні перевірки.
2. Складіть перелік документів, які необхідно отримати до старту або на початку перевірки.
3. Запропонуйте план комунікацій із керівництвом, бухгалтерією, відповідальними за закупівлі та юридичною службою.
4. Визначте ризики організації аудиту в державному секторі.
5. Запропонуйте дії аудитора у випадку обмеження обсягу.

Ситуаційне завдання 7. Аудит фінансової установи: етичні загрози та забезпечення якості аудиторського завдання

Умова.

Аудитор проводить перевірку можливих фінансових правопорушень в АТ «ПраймФін». На етапі планування виявлено обставини, що створюють суттєві етичні ризики. Керівник аудиторської групи має дружні стосунки з фінансовим директором клієнта. Клієнт пропонує додаткову винагороду у розмірі 10 % від вартості послуг «за швидкість» і просить не включати окремі транзакції до вибірки.

Частина даних, необхідних для перевірки, містить персональні дані клієнтів і відомості, що можуть підпадати під режим банківської таємниці. Додатково керівництво натякає, що у разі «незручних висновків» договір на наступний період може бути не продовжений.

Завдання.

1. Визначте етичні загрози під час перевірки.
2. Запропонуйте запобіжники для кожної загрози.
3. Складіть короткий план організації аудиту з урахуванням етики.
4. Визначте можливі рішення у відповідь на загрози.
5. Сформулюйте основні пункти, які мають бути відображені в листі-зобов’язанні або договорі для захисту аудитора та забезпечення якості перевірки.

Ситуаційне завдання 8. Аудит доходів: можливе завищення виручки наприкінці періоду

Умова.

ТОВ «Орієнтир Дистриб’юшн» (оптова торгівля побутовою технікою) завершує аудит фінансової звітності за 2025 рік. За даними звіту про фінансові результати, виручка у IV кварталі 2025 року зросла на 35 % порівняно з IV кварталом 2024 року. Валова маржа одночасно збільшилася з 18 % до 27 %. Керівництво пояснює це «успішними передсвятковими продажами» та «новими каналами збуту».

На 31.12.2025 дебіторська заборгованість становить 14 800 000 грн, із яких 6 200 000 грн припадає на 3 нових покупців, зареєстрованих протягом останніх 2 місяців. У договорах з цими покупцями зазначено відстрочку платежу 90 днів. Під час огляду первинних документів аудитор виявив, що частина накладних

датована 29-31 грудня, але складські журнали та дані системи управління складом фіксують фактичне вибуття товару зі складу вже 2-4 січня 2026 року. Для частини поставок відсутні належні ТТН.

Додатково, у січні 2026 року частка повернень за цими ж покупцями склала 12 % від обсягу відвантажень (звичайний рівень повернень компанії - близько 3 %). Внутрішня переписка менеджерів продажів містить фразу: «домовилися, що повернення оформимо після закриття року». Окремо аудитору стало відомо про існування «додаткових листів» до договорів, що допускають повернення товару без штрафів за спрощеною процедурою.

Завдання.

1. Визначте, які типові схеми фінансового шахрайства можуть пояснювати наведені ознаки, та які твердження фінансової звітності перебувають під найбільшим ризиком.
2. Оцініть ризик суттєвого викривлення через шахрайство відповідно до логіки МСА 240 та МСА 315. Які фактори ризику та «червоні прапорці» ви бачите?
3. Складіть програму аудиторських процедур на основі цифрових даних щодо виручки та дебіторської заборгованості, включно з підтвердженнями, аналізом подальших оплат і повернень.
4. Визначте, які комунікації та управлінські реакції є доречними у разі підтвердження ризику шахрайства.

Ситуаційне завдання 9. Аудит закупівель: ознаки змови з постачальниками та завищення витрат

Умова.

ТОВ «Веста Інжиніринг» (виробництво та сервіс промислового обладнання) за 2025 рік відобразило витрати на ремонт і технічне обслуговування виробничих ліній у сумі 9 600 000 грн, що на 28 % більше порівняно з 2024 роком. При цьому обсяги виробництва зросли лише на 5 %, а кількість аварійних зупинок за даними виробничої служби суттєво не змінювалася.

Під час аналітичних процедур аудитор встановив такі факти:

- протягом 2025 року проведено 15 оплат на користь постачальників сервісних послуг на загальну суму 3 900 000 грн; значна частина рахунків має округлені суми (наприклад, 260 000 грн, 295 000 грн, 310 000 грн);

- у компанії діє внутрішній ліміт: операції понад 300 000 грн потребують погодження фінансовим директором та комітетом закупівель, однак більшість рахунків виставлено на суми 290 000-299 000 грн;
- три постачальники («Сервіс Профі+», «ТехРем Стандарт», «Індустріал Саппорт») мають однакові контактні телефони та схожі домени електронної пошти;
- технічні звіти про виконані роботи містять загальні формулювання без переліку конкретних операцій і використаних матеріалів;
- за даними банку, один із постачальників отримує платежі на рахунок, відкритий у тому ж банку та відділенні, що й рахунок співробітника відділу закупівель.

Керівник закупівель відмовляється надавати повний пакет комерційних пропозицій, посилаючись на «втрату архіву».

Завдання.

1. Визначте можливі схеми шахрайства у закупівлях, які узгоджуються з наведеними ознаками, та сформулюйте цифрову карту ризиків.
2. Складіть перелік процедур аудитора для перевірки реальності послуг і обґрунтованості цін.
3. Визначте, як аудитору діяти при обмеженні доступу до документів.

Ситуаційне завдання 10. Аудит фонду оплати праці: ризики фіктивних нарахувань та маніпуляцій із понаднормовими годинами

Умова.

ТОВ «ГрінФуд Манфекчуринг» (харчове виробництво, близько 600 працівників) проводить річний аудит за 2025 рік. За управлінською звітністю середньооблікова чисельність персоналу зросла лише на 2 %, однак витрати на оплату праці та нарахування збільшилися на 15 % (з 84 000 000 грн у 2024 році до 96 600 000 грн у 2025 році). При цьому витрати на надурочні роботи зросли на 60 %.

Аудитор отримав такі сигнали та факти:

- у листопаді-грудні 2025 року виявлено виплати заробітної плати 7 працівникам, які за даними HR були звільнені ще у вересні 2025 року; сума виплат за цими 7 особами за два місяці склала 420 000 грн;
- у платіжних реєстрах виявлено 18 повторюваних банківських рахунків (IBAN), на які зараховується зарплата різних працівників;

- табелі обліку робочого часу в окремих цехах ведуться вручну, підписуються майстром зміни та затверджуються начальником виробництва без додаткової верифікації;
- права доступу в обліковій системі налаштовані так, що один і той самий працівник відділу кадрів може створювати картку співробітника, змінювати банківські реквізити та формувати реєстр на виплату;
- на «гарячу лінію» надійшло анонімне повідомлення про «мертві душі» у нічних змінах і про те, що надурочні «дописують» для частини працівників.

Завдання.

1. Визначте, які види шахрайства можуть мати місце у цьому кейсі та які статті звітності і твердження знаходяться під ризиком.
2. Запропонуйте процедури по суті та форензик-процедури для виявлення «мертвих душ», дублювання рахунків, маніпуляцій із надурочними та виплат після звільнення.
3. Сформуйте набір аналітичних процедур і показників для перевірки фонду оплати праці.
4. Визначте порядок документування та комунікації в разі підтвердження ознак шахрайства.

14.10. Кейси з оцінки кіберризиків та організації захисту даних на підприємстві

Ситуаційне завдання 1. Фішинг і компрометація облікового запису

Умова.

Аудиторська команда працює з клієнтом у період пікового навантаження, обмінюється файлами через хмарну папку та корпоративну пошту. Один зі співробітників отримує лист нібито від клієнта з темою «Терміново: підтвердіть узгоджені цифри» та посиланням на «документ». Сторінка входу виглядає переконливо, тому працівник вводить логін і пароль. Через кілька хвилин система просить повторно увійти, що сприймається як збій.

Насправді дані доступу перехоплено. Зловмисник входить з іншої локації та налаштовує правило в пошті, щоб частина листування автоматично пересилалася на зовнішню адресу, а окремі сповіщення про входи приховувалися. Далі він відкриває хмарне сховище, переглядає структуру папок, завантажує робочі таблиці й документи та створює кілька «спільних посилань» без пароля, щоб зберегти доступ навіть після зміни пароля.

Завдання.

1. Визначте, які елементи CIA порушено першочергово, а які вторинно.
2. Назвіть 5 слабких місць у сценарії.
3. Запропонуйте мінімальний набір запобіжних і виявляючих контролів.

Ситуаційне завдання 2. Ransomware як бізнес-ризик: простій і строки

Умова.

Аудиторська фірма зберігає робочі документи на файловому сервері та в хмарі. За кілька днів до фінального узгодження звіту команда помічає збої. Фіксується, що файли відкриваються повільно, частина папок стає недоступною, з’являються попередження захисного ПЗ. Уночі значна частина даних шифрується, а файли отримують нові розширення, з’являється повідомлення про шифрування.

Команда реагування ізолює частину робочих станцій, однак шифрування вже зачіпає мережеві каталоги. Під час відновлення з’ясовується, що резервні копії або застарілі, або частково пошкоджені, а відновлення не вкладається у потрібні строки. У результаті порушуються договірні строки, виникають додаткові витрати на відновлення та понаднормову роботу, а клієнт ставить під сумнів надійність аудитора як провайдера послуг.

Завдання.

1. Визначте ключові місця розриву між IT-інцидентом і фінансовими втратами.
2. Складіть перелік первинних доказів масштабу.
3. Запропонуйте 6 контролів, що зменшують імовірність ransomware.

Ситуаційне завдання 3. Треті сторони та ланцюг постачання у файлообміні

Умова.

Аудиторська фірма використовує сторонній сервіс керованого обміну файлами для передавання великих масивів даних. Клієнти завантажують документи, аудитори отримують сповіщення і доступ за посиланням, а сервіс інтегрований із корпоративною поштою та автоматичним збереженням у внутрішньому сховищі.

Провайдер повідомляє про критичну уразливість, яка могла дозволяти несанкціонований доступ до файлів у певному часовому вікні. Частина клієнтів запитує про ризик витоку. Внутрішня перевірка показує, що окремі файли з персональними даними та фінансовими даними могли бути доступні стороннім особам. Через інтеграції також виникає ризик зловживання токенами доступу або технічними обліковими записами. Формується ланцюговий ефект, коли інцидент у постачальника перетворюється на інцидент аудитора і далі – стає клієнтським інцидентом.

Завдання.

1. Поясніть різницю між ризиком третьої сторони та внутрішніми ризиками.
2. Запропонуйте вимоги до постачальника.
3. Сформуйте заходи, що зменшують ланцюговість.

Ситуаційне завдання 4. Управління ідентичністю: витік паролів + неповна MFA

Умова.

У компанії є SSO для частини сервісів, але частина інструментів працює з окремими логінами. MFA увімкнена лише для керівників і IT, для інших «рекомендована». Частина працівників повторно використовує паролі, інколи зберігає їх у браузері без додаткового захисту.

Після витоку облікових даних з одного зовнішнього сервісу зловмисник застосовує ті самі логіни та паролі для корпоративної пошти. Через відсутність

MFA для частини користувачів йому вдається увійти. Далі він знаходить у листуванні запрошення на спільні ресурси та посилання на хмарні папки. Оскільки один обліковий запис відкриває доступ до кількох сервісів, наслідки швидко масштабуються. Служба безпеки бачить підозрілі входи, але реагування затягується через відсутність умовного доступу (геолокація, ризикові входи, контроль пристроїв).

Завдання.

1. Сформуйте перелік змін у політиках IAM.
2. Розділіть вимоги для звичайних і привілейованих облікових записів (PAM, JIT).
3. Поясніть, як Zero Trust обмежує наслідки у цьому сценарії.

Ситуаційне завдання 5. Zero Trust для фінансових систем: мікросегментація й мінімальні привілеї

Умова.

Компанія працює у гібридній моделі, коли частина бухгалтерських операцій у хмарі, частина у локальній ERP. Є різні ролі (бухгалтерія, фінансовий контроль, внутрішній аудит, зовнішні аудитори, IT-адміністратори, керівництво). Для зручності доступи видавалися усім, тому один скомпрометований обліковий запис може бачити й змінювати більше, ніж потрібно.

Керівництво вирішує впровадити принципи Zero Trust. Ця система базується на перевірці кожного доступу, суворому розмежуванні прав, оцінці контексту (пристрій, локація, рівень ризику) і мікросегментації, щоб унеможливити переміщення зловмисника між ресурсами. Потрібно перебудувати доступи без зриву операцій і забезпечити контрольованість доступу до фінансово значущих даних.

Завдання.

1. Запропонуйте структуру RBAC або ABAC і приклади умовних правил доступу.
2. Визначте ключові сегменти для ізоляції.
3. Які журнали подій та метрики потрібні для SIEM або моніторингу?

Ситуаційне завдання 6. Резервне копіювання є, але відновитися неможливо

Умова.

Організація має такий формальний регламент резервного копіювання:

- щоденні копії баз;
- щотижневі архіви документів;
- окремий диск для резервів.

Фактично резерви зберігаються в тому ж домені й мережі, доступні через ті самі облікові записи, а процедури відновлення давно не тестувалися. Частина копій створюється з помилками, але звіти не аналізуються, немає відповідального та KPI якості резервування.

Після інциденту команда намагається відновити дані й виявляє, що останні незаражені копії надто старі, а нові або пошкоджені, або потенційно скомпрометовані. Виникає розрив між формальним виконанням політики і реальною стійкістю, оскільки відновлення не вкладається у потрібні RTO та RPO, що переходить у прямі фінансові втрати через простій і затримку процесів.

Завдання.

1. Визначте RTO або RPO для трьох класів систем і обґрунтуйте.
2. Запропонуйте архітектуру резервування.
3. Складіть план DR-тестів і критерії доказовості.

Ситуаційне завдання 7. Суттєвість кіберподії для звітності та розкриттів

Умова.

Під час аудиту клієнт повідомляє про кіберподію (тимчасову недоступність частини сервісів, витрати на відновлення і консультації, можливі затримки контрактів). Менеджмент стверджує, що подія не суттєва. Водночас аудитору потрібно оцінити коректність відображення витрат, наявність підстав для резервів (штрафи, претензії), потребу в розкриттях та вплив на надійність даних, що формують фінансову звітність.

Навіть за невеликих прямих витрат непрямі наслідки (втрата доходу, простій, перехід у ручний режим, зростання ризику помилок чи шахрайства) можуть бути суттєвими. Завданням аудитора є оцінка контрольного середовища та фінансового відображення ризиків, а не технічного розслідування атаки.

Завдання.

1. Розділіть прямі та непрямі наслідки та сформуйте критерії суттєвості.
2. Визначте необхідні аудиторські докази щодо оцінок менеджменту.
3. Складіть логіку перевірки ланцюга подій до фінансових наслідків.

Ситуаційне завдання 8. ITGC для фінансово значущих систем

Умова.

Клієнт формує звітність на основі ERP, інтегрованої з банківськими виписками, продажами і складом. Частина процесів автоматизована, але наприкінці місяця виконуються ручні коригування. Раніше виявлялося, що окремі користувачі мають надмірні права (створюють контрагентів, змінюють довідники, проводять операції). Деякі зміни в системі виконувалися терміново і без належної документації.

Аудитор має визначити, чи може покладатися на дані ERP як на джерело доказів, і які процедури потрібні для тестування ITGC. У центрі уваги – розділення обов'язків, процес надання або відкликання доступів, контроль змін і можливість відтворити історію коригувань.

Завдання.

1. Сформуйте перелік ITGC та тестів для кожного.
2. Назвіть «червоні прапорці» ризику викривлень звітності.
3. Запропонуйте мінімальний набір доказів.

Ситуаційне завдання 9. BCP та DRP як аудиторський об'єкт, доказовість готовності

Умова.

Керівництво компанії зазначає, що організація підготовлена до інцидентів. Розроблено плани безперервності бізнесу (BCP) і аварійного відновлення (DRP), визначено відповідальних осіб та описано критичні процеси. Під час перевірки виявляється, що тестування нерегулярне, результати тестів не документуються, RTO/RPO визначені формально, а резервні копії не завжди ізольовані. Частина працівників не знає алгоритм дій під час простою ключових систем.

У такій ситуації аудитор оцінює не наявність документів, а дієвість системи підкріплюється актуальністю планів, журналом навчань, пріоритетами відновлення і можливістю відновити критичні сервіси в заданих межах. Оскільки

простій безпосередньо перетворюється на втрату доходів і додаткові витрати, якість BCP/DRP впливає на фінансову стійкість і ризики для звітності.

Завдання.

1. Визначте, які елементи BCP чи DRP використовуються в аудиторських процедурах.
2. Сформуйте перелік запитань менеджменту та потрібних документів і логів.
3. Поясніть зв'язок між DR-тестами і мінімізацією фінансових наслідків.

Ситуаційне завдання 10. Технічний обліковий запис і прихована зміна даних у фінансовій системі

Умова.

У клієнта є локальна ERP. Для інтеграції з банком і складом використовується технічний обліковий запис, пароль якого знають кілька адміністраторів, а MFA немає. Логи ERP зберігаються на тому ж сервері. Після звільнення одного з IT-співробітників виявляють, що в кінці місяця робилися ручні коригування та зміни довідників (контрагенти та рахунки), але частина записів у логах відсутня або обрізана. Фінансовий директор пояснює це технічними роботами. Аудитор сумнівається, чи можна покладатися на дані ERP як джерело доказів.

Завдання.

1. Визначте ключові ризики для звітності (які дані чи процеси під загрозою) і які елементи CIA зачіпає.
2. Складіть перелік первинних доказів масштабу.

Ситуаційне завдання 11. Кіберінцидент у платежах і розрахунок потенційного викривлення

Умова.

У компанії виявлено кіберінцидент у процесі погодження платежів. За 7 днів проведено 420 платежів на суму 38 500 000 грн.

З них 9 платежів були на нові банківські реквізити постачальників на суму 1 860 000 грн.

Після перевірки встановлено, що 3 з 9 платежів були здійснені на шахрайські реквізити на суму 620 000 грн. Банк повернув 140 000 грн. Решта суми не повернута.

Додатково виявлено, що 27 платежів на суму 3 240 000 грн були проведені без MFA у користувачів, для яких MFA мала бути обов’язковою.

Поріг суттєвості для завдання 900 000 грн.

Завдання.

1. Визначте чисті втрати від 3 шахрайських платежів після повернення банком.
2. Обчисліть % частку 27 платежів без MFA від загальної кількості і від загальної суми.
3. Порівняйте чисті втрати з порогом суттєвості 900 000 грн і зробіть висновок, чи є ризик суттєвого викривлення.
4. Запропонуйте аудиторські процедури, які мають підтвердити або спростувати, що інші 6 платежів на нові реквізити є коректними.

14.11. Кейси з інвестиційного консультування в цифровому середовищі

Ситуаційне завдання 1. Онлайн-анкета і рекомендація портфеля

Умова.

Інвестиційна фірма «Альфа Інвест» надає послугу інвестиційного консультування через мобільний застосунок. Клієнт проходить дистанційну ідентифікацію, заповнює анкету з 10 запитань для визначення ризик-профілю (дохід, цілі, горизонт, досвід, толерантність до ризику). Далі система формує рекомендацію портфеля та автоматично генерує звіт інвестиційної рекомендації у PDF.

За IV квартал 2025 року кількість клієнтів зросла на 40 %. Служба комплаєнсу отримала 27 скарг. Клієнти з низькою толерантністю до ризику отримали рекомендації з високою часткою ризикових інструментів та зазнали суттєвих просідань. Внутрішній IT-звіт вказує на оновлення моделі визначення ризику 15.11.2025 та тимчасове спрощення анкети (2 питання зробили необов'язковими). Частина клієнтів не підтвердила ознайомлення з попередженням про ризики (відсутні записи про чекбокс у логах), але PDF-звіт містить позначку «клієнт ознайомлений».

Інвестиційного консультанта залучили як незалежного консультанта для оцінки:

- коректності процесу формування рекомендацій у цифровому середовищі;
- достатності доказів придатності рекомендацій для конкретних клієнтів.

Завдання.

1. Визначте, де саме виникає ризик невідповідної рекомендації.
2. Окресліть ключові ризики для клієнта і для фірми.
3. Складіть план первинних процедур:
   - тести цифрових контролів;
   - аналітичні процедури;
   - процедури по суті.
4. Визначте мінімальний набір цифрових доказів.

Ситуаційне завдання 2. Розкриття винагород і пов’язаності

Умова.

Фірма «Бета Кепітал» надає інвестиційні рекомендації онлайн. У застосунку є розділ «Рекомендовані рішення», де клієнтам пропонують інвестиційні сертифікати та фонди, емітовані компанією з управління активами, пов’язаною з власниками «Бета Кепітал». У договорі з клієнтом є лише загальна фраза «фірма може отримувати винагороду від третіх осіб», без деталізації щодо розміру комісій, умов і пов’язаності. У цифрових звітах рекомендацій не розкривається факт афілійованості та структура винагород.

Аналітика показує, що 78 % клієнтів отримували рекомендації саме цих продуктів незалежно від заявлених цілей (зокрема, клієнтам зі стратегією «збереження капіталу» пропонували інструменти з підвищеним ризиком). У внутрішньому листуванні продукт-менеджера є повідомлення «давайте просувати наші фонди, бо маржа вища».

Завдання.

1. Визначте, чи має ситуація ознаки конфлікту інтересів або неналежного розкриття інформації клієнту (обґрунтуйте).
2. Класифікуйте можливі порушення за логікою, що саме приховано чи спотворено.
3. Окресліть ризики суттєвого викривлення у звітності фірми та ризики для клієнтів.
4. Наведіть нормативні акти або вимоги, які слід врахувати.

Ситуаційне завдання 3. Чат-бот як канал інвестиційного консультування

Умова.

У застосунку інвестфірми є чат-бот-помічник. Спочатку він відповідав загально (що таке ETF, що таке ризик), але після оновлення почав писати: «Вам краще купити …», «Оптимально для вас – …». Частину діалогів система зберігає не повністю (є лише уривки), а в PDF-звіті рекомендації бот не згадується. Кілька клієнтів поскаржилися, що діяли за порадою бота і втратили кошти.

Завдання.

1. Визначте, у чому проблема: де межа між інформацією і персональною рекомендацією.
2. Складіть план перевірки.

3. Запропонуйте варіанти виправлення помічника і наведіть нормативні акти.

Ситуаційне завдання 4. Партнерська винагорода і зміщення рекомендацій

Умова.

Фірма «Прайм» має партнерську програму з брокером та емітентами на купівлю певних інструментів. Фірма отримує винагороду через застосунок. У договорі з клієнтом є загальна фраза «може отримувати винагороду від третіх осіб», але без деталізації.
Аналітика за IV квартал 2025 року показує, що інструменти з партнерською винагородою потрапляли в рекомендації значно частіше, ніж альтернативи з подібним рівнем ризику. Комплаєнс отримав 14 звернень «нам радять те, за що їм платять». У продуктових KPI є показник «конверсія в партнерські інструменти», але відсутній формалізований контроль, який би доводив, що рекомендації формуються незалежно від винагород.
Аудитора залучили для оцінки:

- ризику конфлікту інтересів;
- повноти розкриття інформації клієнту;
- надійності контролів підбору інструментів.

Завдання.

1. Визначте, які ознаки конфлікту інтересів чи неналежного розкриття наявні в ситуації.
2. Складіть план процедур:

- аналіз партнерських договорів і фактичних виплат;
- тестування правил або алгоритмів відбору і ранжування;
- аналітика рекомендацій.

3. Визначте мінімальний набір доказів.

Ситуаційне завдання 5. Підозра доступу до акаунтів і зміна профілю

Умова.

У грудні 2025 року клієнти фірми «Астра Інвест» повідомили про підозрілі входи в акаунт і зміни налаштувань (ризик-профіль, інвестиційні обмеження, контактні дані). Після цього клієнти отримували рекомендації, які не відповідали їхнім попереднім параметрам. Протягом 10 днів зафіксовано 12 звернень.

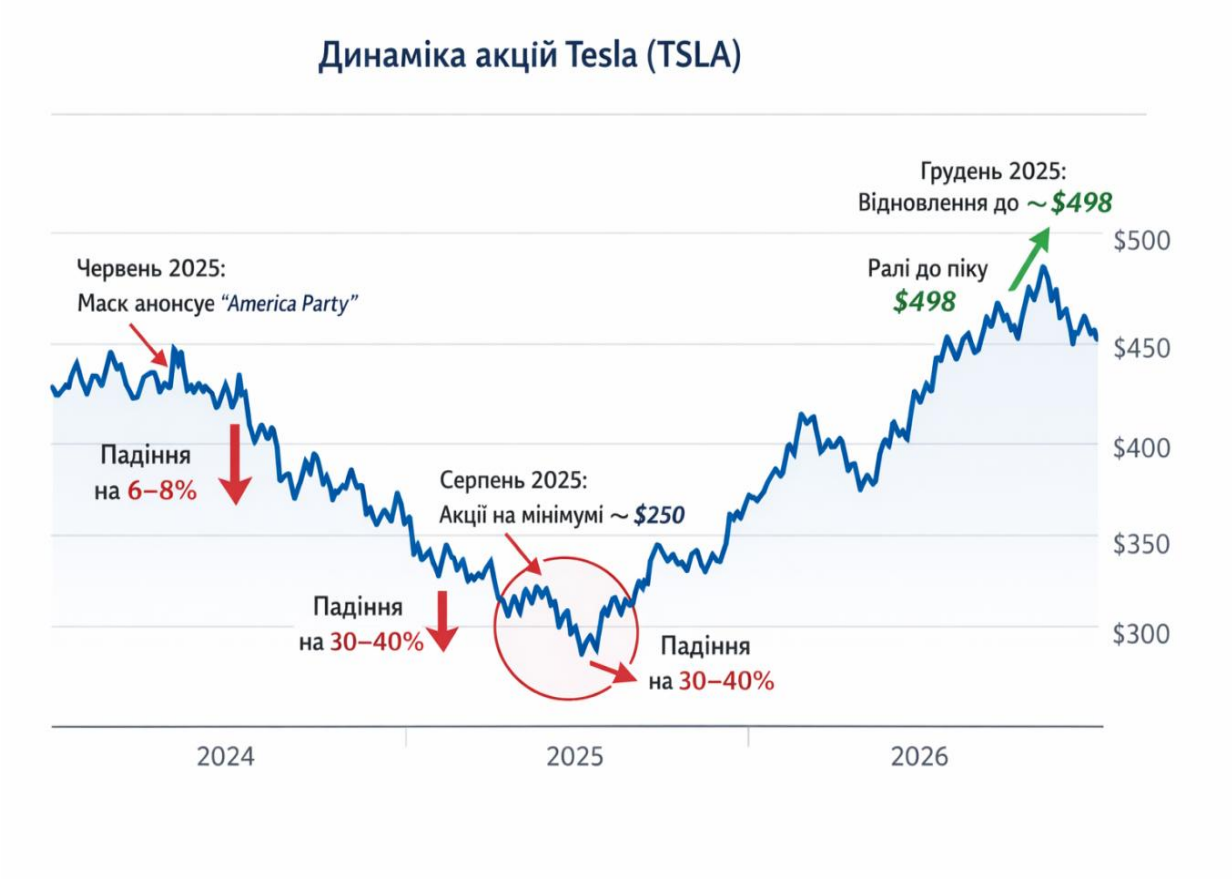
Попередній IT-аналіз показав, що 2FA не є обов’язковим для всіх, журнали безпеки зберігаються в різних системах, а сповіщення про входи з нового пристрою чи чужих IP-адрес налаштовані не для всіх клієнтів. Через розрізненість логів фірма не може швидко відновити ланцюг «вхід → зміна профілю → рекомендація» та довести, що рекомендація формувалася на коректних даних.

Інвестиційного консультанта залучили для оцінки:

- ризиків несанкціонованого доступу;
- достатності доказів щодо коректності профілю клієнта на момент рекомендації.

Завдання.

1. Визначте, у чому основний ризик для клієнта і для фірми.
2. Складіть план процедур.
3. Визначте мінімальний набір цифрових доказів.



Ситуаційне завдання 6. Непередбачувані ризики вітчизняних інвесторів під час інвестицій в акції відомих зарубіжних корпорацій

Умова.

Акції технологічної компанії Tesla до 2025 року постійно зростали в ціні. Вітчизняні інвестори купили їх у червні 2025 року за курсом 450 доларів за акцію. Саме в цей час Ілон Маск оголосив про створення нової політичної партії America Party і розсварився з Дональдом Трампом. Акції Tesla лише за один день впали в ціні на 6–8%, що призвело до втрати близько $65–$70 млрд ринкової капіталізації для акціонерів.

Завдання.

Орієнтуючись на графік курсу акцій за період з червня 2025 до лютого 2026 року, визначити:

1. Чи міг інвестиційний консультант, що радив українським інвесторам купити акції Tesla, передбачити такий варіант подій?
2. Яку пораду варто було дати інвесторам (тримати, купити ще, продати) одразу після червня 2025 року?
3. Визначити дохід або втрати інвестора, якщо він залишив акції у своєму портфелі до лютого 2026 року у нього в портфелі 5 лотів по 100 штук).

Ситуаційне завдання 7. Проектування чат-бота для вітчизняного інвестора, що інвестує у вітчизняні акції та ОВДП (облігації внутрішньої державної позики)

Умова.

Розробити концепцію та логіку функціонування чат-бота, який надає інформаційну та аналітичну підтримку українському приватному інвестору. Вітчизняний інвестор вкладає 60 тис. грн. у акції, що приносять очікувану річну дохідність 14%, і 40 тисяч грн. у ОВДП, що приносять річну дохідність без ризику 18% річних. Чат-бот отримує ці дані і описує можливі результати під час спілкування з інвестором.

Завдання

1. Чи варто змінити питому вагу інвестицій, і як це описати в алгоритмі?
2. Які аргументи варто навести чат-боту в процесі спілкування з інвестором?
3. Коли варто втрутитися інвестиційному консультанту за таких умов?

Ситуаційне завдання 8. Етичні проблеми, що виникають під час інвестиційного консультування та розробка чат-бота, що враховує етику та вимоги законодавства

Умова

Фінансова компанія розробляє чат-бот з інвестиційного консультування фізичних осіб. Інвестор звертається до чат-бота за отриманням консультації щодо інвестування 200 000 грн строком на один рік. Інвестиційний профіль клієнта не визначено. Крім того, виявилося, що компанія – розробник отримує комісійні від продажу цінних паперів, а чат-бот формує рекомендації без аналізу фінансових показників.

Завдання.

1. Визначити потенційні етичні конфлікти, що виникають у даному випадку.
2. Пояснити, чому рекомендація без з'ясування інвестиційного профілю клієнта є неетичною.
3. Проаналізувати конфлікт інтересів, пов'язаного з комісійною винагородою за продаж цінних паперів.

Ситуаційне завдання 9. Різниця в інвестиційному консультуванні стратегічного та портфельного інвесторів

Умова.

До аудиторської фірми, що має у штаті інвестиційного консультанта, одночасно звернулася юридична особа, що бажає інвестувати у значну суму інвестицій в українську аграрну компанію PrJSC MHP (Myronivsky Hliboproduct) – один із найбільших виробників курятини та продуктів харчування в Україні, що провів IPO на Лондонській фондовій біржі LSE, а також фізична особа, що бажає купити акції цієї компанії.

Завдання.

1. Чим має відрізняти звіт для цих інвесторів?
2. Чи досить для фізичної особи аналізу курсу акцій за минулий рік для вироблення рекомендацій щодо інвестування?
3. Які крім фінансових звітів мають аналізуватися документи для вироблення інвестиційних пропозицій для юридичної особи, що хоче стати стратегічним інвестором?

Ситуаційне завдання 10. Як консультувати портфельних інвесторів, що купують акції вітчизняних агрохолдингів

Умова.

Основні аграрні холдинги України, представлені на Варшавській фондовій біржі (WSE): Kernel Holding, Astarta Holding, Milkiland. Фактичні котирування можна переглянути на фінансових платформах (TradingView, WSE, Yahoo Finance або Google Finance).

Завдання.

1. Які основні рекомендації може надати інвестиційний консультант щодо купівлі акцій агрохолдингів?
2. Чи варто тримати акції агрохолдингів за умови значної волатильності?
3. Чи досить даних котирування акцій агрохолдингів для надання рекомендацій щодо їх купівлі?

14.12 Кейси з інтеграції штучного інтелекту в аудиторські процедури

Ситуаційне завдання 1. Якість даних і процес ETL у підготовці аудиторських доказів

Умова.

Аудиторська група отримала від клієнта дані для суцільного аналізу транзакцій. Джерела різні, зокрема ERP, банк, скани договорів та журнали складської системи.

Під час первинного завантаження виявлено такі проблеми:

- частина контрагентів дублюється через різні варіанти написання назви;
- у 18% записів відсутній код центру витрат;
- дати в банківській виписці зсунуті на один день через різні часові пояси;
- для окремих операцій немає зв'язку між накладною та записом у головній книзі.

Завдання.

1. Визначте щонайменше п'ять ризиків викривлення результатів аналізу через помилки на етапах вилучення, трансформації та завантаження даних.
2. Запропонуйте контрольні заходи, які мають бути в клієнта або в аудиторській фірмі для забезпечення цілісності цифрового сліду.
3. Складіть план аудиторських процедур для верифікації якості даних перед запуском моделей.

Ситуаційне завдання 2. Модель машинного навчання для виявлення аномалій у закупівлях

Умова.

Клієнт просить використати модель машинного навчання для детекції аномалій у закупівлях. Модель навчається на даних попередніх періодів і формує список підозрілих транзакцій.

Під час пілоту команда помітила такі обставини:

- у минулих періодах випадки шахрайства майже не маркувалися;
- після зміни політики знижок у поточному році зросла кількість хибних спрацювань;
- розробник не може чітко пояснити, чому модель підсвічує окремі операції.

Завдання.

1. Опишіть життєвий цикл моделі для цієї задачі, включаючи підготовку даних, навчання та ретротестування.
2. Запропонуйте, як сформувати навчальну вибірку за умов недостатнього маркування, щонайменше три підходи.
3. Поясніть, за яких умов результати моделі можуть бути використані як аудиторські докази, і які додаткові підтвердження потрібні.

Ситуаційне завдання 3. Прогнозна аналітика доходів на основі нефінансових даних

Умова.

Аудитор застосовує прогнозну модель для оцінки доходів. Модель використовує нефінансові індикатори, зокрема відвантаження, трафік на сайті та споживання електроенергії.

У звітному кварталі фактична виручка суттєво перевищує прогноз моделі, але менеджмент пояснює це успішною маркетинговою кампанією.

Додатково встановлено такі факти:

- маркетингові витрати зросли, але підтверджувальні документи частково відсутні;
- у системі логістики є ручні коригування даних про відвантаження.

Завдання.

1. Визначте, які ризики суттєвого викривлення доходів тут можливі та які твердження фінансової звітності застосовуються.
2. Запропонуйте план аудиторських процедур, який поєднує аналітичні процедури і тестування деталей.
3. Сформулюйте критерії, за якими аудитор має вирішити, чи розширювати тестування.

Ситуаційне завдання 4. NLP-аналіз договорів і ризик хибних висновків

Умова.

Клієнт має понад 6000 договорів із постачальниками. Для пошуку нестандартних умов використовується система обробки природної мови, яка автоматично позначає договори з ризиковими пунктами.

Під час перевірки результатів виявлено такі проблеми:

- частина сканів низької якості, у тексті багато помилок розпізнавання;
- система позначила як ризикові договори зі стандартними умовами;
- у деяких резюме система вказує умови, яких у тексті договору немає.

Завдання.

1. Оцініть ризики використання OCR та автоматичних резюме для аудиторських цілей.
2. Складіть процедури контролю якості для потоку договорів, включаючи перевірку точності розпізнавання і валідацію висновків, не менше шести процедур.
3. Запропонуйте підхід до вибірки договорів для ручної перевірки, щоб оцінити помилки системи.
4. Сформулюйте правила документування роботи з результатами NLP, щоб забезпечити доказовість.

Ситуаційне завдання 5. Інвентаризація із застосуванням Computer Vision та дронів

Умова.

На складі клієнта проводиться інвентаризація запасів. Клієнт використовує дрони і комп'ютерний зір для підрахунку палет та розпізнавання маркувань.

Аудитор отримав звіт системи, але під час контрольного огляду виявив такі проблеми:

- частина товару накрита плівкою, маркування не зчитується;
- у зоні з поганим освітленням система занижує підрахунок;
- у звіті немає прив'язки результатів до конкретних комірок складу.

Завдання.

1. Визначте ризики суттєвого викривлення обліку запасів при використанні комп'ютерного зору.
2. Запропонуйте комбінований підхід до інвентаризації, який поєднує цифрові результати та спостереження аудитора.
3. Складіть перелік процедур для валідації точності підрахунку системи.
4. Запропонуйте два показники якості для контролю роботи системи підрахунку.

Ситуаційне завдання 6. Блокчейн, потрійний запис і аудит смарт-контрактів

Умова.

Дві компанії ведуть розрахунки через спільний розподілений реєстр. Смарт контракт автоматично здійснює оплату, коли датчик на складі підтверджує надходження товару. Аудитор має доступ до реєстру на читання.

Водночас виявлено такі обставини:

- у постачальника були збої датчиків, але оплати проходили;
- у смарт контракті є можливість ручного перевизначення статусу доставки;
- клієнт не має формалізованого процесу зміни коду смарт контракту.

Завдання.

1. Опишіть, які аудиторські процедури змінюються в середовищі потрійного запису і що залишається критичним.
2. Визначте ключові ризики, пов’язані з кодом смарт контракту та достовірністю даних датчика.
3. Складіть план аудиту смарт контракту як елемента контролю, не менше семи процедур.
4. Запропонуйте мінімальний набір контролів управління змінами для смарт контрактів.

Ситуаційне завдання 7. Використання генеративного ШІ для підготовки аудиторської документації

Умова.

Аудиторська фірма дозволила командам використовувати генеративний ШІ для підготовки чернеток запитів, опису виявлених недоліків і фрагментів звіту.

Один із співробітників завантажив у чат частину робочих файлів клієнта, щоб прискорити написання меморандуму.

Пізніше з’ясувалося, що сервіс працює у хмарі та зберігає історію запитів.

Завдання.

1. Визначте ризики конфіденційності, інформаційної безпеки та дотримання вимог щодо персональних даних.
2. Запропонуйте політику використання генеративного ШІ в аудиті.

3. Складіть перелік контролів якості, які мають гарантувати, що текстові чернетки не містять помилок і не підміняють професійне судження.
4. Опишіть, як документувати використання генеративного ШІ в робочих документах і які розкриття потрібні в межах системи контролю якості.

Ситуаційне завдання 8. Алгоритмічна упередженість у рейтингу ризику контрагентів

Умова.

Клієнт використовує модель, яка формує рейтинг ризику контрагентів. Це інколи називають скорингом. Суть проста: алгоритм присвоює кожному постачальнику числовий бал ризику, наприклад від 0 до 100, де більший бал означає вищий ризик.

Далі цей бал застосовують для відбору контрагентів, які підлягають посиленій перевірці, а також для планування обсягу аудиторських процедур.

Під час аналізу аудитор помітив, що модель систематично присвоює вищі бали ризику постачальникам з окремих регіонів, хоча фактична частота порушень у цих регіонах не вища.

Додатково встановлено такі обставини:

- навчальна вибірка містить переважно дані великих контрагентів, а малих майже немає;
- серед ознак моделі є показник, який тісно пов’язаний з географічною ознакою, наприклад тип логістики або віддаленість складу.

Завдання.

1. Поясніть, які види упередженості можливі в цій ситуації та як вони можуть вплинути на аудиторський підхід і ризик оцінювання.
2. Складіть перелік вимог до прозорості моделі, зокрема які параметри, ознаки та правила прийняття рішень мають бути задокументовані.
3. Запропонуйте, як перевіряти, що використання рейтингу ризику не порушує принципів етики та не створює дискримінаційних наслідків у вибірці для перевірки.

Ситуаційне завдання 9. Генеративний ШІ у роботі аудитора, розрахунок економічного ефекту і контроль ризику

Умова.

Команда аудиту з 6 осіб використовує генеративний ШІ для чернеток запитів до клієнта, опису відхилень і фрагментів управлінського листа.

За 4 тижні зафіксовано 240 запитів до сервісу. На основі цих запитів підготовлено 48 чернеток робочих документів.

Середній час на підготовку 1 чернетки без ШІ був 55 хв, з ШІ став 30 хв. На додаткову перевірку і правки витрачають у середньому 12 хв на 1 чернетку.

Середня внутрішня погодинна ставка аудитора – 900 грн за годину. З 240 запитів 60 містили ПІБ, 18 містили ІПН, 8 містили IBAN. Політика фірми вимагає 0 таких випадків, якщо сервіс не є корпоративним і не має договору обробки даних.

Завдання.

1. Визначте загальну економію часу на 48 чернетках з урахуванням додаткової перевірки.
2. Обчисліть економію витрат у грн, використовуючи ставку 900 грн за годину.
3. Обчисліть % частку запитів, що містили ПІБ, ІПН і IBAN.
4. Якщо фірма встановлює допустимий ліміт 1% запитів з персональними даними, порахуйте, на скільки % пунктів перевищено ліміт для ПІБ.
5. Сформулюйте декілька контрольних правил використання ШІ, які зменшують ризик витоку даних і одночасно не нівелюють отриману економію часу.

Ситуаційне завдання 10. Описова аналітика виручки і контроль сезонності

Умова.

Аудитор перевіряє торговельну компанію, яка продає через магазин та інтернет. У головній книзі виручка за 12 місяців становить 124 800 000 грн. Клієнт надав таблицю щомісячної виручки та повернень. На графіку видно піки у березні та листопаді, а у серпні різке падіння на 28 % порівняно з липнем. Керівництво пояснює це маркетинговою паузою, але одночасно збільшилися повернення у вересні.

Завдання.

1. Побудуйте короткий описовий аналіз виручки і повернень за місяцями та визначте, які періоди є нетиповими.

2. Запропонуйте, які первинні дані і звіти треба зіставити, щоб підтвердити причини падіння виручки у серпні.

3. Визначте, які твердження фінансової звітності є найбільш ризиковими у цій ситуації.

Ситуаційне завдання 11. Прогнозна аналітика доходу з використанням нефінансових показників

Умова.

Компанія надає послуги і має виражену залежність доходу від кількості замовлень та споживання електроенергії обладнанням. Аудитор отримав дані за 24 місяці: дохід, кількість замовлень, години роботи обладнання і споживання електроенергії. У поточному місяці за обліком дохід становить 9 300 000 грн, а за нефінансовими показниками очікуваний рівень виглядає нижчим.

Завдання.

1. Визначте, які фактори доцільно використати для прогнозу очікуваного доходу та як перевірити їх якість.

2. Запропонуйте, як зіставити прогноз з даними обліку і як інтерпретувати різницю між очікуваним та відображеним доходом.

3. Складіть перелік можливих причин відхилення, які потребують перевірки на рівні операцій.

4. Опишіть, як зафіксувати використання прогнозної аналітики у робочих документах аудитора.

Ситуаційне завдання 12. Ризики некоректних даних у машинному навчанні для аудиту

Умова.

Аудитор планує застосувати інструменти аналізу даних і машинного навчання. Дані збираються з 3 джерел:

- облікова система;
- банківські виписки;
- електронний документообіг.

Під час попередньої підготовки з’ясувалося, що назви контрагентів у різних джерелах відрізняються, частина документів має різні дати, а у банківських випсках є платежі без призначення. Є ризик, що модель навчиться на некоректних даних і видасть хибні сигнали.

Завдання.

1. Опишіть ланцюг підготовки даних від джерела до набору для аналізу та вкажіть критичні точки, де можливі спотворення.

2. Визначте, які правила очищення і узгодження довідників потрібні перед використанням даних у моделі.

3. Запропонуйте, як перевірити повноту та узгодженість даних між 3 джерелами до початку аналітики.

4. Складіть коротке рішення аудитора, чи можна використовувати ці дані для машинного навчання без додаткової підготовки.

Ситуаційне завдання 13. Модель машинного навчання для виявлення аномалій у платежах

Умова.

У компанії 18 400 вихідних платежів за рік. Клієнт впровадив модель, яка позначає підозрілі платежі за ознаками суми, частоти, нового одержувача, змін реквізитів та часу проведення. За останній місяць модель позначила 420 платежів як підозрілі. Після ручної перевірки служба контролю підтвердила 12 помилкових або шахрайських операцій. Аудитор має оцінити, чи можна покладатися на таку модель як на елемент внутрішнього контролю.

Завдання.

1. Поясніть, які показники якості роботи моделі доцільно оцінити на підставі даних про позначені та підтверджені випадки.

2. Визначте, які дані про навчання моделі і її оновлення потрібно запросити у клієнта.

3. Запропонуйте, як аудитору діяти, якщо частка хибних спрацювань дуже висока і перевантажує ручну перевірку.

Ситуаційне завдання 14. Обробка природної мови для аналізу договорів і листування

Умова.

Аудитор отримав 1 100 договорів та 6 500 листів з контрагентами. Клієнт пропонує використати систему обробки текстів, яка автоматично виділяє умови про штрафи, відстрочку платежу, зміну ціни та право розірвання. Частину договорів укладено як скан-копії, частину у текстовому форматі. Аудитор має

вирішити, як використати результати такого аналізу для оцінки резервів і зобов’язань.

Завдання.

1. Визначте, які саме умови договорів і листування мають значення для фінансової звітності у цій ситуації.
2. Запропонуйте, як перевірити точність автоматичного виділення умов на вибірці документів.
3. Складіть підхід до документування результатів аналізу текстів як частини аудиторських доказів.
4. Оцініть ризики конфіденційності під час обробки листування та договорів і запропонуйте запобіжні дії.

Ситуаційне завдання 15. Автоматичне формування резюме і ризик помилкових висновків

Умова.

У команді аудиту використовується інструмент, який формує короткі резюме виявлених відхилень і чернетки формулювань для управлінського листа. Після внутрішньої перевірки якості з’ясувалося, що у 3 із 10 резюме інструмент некоректно вказав причину відхилення, а в одному випадку додав факт, якого немає у робочих документах. Керівник завдання хоче залишити інструмент через економію часу.

Завдання.

1. Визначте, як організувати перевірку і затвердження таких резюме перед включенням у документацію.

14.13 Кейси з цифрових технологій інклюзивного аудиту

Ситуаційне завдання 1. Нерівний доступ до подання звернень

Умова.

У громаді вирішили спростити комунікацію мешканців з владою і зменшити черги на телефонній лінії, тому основним каналом подання звернень зробили чат-бот у месенджері. Робилось це для того, щоб звернення подавалися в кілька дій і люди швидше отримуватимуть відповіді, а працівники менше перевантажувалися.

Через 1–2 місяці після запуску почали надходити повідомлення зворотного зв'язку. Частина мешканців задоволена швидкістю комунікації, але з'явилися скарги від людей старшого віку та від тих, хто має порушення зору. Вони пояснюють, що сценарій занадто довгий, багато термінів незрозумілі, а кнопки та пункти меню не завжди зрозумілі та зручні екранному читачу. Старости з віддалених населених пунктів зазначають іншу проблему, а саме нестабільний інтернет. Через поганий сигнал, люди часто не завершують подання звернення і не розуміють, як повернутися до незавершеної заявки.

Щоб знизити негатив у звітах, адміністратор бота додатково налаштував автоматичне об'єднання частини однотипних звернень у загальну категорію. Формально кількість скарг у статистиці стала меншою, але це приховує реальну картину доступності та задоволеності сервісами.

Завдання.

1. Сформулюйте мету інклюзивного аудиту чат-бота як каналу надання публічної послуги.

2. Визначте ризики доступності, зрозумілості і спотворення статистики звернень.

3. Запропонуйте критерії оцінювання роботи чат-бота для різних груп користувачів.

4. Складіть програму аудиторських процедур і перелік джерел інформації.

Ситуаційне завдання 2. Цифровий розрив в отриманні послуг ЦНАП

Умова.

ЦНАП прагне зробити обслуговування населення швидшим, тому запис на прийом поступово перенесли на сайт та в мобільний застосунок. Передбачалося, що це зменшить скупчення людей і дасть змогу полегшити

роботу адміністраторів. Для громадян, які не мають власних смартфонів, у приміщенні встановили термінал самообслуговування. При цьому відмовились від консультанта в холі, щоб не збільшувати витрати.

З часом працівники почали чути від відвідувачів, що частина людей не може записатися на прийом, оскільки не всі мають електронну пошту або не всі вміють користуватися онлайн-формами; хтось має порушення моторики і не встигає зробити необхідні дії або закінчити запис до завершення сесії; хтось погано бачить текст на терміналі через дрібний шрифт і слабкий контраст. Разом із тим, виникла проблема, коли запис відкривається о певній годині, і вільні місця зникають за кілька хвилин. Це створює враження, що шанс мають переважно ті, хто має швидкий інтернет і цифрові навички.

При цьому керівництво орієнтується на низьку кількість скарг. Проте глибинний аналіз ситуації засвідчує, що значна частина невдоволення звучить усно і не потрапляє в офіційну статистику.

Завдання.

1. Визначте ризики інклюзивності електронного запису у ЦНАП.

2. Запропонуйте критерії оцінювання доступності сайту, мобільного застосунку і терміналу.

3. Складіть програму аудиторських процедур щодо запису і фіксації скарг.

4. Запропонуйте коригувальні заходи з вимірюваним результатом.

Ситуаційне завдання 3. Викривлення статистики звернень і скарг

Умова.

Організація прагне краще управляти якістю сервісу, тому запровадила систему обліку та аналізу звернень. Рішення є сучасним та дієвим, оскільки звернення з різних каналів збираються в одному місці, система автоматично визначає тему звернення, розраховує швидкість реагування, а керівництво бачить рейтинги підрозділів за кількістю скарг.

Через деякий час після запуску кількість скарг зменшилась на 30%. Проте працівники фронт-офісу пояснюють, що люди дедалі частіше скаржаться усно, або намагаються писати ввічливіше і стриманіше, побоюючись, що агресивний контекст уповільнять розгляд їх скарг. Громадські активісти звернули увагу на те, що тексти з помилками, простими фразами чи діалектом система часто класифікує як запит або довідку, а не як скаргу. Значна частина звернень про бар'єри доступності потрапляє в категорію «інше» і фактично не включається до аналізу.

Додатково стало відомо, що оператори мають можливість вручну змінювати категорію звернення перед закриттям, і це безпосередньо впливає на показники в аналітичній панелі.

Завдання.

1. Визначте ризики викривлення звітності через автоматичну класифікацію звернень.

2. Сформулюйте критерії перевірки якості класифікації звернень і скарг та ролі їх групи під назвою «інше».

3. Оцініть контроль ручних змін категорій і визначте їх вплив на аналітичні показники.

4. Складіть висновки аудиту і рекомендації щодо усунення виявлених викривлень.

Ситуаційне завдання 4. Приховані бар'єри доступності послуг ЦНАП

Умова.

У ЦНАП громади керівництво прагне показати, що організація працює ефективно й організовано, тому в управлінських звітах акцент робиться на показниках швидкості та продуктивності. Середній час обслуговування становить близько 12 хвилин. Заплановані цільові показники виконуються на належному рівні, а скарг у формалізованій статистиці небагато. На підставі цих даних робиться висновок, що якість надання адміністративних послуг є високою.

Водночас упродовж останніх двох місяців до керівництва ЦНАП почали надходити звернення відвідувачів щодо труднощів отримання послуг для окремих категорій населення. Люди з інвалідністю, батьки з дитячими візками та літні громадяни пояснюють, що на практиці стикаються з такими перешкодами, як: частині відвідувачів складно фізично дістатися до потрібних зон обслуговування через сходи, пороги або вузькі проходи та через відсутність зрозумілої навігації в приміщенні; інші звертають увагу на інформаційні та комунікаційні бар'єри. Це пояснюється тим, що бланки й інструкції сформульовані складно, роз'яснення подаються не в достатньо зрозумілій формі, через що зростає кількість уточнень і повторних візитів. Окремо відвідувачі описують ситуації, коли їм пропонують прийти іншим разом або надати додаткові документи. Ці вимоги прямо не випливають із регламенту надання послуг, що створює відчуття нерівного ставлення та фактичного обмеження доступу до адміністративних послуг ЦНАП.

У відповідь на ці звернення керівництво ЦНАП наполягає, що базові елементи безбар’єрності вже забезпечені, оскільки у приміщенні встановлено пандус і кнопку виклику працівника, а отже, на їхню думку, питання доступності послуг є вирішеним.

Завдання.

1. Сформулюйте мету інклюзивного аудиту адміністративних послуг у ЦНАП.

2. Запропонуйте критерії оцінювання фізичної доступності середовища ЦНАП, його інформаційного та комунікативного забезпечення, а також процедур надання адміністративних послуг.

3. Визначте джерела аудиторської інформації та види аудиторських процедур.

4. Оцініть аудиторський ризик викривлення звітності та вкажіть, які KPI можуть приховувати проблеми інклюзивності.

Ситуаційне завдання 5. Рівні правила конкурсного відбору без рівних можливостей

Умова.

Комунальна установа проводить конкурсний відбір на посаду адміністратора і прагне продемонструвати, що процедура є організованою та однаковою для всіх. Саме тому конкурсні етапи заздалегідь визначені як стандартні: тестування, співбесіда та коротке практичне завдання. Керівництво комунальної установи вважає, що такий уніфікований підхід автоматично гарантує чесність і прозорість відбору.

Під час проведення конкурсу виявилося, що для окремих кандидатів стандартний формат участі створює об’єктивні труднощі. Один із кандидатів має порушення слуху і пояснив, що для повноцінного розуміння запитань та умов виконання завдань йому потрібні письмові інструкції або перекладач жестової мови. Інша кандидатка, яка нещодавно повернулася до професійної діяльності після декретної відпустки, зазначила, що на період адаптації та випробувального терміну їй необхідний гнучкий графік роботи. Обидва звернення фактично стосувалися не зміни вимог до компетентності, а створення умов, за яких кандидати могли б на рівних пройти відбір і виконувати посадові обов’язки.

Однак конкурсна комісія відмовила в урахуванні цих потреб, аргументуючи це тим, що процедура є стандартною і не передбачає жодних відхилень чи пристосувань. У результаті частина кандидатів опинилася в ситуації, коли формально однакові правила означали різні можливості участі. Після

завершення конкурсу керівник установи у підсумковому звіті зробив висновок, що відбір був прозорим і дискримінації не було, оскільки правила застосовувалися однаково до всіх учасників.

Завдання.

1. Визначте, де у конкурсі виникає нерівність можливостей і як враховуються потреби кандидатів.

2. Складіть карту ризиків для установи у разі формального підходу до рівності.

3. Запропонуйте критерії аудиту інклюзивності процедури кадрового відбору і документування рішень конкурсної комісії.

4. Сформулюйте рекомендації щодо порядку розгляду запитів і комунікації з кандидатами.

Ситуаційне завдання 6. Доступність та якість транспортних послуг для школярів

Умова.

Громада організовує підвезення школярів до опорної школи і, плануючи закупівлю транспортних послуг, виходить із потреби забезпечити регулярне перевезення дітей у визначені години. При виборі постачальника послуги основний акцент було зроблено на економії бюджетних коштів, тому переможцем визначили перевізника, який запропонував найнижчу ціну. Передбачалося, що за умови наявності договору та затвердженого маршруту питання якості та доступності перевезення буде вирішене автоматично.

Після фактичного запуску маршруту батьки та працівники школи почали помічати, що організоване перевезення підходить не всім дітям однаково. Зокрема, виявилося, що автобус не обладнаний підйомником і не має передбаченого місця для перевезення дитини на візку, а також відсутні інші елементи, які полегшують посадку та висадку для дітей, яким потрібна додаткова підтримка. Батьки повідомляють, що водій у спірних ситуаціях відмовляється допомагати, посилаючись на те, що це не входить у його обов’язки.

Окремою проблемою стало планування графіка перевезень та зупинок, так як маршрут і час прибуття не враховують потреби дітей з особливими освітніми потребами та дітей із віддалених населених пунктів. Через це частина школярів змушена довго чекати транспорт на холоді, а тривалість дороги для окремих сімей стає непропорційно більшою. У результаті батьки подали колективну

скаргу, наголошуючи, що фактично створено нерівні умови доступу до освіти через спосіб організації перевезення школярів до місця навчання.

У відповідь замовник аргументує свою позицію тим, що в технічних вимогах закупівлі не були прямо прописані спеціальні умови доступності, а отже, на його думку, формального порушення умов конкурсу немає, навіть якщо на практиці частина дітей не може користуватися транспортною послугою на рівних.

Завдання.

1. Визначте, як оцінювати інклюзивність у публічній закупівлі транспортних послуг.

2. Запропонуйте вимоги доступності і безпеки до транспорту, сервісу і маршруту такого виду перевезень.

3. Складіть програму аудиторських процедур щодо тендеру і виконання договору.

4. Сформулюйте висновок аудитора, зазначивши порушення та слабкі місця, а також запропонуйте коригувальні дії для замовника і перевізника.

Ситуаційне завдання 7. Можливості та обмеження онлайн-запису на прийом

Умова.

Медичний заклад первинної ланки запровадив проведення телемедичних консультацій та організував онлайн-запис для того, щоб розвантажити реєстратуру і зменшити черги. Поступово персонал почав спрямовувати пацієнтів саме в онлайн: для запису на прийом – у застосунок, для перегляду результатів аналізів – у електронний кабінет, отримати консультацію – за допомогою телефона або відео-зв’язку. Для закладу це ефективне і раціональне рішення, оскільки зменшується кількість черг у коридорах і зростає кількість приймів за день.

Однак пацієнти з віддалених сіл, літні люди та люди з порушеннями слуху та мовлення почали пояснювати, що така модель для них незручна. Хтось не може стабільно підключитися; хтось не розуміє, як користуватися електронним кабінетом; хтось потребує іншого формату комунікації. З’явилися ситуації, коли люди відкладають звернення до лікаря, адже можуть не впоратись із інтерфейсом онлайн-каналу запису. Частина скарг не фіксується офіційно, оскільки пацієнти говорять про проблему на місці, але не пишуть заяв.

Керівництво при цьому орієнтується на показники кількості онлайн-записів і часу прийому.

Завдання.

1. Визначте ризики інклюзивності, якщо онлайн формат стає основним способом запису на прийом.

2. Запропонуйте критерії оцінювання доступності процедури запису на прийом і комунікації для різних груп пацієнтів.

3. Складіть програму аудиторських процедур щодо даних запису, скарг і практики обслуговування.

4. Запропонуйте коригувальні заходи, що зменшують цифровий розрив та значно підвищують інклюзивність.

Ситуаційне завдання 8. Цифрова доступність сайту громади

Умова.

Громада активно впроваджує цифрові технології в процес комунікації з мешканцями і активно наповнює офіційний сайт важливою інформацією про громаду, основні аспекти її функціонування та стратегічні напрямки розвитку. На ньому розміщені важливі оголошення, рішення ради, порядок отримання публічних послуг, форми заяв, контакти, новини, а також інструкції. Мета такого нововведення – зібрати всю інформацію в одному місці, аби люди могли швидше її знаходити і менше зверталися за нею телефоном та електронною поштою.

Однак працівники органу місцевого самоврядування помічають, що кількість дзвінків із питаннями «де знайти бланк», «як заповнити заяву», «чому не відкривається документ» не зменшується. Під час спілкування мешканці називають різні причини: комусь складно орієнтуватися через заплутану структуру меню; у когось сторінки погано відображаються на телефоні; люди з порушеннями зору кажуть, що частина елементів не читається екранними читачами або має низький контраст; батьки дітей з особливими освітніми потребами та літні люди скаржаться на надто складну мову і відсутність зрозумілих коротких інструкцій.

Окрема проблема стосується документів, так як багато файлів публікуються у форматі PDF або як скан-копії. Мешканці повідомляють, що такі документи часто неможливо швидко знайти через пошук, неможливо виділити текст, а також важко читати з телефону. При цьому в установі вважають, що вимоги виконані, бо інформацію оприлюднено, а скарг у письмовому вигляді небагато.

Керівництво громади просить аудитора оцінити, чи є цифровізація громади інклюзивною, чи відповідає сайт вимогам і чи інформація реально доступна для використання різними групами населення.

Завдання.

1. Сформулюйте мету аудиту цифрової доступності сайту громади і електронних документів.

2. Запропонуйте критерії оцінювання навігації, контенту і якості документів.

3. Складіть програму аудиторських процедур з тестуванням типових маршрутів користувача.

4. Визначте докази для підтвердження висновків і сформулюйте пріоритетні зміни.

Ситуаційне завдання 9. Цифрова доступність електронної черги

Умова.

У ЦНАП громади запровадили електронну чергу. Талон формують у терміналі або через сайт, а виклик до вікна надходить як повідомлення на екрані та як SMS на номер, який людина вказує під час реєстрації.

Після запуску керівництво звітує про скорочення черг, однак відвідувачі почали скаржитися на проблеми з доступом. Частина людей не отримує SMS через нестабільний мобільний зв’язок, а дехто не має телефона або не користується повідомленнями. У таких випадках талон автоматично скасовується, якщо людина не підійшла до вікна протягом 3 хвилин.

Відвідувачі похилого віку повідомляють, що термінал має дрібний шрифт і слабкий контраст, а на екрані виклику швидко змінюються номери. Люди з порушеннями зору не можуть скористатися терміналом без сторонньої допомоги, а окремі відвідувачі з порушеннями слуху зазначають, що персонал інколи дублює виклик голосом, але не завжди.

Працівники пояснюють, що в пікові години вони вручну «закривають» частину талонів як неявку, щоб система не показувала затримки. Формально показники часу очікування покращилися, але є підозра, що статистика не відображає реальну доступність і рівність доступу до послуг.

Завдання.

1. Сформулюйте мету інклюзивного аудиту електронної черги як частини процесу надання послуг.

2. Визначте ризики доступності, справедливості черги і викривлення показників очікування.

3. Запропонуйте критерії оцінювання роботи термінала, виклику до вікна і альтернативних способів інформування.

4. Складіть програму аудиторських процедур і визначте джерела доказів.

Ситуаційне завдання 10. Цифрова доступність порталу соціальної допомоги

Умова.

Громада запустила портал для подання заяв на соціальну допомогу. Подати заяву можна лише онлайн через особистий кабінет. Для входу потрібна електронна ідентифікація, а документи необхідно завантажувати у форматі PDF.

Після запуску працівники соціального відділу почали спрямовувати заявників на портал, пояснюючи це швидкістю обробки. Однак з’явилися скарги від людей, які не мають банківського застосунку або не можуть пройти електронну ідентифікацію. Частина заявників користується кнопковими телефонами або має обмежений доступ до інтернету.

У заяві є поля з технічними термінами, а повідомлення про помилки сформульовані незрозуміло. Якщо документ завантажено неправильно або система не прийняла файл, заявник не бачить, що саме потрібно виправити. Деякі заявки відхиляються автоматично через невідповідність даних у реєстрах, але пояснення причин не надається.

Керівництво оцінює успішність цифровізації за кількістю поданих заяв і середнім часом обробки. Водночас працівники фронт-офісу повідомляють, що люди часто приходять особисто, щоб попросити про допомогу щодо подання онлайн, але ці звернення не фіксуються як проблема доступності.

Завдання.

1. Складіть карту шляху заявника від входу до отримання рішення та визначте етапи, де виникають бар’єри доступу.

2. Оцініть, як портал повідомляє про помилки, відмови та автоматичні відхилення, і як це впливає на можливість подати заяву повторно.

3. Визначте, які аудиторські докази потрібні для перевірки рівності доступу до послуги, включно з даними про спроби подання заяв і зверненнями по допомогу.

4. Запропонуйте заходи, які зменшують бар’єри та забезпечують коректне відображення проблем доступності в управлінській звітності.

Розділ 15

ТЕСТИ ДЛЯ САМОПЕРЕВІРКИ І ПІДСУМКОВОГО КОНТРОЛЮ

Тестові завдання до розділу 1

1. Визначте, що найточніше описує оцифрування.

а) Переведення інформації з паперової або аналогової форми в електронний формат

б) Масштабне переосмислення бізнес-моделі та корпоративної культури під впливом цифрових технологій

в) Управління бізнесом виключно через показники фінансової звітності без змін у процесах

г) Відмова від електронних документів на користь паперових архівів

2. Вкажіть, що у розділі визначено як цифровізацію.

а) Створення цифрового архіву документів без оптимізації операцій

б) Впровадження цифрових технологій у наявні процеси для підвищення їх ефективності

в) Заміну управлінських рішень випадковими алгоритмами без контролю

г) Перехід від електронних даних до аналогових носіїв

3. Визначте ключову ознаку цифрової трансформації.

а) Локальна автоматизація окремих операцій без зміни підходів до управління

б) Лише впровадження IT-рішень у бухгалтерії без перегляду процесів

в) Масштабне переосмислення процесів, клієнтського досвіду та способів управління на основі цифрових технологій

г) Переорієнтація компанії виключно на збільшення кількості паперових процедур

4. Оберіть, що в розділі визначено як центр цифрової трансформації компанії.

а) Лише організаційна структура підрозділів

б) Бізнес-процеси

в) Виключно податкове планування

г) Лише форма подання фінансової звітності

5. Назвіть приклад внутрішнього мотиватора цифрової трансформації бізнесу.

а) Підвищення продуктивності та оптимізація витрат через автоматизацію процесів

б) Зменшення конкуренції на ринку

в) Повна відмова від цифрових каналів взаємодії з клієнтами

г) Ізоляція даних у різних підрозділах без інтеграції

6. Визначте приклад зовнішнього регуляторного чинника, що стимулює цифрову трансформацію.

а) Вимоги законодавства щодо захисту даних та дотримання правил обробки інформації

б) Скасування будь-яких стандартів і правил звітності

в) Заміна контролю на самоперевірку без документування

г) Повне ігнорування кіберризиків у фінансовій сфері

7. Оберіть організаційну зміну, характерну для реінжинірингу бізнес-процесів у цифровій трансформації.

а) Закріплення всіх завдань лише за одним підрозділом без взаємодії

б) Повернення до жорсткої ієрархії та посилення функціональних бар'єрів

в) Формування крос-функціональних команд, орієнтованих на наскрізні процеси

г) Повна відмова від управління змінами та навчання персоналу

8. До якої групи в класифікації цифрових технологій віднесено хмарні технології?

а) Інфраструктурні технології

б) Лише організаційні інструменти без IT-складника

в) Методи фінансового аналізу без використання даних

г) Окремі паперові процедури без автоматизації

9. Визначте, яка технологія в класифікації віднесена до інтелектуальних технологій.

а) Паперовий документообіг

б) Штучний інтелект і машинне навчання

в) Ручна інвентаризація без використання датчиків

г) Складання звітів у статичному форматі без аналізу

10. Вкажіть, що НБУ дозволив банкам у 2022 році для забезпечення безперервної роботи під час війни.

а) Використання хмарних послуг у дата-центрах ЄС, США, Великої Британії та Канади

б) Використання лише локальних серверів без резервування

в) Повну заборону віддаленого доступу до фінансових систем

г) Зберігання облікових даних тільки на паперових носіях

11. Визначте одну з ключових переваг хмарних технологій для бухгалтерського обліку.

а) Зниження доступності даних через відсутність віддаленої роботи

б) Можливість гнучкого доступу до даних онлайн і підтримка роботи з різних локацій

в) Скасування потреби в контролях і перевірках безпеки

г) Збільшення витрат на власні дата-центри як обов’язкова умова

12. Який аспект аудитор має оцінити при використанні клієнтом хмарних систем?

а) Наявність резервних копій і можливість відновлення даних

б) Колір інтерфейсу облікової програми

в) Кількість друкованих документів у сейфі

г) Рівень вологості в офісі бухгалтерії

13. Оберіть твердження, яке в розділі подано як ключову можливість Big Data для аудиту і контролю.

а) Перехід від аналізу даних до повної відмови від перевірок

б) Зменшення обсягу даних шляхом видалення транзакцій

в) Можливість аналізувати 100 % транзакцій і документів замість вибірки

г) Обмеження аудиторських процедур лише усними поясненнями персоналу

14. Назвіть приклад застосування аналітики Big Data у публічних закупівлях, наведений у розділі.

а) Ручне погодження кожної закупівлі без ризик-оцінювання

б) Випадковий відбір закупівель для перевірки без алгоритмів

в) Автоматизовані ризик-індикатори в Prozorro з передачею підозрілих закупівель на перевірку

г) Виключно паперове оформлення тендерної документації без цифрових систем

15. Визначте, що таке RPA (Robotic Process Automation).

а) Ручне виконання операцій без використання програмних інструментів

б) Технологія програмних роботів для автоматизації рутинних завдань у бізнес-процесах

в) Метод збільшення кількості паперових регламентів

г) Процедура відмови від інтеграції систем і даних

16. Оберіть приклад типового застосування RPA в обліку, наведений у розділі.

а) Банківська реконсиляція та звірка операцій між системами

б) Проведення інвентаризації лише на папері без даних

в) Визначення стратегії розвитку компанії без використання облікової інформації

г) Формування звітності шляхом ручного переписування даних з екрана

17. Вкажіть властивість RPA, яка підсилює контроль і доказовість в аудиті.

а) Відсутність журналів операцій і неможливість відстежити дії

б) Заміна облікових даних випадковими значеннями

в) Записування кожної дії бота під час виконання операцій

г) Приховування змін у даних без фіксації подій

18. Дайте визначення Інтернету речей у контексті цифровізації обліку.

а) Мережа фізичних пристроїв із датчиками, що збирають дані та передають їх до інформаційних систем

б) Лише внутрішній облік без будь-яких технічних засобів

в) Ручне введення даних у систему без автоматичного збору

г) Сховище паперових актів і накладних без електронних записів

19. Визначте, яке значення KPI-матриця наводить для тривалості закриття звітного періоду після цифровізації.

а) 8 днів

б) 5 днів

в) 2 дні

г) 15 днів

20. Які мінімальні заходи потрібно вжити, щоб зменшити ризик компрометації облікового запису?

а) MFA, журналювання, обмеження прав

б) Вимкнення журналів подій і обмеження моніторингу

в) Відмова від резервного копіювання та планів відновлення

г) Надання всім користувачам адміністративних прав без обмежень

Ключ відповідей

1 – а; 2 – б; 3 – в; 4 – б; 5 – а; 6 – а; 7 – в; 8 – а; 9 – б; 10 – а.

11 – б; 12 – а; 13 – в; 14 – в; 15 – б; 16 – а; 17 – в; 18 – а; 19 – в; 20 – а.

Тестові завдання до розділу 2

1. Визначте ключову ознаку функціонального підходу в організації обліково-аудиторської діяльності.

а) Орієнтація на наскрізні процеси створення цінності

б) Управління за окремими функціями та підрозділами

в) Інтеграція обліку, контролю та аудиту

г) Фокус на управлінських результатах

2. Вкажіть основний недолік функціонального підходу з позиції аудиту.

а) Надмірна деталізація процесів

б) Відсутність нормативного регулювання

в) Фрагментація інформації та відповідальності

г) Орієнтація на управлінські рішення

3. Оберіть визначення, що відповідає процесному підходу.

а) Управління діяльністю за окремими видами робіт

б) Контроль виконання функцій структурних підрозділів

в) Управління сукупністю взаємопов’язаних процесів

г) Перевірка результатів фінансової звітності

4. Визначте, на чому зосереджується процесно-орієнтована модель обліку та аудиту.

а) На повноваженнях окремих виконавців

б) На логіці послідовного формування інформації

в) На формальній перевірці документів

г) На підроздільній структурі підприємства

5. Що є об’єктом управління в процесно-орієнтованому підході?

а) Окремі облікові функції

б) Структурні підрозділи

в) Наскрізні обліково-аудиторські процеси

г) Фінансова звітність

6. Визначте роль внутрішнього контролю в процесній моделі.

а) Самостійна ізольована функція

б) Формальний етап після завершення операцій

в) Інтегрований елемент процесу

г) Виключно інструмент аудиту

7. Оберіть характеристику процесно-орієнтованого аудиту.

а) Перевірка окремих показників звітності

б) Аналіз логіки формування інформації

в) Формальний контроль дотримання стандартів

г) Оцінювання діяльності підрозділів

8. Вкажіть, на якому рівні процесного опису визначаються межі аудиторської перевірки.

а) Операційному

б) Аналітичному

в) Загальному

г) Деталізованому

9. Визначте призначення аналітичного рівня процесної моделі

а) Фіксація первинних документів

б) Формування фінансової звітності

в) Виявлення ризиків на етапах процесу

г) Проведення тестів контролю

10. На якому рівні здійснюються конкретні аудиторські процедури?

а) Загальний

б) Аналітичний

в) Операційний

г) Стратегічний

11. Як у процесному підході трактуються аудиторські ризики?

а) Як помилки окремих виконавців

б) Як випадкові порушення

в) Як властивість організації процесів

г) Як результат перевірки звітності

12. Визначте джерело аудиторського ризику в процесному аналізі.

а) Обсяг фінансової звітності

б) Різниця між нормативною та фактичною моделлю

в) Кількість облікових рахунків

г) Періодичність перевірки

13. Оберіть визначення поняття «вузьке місце» процесу.

а) Етап з найбільшою кількістю документів

б) Підрозділ з найбільшим навантаженням

в) Етап, що обмежує ефективність процесу

г) Контрольна процедура аудиту

14. Вкажіть приклад типового вузького місця в облікових процесах.

а) Автоматичне формування звітності

б) Ручне введення та перенесення даних

в) Використання інтегрованих систем

г) Аналітичні процедури аудиту

15. Визначте головне призначення аналітичних інструментів у процесному аудиті.

а) Формування первинної інформації

б) Перехід від опису до оцінювання процесів

в) Заміна професійного судження аудитора

г) Автоматизація бухгалтерського обліку

16. Оберіть інструмент, що дає змогу оцінити ефективність процесу.

а) Узагальнення нормативних вимог

б) Аналіз тривалості виконання етапів

в) Формування облікової політики

г) Перевірка фінансових показників

17. З чого має починатися оптимізація обліково-аудиторських процесів?

а) З впровадження програмного забезпечення

б) З аналізу та моделювання процесів

в) З посилення контролю

г) З перегляду звітності

18. Визначте основний критерій оптимізації в обліку та аудиті.

а) Максимальне скорочення часу

б) Мінімізація витрат

в) Баланс ефективності та контролю

г) Повна автоматизація

19. Оберіть роль аудитора в процесно-орієнтованому підході.

а) Виключно контролююча

б) Технічна

в) Аналітично-консультативна

г) Адміністративна

20. Яка ключова перевага інтеграції результатів процесного моделювання в управління?

а) Спрощення облікових процедур

б) Зменшення кількості перевірок

в) Обґрунтованість управлінських рішень

г) Скорочення звітних форм

Ключ відповідей

1 – б; 2 – в; 3 – в; 4 – б; 5 – в; 6 – в; 7 – б; 8 – в; 9 – в; 10 – в.

11 – в; 12 – б; 13 – в; 14 – б; 15 – б; 16 – б; 17 – б; 18 – в; 19 – в; 20 – в.

Тестові завдання до розділу 3

1. Наведіть формулювання, що найточніше відображає сутність цифрової трансформації аудиту.

а) Автоматизація окремих рутинних операцій без зміни підходів до контролю та доказів

б) Комплексна зміна цілей, процедур і доказової бази з фокусом на цифрових даних, IT-контролях та надійності процесів

в) Перехід до перевірки лише паперових документів для підвищення контрольованості

г) Повна відмова від професійного судження аудитора на користь алгоритмів

2. Оберіть приклад простої автоматизації, а не цифрової трансформації.

а) Встановлення бухгалтерської програми для введення даних без перегляду процесів і контрольного середовища

б) Перебудова процесів, інтеграцій та контролів із переходом до системної роботи з електронними доказами

в) Запровадження управління доступами за принципом «необхідного мінімуму» разом із журналюванням подій

г) Організація безперервного моніторингу ризиків і надійності цифрових процедур

3. Вкажіть фактор, що належить до групи «законодавчі та державні вимоги» як драйвер цифровізації обліку й аудиту.

а) Перехід взаємодії з державними органами в електронний формат та вимоги до електронних документів і захисту даних

б) Прагнення підвищити продуктивність через стандартизацію робочих процедур

в) Ринковий тиск на швидкість і прозорість управлінської інформації

г) Стратегічна зміна бізнес-моделі та каналів створення цінності

4. Яка з наведених нижче ознак ринкового тиску позиціонується як фактор цифрових змін у сфері обліку та аудиту?

а) Запит клієнтів та інвесторів на швидкість, прозорість і сумісність процесів, звітності та контролів

б) Зменшення вимог до звітності та контролів унаслідок конкуренції

в) Відмова від цифрових каналів взаємодії для мінімізації ризиків

г) Обмеження доступу до даних лише одним підрозділом без інтеграції

5. Позначте внутрішній драйвер цифрової трансформації, що має економічну природу.

а) Операційна ефективність і оптимізація витрат через автоматизацію повторюваних операцій та регламентних процедур

б) Перехід державних сервісів у режим е-урядування

в) Глобалізація ринку аудиторських послуг

г) Збільшення кількості паперових погоджень для посилення дисципліни

6. Визначте зміст фактору «ризики, безпека та стійкість бізнесу» у цифровому середовищі.

а) Підвищення значущості кіберризиків, управління інцидентами, розмежування повноважень та забезпечення довіри до облікових систем

б) Зменшення потреби в контролі інтеграцій завдяки цифровим каналам

в) Скорочення вимог до документування через швидкість операцій

г) Повна заміна контролю аналітичними процедурами без оцінки IT-середовища

7. Наведіть приклад електронних доказів, значимих для аудиту у цифровому середовищі.

а) Логи, журнали змін і метадані, що підтверджують події та контрольованість цифрових процедур

б) Усні пояснення працівників без будь-якого документування

в) Лише паперові документи без зв’язку з інформаційними системами

г) Суб’єктивні оцінки без перевірки джерел даних

8. Оберіть твердження, яке правильно описує зміну акценту цілей аудиту в умовах цифровізації.

а) Фокус зміщується від підтвердження результату до підтвердження надійності цифрових процесів, що формують цей результат

б) Фокус зміщується від оцінки контролів до повної відмови від контролю

в) Фокус зміщується від цифрових доказів до виключно паперових документів

г) Фокус зміщується від ризик-орієнтованого підходу до інтуїтивних оцінок

9. Вкажіть набір показників якості даних, які аудитор має враховувати у цифровому середовищі.

а) Повнота, точність, своєчасність, узгодженість, унікальність

б) Дизайн, шрифт, колір, форматування, стилі

в) Швидкість інтернету, тип браузера, модель комп’ютера, роздільна здатність екрана

г) Кількість підписів у листуванні та обсяг паперового архіву

10. Визначте ключове завдання етапу планування аудиту у цифровому середовищі.

а) Складання програми перевірки з визначенням обсягу процедур, строків та відповідальних осіб

б) Фінальне узагальнення результатів і формування висновків

в) Виконання процедур первинної верифікації масивів даних

г) Налаштування систем клієнта та впровадження контрольних правил

11. Наведіть дію, характерну для етапу підготовки цифрових інструментів і процедур.

а) Підготовка стандартних програм аналізу, правил відбору, контрольних звітів і форм вивантаження

б) Підписання аудиторського висновку без виконання процедур

в) Передавання робочих файлів третім особам без контролю

г) Проведення лише інтерв’ю без роботи з даними

12. Що належить до первинної верифікації даних після їх отримання з інформаційних систем клієнта?

а) Перевірка повноти даних, коректності періоду та структури масивів перед подальшим аналізом

б) Узгодження управлінських рішень щодо контролів у системі клієнта

в) Виконання реагування на інциденти та відновлення даних

г) Формування річної звітності за клієнта

13. Яка мета аналітичних процедур у цифровому аудиті після підготовки даних?

а) Отримання висновків щодо рівня ризиків та надійності контрольних процедур

б) Заміна робочих документів аудитора на результати листування

в) Відмова від оцінювання контролів через наявність великого масиву даних

г) Заміщення аудитора працівниками служби безпеки

14. Який із наведених нижче варіантів окреслює зміст завершального етапу цифрових процедур?

а) Узагальнення результатів, формування висновків щодо викривлень і недоліків контролю та підготовка висновку і, за потреби управлінського листа

б) Лише вивантаження даних із систем без будь-яких перевірок

в) Лише налаштування доступів у системі клієнта без оцінювання

г) Лише складання первинних документів замість клієнта

15. Оберіть групи методичних прийомів аудиту, які є базовими для збирання доказів.

а) Органолептичні, розрахунково-аналітичні, документальні

б) Інтуїтивні, експериментальні, художні

в) Тільки юридичні без аналітики та документування

г) Виключно статистичні без перевірки первинних джерел

16. Вкажіть перелік складових корпоративного управління, з якими пов’язано аудит і фінансову безпеку.

а) Комплаєнс, ризик-менеджмент, внутрішній контроль, IT-безпека

б) Маркетинг, логістика, реклама, PR

в) Продажі, виробництво, склад, постачання

г) Виключно бухгалтерія та кадрова служба

17. Яка роль аудитора у системі контролю в цифровому середовищі?

а) Незалежна оцінка ризиків і контролів та підтвердження надійності процесів і систем, що формують звітні показники

б) Впровадження та адміністрування контрольних правил у системі клієнта

в) Оперативне реагування на інциденти та розслідування атак

г) Керування бізнес-процесами та розподіл функцій між підрозділами

18. Яка роль фахівця з фінансової безпеки у цифровому середовищі?

а) Превентивна й операційна функція: організація моніторингу, впровадження механізмів захисту та координація дій під час інцидентів

б) Висловлення незалежної думки щодо фінансової звітності

в) Повна заміна внутрішнього аудиту у питаннях оцінки контролів

г) Розроблення аудиторської програми та формування робочих документів

19. Яка з наведених нижче ситуацій найбільш влучно відображає створення конфлікту інтересів і загрозу незалежності аудитора в цифрових проєктах?

а) Участь аудитора у налаштуванні систем або контролів, які надалі підлягають його оцінці

б) Фіксація обмежень доступу та документування якості даних у робочих файлах

в) Застосування альтернативних процедур для підтвердження висновків за потреби

г) Підготовка управлінського листа з рекомендаціями за результатами перевірки

20. Оберіть пакет заходів цифрової безпеки, що відповідає вимогам конфіденційності та принципу «необхідного мінімуму» щодо доступу.

а) Керування доступами, багатофакторна автентифікація, шифрування, обмеження копіювання та контролі обміну даними

б) Надання всім користувачам адміністративних прав і вимкнення журналів подій

в) Вільне копіювання робочих файлів на особисті носії без обліку доступів

г) Передавання даних через електронну пошту без контролю та політик

Ключ відповідей

1 – б; 2 – а; 3 – а; 4 – а; 5 – а; 6 – а; 7 – а; 8 – а; 9 – а; 10 – а

11 – а; 12 – а; 13 – а; 14 – а; 15 – а; 16 – а; 17 – а; 18 – а; 19 – а; 20 – а

Тестові завдання до розділу 4

1. Яке твердження відповідає підходу МСА до цифрового аудиту?

а) Для цифрового аудиту передбачено окремий міжнародний стандарт, який замінює інші МСА

б) Вимоги щодо ІТ та цифрових інструментів інтегровано в чинні МСА без виокремлення окремого стандарту

в) Цифрові інструменти застосовують лише під час складання аудиторського висновку

г) МСА дозволяють ігнорувати ІТ-середовище клієнта, якщо є паперові документи

2. На чому акцентує МСА 315 під час оцінювання ризиків в ІТ-середовищі?

а) Лише на перевірці друкованих форм без аналізу системи

б) На глибокому розумінні технологічного середовища, доступу до даних та наявності загальних і прикладних ІТ-контролів

в) Виключно на підтвердженні залишків через запити контрагентам

г) Лише на оцінці компетентності керівництва без аналізу процесів і систем

3. Яке завдання МСА 330 пов’язано з ризиками, що походять з ІТ?

а) Визначення вимог до електронного підпису в системі клієнта

б) Дії аудитора у відповідь на оцінені ризики, у тому числі перевірка того, як суб’єкт господарювання відповів на ІТ-ризики

в) Затвердження облікової політики клієнта

г) Організація електронного документообігу на підприємстві

4. У якій із наведених нижче ситуацій зростає ризик суттєвого викривлення фінансової звітності через ІТ?

а) Використання простого паперового журналу операцій

б) Застосування складних ERP-систем або хмарних рішень без належних ІТ-контролів

в) Повна відсутність облікових записів у системі

г) Застосування виключно ручних підписів на паперових документах

5. Визначте, що є наслідком неналежного використання цифрових інструментів під час аудиту.

а) Автоматичне зниження аудиторського ризику без додаткових процедур

б) Ризик викривлення результатів перевірки або неналежної оцінки інформаційних ризиків

в) Повне усунення потреби в аудиторських доказах

г) Скасування вимог до незалежності аудитора

6. Який основний нормативно-правовий акт визначає засади аудиторської діяльності в Україні за умов цифровізації?

а) Закон України «Про інформацію»

б) Закон України «Про аудит фінансової звітності та аудиторську діяльність»

в) Закон України «Про електронні документи та електронний документообіг»

г) Закон України «Про захист інформації в інформаційно-комунікаційних системах»

7. Наведіть перелік принципів, які у розділі підкреслено як базові для аудиту незалежно від цифрового формату.

а) Належне документування, професійне судження, незалежність та відповідальність аудитора

б) Маркетинг, ціноутворення, розширення клієнтської бази та реклама

в) Оперативність, гнучкість, мінімізація контролів та максимальна автоматизація

г) Перехід на виключно усні підтвердження без документування

8. Вкажіть, що означає вимога належного документування у цифровому аудиті.

а) Достатньо зберегти лише кінцевий аудиторський висновок без робочих документів

б) Потрібно фіксувати хід процедур, отримані докази та застосовані цифрові інструменти у робочій документації

в) Документування не потрібне, якщо використано аналітичні процедури

г) Документування замінюється лише скріншотами без опису процедур

9. Позначте закон, який визначає правовий режим створення, обробки, зберігання та використання електронних документів.

а) Закон України «Про електронні документи та електронний документообіг»

б) Закон України «Про аудит фінансової звітності та аудиторську діяльність»

в) Закон України «Про бухгалтерський облік та фінансову звітність в Україні»

г) Закон України «Про господарські товариства»

10. Встановіть, які ключові поняття прямо названо в розділі як такі, що визначені Законом «Про електронні документи».

а) Електронний документ, електронний підпис, оригінал електронного документа, електронний документообіг, суб’єкти електронного документообігу

б) Тільки електронна пошта та вебсайт підприємства

в) Лише бухгалтерські рахунки та регістри обліку

г) Виключно фінансова звітність і аудиторський висновок

11. У чому полягає значення норм про електронні документи для цифрового аудиту?

а) Електронні документи не можуть бути аудиторськими доказами

б) Електронні документи визнаються юридично значущими та можуть бути рівноцінними паперовим доказам

в) Електронні документи дозволено використовувати лише для внутрішнього обігу

г) Електронні документи визнаються лише після нотаріального посвідчення

12. Який із наведених нижче законів пов’язаний з електронною ідентифікацією та довірчими послугами?

а) Закон України «Про електронну ідентифікацію та електронні довірчі послуги»

б) Закон України «Про рекламу»

в) Закон України «Про державну статистику»

г) Закон України «Про бухгалтерський облік та фінансову звітність в Україні»

13. Вкажіть, яку функцію для цифрового аудиту виконує законодавство про захист інформації в інформаційно-комунікаційних системах.

а) Регулює порядок ведення касових операцій

б) Встановлює вимоги до конфіденційності, цілісності та доступності електронних доказів і даних

в) Скасовує потребу в контролях доступу до облікових систем

г) Дозволяє зберігати аудиторські документи без обмежень та захисту

14. Визначте елемент, доступ аудитора до якого прямо пов’язано з вимогами захисту інформації.

а) Календар зустрічей керівництва

б) Віддалені підключення до систем клієнта

в) Дизайн маркетингових матеріалів

г) Плани продажів за майбутні періоди

15. Які органи в Україні здійснюють суспільний нагляд і професійне регулювання аудиторської діяльності?

а) Національний банк України та Державна податкова служба України

б) Орган суспільного нагляду за аудиторською діяльністю та Аудиторська палата України

в) Міністерство культури України та Державна служба статистики

г) Антимонопольний комітет України та Рахункова палата України

16. Визначте, який аспект цифровізації все більше враховує система зовнішнього контролю якості аудиторських послуг.

а) Наявність рекламних матеріалів аудиторської фірми

б) Дотримання цифрових процедур і належне зберігання електронних робочих документів

в) Кількість паперових копій звітності клієнта

г) Відсутність будь-яких цифрових інструментів у роботі аудитора

17. Укажіть, як у розділі сформульовано визначення електронного документа.

а) Документ, що існує лише у вигляді паперової копії

б) Документ, інформація в якому зафіксована у формі електронних даних і містить обов’язкові реквізити

в) Будь-яке повідомлення в соціальній мережі без реквізитів

г) Файл без ідентифікації автора та без реквізитів

18. Встановіть, чим у цивільно-правових відносинах зазвичай визначається порядок обміну електронними документами між контрагентами.

а) Лише усною домовленістю без фіксації умов

б) Домовленістю сторін і умовами договору

в) Виключно наказом керівника одного з контрагентів

г) Тільки рішенням аудиторської фірми

19. Позначте інструмент, який у розділі названо ключовим для цілісності та доказовості електронної інформації.

а) Електронна таблиця без захисту

б) Електронний цифровий підпис або кваліфікований електронний підпис

в) Скан-копія документа без реквізитів

г) Будь-який пароль користувача без сертифіката

20. Укажіть, які саме елементи електронного документообігу можуть слугувати джерелами аудиторських доказів.

а) Лише фінансові коефіцієнти без первинних даних

б) Метадані документа, час підписання, відомості про підписанта, історія змін і журнали подій

в) Виключно усні пояснення відповідальних осіб

г) Лише зведені підсумки без можливості простеження документа

Ключ відповідей

1 – б; 2 – б; 3 – б; 4 – б; 5 – б; 6 – б; 7 – а; 8 – б; 9 – а; 10 – а

11 – б; 12 – а; 13 – б; 14 – б; 15 – б; 16 – б; 17 – б; 18 – б; 19 – б; 20 – б

Тестові завдання до розділу 5

1. Визначте, що найточніше характеризує моніторинг фінансової безпеки підприємства.

а) Систематичне спостереження, вимірювання та оцінювання стану фінансової безпеки з раннім виявленням загроз

б) Разова перевірка фінансової звітності після завершення року

в) Лише контроль правильності первинних документів бухгалтерією

г) Виключно аналіз ринкової кон’юнктури без оцінювання внутрішніх ризиків

2. Укажіть приклад події, яка є сигналом для посиленого моніторингу ліквідності.

а) Зростання частки безготівкових розрахунків у продажах

б) Повторювані касові розриви та затримки платежів постачальникам

в) Збільшення кількості працівників у штаті

г) Перехід на інший формат управлінської звітності

3. Яка роль моніторингу в оперативно-тактичному управлінні фінансовою безпекою?

а) Забезпечення швидкого реагування на відхилення показників і появу загроз

б) Формування аудиторського висновку щодо фінансової звітності

в) Визначення стратегічної місії підприємства

г) Підготовка податкових декларацій

4. Які джерела даних доцільно використовувати для індикаторів фінансової безпеки, окрім фінансової звітності?

а) Лише статистичні звіти зовнішніх органів

б) Управлінська та нефінансова звітність, параметри організації процесів і технічні характеристики захисту

в) Виключно маркетингові опитування споживачів

г) Тільки дані про котирування акцій на біржі

5. Оберіть показник, який належить до індикаторів ефективності системи фінансової безпеки.

а) Окупність

б) Захищеність

в) Відновлюваність

г) Сумісність з іншими системами

6. Визначте, який індикатор системи фінансової безпеки характеризує час реагування на загрози та швидкість оброблення інформації для ухвалення рішень.

а) Час реакції на загрозу та швидкість оброблення інформації для ухвалення рішень

б) Частку інформаційних систем, що перебувають у хмарі

в) Суму активів, захищених договорами страхування

г) Рівень податкового навантаження підприємства

7. Що характеризує індикатор «частота моніторингу»?

а) Періодичність оновлення й перевірки контрольних показників для своєчасного виявлення загроз

б) Кількість видів фінансової звітності, яку складає підприємство

в) Частоту зміни керівника фінансової служби

г) Інтенсивність рекламних кампаній

8. Наведіть приклад IT-ризику, пов’язаного з порушенням принципу розмежування повноважень.

а) Одна особа може створювати, погоджувати і відображати операції без незалежної перевірки

б) Сезонне зростання попиту на продукцію

в) Підвищення курсу іноземної валюти

г) Збільшення кількості точок продажу

9. Позначте наслідок для аудиту, який є найімовірнішим за відсутності належного резервного копіювання даних.

а) Зменшення податкових платежів

б) Втрата первинної інформації та обмеження можливості підтвердження операцій

в) Автоматичне підвищення достовірності звітності

г) Спрощення процедур інвентаризації

10. Який опис найкраще відповідає ризикам ліквідності?

а) Втрати через коливання валютних курсів

б) Брак грошових коштів для своєчасних розрахунків за зобов’язаннями

в) Зростання витрат через зміну процентних ставок

г) Неповернення дебіторської заборгованості

11. У чому полягає суть комплексного підходу до планування аудиту з урахуванням IT-ризиків і ризиків фінансової безпеки?

а) Перевіряються лише арифметичні підрахунки у фінансовій звітності

б) Оцінюється надійність цифрового середовища формування даних і фінансова стійкість підприємства у різних горизонтах

в) Аналізуються тільки показники прибутковості без урахування ризиків

г) Виключається використання аналітичних процедур

12. Яка з наведених нижче дій аудитора найбільш точно відповідає етапу попереднього ознайомлення з клієнтом?

а) Аналіз моделі бізнесу, джерел фінансування та загальної залежності від інформаційних систем

б) Виконання суцільної інвентаризації всіх запасів

в) Складання податкової звітності за клієнта

г) Визначення остаточного аудиторського висновку

13. На якому етапі планування доцільно аналізувати інформаційні потоки та логіку формування фінансових показників?

а) Попереднє ознайомлення

б) Оцінка середовища внутрішнього контролю

в) Ідентифікація суттєвих ризиків

г) На етапі аналізу інформаційних потоків та інтеграції систем

14. Вкажіть, чому під час планування важливо оцінювати залежність від зовнішніх ІТ-постачальників.

а) Щоб уникнути формування фінансової звітності

б) Щоб визначити вплив SLA (угоди про рівень сервісу), безперервності сервісу та контролів постачальника на ризики викривлення даних і безперервність діяльності

в) Щоб замінити внутрішній контроль зовнішнім провайдером

г) Щоб зменшити кількість процедур підтвердження від третіх сторін до нуля

15. Визначте, що найбільш коректно описує аудиторські докази.

а) Будь-яка інформація, отримана аудитором і використана для обґрунтування висновків і підтвердження тверджень звітності

б) Лише усні пояснення керівництва без документів

в) Тільки первинні документи на папері

г) Виключно результати інвентаризації

16. За яким набором критеріїв слід оцінювати отримані докази?

а) Обсяг доказів і швидкість їх отримання

б) Доречність, надійність і достатність

в) Лише наявність електронного підпису

г) Лише відповідність доказів бюджету аудиту

17. Укажіть приклад ІТ-доказів.

а) Протоколи інвентаризації основних засобів

б) Журнали подій, логи доступу та системні звіти з облікової системи

в) Фотографії виробничих приміщень

г) Виписки з реєстрів судових рішень

18. Позначте характеристику цифрових доказів, яка пов’язана з наявністю «аудиторського сліду» дій користувачів.

а) Електронна форма

б) Логування та сліди дій користувачів

в) Швидкість накопичення даних

г) Множинність джерел

19. Визначте ризик, який посилюється через дистанційний доступ до цифрових даних під час аудиту.

а) Підвищення ймовірності несанкціонованого доступу та потреба в сильній автентифікації і захищених каналах

б) Автоматичне зниження ризику шахрайства

в) Відсутність необхідності в підтвердженнях від банків

г) Повне усунення потреби у професійному судженні аудитора

20. Вкажіть основне призначення робочих документів аудитора в цифровому середовищі.

а) Оформлення маркетингових матеріалів для клієнта

б) Фіксація виконаних процедур, отриманих доказів і професійних суджень із забезпеченням простежуваності та контролю доступу

в) Заміна системи внутрішнього контролю підприємства

г) Автоматичне формування фінансової звітності замість бухгалтерії

Ключ відповідей

1 – а; 2 – б; 3 – а; 4 – б; 5 – а; 6 – а; 7 – а; 8 – а; 9 – б; 10 – б.

11 – б; 12 – а; 13 – г; 14 – б; 15 – а; 16 – б; 17 – б; 18 – б; 19 – а; 20 – б.

Тестові завдання до розділу 6

1. Дайте визначення інформаційної системи підприємства.

а) Набір окремих електронних таблиць для обліку

б) Сукупність програмних засобів, баз даних, технічної інфраструктури та організаційних процедур

в) Лише база даних із первинними документами без процедур роботи

г) Будь-яка комп’ютерна мережа, незалежно від її призначення

2. В чому полягає суть ефекту «одного джерела інформації»?

а) Кожен підрозділ веде власні дані й узгоджує їх вручну наприкінці місяця

б) Дані дублюються в різних системах для підвищення надійності

в) Дані вводяться один раз і використовуються всіма підрозділами у спільному інформаційному просторі

г) Дані зберігаються лише локально на робочих станціях бухгалтерів

3. Визначте вимогу до інформаційної системи, яка безпосередньо підтримує аудит і контроль.

а) Максимальне скорочення кількості первинних документів

б) Простежуваність облікових даних від первинного документа до звітності

в) Повна відмова від правил доступу для прискорення роботи

г) Заміна внутрішніх регламентів виключно зовнішніми стандартами

4. Зазначте завдання інформаційних систем підприємства, наведене у розділі.

а) Проведення юридичної експертизи договорів замість підрозділу права

б) Передавання й обмін інформацією між підрозділами та зовнішніми контрагентами і державними системами

в) Формування аудиторського висновку автоматично без участі аудитора

г) Управління персоналом виключно через усні розпорядження

5. Оберіть опис, який відповідає гібридному розгортанню інформаційної системи.

а) Система працює лише на серверах підприємства без доступу ззовні

б) Система повністю розміщена у постачальника з доступом через інтернет

в) Частина сервісів у хмарі, а частина – локально на ресурсах підприємства

г) Система працює лише на одному пристрої без мережі

6. Розпізнайте режим обробки даних «онлайн або реального часу».

а) Операції й контроль виконуються одразу під час введення даних

б) Обробка виконується періодами за розкладом без негайного контролю

в) Дані вводяться лише після завершення звітного періоду

г) Контроль здійснюється виключно вручну після вивантаження даних у файл

7. На якому етапі життєвого циклу інформаційні системи виконують обстеження об’єкта автоматизації та аналіз бізнес-процесів?

а) Розробка концепції інформаційної системи

б) Реалізація і адаптація програмного продукту

в) Сервісне обслуговування та оновлення в експлуатації

г) Промислова експлуатація після приймання

8. На якому етапі формується технічне завдання як основний документ із вимогами до якості, безпеки та інтеграції?

а) Етап розробки концепції

б) Етап розроблення технічного завдання

в) Етап сервісного супроводу

г) Етап архівації даних

9. Що, згідно з розділом, входить до етапу впровадження в експлуатацію, тестування та налагодження?

а) Лише написання коду без перевірок і документації

б) Перевірка відповідності вимогам технічного завдання, дослідна експлуатація, навчання персоналу та приймальні випробування

в) Тільки вибір постачальника обладнання без налаштування системи

г) Виключно перенесення даних без усунення недоліків

10. Позначте логічний ланцюг, на якому базується послідовність роботи BAS у розділі.

а) Звітність → проведення → первинний документ → регістри

б) Первинний документ → проведення → регістри або обороти → звітність

в) Регістри → первинний документ → звітність → проведення

г) Довідники → звітність → первинні документи → каса

11. У чому полягає аудиторська цінність BAS як середовища перевірки?

а) Дає змогу ігнорувати первинні документи, використовуючи лише підсумкові показники

б) Дозволяє простежити «ланцюг доказів» від події до показника у фінансовій звітності

в) Забезпечує автоматичне підтвердження всіх операцій без контролю доступів

г) Повністю виключає потребу в професійному судженні аудитора

12. Вкажіть джерело в BAS, яке дозволяє встановити, які дії виконували користувачі та які події відбувалися в інформаційній базі.

а) Лише друкована форма облікової політики

б) Журнал реєстрації подій

в) Паперовий журнал реєстрації господарських операцій

г) Опис посадових інструкцій бухгалтерів

13. Визначте, до яких загальних IT-контролів у розділі віднесено розмежування доступів і ролей.

а) До прикладних контролів введення даних у документах

б) До загальних контролів IT-середовища

в) До контролів узгодження платежів перед проведенням

г) До контрольних звірок залишків після обробки даних

14. Позначте приклад прикладного контролю, наведений у розділі.

а) Регулярні резервні копії та тестові відновлення

б) Перевірка обов’язкових реквізитів документів під час введення

в) Політика зберігання архівів і доступу до них

г) План дій на випадок технічних збоїв

15. Оберіть приклад контрольної звірки на виході, що доповнює прикладні контролі.

а) Виявлення від’ємних залишків запасів та аналіз непроведених документів

б) Створення нових ролей доступу для користувачів

в) Погодження змін у програмному коді постачальником

г) Перенесення бази даних на інший сервер без перевірок

16. Визначте контроль, який у розділі пов’язано зі зниженням ризику несанкціонованого доступу до бази.

а) Спільні логіни для швидкого входу всіх користувачів

б) Індивідуальні користувачі, ролі та мінімально необхідні права доступу, заборона спільних логінів

в) Надання всім користувачам прав адміністратора для уникнення блокувань

г) Відсутність журналу входів для зменшення навантаження на систему

17. Укажіть, який контроль застосовують для зменшення ризику внесення змін у минулі періоди та маніпуляції показниками звітного періоду.

а) Повна заборона створення первинних документів

б) Закриття періоду та обмеження редагування в закритих періодах, коригування через окремі документи

в) Скасування регламенту закриття місяця

г) Дозвіл перепроводити будь-які документи без фіксації подій

18. Позначте набір контролів, який у розділі віднесено до забезпечення безперервності та збереження даних.

а) Резервні копії, контроль доступу до архівів, тестові відновлення та плани дій на випадок технічних збоїв

б) Тільки погодження платежів перед проведенням

в) Лише контроль допустимих значень у довідниках

г) Виключно контроль унікальності нумерації документів

19. Визначте, що найкраще описує процедуру управління змінами в IT-середовищі.

а) Зміни виконуються одразу в робочій базі без тестування, щоб не втрачати час

б) Використовують тестову базу, погодження, фіксацію версій та план впровадження змін

в) Оновлення виконують лише за усною вказівкою без документування

г) Будь-які доопрацювання заборонені незалежно від потреб бізнесу

20. Знайдіть мету прикладу контролю «перевірка проведення документів за певний період», наведеного у розділі.

а) Підвищити швидкість введення документів шляхом зменшення реквізитів

б) Виявити непроведені документи, які не відображені в обліку та звітності

в) Забезпечити автоматичне погодження всіх операцій без участі відповідальних осіб

г) Замінити звірку оборотів і залишків виключно інтуїтивною оцінкою

Ключ відповідей

1 – б; 2 – в; 3 – б; 4 – б; 5 – в; 6 – а; 7 – а; 8 – б; 9 – б; 10 – б.

11 – б; 12 – б; 13 – б; 14 – б; 15 – а; 16 – б; 17 – б; 18 – а; 19 – б; 20 – б.

Тестові завдання до розділу 7

1. Визначте, що найточніше описує комп’ютеризовані засоби аудиту (CAATs).

а) Набір шаблонів робочих документів аудитора для оформлення висновку

б) Сукупність інструментів і методів, що допомагають виконувати аудиторські процедури та отримувати докази в електронному середовищі

в) Лише програмні засоби бухгалтерського обліку підприємства

г) Виключно статистичні методи формування вибірки без використання IT

2. Вкажіть методологічне значення класифікації CAATs.

а) Дозволяє обрати інструменти під конкретні цілі, етапи та рівень автоматизації аудиту

б) Потрібна лише для юридичного визначення вартості ліцензій

в) Використовується виключно для навчальних прикладів без практичної цінності

г) Застосовується тільки для розподілу користувачів за ролями в ERP

3. Оберіть класифікаційну ознаку, за якою CAATs поділяються на частково та повністю автоматизовані.

а) За типом програмного забезпечення

б) За ступенем автоматизації аудиторських процедур

в) За характером оброблюваних даних

г) За рівнем інтеграції з корпоративними системами

4. Визначте, до якої категорії CAATs віднесено табличні процесори Microsoft Excel і Google Sheets.

а) Повністю автоматизовані засоби без участі аудитора

б) Частково автоматизовані засоби аудиту загального призначення

в) Виключно засоби документування аудиту

г) Засоби тестування контролів на рівні прикладних систем

5. Який основний напрям використання табличних процесорів в аудиті?

а) Побудова бухгалтерських проводок замість облікової системи

б) Підготовка даних, первинна перевірка та виконання аналітичних процедур

в) Автоматичне визначення суттєвості без професійного судження

г) Заміна аудиторського висновку автоматично згенерованим звітом

6. Чому підготовка і первинна перевірка даних у табличному процесорі розглядається як аналітична процедура?

а) Тому що це єдина процедура, яку дозволяють стандарти аудиту

б) Тому що аудитор має інтерпретувати результати перевірок і оцінювати ризики, а не лише виконувати технічні дії

в) Тому що вона завжди виконується без імпорту даних з облікових систем

г) Тому що її можна виконувати лише безпосередньо в ERP без експорту

7. Оберіть інструмент табличного процесора, який найдоцільніше застосувати для швидкого виділення ризикових операцій за заданими умовами.

а) Умовне форматування

б) Перевірка правопису

в) Зміна теми оформлення аркуша

г) Автозаповнення серій назв файлів

8. Вкажіть крок, який відповідає етапу імпорту даних у табличний процесор.

а) Додавання колонок «Місяць операції» та «Ознака ризику»

б) Побудова зведених таблиць і графіків для оцінки тенденцій

в) Завантаження файлу з облікової системи та перевірка коректності полів і форматів, зокрема дат

г) Формування остаточного аудиторського висновку

9. Визначте, яку типову проблему даних пов’язують з ризиком завищення доходів або витрат.

а) Дублювання записів, зокрема повторення номера документа

б) Від’ємні суми як ознака коригувань

в) Текстовий формат сум

г) Відсутність суми або дати операції

10. Оберіть приклад хибних даних, які прямо пов’язані з ризиком помилок у розрахунках.

а) Від’ємні суми

б) Текстовий формат сум

в) Повторення номера документа

г) Відсутня дата операції

11. Яке завдання належить до типових процедур первинної перевірки даних у табличному процесорі?

а) Пошук порожніх значень, повторюваних номерів документів та операцій з нульовими або від’ємними сумами

б) Визначення аудиторського ризику лише за експертною оцінкою без аналізу даних

в) Створення резервної копії ERP та відновлення бази даних

г) Формування плану рахунків і кореспонденцій для обліку

12. Що означає «структурування даних» після первинної перевірки?

а) Видалення всіх нетипових операцій без аналізу причин

б) Перенесення даних у текстовий формат для зручності читання

в) Додавання допоміжних колонок для подальшого групування та аналізу динаміки показників

г) Зміна кольорів таблиці для кращої візуалізації

13. Вкажіть корисну для командного аудиту функцію Google Sheets.

а) Спільна робота та коментування

б) Автоматичне підписання аудиторського висновку КЕП

в) Налаштування прав доступу до журналів подій ERP

г) Формування бухгалтерських регістрів без облікової системи

14. Оберіть формулу, яка є прикладом для виділення місяця операції в Google Sheets.

а) =TEXT(A2;"MMMM")

б) =SUM(A2:A100)

в) =VLOOKUP(A2;B:C;2;0)

г) =IFERROR(A2;0)

15. Визначте ключову методологічну перевагу спеціалізованих аналітичних платформ IDEA та ACL.

а) Використання лише ручних вибірок замість суцільного аналізу

б) Можливість суцільного аналізу великих масивів даних та автоматизованого виявлення аномалій

в) Відмова від документування процедур на користь усних пояснень

г) Фокус виключно на оформленні звітів без аналізу транзакцій

16. Вкажіть одну з базових функціональних можливостей IDEA.

а) Автоматизоване тестування відповідності дизайну інтерфейсу корпоративним стандартам

б) Автоматизований пошук дублікатів, пропущених реквізитів і нетипових значень

в) Створення електронної пошти для комунікації з клієнтом

г) Ручне введення проведень за журналом операцій

17. Оберіть ключову характеристику, яка описує ACL.

а) Надає можливість формувати складні сценарії перевірки через правила і алгоритми виявлення відхилень

б) Призначений лише для форматування таблиць і графіків

в) Використовується виключно для ведення робочих файлів аудитора

г) Є модулем бухгалтерського обліку для формування проводок

18. Визначте основне призначення CaseWare у системі інструментів.

а) Суцільний аналіз транзакційних масивів як основна функція

б) Ведення електронних робочих файлів аудитора та стандартизоване документування процедур

в) Адміністрування прав доступу користувачів до ERP

г) Автоматичне виконання всіх аудиторських процедур без планування

19. Яку з функцій TeamMate віднесено до базової?

а) Моніторинг виконання рекомендацій та централізоване зберігання результатів перевірки

б) Перевірка текстового формату сум у електронних таблицях

в) Очищення даних шляхом перетворення дат у текст

г) Створення динамічних діаграм для презентації клієнту

20. Яка ключова ролі аудитора під час використання спеціалізованого ПЗ разом з ERP-системами?

а) Роль аудитора зводиться до ручного перегляду первинних документів без аналізу даних

б) Роль аудитора зміщується до оцінювання ризиків, інтерпретації результатів аналізу та підтвердження виявлених аномалій

в) Професійне судження аудитора стає непотрібним, оскільки все визначає алгоритм

г) Аудитор більше не формує доказів, а лише налаштовує візуальне оформлення звіту

Ключ відповідей

1 – б; 2 – а; 3 – б; 4 – б; 5 – б; 6 – б; 7 – а; 8 – в; 9 – а; 10 – б.
11 – а; 12 – в; 13 – а; 14 – а; 15 – б; 16 – б; 17 – а; 18 – б; 19 – а; 20 – б.

Тестові завдання до розділу 8

1. Сформулюйте призначення концептуальної моделі «Безпека–інклюзія–аудит».

а) Ізоляція функцій безпеки від інклюзивних програм для уникнення конфлікту цілей

б) Інтеграція безпеки, інклюзії та аудиту в узгоджену систему управлінських рішень

в) Заміна внутрішнього контролю виключно зовнішнім аудитом

г) Перенесення відповідальності за безпеку на користувачів фінансових послуг

2. Яка роль аудиту в моделі «Безпека–інклюзія–аудит»?

а) Лише фіксація порушень і складання санкційних переліків

б) Технічний контроль IT без участі у прийнятті рішень

в) Об’єктивна оцінка відповідності практик цілям безпеки й інклюзії та формування зворотного зв’язку

г) Адміністрування клієнтських операцій замість управлінського персоналу

3. Оберіть компонент моделі, який виконує функцію зворотного зв’язку для коригування політик і процедур.

а) Безпека

б) Інклюзія

в) Аудит

г) Маркетинг фінансових послуг

4. Наведіть формулювання, що найточніше відповідає розумінню безпеки у моделі.

а) Разове технічне посилення захисту інформаційних систем

б) Комплекс умов і правил, що забезпечують стабільність, надійність, довіру, а також визначення меж відповідальності

в) Локальна функція служби охорони без зв’язку з управлінням

г) Виключно дотримання вимог фізичного захисту активів

5. Вкажіть дію, яку в розділі віднесено до етапу впровадження моделі.

а) Скасування внутрішніх політик безпеки як таких, що обмежують інклюзію

б) Оновлення внутрішніх політик безпеки та визначення відповідальних осіб за моніторинг і перевірку

в) Припинення збору зворотного зв’язку від користувачів

г) Передача контролю інклюзивних процедур виключно зовнішнім органам нагляду

6. Які складові визначено як елементи результативного аудиту в моделі?

а) Опис ризиків, визначення бюджетів, погодження маркетингових кампаній

б) Системне оцінювання відповідності, аналітичне узагальнення результатів, рекомендаційна функція

в) Технічне обслуговування ІТ, аудит персоналу, погодження договорів

г) Моніторинг курсів валют, прогнозування попиту, сегментація клієнтів

7. Зазначте, що в розділі підкреслено як мету підготовки персоналу під час впровадження моделі.

а) Навчання лише роботі з первинними документами без фокусу на безпеці

б) Формування культури усвідомленої безпеки та відповідального ставлення до інклюзивних процедур

в) Заміна політик безпеки індивідуальними домовленостями з працівниками

г) Відмова від навчання, оскільки цифрові системи усувають людський фактор

8. Охарактеризуйте підхід до інклюзії, який закладено у моделі.

а) Лише розширення доступу до послуг без зміни правил і процедур

б) Створення умов повноцінної участі різних груп з доступом до інформації, сервісів і процедур прийняття рішень

в) Обмеження доступу до сервісів для зниження ризиків

г) Надання послуг виключно через посередників без прямого контакту з клієнтом

9. Визначте зміст подвійного ефекту фінансової інклюзії, описаного в розділі.

а) Зниження обсягів операцій одночасно зі зростанням кількості ризиків

б) Зростання прозорості без будь-якого впливу на навантаження системи безпеки

в) Зростання навантаження та нових ризиків при потенційному посиленні стійкості за умови належних контролів і грамотності

г) Повне усунення шахрайства завдяки розширенню доступу до фінансових послуг

10. Укажіть тип навантаження, яке пов’язано з інтеграцією віддаленої ідентифікації клієнтів (KYC).

а) Операційне

б) Кредитне

в) Контрольне

г) Стратегічне (позитивне)

11. Який із компенсаторних механізмів належить до ризику кіберзлочинності та витоку персональних даних під час цифровізації послуг?

а) Зменшення частоти оновлень систем безпеки

б) Кіберзахист і багаторівнева автентифікація

в) Відмова від цифрових каналів та повернення до готівкових розрахунків

г) Підвищення лімітів безконтрольних операцій

12. Назвіть компенсаторний механізм для ризику погіршення якості кредитного портфеля у разі активізації мікрокредитування.

а) Скорочення обсягу кредитної інформації про позичальника

б) Скоринг-моделі, резервування та диверсифікація ризиків

в) Відмова від аналізу платоспроможності як дискримінаційного інструменту

г) Переорієнтація на ручну обробку всіх заявок без моделей

13. Оберіть твердження, що відповідає наслідкам розвитку фінтех-платформ для системи фінансової безпеки.

а) Зменшується потреба у нормативному регулюванні, оскільки фінтех самостійно забезпечує безпеку

б) Зростає регуляторне навантаження через появу нових посередників та потребу адаптації правил

в) Скасовуються процедури ліцензування і нагляду як зайві

г) Зникає асиметрія інформації між учасниками ринку автоматично

14. Наведіть приклад ризику та відповіді на нього для програм державної підтримки через фінансові інструменти, згаданий у розділі.

а) Ризик нецільового використання коштів і цифрове відстеження транзакцій із аудитом програм

б) Ризик валютних коливань і повна відмова від звітності

в) Ризик дефіциту ліквідності і підвищення комісій без контролю

г) Ризик шахрайства і скасування процедур ідентифікації

15. Вкажіть довгостроковий ефект структурних змін від розширення інклюзії, який наведено в розділі.

а) Посилення фрагментації контролю та зростання ізоляції інститутів

б) Формування мережевої моделі управління і координації

в) Відмова від міжінституційної взаємодії як неефективної

г) Зменшення потреби у регулюванні через стабілізацію ризиків

16. Визначте ресурсну зміну, яка пов’язана з переходом до цифрових форматів обслуговування.

а) Зменшення потреби в кіберзахисті та захисті персональних даних

б) Інвестування в кіберзахист і захист персональних даних із зростанням капітальних витрат

в) Відмова від IT-інфраструктури на користь паперового документообігу

г) Повне усунення витрат на безпеку через автоматизацію

17. Оберіть приклад «вузького місця» ризиків інклюзивних страхових або пенсійних програм, який випливає з розділу.

а) Неможливість цифрових виплат через відсутність інфраструктури

б) Неправильна оцінка страхових ризиків та потреба актуарного контролю

в) Зростання частки готівкових операцій як базовий ризик

г) Відсутність необхідності державного нагляду в страхуванні

18. Зазначте принцип побудови інтегрованих систем, який спрямований на уникнення дублювання інформації та забезпечення централізованого доступу до даних.

а) Модульності та масштабованості

б) Єдності даних та централізованого доступу

в) Рівнево-структурної організації

г) Гнучкості та адаптивності

19. Яка можливість інтегрованих систем забезпечує попередження кризових ситуацій до їх виникнення?

а) Звітування та підтримка прийняття рішень

б) Системи раннього попередження

в) Регуляторний моніторинг

г) Інфраструктурний моніторинг

20. Які показники у розділі віднесено до інфраструктурного моніторингу?

а) Кредитний рейтинг і фінансова активність клієнта

б) Коливання курсів валют і ставок

в) Доступність платіжних систем та стан IT-ресурсів

г) Виконання нормативів і внутрішніх політик

Ключ відповідей

1 – б; 2 – в; 3 – в; 4 – б; 5 – б; 6 – б; 7 – б; 8 – б; 9 – в; 10 – в

11 – б; 12 – б; 13 – б; 14 – а; 15 – б; 16 – б; 17 – б; 18 – б; 19 – б; 20 – в

Тестові завдання до розділу 9

1. Визначте ключовий чинник, який є рушієм зростання фінансового шахрайства в цифровому середовищі.

а) Поширення цифрових інструментів та електронних розрахунків

б) Скорочення частки безготівкових операцій

в) Повна відмова бізнесу від хмарних сервісів

г) Зменшення транскордонної торгівлі

2. Вкажіть ознаку, яка дозволяє розмежувати помилку та шахрайство в аудиті.

а) Рівень суттєвості викривлення

б) Наявність умислу у викривленні

в) Форма подання звітності

г) Частота господарських операцій

3. Оберіть формулювання, що відповідає визначенню шахрайства за МСА 240.

а) Ненавмисне викривлення через арифметичні неточності

б) Навмисна дія із застосуванням обману для отримання неправомірної або незаконної вигоди

в) Випадкова помилка класифікації статей звітності

г) Результат технічного збою облікової системи

4. Встановіть, яка з наведених дій належить до неправдивої фінансової звітності за МСА 240.

а) Ненавмисна помилка підсумовування у відомості

б) Маніпулювання або фальсифікація облікових записів чи підтверджувальної документації

в) Втрата первинних документів через стихійне лихо

г) Зміна валютного курсу після дати балансу

5. Визначте компонент моделі «трикутника шахрайства», який описує психологічне раціоналізування протиправних дій.

а) Мотив

б) Виправдання

в) Сприятливі можливості

г) Зовнішній контроль

6. Вкажіть приклад «легендованого» заходу контролю, який описаний у розділі.

а) Суцільна перевірка регістрів обліку

б) Таємний покупець

в) Підписання листів-підтверджень дебіторами

г) Інвентаризація активів наприкінці року

7. Наведіть правильну комбінацію трьох основних «гілок» «дерева шахрайства».

а) Незаконне привласнення активів; корупційні діяння; фальсифікація фінансової звітності

б) Помилки обліку; податкові різниці; управлінські рішення

в) Ліквідність; прибутковість; платоспроможність

г) Планування; виконання; завершення аудиту

8. Оберіть приклад кібершахрайства, який належить до ключових інструментів реалізації.

а) Фішинг

б) Хабарництво

в) Фіктивне банкрутство

г) Нецільове використання коштів

9. Визначте сферу ризику, до якої віднесено індикатор «ускладненість або заплутаність організаційної структури та структури власності».

а) Корпоративна структура та власність

б) Соціально-демографічні фактори

в) Природні фактори

г) Науково-технічні фактори

10. Означте сферу ризику, для якої індикатором є розміщення ключових підрозділів у юрисдикціях із пільговим податковим режимом.

а) Операційне середовище та бізнес-модель

б) Географія діяльності та юрисдикція

в) Фінансовий стан та облікова політика

г) Система управління та внутрішній контроль

11. Який макрофактор зовнішнього середовища описує появу інноваційних технологій, що змінюють умови діяльності підприємств?

а) Економічні

б) Законодавчо-регуляторні

в) Науково-технічні

г) Природні

12. Оберіть порушення в обліку, яке спричиняє зростання дебіторської заборгованості за одночасного зниження чистого доходу.

а) Визнання доходу від реалізації без одночасного відображення дебіторської заборгованості

б) Відображення дебіторської заборгованості за відсутності факту визнання доходу від реалізації

в) Ігнорування в обліку наданих покупцям знижок

г) Неправомірна капіталізація операційних витрат

13. Визначте нефінансову ознаку потенційних викривлень в аудиті.

а) Надзвичайно жорстка конкуренція на ринку

б) Постійна зміна зовнішнього аудитора

в) Міграція кваліфікованих кадрів з країни

г) Проведення частих податкових перевірок

14. Вкажіть інструмент, який забезпечує незмінний реєстр транзакцій і унеможливлює коригування записів «заднім числом».

а) Роботизована автоматизація процесів

б) Технологія блокчейн

в) Електронна таблиця

г) Нарахування резервів

15. Оберіть метод, який у розділі віднесено до аналітики великих даних і використовується для пошуку нетипових журнальних проводок.

а) Автоматизований пошук нетипових бухгалтерських записів за часом, сумою або автором

б) Формування облікової політики підприємства

в) Ручний перегляд первинних документів без вибірки

г) Розрахунок амортизації за прямолінійним методом

16. Встановіть, що в розділі названо ключовою функцією штучного інтелекту та машинного навчання у виявленні шахрайства.

а) Формування смарт-контрактів для виконання зобов’язань

б) Автоматичне виявлення аномалій як відхилень від профілю нормальної поведінки

в) Проведення інвентаризації запасів

г) Юридичне тлумачення договорів

17. Яка характеристика відповідає предиктивній аналітиці в контексті протидії шахрайству?

а) Оцінка ймовірності шахрайства за транзакцією до її завершення на основі історичних даних

б) Формування бухгалтерських проводок на підставі первинних документів

в) Погодження бюджету підприємства на наступний період

г) Визначення ринкової вартості активів

18. Який підхід у форензік-аудиті ґрунтується на закономірностях розподілу чисел і може застосовувати закон Бенфорда?

а) Психофізіологічні методи

б) Математичні методи

в) Нормативно-правовий аналіз

г) Процедури зовнішнього підтвердження

19. Який принцип визначає розмежування ролей: управлінський персонал відповідає за запобігання шахрайству, а аудитор – за оцінку ризиків і отримання доказів?

а) Принцип розмежування відповідальності

б) Принцип професійного скептицизму

в) Принцип ризик-орієнтованого підходу

г) Принцип обов'язкового реагування на ризики

20. Який принцип зобов’язує аудитора адаптувати процедури та виконувати додаткові дії у відповідь на виявлені ризики шахрайства?

а) Принцип розмежування відповідальності

б) Принцип професійного скептицизму

в) Принцип ризик-орієнтованого підходу

г) Принцип обов'язкового реагування на ризики

Ключ відповідей

1 – а; 2 – б; 3 – б; 4 – б; 5 – б; 6 – б; 7 – а; 8 – а; 9 – а; 10 – б.

11 – в; 12 – б; 13 – б; 14 – б; 15 – а; 16 – б; 17 – а; 18 – б; 19 – а; 20 – г.

Тестові завдання до розділу 10

1. Яка хаарктеристика у триаді CIA інформаційної безпеки найточніше відповідає ситуації, коли сервіс або система недоступні користувачам?

а) Конфіденційність

б) Цілісність

в) Доступність

г) Автентичність

2. Як трактується поняття «поверхня атаки»?

а) Сукупність усіх точок входу та каналів взаємодії, через які можливе проникнення або вплив на систему

б) Перелік санкцій за порушення політик безпеки

в) Набір антивірусних засобів та засобів шифрування

г) Окрема вразливість у програмному забезпеченні

3. Яка комбінація елементів утворює трикутник аналізу кіберризику?

а) Загроза – інцидент – збиток

б) Загроза – уразливість – контроль

в) Актив – контроль – відповідальність

г) Вектор – канал – наслідок

4. Яка з наведених цілей фішингу вважається типовою?

а) Оптимізація бізнес-процесів через автоматизацію

б) Викрадення облікових даних (логінів і паролів)

в) Підвищення точності фінансового прогнозування

г) Створення резервних копій на ізольованому сховищі

5. До яких контрольних практик безпосередньо прив’язується фаза Initial access у ланцюгу кібератаки?

а) Класифікація даних і політики DLP

б) Наявність MFA дисципліна паролів, правила віддаленого доступу та виявлення підозрілих спроб входу

в) Планування RPO і RTO та тестування відновлення

г) Розрахунок матеріальності та підготовка розкриттів у звітності

6. Етапи Privilege escalation та Lateral movement у моделі ланцюга атаки описують насамперед.

а) Перевірку достовірності фінансової звітності

б) Перехід з обмежених прав до привілейованих та поширення атаки у середовищі

в) Формування політик шифрування даних на дисках

г) Резервне копіювання і контроль цілісності копій

7. Який висновок про ефективний захист робиться на основі матриці загроз і векторів?

а) Достатньо посилити тільки антивірус

б) Захист має бути багаторівневим і включати політики доступу, моніторинг та дисципліну змін

в) Ключовим є лише шифрування трафіку в мережі

г) Основний акцент слід робити на зовнішньому аудиті

8. Який із перелічених принципів Zero Trust забезпечує верифікацію доступу не лише під час входу?

а) Периметрова довіра до внутрішньої мережі

б) Безперервна верифікація

в) Єдиний пароль для всіх сервісів

г) Відмова від журналювання подій

9. Вкажіть один із основних принципів найменших привілеїв у контексті Zero Trust.

а) У повному обсязі для всіх користувачів після первинної перевірки

б) Лише мінімально необхідний і лише на час виконання конкретного завдання

в) Тільки адміністраторам незалежно від контексту

г) Виключно через внутрішню мережу без додаткових перевірок

10. Які центральні логічні компоненти Zero Trust-архітектури названо у NIST SP 800-207?

а) Firewall IDS SIEM

б) Policy Engine, Policy Administrator, Policy Enforcement Point

в) RBAC DAC MAC

г) Backup Replication Snapshot

11. Оберіть модель контролю доступу, якій характерне централізоване встановлення незмінних правил.

а) RBAC

б) DAC

в) MAC

г) ABAC

12. Яке з наведених тверджень найкраще описує логіку прийняття рішень у моделі керування доступом на основі атрибутів (ABAC)?

а) Доступ надається виключно на основі того, до якої групи або ролі належить користувач у системі

б) Доступ визначається через аналіз сукупності характеристик користувача, параметрів ресурсу та поточних умов запиту

в) Надання прав базується лише на часі доби, коли користувач намагається увійти в систему

г) Рішення про доступ залежить від того, чи встановлено на комп'ютері користувача актуальне антивірусне програмне забезпечення

13. Яке основне призначення сегментації мережі на зони безпеки?

а) Прискорити роботу мережі за рахунок скорочення маршрутів

б) Обмежити переміщення атакувальника у разі компрометації та ізолювати критичні сегменти

в) Скасувати потребу в MFA

г) Замінити політики доступу на ручне адміністрування

14. Яку функцію забезпечує ZTNA?

а) Надає доступ до всієї внутрішньої мережі після входу

б) Забезпечує доступ до конкретного сервісу після автентифікації та перевірки політик і приховує внутрішні ресурси

в) Автоматично генерує фінансову звітність

г) Використовується лише для резервного копіювання

15. Яка дія належить до реакцій EDR або ITDR на підозрілий доступ?

а) Ізоляція кінцевих станцій, відкликання маркерів сесій і примусове скидання паролів

б) Відключення резервного копіювання до завершення інциденту

в) Скасування журналювання, щоб зменшити навантаження

г) Передача облікового запису адміністратора у спільне користування

16. Які можливості надає організаціям впровадження підходу Data Loss Prevention (DLP)?

а) Застосування повного шифрування накопичувачів без контролю за трафіком

б) Моніторинг та припинення спроб передачі конфіденційних даних, що порушують встановлені правила безпеки

в) Регулярне проведення імітацій кібератак для пошуку вразливостей

г) Автоматичне переведення системи з рольового керування доступом на дискреційне

17. Яким правилом формулюється класична рекомендація для надійного резервного копіювання?

а) 1-1-1 одна копія один носій один майданчик

б) 3-2-1 три копії на двох різних носіях одна копія поза основним майданчиком

в) 2-2-0 дві копії на двох носіях без винесення за межі майданчика

г) 5-1-0 п’ять копій на одному носії без ізоляції

18. Що характеризує показник RPO (Recovery Point Objective) у стратегії резервного копіювання?

а) Допустиму втрату даних у часі

б) Максимально допустимий час простою системи

в) Рівень шифрування резервних копій

г) Перелік прав адміністратора в системі

19. Оберіть визначення поняття RTO (Recovery Time Objective).

а) Допустима втрата даних у часі

б) Час, за який після інциденту системи мають знову стати функціональними

в) Обсяг даних що підлягає класифікації

г) Кількість факторів у MFA

20. Вкажіть, який із наведених ефектів не входить до переліку матеріальних фінансових наслідків кіберризиків.

а) Втрата виручки внаслідок простою

б) Витрати на відновлення

в) Зростання доходів конкурентів

г) Судові витрати

Ключ відповідей

1 – в; 2 – а; 3 – б; 4 – б; 5 – б; 6 – б; 7 – б; 8 – б; 9 – б; 10 – б.

11 – в; 12 – б; 13 – б; 14 – б; 15 – а; 16 – б; 17 – б; 18 – а; 19 – б; 20 – в.

Тестові завдання до розділу 11

1. Який чинник визначено як головну перешкоду розвитку інвестиційного консалтингу в Україні?

а) Надмірна кількість інвесторів та перенасичення ринку послугами

б) Відсутність довіри до інвестиційного консалтингу з боку бізнесу

в) Переважання паперових документів над цифровими доказами

г) Повна заборона на консалтинг з боку аудиторів

2. Вкажіть, що належить до змісту аудиторських послуг відповідно до Закону України «Про аудит фінансової звітності та аудиторську діяльність».

а) Огляд фінансової звітності, завдання з надання іншої впевненості та інші професійні послуги відповідно до міжнародних стандартів аудиту

б) Лише складання фінансової звітності та відновлення бухгалтерського обліку

в) Виключно податкове консультування та представництво в суді

г) Будь-які управлінські рішення щодо інвестування замість клієнта

3. Яке з наведених тверджень відповідає характеристиці підготовки інвестиційних консультантів в Україні?

а) Існує стандартизована державна програма підготовки, аналогічна підготовці аудиторів

б) Підготовка повністю здійснюється виключно в межах спеціальності «Аудит» без інших траєкторій

в) Відсутня сформована система підготовки та «поріг входження» у професію

г) Показником кваліфікації є лише стаж роботи, а сертифікації не застосовуються

4. Яку організацію в Україні згадано в розділі як представника міжнародної спільноти CFA?

а) IFAC Ukraine

б) CFA Society Ukraine

в) ACCA Ukraine

г) IAASB Ukraine

5. Наведіть три базові варіанти рекомендацій інвестиційного консультанта.

а) Створити, реорганізувати, ліквідувати

б) Погодити, відхилити, перенести

в) Тримати, купувати, продавати

г) Перевірити, задокументувати, архівувати

6. Оберіть визначення, що найбільше відповідає сутності фундаментального аналізу в інвестиційному консалтингу.

а) Оцінка справедливої вартості активу на основі фінансових показників та макроекономічних і галузевих чинників

б) Прогнозування ціни активу за графіками та індикаторами без аналізу економічних факторів

в) Визначення податкових зобов’язань інвестора за операціями з цінними паперами

г) Перевірка первинних документів без моделювання майбутніх грошових потоків

7. Яка з перелічених ознак відповідає технічному аналізу?

а) Зосередження на перспективі довгострокового контролю над бізнесом

б) Використання математичних методів та ринкових графіків для прогнозування цінових змін у реальному часі

в) Формування висновку виключно на підставі аудиторських доказів щодо минулих періодів

г) Оцінка лише юридичних ризиків без аналізу ринкових даних

8. Вкажіть, за якої умови інвестиційне консультування з боку аудитора може вважатися прийнятним з точки зору незалежності.

а) Коли аудиторська фірма не проводить аудит цього клієнта

б) Коли аудитор одночасно впроваджує контрольні правила у системі клієнта і потім їх перевіряє

в) Коли винагорода аудитора залежить від результату інвестиційного рішення клієнта

г) Коли аудитор бере участь у прийнятті управлінських рішень замість керівництва підприємства

9. Оберіть ситуацію, описану як несумісну з роллю аудитора-інвестиційного консультанта.

а) Надання загальної економічної інформації без впливу на конкретне рішення клієнта

б) Консультування, результати якого впливають на фінансову звітність, що підлягає аудиту

в) Підготовка рекомендацій щодо підвищення прозорості процесів і контролів

г) Оцінка надійності процесів формування фінансових показників у цифровому середовищі

10. У чому полягає ключова відмінність стратегічного інвестора від портфельного інвестора?

а) Стратегічний інвестор орієнтується на встановлення довгострокового контролю та розвиток бізнесу, портфельний – на доходність і ліквідність цінних паперів

б) Стратегічний інвестор працює лише з державними облігаціями, портфельний – лише з приватними компаніями

в) Стратегічний інвестор не використовує цифрові дані, портфельний – використовує тільки цифрові

г) Стратегічний інвестор аналізує лише бухгалтерські рахунки, портфельний – лише первинні документи

11. Наведіть перелік чотирьох базових принципів етики, які віднесено до підходу ІІА.

а) Цілісність, об’єктивність, конфіденційність, компетентність

б) Справедливість, креативність, інноваційність, лідерство

в) Швидкість, точність, автоматизація, масштабованість

г) Незворотність, децентралізація, токенізація, консенсус

12. Які принципи є складовими Кодексу етики AICPA?

а) Відповідальність, цілісність, об’єктивність і незалежність, належна ретельність, сфера та характер послуг

б) Доступність, резервування, відновлення, тестування на проникнення, реагування на інциденти

в) Аудиторський скептицизм, вибірка, інвентаризація, підтвердження, перерахунок

г) Приватність, токенізація, майнінг, стейкінг, децентралізоване управління

13. Що у розділі розуміють під «незалежністю зовнішнього вигляду»?

а) Наявність формального договору без розкриття будь-яких додаткових відносин

б) Відсутність будь-яких контактів аудитора з клієнтом протягом проєкту

в) Відсутність навіть враження про можливу упередженість суджень аудитора з огляду на зв’язки або інтереси

г) Обов’язкове використання лише автоматизованих інструментів без професійного судження

14. Оберіть приклад етичного ризику цифровізації інвестиційного консалтингу.

а) Алгоритмічна упередженість при ухваленні рішень системами штучного інтелекту

б) Поява додаткових паперових погоджень у процесі підготовки звітів

в) Зменшення обсягу цифрових даних через обмеження доступу

г) Повна відмова від аналізу ризиків унаслідок використання автоматизації

15. Яку дію рекомендовано виконати першою при підготовці Big Data-аналітики для оцінки інвестиційної привабливості?

а) Побудувати карту даних із визначенням джерел, доступів, власників та критичних полів

б) Одразу сформувати фінальну рекомендацію «купувати чи продавати» без верифікації даних

в) Вимкнути журналювання подій у системах для прискорення обробки

г) Заміщувати відсутні дані довільними значеннями без документування

16. Визначте, який метод Data Mining пов’язаний із групуванням об’єктів за схожістю для виявлення типових профілів.

а) Класифікація

б) Регресія

в) Кластеризація

г) Вибіркове підтвердження

17. Як доцільно будувати прогнозні моделі для короткого та довгого горизонту?

а) Доцільно застосовувати одну модель для всіх горизонтів без налаштування параметрів

б) Рекомендується формувати набір моделей для різних горизонтів (коротких і довгих) з урахуванням відмінностей у даних та цілях

в) Сентимент-аналіз застосовується лише для оцінки історичних показників без прогнозів

г) Будь-яке прогнозування в цифровому середовищі є недоцільним і має бути виключене

18. Які характеристики цифрових даних є критичними, окрім їхнього обсягу?

а) Різноманітність, швидкість надходження, достовірність

б) Колір, шрифт, форматування

в) Лише наявність печатки та підпису на документах

г) Кількість паперових копій та архівних папок

19. Наведіть призначення цифрового двійника підприємства в контексті інвестиційного консалтингу.

а) Створення рекламних матеріалів для просування бренду на ринку

б) Тестування сценаріїв і управлінських рішень у моделі без ризику реальних втрат і простоїв

в) Заміна фінансової звітності підприємства набором презентацій

г) Відмова від аналізу даних на користь експертної інтуїції

20. Яке твердження найточніше відображає межу відповідальності інвестиційного консультанта під час підготовки рекомендації клієнту?

а) Консультант приймає інвестиційні рішення замість клієнта і несе повну відповідальність за фінансовий результат

б) Консультант надає рекомендацію на основі аналізу та розкриває припущення і ризики, а остаточне рішення ухвалює клієнт

в) Консультант гарантує дохідність інвестиції, якщо клієнт дотримується рекомендації

г) Консультант не зобов’язаний перевіряти якість даних, якщо джерело є публічним

Ключ відповідей

1 – б; 2 – а; 3 – в; 4 – б; 5 – в; 6 – а; 7 – б; 8 – а; 9 – б; 10 – а

11 – а; 12 – а; 13 – в; 14 – а; 15 – а; 16 – в; 17 – б; 18 – а; 19 – б; 20 – б

Тестові завдання до розділу 12

1. Яка основна мета аудиту фінансової звітності у законодавчому визначенні?

а) Оцінка доцільності інвестиційних проєктів клієнта

б) Висловлення незалежної думки щодо відповідності фінансової звітності в усіх суттєвих аспектах вимогам стандартів

в) Складання первинних документів і регістрів бухгалтерського обліку

г) Управління операційними ризиками підприємства

2. Як у Концепції розвитку штучного інтелекту в Україні визначено «штучний інтелект»?

а) Будь-яке програмне забезпечення, що автоматизує документообіг

б) Організована сукупність інформаційних технологій, здатних виконувати складні завдання через наукові методи та алгоритми обробки інформації

в) Набір формул для обчислення фінансових коефіцієнтів і рейтингів

г) Цифровий архів документів без можливості редагування

3. Для чого під час підготовки економічної інформації до аналізу застосовують процес ETL?

а) Щоб автоматично сформувати аудиторський висновок без перевірок

б) Щоб витягти, перетворити та завантажити дані з різних джерел у форму, придатну для аналітичних процедур

в) Щоб замінити фінансові дані на нефінансові KPI

г) Щоб зберегти дані лише у вигляді скан-копій без структурування

4. Яку фундаментальну зміну в методології аудиту пов'язують з інтеграцією ШІ?

а) Перехід від суцільної перевірки до вибіркового тестування

б) Відмова від аналітичних процедур на користь інтерв'ю з персоналом

в) Перехід від ризик-орієнтованих вибірок до суцільного аналізу даних і акценту на аномаліях

г) Перехід від професійного судження до повної автоматизації думки аудитора

5. Що означає ризик вибірки в аудиті?

а) Ризик втрати доступу до даних через кібератаку

б) Ймовірність того, що висновок за результатами вибірки відрізнятиметься від висновку за перевірки всієї сукупності

в) Ризик помилки у застосуванні стандартів фінансової звітності

г) Ризик невідповідності паролів політиці безпеки

6. Яка характеристика найточніше описує обсяг перевірки в аудиті з використанням ШІ?

а) Вибіркова перевірка з фокусом на репрезентативності вибірки

б) Вибіркова перевірка з фокусом на листах-підтвердженнях

в) Суцільний аналіз даних з фокусом на аномаліях та відхиленнях

г) Суцільний аналіз лише формальних реквізитів без пошуку відхилень

7. Як змінюється роль аудитора в аудиті з використанням ШІ порівняно з традиційним аудитом?

а) Основний акцент робиться на зборі, агрегації та ручній перевірці даних

б) Аудитор виконує функції бухгалтера і формує первинні документи

в) Аудитор налаштовує алгоритми, інтерпретує результати та застосовує професійне судження

г) Аудитор повністю усувається з процесу формування висновку

8. Який напрям трансформації методології аудиту означає перманентний контроль бізнес-процесів замість періодичного?

а) Автоматизація процедур

б) Безперервний моніторинг

в) Ризик-орієнтована аналітика

г) Забезпечення прозорості та валідації

9. Який рівень аналітики даних відповідає на запитання «Що сталося»?

а) Описова аналітика

б) Діагностична аналітика

в) Прогнозна аналітика

г) Приписувальна (прескриптивна) аналітика

10. Який рівень аналітики даних найкраще відповідає завданню оцінки безперервності діяльності підприємства у майбутньому?

а) Описова аналітика

б) Діагностична аналітика

в) Прогнозна аналітика

г) Приписувальна (прескриптивна) аналітика

11. Що означає підхід доповненого інтелекту в аудиті?

а) ШІ замінює аудитора у формуванні професійної думки

б) ШІ підсилює професійне судження аудитора та знижує когнітивне навантаження

в) Аудитор відмовляється від професійного судження на користь статистики

г) Аудитор використовує лише дашборди без моделей машинного навчання

12. Яка технологія найбільш придатна для автоматичного аналізу великої кількості контрактів і пошуку нестандартних умов?

а) NLP (обробка природної мови)

б) RPA (роботизація)

в) Process Mining

г) Computer Vision без текстового аналізу

13. Яка технологія найчастіше використовується для звірки розрахунків між різними системами через імітацію дій користувача?

а) NLP

б) RPA

в) блокчейн

г) ETL

14. Яка технологія застосовується для тестування засобів контролю через відображення фактичних потоків процесу та пошук відхилень від регламенту?

а) GenAI

б) NLP

в) Process Mining

г) ETL

15. Яка комбінація технологій у розділі наведена для інвентаризації та підтвердження активів?

а) NLP / GenAI / RPA

б) Process Mining / ML / ETL

в) ETL / BI / RPA

г) Computer Vision / IoT / Blockchain

16. Який тип машинного навчання доречний для групування об’єктів або пошуку нових патернів без розмічених прикладів?

а) Контрольоване навчання

б) Навчання без учителя

в) Навчання з підкріпленням

г) ETL

17. У чому полягає ретротестування ML-моделі в аудиті?

а) У шифруванні та архівуванні даних для комплаєнсу

б) У тестуванні моделі на історичних даних для перевірки якості прогнозу подій, що вже відбулися

в) У маркуванні всіх транзакцій вручну як «помилкові»

г) У розгортанні моделі в промислову експлуатацію без перевірки

18. Який ризик з боку даних або моделі описує генерацію системою ШІ недостовірних фактів або вигаданих тверджень?

а) «Отруєння даних»

б) Застарілість даних

в) «Галюцинації»

г) Історична упередженість

19. Який рівень непрозорості пов’язаний із закритістю коду комерційного програмного забезпечення та обмеженням доступу до алгоритму?

а) Технічна непрозорість

б) Процедурна непрозорість

в) Комерційна непрозорість

г) Операційна непрозорість

20. Який принцип управління ризиками ШІ безпосередньо вимагає пояснюваності рішень і визначення відповідальності за них?

а) Прозорість та відповідальність

б) Справедливість та недискримінація

в) Збалансований підхід до даних та алгоритмів

г) Мінімізація витрат на ІТ-інфраструктуру

Ключ відповідей

1 – б; 2 – б; 3 – б; 4 – в; 5 – б; 6 – в; 7 – в; 8 – б; 9 – а; 10 – в.

11 – б; 12 – а; 13 – б; 14 – в; 15 – г; 16 – б; 17 – б; 18 – в; 19 – в; 20 – а.

Тестові завдання до розділу 13

1. Визначте, яке твердження найточніше розкриває зміст інклюзивного аудиту.

а) Перевірка правильності бухгалтерського обліку та фінансової звітності

б) Оцінювання інклюзивності управлінських рішень, процесів і результатів з позиції рівності можливостей та доступності

в) Контроль дотримання податкового законодавства і внутрішніх регламентів

г) Підтвердження економічної ефективності діяльності організації

2. Укажіть ознаку, що відрізняє інклюзивний аудит від традиційних видів аудиту.

а) Фокус лише на відповідності нормативним вимогам

б) Використання виключно фінансових показників як доказів

в) Оцінювання впливу діяльності організації на доступ і участь різних груп персоналу та стейкхолдерів

г) Проведення перевірки тільки за підсумками року

3. Оберіть управлінське питання, на яке інклюзивний аудит покликаний надати вимірювану відповідь.

а) Чи зростає прибутковість організації порівняно з минулим періодом

б) Чи відповідають витрати на оплату праці середньоринковому рівню

в) Чи є фінансова звітність складеною без арифметичних помилок

г) Чи забезпечує організація безпечні, доступні та справедливі умови взаємодії для персоналу й стейкхолдерів

4. Що найкраще описує бар’єроорієнтований підхід в інклюзивному аудиті?

а) Виявлення конкретних точок виключення, встановлення причин бар’єрів і оцінювання їх наслідків

б) Порівняння фінансових коефіцієнтів із середньогалузевими значеннями

в) Формування узагальненого висновку без деталізації проблемних зон

г) Оцінювання лише формальної наявності регламентів

5. Вкажіть складові тривекторної моделі інклюзивного аудиту.

а) Персонал, активи, зобов’язання

б) Управлінські рішення, процеси, результати

в) Стратегія, бюджет, звітність

г) Ризики, контролі, тести контролю

6. Що з наведеного нижче перевіряється у межах інклюзивного аудиту управлінських рішень?

а) Класифікація витрат за елементами

б) Правильність нарахування амортизації

в) Прозорість ухвалення рішень і наявність документованого обґрунтування

г) Зіставність показників фінансової звітності

7. Визначте, який блок показників найбільш характерний для інклюзивного аудиту процесів.

а) Фінансова стійкість і ліквідність

б) Рентабельність продажів

в) Собівартість продукції

г) Процедури розумного пристосування та доступність робочих місць

8. Що є предметом оцінювання в інклюзивному аудиті результатів?

а) Підтверджені показниками наслідки, зокрема доступність сервісів, динаміка скарг та індикатори залученості

б) Наміри керівництва, зафіксовані у стратегії

в) Лише наявність внутрішніх політик і процедур

г) Тільки відповідність організаційної структури штатному розпису

9. Яка дія відповідає етапу встановлення критеріїв інклюзивності та системи індикаторів?

а) Фіксація фактів порушень у робочих документах аудитора

б) Визначення показників, за якими робиться висновок про інклюзивність рішень, процесів і результатів

в) Розрахунок податкових різниць за результатами періоду

г) Підготовка проєкту фінансової звітності

10. Оберіть вимогу до якості інформації, що забезпечує можливість перевірити ланцюг «джерело → обробка → результат».

а) Актуальність

б) Повнота

в) Перевірюваність походження інформації

г) Однозначність інтерпретації

11. Укажіть джерело даних, яке найдоцільніше використовувати для виявлення цифрових бар’єрів у взаємодії з організацією.

а) Лише баланс і звіт про фінансові результати

б) Розрахунок собівартості за статтями

в) Інвентаризаційні описи запасів

г) Результати тестування цифрової інклюзивності сайтів, форм і сервісів

12. Визначте тип бар’єру, який проявляється як недоступні сайти, форми або цифрові документи.

а) Цифровий

б) Фізичний

в) Економічний

г) Освітній

13. Вкажіть приклад причини інформаційних бар’єрів в організації.

а) Надмірна автоматизація облікових процедур

б) Відсутність стандартів доступної комунікації та фрагментація каналів інформування

в) Висока точність первинних документів

г) Наявність розвиненої системи зворотного зв’язку

14. Що з наведеного нижче, обов’язково слід встановити під час обґрунтування управлінських заходів з усунення бар’єрів?

а) Лише загальний опис проблеми без відповідальних

б) Перелік бухгалтерських рахунків, яких стосується проблема

в) Відповідальних виконавців, строки реалізації та контрольні показники

г) План інвентаризації на наступний квартал

15. Оберіть групу цифрових технологій, що дозволяє реконструювати фактичний перебіг процесу за подієвими журналами.

а) Технології бізнес-аналітики та візуалізації

б) Технології збору та фіксації аудиторської інформації

в) Технології управління виконанням рекомендацій і моніторингу

г) Технології аналітики процесів і виявлення «вузьких місць»

16. Зазначте основне призначення технологій інтеграції та підготовки даних в інклюзивному аудиті.

а) Уніфікувати дані з різних джерел, усунути дублювання та підготувати масиви до розрахунку індикаторів

б) Замінити професійне судження аудитора автоматичними висновками

в) Здійснювати лише архівування документів без аналізу

г) Формувати фінансову звітність замість бухгалтерії

17. Чому інтеграція даних є критичною для інклюзивного аудиту?

а) Щоб збільшити кількість регламентів у документообігу

б) Щоб забезпечити єдине трактування показників і коректну порівнюваність результатів

в) Щоб замінити опитування персоналу фінансовими даними

г) Щоб скоротити кількість джерел інформації до одного документа

18. Оберіть технологію, найбільш придатну для систематизації звернень і скарг та виявлення повторюваних проблем у текстах.

а) Нарахування резервів за сумнівними боргами

б) Звіряння оборотно-сальдової відомості

в) Тематичний аналіз текстових даних і класифікація причин звернень

г) Калькулювання собівартості

19. Яку функцію виконують технології бізнес-аналітики та візуалізації результатів в інклюзивному аудиті?

а) Визначають ставки податків і зборів

б) Здійснюють юридичну експертизу договорів

в) Підміняють процедури збору даних опитуваннями

г) Формують індикатори у вигляді, придатному для управлінських рішень і контролю динаміки

20. Визначте, для чого застосовують технології управління виконанням рекомендацій і моніторингу.

а) Для планування заходів, контролю строків, фіксації статусів і повторних перевірок результатів

б) Для складання фінансової звітності за МСФЗ

в) Для обліку основних засобів

г) Для організації інвентаризації матеріальних цінностей

Ключ відповідей

1 – б; 2 – в; 3 – г; 4 – а; 5 – б; 6 – в; 7 – г; 8 – а; 9 – б; 10 – в

11 – г; 12 – а; 13 – б; 14 – в; 15 – г; 16 – а; 17 – б; 18 – в; 19 – г; 20 – а

Глосарій

ГЛОСАРІЙ

(складений на основі опрацьованих літературних джерел)

Поняття	Зміст
Автоматизація	процес застосування технологій для автоматичного виконання завдань без безпосередньої участі людини, часто використовується у виробництві, обробці даних і наданні послуг
Автоматизація аудиторських процедур	використання програмних засобів для зменшення ручної роботи аудитора та підвищення точності перевірок
Автоматизація бізнес-процесів	впровадження технологій для автоматичного виконання рутинних задач у бізнесі, що підвищує ефективність, зменшує витрати та мінімізує людські помилки
Агент штучного інтелекту (AI Agent)	програмний компонент, який автономно виконує завдання, приймає рішення і взаємодіє з навколишнім середовищем на основі заданих алгоритмів і отриманих даних
Аналіз великих даних (Big Data)	методи обробки та аналізу великих обсягів даних, що дозволяють виявляти тренди, патерни та взаємозв'язки в складних та неоднорідних наборах даних для прийняття рішень
Аналіз даних	процес збору, обробки та аналізу даних з цифрових каналів для розуміння поведінки користувачів, оцінки ефективності маркетингових кампаній та оптимізації маркетингових стратегій
Аналітичний рівень процесної моделі	рівень опису, що дозволяє аналізувати логіку процесів, взаємозв'язки між етапами та зони відповідальності
Аналітичні процедури	аналіз та оцінка отриманої аудитором інформації
Аномалія	нетипова транзакція або значення, що відхиляється від звичного патерну та може вказувати на помилку або ризик
Антикризове управління	комплекс заходів, спрямованих на запобігання фінансовій кризі або мінімізацію її наслідків для підприємства
Атака на відмову в обслуговуванні	це тип кібератаки, який полягає у перевантаженні сервісу запитами або трафіком з метою зробити його недоступним для легітимних користувачів
Атрибутивна перевірка	перевірка з метою встановлення, як часто у звітному періоді, що перевіряється, порушувались норми внутрішнього контролю

Поняття	Зміст
Атрибутна модель контролю доступу	це модель доступу, за якої рішення дозволити або заборонити приймається на основі атрибутів користувача, ресурсу та контексту запиту (ABAC)
Аудит	перевірка даних бухгалтерського обліку і показників фінансової звітності суб'єкта господарювання з метою висловлення незалежної думки аудитора про її достовірність в усіх суттєвих аспектах та відповідність вимогам законів України, НП(С)БО або інших правил (внутрішніх положень суб'єктів господарювання) згідно з вимогами користувачів
Аудит ефективності	це форма контролю, яка спрямована на визначення ефективності використання бюджетних коштів для реалізації запланованих цілей та встановлення факторів, які цьому перешкоджають. Аудит ефективності здійснюється з метою розроблення обґрунтованих пропозицій щодо підвищення ефективності використання коштів державного та місцевих бюджетів у процесі виконання бюджетних програм
Аудит на відповідність	аудит, який дозволяє визначити, чи дотримуються в господарській системі специфічні процедури або правила, що запропоновані персоналові вищим керівництвом
Аудиторська діяльність	підприємницька діяльність, яка включає організаційне та методичне забезпечення аудиту, практичне виконання аудиторських перевірок та надання інших аудиторських послуг
Аудиторська перевірка ініціативна	перевірка, що проводиться за рішенням економічного суб'єкта, у тому числі й за ініціативи одного з власників
Аудиторська перевірка обов'язкова	перевірка, яка проводиться аудиторською фірмою (аудитором) за документами фінансової звітності у випадках, прямо передбачених законодавством
Аудиторська процедура	певний порядок та послідовність дій аудитора щодо отримання необхідних аудиторських доказів на повному відрізку аудиту
Аудиторський висновок	офіційний документ, що складається за результатами аудиторської перевірки та має правове значення
Аудиторський ризик	ризик, який бере на себе аудитор при наданні висновку про повну достовірність даних зовнішньої звітності, водночас можливі помилки та пропуски, що не потрапили в поле зору аудитора

Поняття	Зміст
Аудиторські дані	структуровані цифрові дані бухгалтерського, фінансового та управлінського обліку, що використовуються для проведення аудиторських процедур
Аудиторські докази	інформація, отримана аудитором у процесі перевірки, яка слугує підґрунтям для формування аудиторської думки
Багатофакторна автентифікація	це механізм підтвердження особи, за якого вхід виконується щонайменше за двома незалежними факторами знання, володіння або біометрія (MFA)
Бізнес-процес	послідовність взаємопов'язаних дій, що виконуються в межах організації для досягнення конкретного результату, зокрема формування облікової інформації або реалізації контрольних процедур
Біометричні технології	технології, що використовують унікальні фізіологічні або поведінкові характеристики людини (відбитки пальців, особливості обличчя, голосу тощо) для верифікації особи та забезпечення безпеки доступу до цифрових або фізичних ресурсів
Блокчейн	технологія розподілених реєстрів, яка забезпечує безпечне та прозоре зберігання інформації та фінансових транзакцій без необхідності в центральному органі, використовується для криптовалют, контрактів, голосувань тощо
Блокчейн 2.0	покращена версія технології блокчейн, яка включає в себе смарт-контракти, що дозволяють автоматизувати виконання угод без необхідності в посередниках, та інші новітні функції для підвищення безпеки і прозорості транзакцій
Валідація даних	перевірка коректності, повноти та узгодженості даних перед використанням в аналітиці та аудиті
Веб-аналітика	процес збору, вимірювання і аналізу даних про поведінку користувачів на веб-сайтах з метою оптимізації бізнес-процесів
Великі дані (Big Data)	велика кількість інформації, що збирається та зберігається цифровими засобами, яку аналізують за допомогою спеціальних програм і алгоритмів для отримання корисних бізнес-інсайтів
Вибірка в аудиті	процес вибірки та аналізу частини даних з метою отримання інформації чи оцінки стану всієї сукупності

Поняття	Зміст
Викид	окреме значення, що суттєво відрізняється від решти; може бути помилкою або рідкісною валідною подією
Викривлення в даних	нетипове значення або операція, що відхиляється від очікуваного шаблону моделі та може свідчити про помилку, порушення або шахрайство
Викривлення фінансових звітів	викривлення, яке виникає внаслідок шахрайства або помилок
Виняток	запис/транзакція, що не проходить правило або контроль і потребує додаткового аналізу
Виявлення аномалій	методи пошуку нетипових операцій у даних (за сумою, частотою, контрагентом, часом тощо)
Виявлення дублікатів	пошук повторів записів (рахунків, платежів, постачальників) для виявлення помилок та зловживань
Відтворюваність	можливість повторити аналіз і отримати той самий результат за рахунок фіксації версій даних, коду та параметрів
Відтворюваність аудиту	властивість аудиторських процедур і результатів бути повторюваними за однакових умов і параметрів аналізу
Візуалізація даних	подання результатів аналізу у вигляді графіків і дашбордів для інтерпретації ризиків та висновків
Віртуальна реальність (VR)	технологія, що створює імітацію реального світу або штучного середовища, в яке користувач може потрапити через спеціальні пристрої (шоломи VR).
Внутрішні загрози фінансовій безпеці	ризики, що виникають унаслідок неефективного управління, помилок у фінансовому плануванні, зловживань, низької якості фінансового контролю або недосконалості внутрішніх процесів
Внутрішній аудит	здійснюється аудиторськими відділами економічних суб'єктів чи вищих органів управління; слугує основою для прийняття управлінських рішень щодо вдосконалення власної фінансової та господарської діяльності
Вразливість	це слабке місце в системі або процесі, яке створює умови для реалізації загрози, наприклад, відсутність MFA, помилки конфігурації або надмірні права
Вузьке місце процесу	етап або елемент процесу, який знижує його ефективність, створює затримки або підвищує ризики помилок

Поняття	Зміст
ГААП (Generally Accepted Accounting Principles)	дослівно – загальноприйняті бухгалтерські принципи. Міжнародні стандарти, що описують бухгалтерські процедури
Генеральна сукупність	повний масив облікових даних або господарських операцій, що є об’єктом аудиторської перевірки
Генерація даних	процес створення та збору даних через різноманітні цифрові канали, включаючи онлайн-платформи, сенсори, пристрої IoT (Інтернет речей) та інші джерела цифрової інформації
Генерація та аналіз великих даних (Big Data)	технології та методи збору, зберігання, обробки та аналізу величезних обсягів даних з різних джерел для виявлення трендів, покращення рішень і прогнозування подій у бізнесі, медицині, науці та інших сферах
Дані-озеро	сховище сирих даних різних форматів (структурованих/неструктурованих) для подальшої обробки
Дашборд	інтерактивна панель показників, що відображає ключові метрики, ризики та винятки в режимі близькому до реального часу
Двофакторна автентифікація	це різновид багатофакторної автентифікації, за якого використовується рівно два фактори підтвердження особи (2FA)
Деталізація	перехід від агрегованого показника до первинних транзакцій і документів для підтвердження висновків
Децентралізовані фінанси (DeFi)	фінансові сервіси, що функціонують без посередників, використовуючи технології блокчейн і смарт-контракти для надання кредитів, позик, страхових послуг та інших фінансових операцій.
Диджитал-інфраструктура	технологічна інфраструктура, яка забезпечує підтримку цифрових рішень, включаючи хмарні платформи, бази даних, мережеві рішення та інші інструменти для ефективного ведення бізнесу в цифровому середовищі
Дискреційна модель контролю доступу	це модель, за якої права доступу визначає власник ресурсу або уповноважена особа шляхом надання або відкликання дозволів (DAC)

Поняття	Зміст
Діджиталізація	процес переходу від традиційних методів обробки інформації до використання цифрових технологій, що включає в себе автоматизацію бізнес-процесів, введення цифрових платформ і інструментів, а також інтеграцію сучасних технологій у повсякденну діяльність
Діяльність (підрозділ) внутрішнього аудиту	відділ, підрозділ, група консультантів або інших фахівців, що надає незалежні та об'єктивні гарантії і консультації, спрямовані на вдосконалення діяльності організації. Внутрішній аудит допомагає організації досягати поставлених цілей, використовуючи систематизований і послідовний підхід до оцінки і підвищення ефективності процесів корпоративного управління, управління ризиками і контролю
Доповнена реальність (AR)	технологія, яка накладає цифрові елементи на реальний світ, дозволяючи користувачам взаємодіяти з цифровими об'єктами в реальному середовищі
Допустима похибка	максимальна похибка в генеральній сукупності, яку аудитор погодився прийняти
Доступність	це властивість інформації та сервісів бути доступними для легітимних користувачів у потрібний час і в потрібному обсязі, компонент CIA
Доступність фінансових послуг	можливість отримання фінансових продуктів з урахуванням географічних, фізичних, економічних та цифрових бар'єрів
Дрейф моделі	погіршення якості моделі через зміну процесів або розподілів даних з часом
Економічний аналіз	наукове дослідження результатів господарської діяльності підприємства на основі показників планів, обліку, звітності та інших джерел інформації
Екосистема цифрової економіки	мережа взаємопов'язаних цифрових платформ, компаній, споживачів та інструментів, що разом створюють цілісну цифрову економічну структуру для реалізації послуг та товарів у цифровому середовищі
Експертиза	дослідження досвідченим спеціалістом (експертом) будь-якого питання, що вимагає спеціальних знань
Екстраполяція	поширення вибіркових даних на другу частину сукупності, не віднесену до огляду

Поняття	Зміст
Електронна ідентифікація	процес встановлення особи за допомогою цифрових технологій, таких як електронні підписи, біометричні дані або цифрові сертифікати, для надання доступу до різноманітних онлайн-сервісів або здійснення юридичних операцій
Електронна комерція (e-commerce)	бізнес-процеси купівлі, продажу, обміну товарами, послугами або інформацією за допомогою Інтернету чи інших цифрових технологій
Електронний документ	документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа
Електронний документообіг	організована система створення, обробки, погодження, підписання, передавання, зберігання та використання документів у цифровій формі з використанням визначених правил і технологій
Електронний підпис	дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних
Електронний уряд (e-government)	використання інформаційних технологій і цифрових платформ для надання державних послуг громадянам, підприємствам та організаціям, а також для спрощення міжурядових процесів
Електронний цифровий підпис	вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача
Етичний консалтинг	гармонійне поєднання трьох елементів: незалежності експерта, управління конфліктами інтересів та дотримання цифрової етики. Незалежність забезпечує об'єктивність; контроль конфліктів інтересів зменшує вплив особистої вигоди; цифрова етика регулює використання технологій, підвищуючи прозорість та безпеку. У центрі перетину цих сфер інтегрований підхід до управління ризиками, де для кожної ситуації підбирають відповідні методи моніторингу, аудиту, розкриття інформації та технічного захисту
Етичні принципи	загальноприйняті етичні норми поведінки у сфері аудиту, яких має дотримуватися аудитор у своїй діяльності
Журнал подій	системні записи про дії користувачів і процесів (логи), що використовуються для перевірки доступів, змін та інцидентів

Поняття	Зміст
Журналювання	це процес системної фіксації подій доступу та змін у системі для контролю, розслідування та доказовості
Завдання з обов'язкового аудиту фінансової звітності	завдання з надання обґрунтованої впевненості, що приймається і виконується суб'єктом аудиторської діяльності відповідно до вимог Закону та міжнародних стандартів аудиту шляхом перевірки фінансової звітності або консолідованої фінансової звітності з метою висловлення незалежної думки аудитора про її відповідність в усіх суттєвих аспектах і відповідність вимогам міжнародних стандартів фінансової звітності або національних положень (стандартів) бухгалтерського обліку та законів України
Загальна стратегія аудиту	встановлює обсяг, час і напрямок аудиту та допомагає в розробці більш детального плану аудиту
Загальний рівень процесної моделі	рівень опису, на якому процеси подаються укрупнено без деталізації окремих дій і процедур
Загальні ІТ-контролі	контролі ІТ-середовища (доступи, зміни, резервне копіювання, операційні процедури), що впливають на надійність систем
Загроза	це потенційне джерело небажаної події, яке може спричинити порушення безпеки, наприклад зловмисник, шкідливе ПЗ або помилка користувача
Закон Бенфорда	статистичний тест розподілу перших цифр числових даних; застосовується як індикатор можливих викривлень (не є прямим доказом шахрайства)
Захист прав споживачів фінансових послуг	система правових і організаційних заходів, спрямованих на забезпечення прозорості, справедливості та безпеки фінансових операцій
Звірка	узгодження даних між системами або реєстрами (наприклад, головна книга і субреєстри, банк і каса)
Зовнішні загрози фінансовій безпеці	ризики, зумовлені змінами макроекономічного середовища, державного регулювання, конкуренції, фінансових ринків, політичної та економічної нестабільності.
Зовнішній аудит (незалежний аудит)	це незалежна перевірка фінансової звітності, що виконується аудитором або аудиторською фірмою з метою надання обґрунтованої впевненості та висловлення думки

Поняття	Зміст
Імпорт даних	процес завантаження облікової інформації з зовнішніх джерел (ERP-систем, бухгалтерських програм, файлів CSV, XLSX, баз даних) у середовище аналітичного інструменту
Інвентаризація	виявлення фактичної наявності майна та зіставлення його з даними бухгалтерського обліку
Інвестиційна привабливість	багатовимірне поняття, що відображає думку інвесторів щодо перспектив подальшого успішного функціонування об'єкта інвестування, є сукупністю об'єктивних ознак, властивостей і можливостей, які визначають потенційний платіжний попит на інвестиції
Інвестиційний консультант (радник)	професіонал з інвестування, з об'єктів інвестицій, з вкладання капіталу з отриманням максимального прибутку при мінімальних ризиках, з розподілу фінансів як фізичних, так юридичних осіб. Вихідною рамкою у даному випадку є його фаховість як експерта, який висловлює думку не тільки щодо достовірності фінансової звітності, але й допомагає клієнтові приймати економічні рішення, зокрема щодо структури капіталу, купівлі активів, інвестицій у цінні папери, беручи на себе частину відповідальності за наслідки цих рішень
Індикатори фінансової безпеки	кількісні та якісні показники, що відображають рівень фінансової стійкості, платоспроможності та ризиків підприємства
Інклюзивна фінансова система	сукупність фінансових інститутів, інструментів і регуляторних механізмів, що забезпечують доступність, прозорість та безпечність фінансових послуг для широкого кола користувачів
Інклюзивний аудит	комплексний інструмент управлінської діагностики, спрямований на оцінювання інклюзивних наслідків управлінських рішень, процесів і результатів діяльності організації з позиції рівності можливостей, недискримінації, доступності та залученості персоналу і зацікавлених сторін
Інклюзивний аудит процесів	системна оцінка того, як організація вибудовує й реалізує управлінські та кадрові процеси через: інклюзивність колективу і стейкхолдерів, інклюзивність робочих місць, інклюзивні комунікації та участь, інклюзивну культуру – для виявлення бар'єрів і ризиків, що впливають на рівність можливостей і залученість

Поняття	Зміст
Інклюзивний аудит результатів	оцінювання досягнутих результатів діяльності організації з позицій інклюзивності, що ґрунтується на аналізі вимірюваних показників і підтверджених ефектів: рівня безбар'єрності (зокрема універсального дизайну), соціальної відповідальності, фактичної рівності можливостей, а також динаміки індикаторів, які відображають зменшення бар'єрів, скарг і проявів дискримінації та зростання залученості й психологічної безпеки
Інклюзивний аудит управлінських рішень	оцінювання процедур прийняття рішень з погляду їх інклюзивних, соціальних і управлінських наслідків для трудового колективу та зацікавлених сторін
Інноваційні технології	новітні технології, що мають потенціал радикально змінити існуючі процеси в бізнесі, науці та інших сферах діяльності, часто стають основою для розвитку цифрової економіки
Інтеграція процесних результатів	використання результатів процесного моделювання та аналізу в системі управлінських, облікових і контрольних рішень
Інтеграція цифрових технологій в економіку	процес впровадження цифрових рішень і інструментів у традиційні економічні процеси з метою підвищення ефективності, скорочення витрат і розширення можливостей для розвитку бізнесу
Інтегрована модель управління фінансовою безпекою	комплексна система управління, що поєднує фінансові, організаційні, інформаційні, ризик-орієнтовані та стратегічні інструменти з метою забезпечення стійкості фінансової системи підприємства та мінімізації загроз.
Інтелектуальна автоматизація	поєднання штучного інтелекту та автоматизації для виконання складних завдань, таких як обробка даних, прийняття рішень та управління виробничими процесами з мінімальним людським втручанням
Інтелектуальна власність в цифровому середовищі	права на результати творчої діяльності в цифровій сфері, такі як патенти, авторські права на програмне забезпечення, торгові марки для онлайн-платформ і контенту
Інтелектуальні бізнес-мережі	платформи, що забезпечують компаніям обмін даними, а також аналіз інформації для поліпшення бізнес-рішень, прогнозування попиту та пропозиції, оптимізації ланцюгів постачання

Поняття	Зміст
Інтелектуальні системи	комп’ютерні системи, які використовують методи штучного інтелекту для автономного виконання складних завдань, навчання на досвіді і адаптації до змін у навколишньому середовищі
Інтернет економіка	частина цифрової економіки, що включає всі економічні та фінансові операції, які здійснюються через Інтернет, включаючи електронну комерцію, цифрові платежі та онлайн-послуги
Інтернет речей (IoT)	мережа фізичних пристроїв, що підключені до Інтернету і можуть збирати, передавати та обробляти дані для підвищення ефективності процесів, зокрема в бізнесі, медицині та побуті
Інтернет-бізнес	комерційна діяльність, що здійснюється через Інтернет, включаючи електронну комерцію, онлайн-рекламу, електронні послуги та інші види цифрового бізнесу
Інтероперабельність систем	здатність різних інформаційних систем і технологій обмінюватися даними і працювати разом без порушень і необхідності в додаткових налаштуваннях
Інтерфейс програмування застосунків	програмний інтерфейс (API) для отримання даних із систем (ERP/CRM/банкінг) та автоматизації збору доказів
Інференс	застосування навченої моделі до нових даних для прогнозу або класифікації ризику
Інформаційна безпека	це стан і система заходів, що забезпечують конфіденційність, цілісність і доступність даних та не допускають їх розкриття, спотворення або втрати доступу
Інформаційна безпека фінансових даних	захищеність фінансової інформації від несанкціонованого доступу, втрати, спотворення або використання з метою заподіяння шкоди підприємству.
IT-контролі прикладні	контролі бізнес-логіки в системі (перевірки введення, ліміти, узгодження тощо)
Кібератаки	атаки на комп’ютерні системи або мережі з метою викрадення даних, зупинки бізнес-процесів або завдання шкоди компанії чи державі
Кібербезпека	практика захисту комп’ютерних систем, мереж і даних від несанкціонованого доступу, атак або ушкоджень, що стає особливо важливим у цифровій економіці

Поняття	Зміст
Кіберінцидент	це реалізація загрози у формі порушення конфіденційності, цілісності або доступності даних
Кіберризик	це ймовірність та потенційний вплив реалізації кіберзагрози з урахуванням вразливостей і наявних контролів, що може спричинити фінансові та операційні втрати
Кіберфінансова безпека	захищеність фінансових операцій та цифрових фінансових сервісів від кібератак, шахрайства та несанкціонованого доступу
Кластеризація	метод ненаглядного навчання для групування схожих транзакцій/контрагентів без наперед заданих міток
Ключове поле	унікальний ідентифікатор (ID), за яким поєднуються таблиці та зв'язуються записи між системами
Комп'ютеризовані методи аудиту	використання програмних засобів (CAATs) для суцільного тестування, звірок, пошуку аномалій та контролів
Контроль	обов'язковий елемент управління, метою якого є виявлення відхилень від прийнятих стандартів, а також порушень принципів законності, ефективності й економії ресурсів
Контрольна точка процесу	етап процесу, на якому здійснюється перевірка, погодження або підтвердження правильності виконання дій
Конфіденційність	це властивість даних бути доступними лише уповноваженим особам і не розкриватися стороннім, компонент CIA
Конфіденційність даних	захист персональних і чутливих даних (мінімізація, маскування, контроль доступу, шифрування)
Кореляція та причинність	кореляція у даних не означає причинно-наслідковий зв'язок; важливо для коректних аудиторських висновків
Корпоративне управління	система взаємовідносин між власниками, керівництвом та іншими зацікавленими сторонами, що визначає правила прийняття рішень і контроль за діяльністю підприємства, у тому числі у сфері фінансової безпеки
Краудсорсинг	залучення широкої аудиторії або спільноти до виконання завдань або збору інформації через цифрові платформи

Поняття	Зміст
Краудфандинг	процес залучення фінансування для проєктів або стартапів через масову підтримку від великої кількості людей, зазвичай через онлайн-платформи, де кожен може зробити внесок у фінансування ідеї
Криптовалюти	цифрові або віртуальні валюти, що використовують криптографію для забезпечення безпеки та незалежні від традиційних фінансових інститутів і центральних банків. Прикладами є Bitcoin, Ethereum, Ripple та інші
Криптографія	наука про шифрування та захист інформації, яка забезпечує конфіденційність і цілісність даних у цифрових системах, зокрема в платіжних системах і криптовалютах
Лінія походження даних	опис шляху даних від джерела до звіту/аналітики (перетворення, завантаження, агрегування) для підтвердження надійності
Людський фактор	суб’єктивні помилки або упередження, що можуть виникати під час ручного виконання аудиторських процедур
Мандатна модель контролю доступу	це модель, за якої правила доступу встановлюються централізовано політикою безпеки за рівнями допуску або класифікації, а користувачі не можуть їх змінювати (MAC)
Маркування даних	присвоєння міток записам (наприклад, «норма/виняток») для навчання та оцінювання моделей
Машинне навчання	алгоритми, що навчаються на історичних даних для класифікації, прогнозу та виявлення аномалій в аудиті
Мета аудиторської діяльності	підвищення ступеня довіри визначених користувачів до фінансової звітності
Метадані	дані про дані: джерело, час створення, автор, права доступу, версії, атрибути записів
Метод аудиту	сукупність прийомів, за допомогою яких оцінюється стан досліджуваних об’єктів
Методологія моделювання бізнес-процесів	система правил, принципів і умовних позначень, що використовуються для побудови процесних моделей
Мікрофінансування	надання невеликих фінансових ресурсів фізичним особам або малому бізнесу з обмеженим доступом до традиційних банківських послуг

Поняття	Зміст
Мобільний банкінг	фінансові послуги, що надаються через мобільні додатки або веб-платформи, дозволяючи користувачам здійснювати операції, такі як переведення коштів, оплата рахунків або отримання кредитів, через свої смартфони або планшети
Мобільні платежі	система електронних фінансових транзакцій, які виконуються через мобільні пристрої, наприклад, смартфони чи планшети, дозволяючи користувачам здійснювати покупки, перекази та інші фінансові операції без використання фізичних карток
Мобільні платформи	онлайн-сервіси та додатки, доступні через мобільні пристрої, які дозволяють користувачам взаємодіяти з продуктами, послугами та іншими користувачами, а також здійснювати операції, такі як покупки, бронювання, перевезення тощо.
Мобільні платформи для управління ланцюгами постачання (Supply Chain Management Mobile Platforms)	мобільні додатки та платформи, що дозволяють компаніям здійснювати моніторинг, управління та оптимізацію логістичних процесів через мобільні пристрої
Мобільні технології	технології, що дозволяють здійснювати комунікацію, обробку даних та здійснювати операції через мобільні пристрої (смартфони, планшети), що є важливою частиною цифрової економіки
Модель нульової довіри	це підхід безпеки, за якого жоден запит не вважається надійним за замовчуванням, а доступ надається лише після постійної перевірки та за принципом мінімальних привілеїв (Zero Trust)
Моделювання бізнес-процесів	процес створення структурованого опису діяльності підприємства з метою її аналізу, оцінювання та вдосконалення
Незалежний експерт	спеціаліст, що не входить до складу аудиторської організації, має достатні знання та досвід в конкретній області, що відрізняється від бухгалтерського обліку та аудиту та надає висновок з питань даної галузі
Незалежність	свобода від умов, які загрожують службі внутрішнього аудиту неупереджено виконувати свої обов’язки

Поняття	Зміст
Нейронні мережі	технологія штучного інтелекту, яка моделює роботу людського мозку для вирішення складних задач, таких як розпізнавання образів, автоматичний переклад, прогнозування тощо
Ненаглядне навчання	підхід ML без розмічених даних (кластеризація, пошук аномалій) для виявлення нетипових патернів
Несистематичні записи	записи, якими оформлюються одиничні, неповторювані постійно господарські операції
Нетипові операції	господарські операції, нехарактерні для діяльності підприємства чи такі, що виконуються рідко або за нетипових умов та потребують додаткової уваги аудитора
Нечітке співставлення	алгоритми пошуку схожих записів за неповного збігу (імена контрагентів, адреси) для де-дуплікації та звірок
Нормалізація даних	приведення даних до узгодженого вигляду (формати дат, коди валют, довідники) для коректного аналізу
Об’єднання таблиць	операція JOIN для з’єднання наборів даних за ключами (платежі ↔ інвойси ↔ постачальники)
Обов’язкові реквізити документа	обов’язкові дані в електронному документі, без яких він не може бути підставою для обліку і не матиме юридичної сили
Обробка природної мови	методи (NLP) для аналізу текстів договорів, листування, призначень платежів та приміток у системах
Обробка природної мови (NLP)	галузь штучного інтелекту, що займається взаємодією між комп’ютерами та людською мовою для її розпізнавання і аналізу.
Обсяг аудиту	сукупність аудиторських процедур, необхідних для виконання поставлених завдань, обсяг і термін їх виконання
Озеро даних	централізоване сховище, яке зберігає дані у первинних форматах для подальшого аналізу
Омніканальність (Omnichannel)	стратегія взаємодії з клієнтами через різні цифрові і традиційні канали, що забезпечує безшовний і послідовний досвід користувача незалежно від точки контакту
Операційний рівень процесної моделі	найбільш детальний рівень опису процесів, який використовується як основа для виконання та перевірки конкретних процедур

Поняття	Зміст
Оптимізація бізнес-процесів	цілеспрямоване вдосконалення процесів з метою підвищення їх ефективності, скорочення часу виконання та зменшення витрат при збереженні контролю
Параметризований тест	тест/правило з налаштовуваними порогами (сума, частота, часові вікна), який легко адаптувати до різних періодів
Перенавчання	ситуація, коли модель добре працює на навчальних даних, але погано узагальнює на нових
Персоналізація	процес адаптації продуктів, сервісів або маркетингових повідомлень під індивідуальні потреби і вподобання користувача
Платежі через мобільні додатки	система безготівкових платежів, що здійснюються через мобільні додатки, дозволяючи користувачам оплачувати товари та послуги безпосередньо через свої смартфони або інші мобільні пристрої
Платформа	цифровий інструмент або сервіс, що забезпечує взаємодію між користувачами і різними додатками або системами
Поверхня атаки	це сукупність усіх точок входу й каналів взаємодії, через які можливе порушення безпеки, зокрема акаунти, віддалений доступ, хмара, інтеграції та API, пристрої (attack surface)
Повнота	твердження, що всі операції, які мають бути відображені, відображені у даних/звітності (ризик: «випадіння» транзакцій)
Портфельний інвестор	вкладає кошти у цінні папери (часткові та боргові) з метою отримання доходу у вигляді дивідендів, якщо на момент їх виплати акції будуть у його власності, або різниці в цінах купівлі та продажу. Як правило, не втручається в управління компанією, оскільки його пакети цінних паперів є незначними (міноритарними), його цікавить лише ліквідність цінних паперів
Поточний контроль	контроль, що здійснюється в процесі господарської діяльності та проводиться на основі даних оперативного обліку
Пояснюваність	здатність моделі пояснити, чому транзакція позначена як ризикова, щоб обґрунтувати аудиторські висновки
Принцип мінімальних привілеїв	надання користувачам лише тих прав доступу, які необхідні для виконання їхніх обов’язків

Поняття	Зміст
Принцип найменших привілеїв	це правило, за яким користувачу або процесу надається мінімально необхідний доступ і лише на час виконання завдання (Least Privilege)
Прогнозна аналітика	оцінка ймовірності подій (прострочка, помилка, ризик шахрайства) на основі історичних даних
Програма аудиту	документ, що містить завдання аудиту для конкретного об’єкта
Програмні засоби моделювання процесів	інструменти, що використовуються для створення, аналізу та візуалізації процесних моделей (BPMN-редактори, BPM-платформи тощо
Професійне судження аудитора	застосування знань, досвіду та етичних принципів аудитора при прийнятті рішень у процесі планування та проведення аудиту
Процеси ETL/ELT	витягання, трансформація і завантаження даних (ETL) або витягання, завантаження і трансформація (ELT)
Процес-майнінг	відновлення реального бізнес-процесу з логів подій та виявлення відхилень, обхідних шляхів і порушень контролів
Процесний аналіз	дослідження бізнес-процесів з метою виявлення неефективних етапів, ризиків та можливостей удосконалення
Процесно-орієнтована модель	графічне або логічне представлення бізнес-процесів, яке відображає послідовність дій, учасників, інформаційні потоки та контрольні точки
Процесно-орієнтований підхід	підхід до організації діяльності, за якого облік, контроль і аудит розглядаються як система взаємопов’язаних процесів, а не як сукупність окремих функцій або підрозділів
Ревізія	документальний спосіб перевірки діяльності суб’єкта господарювання з точки зору дотримання законності та доцільності здійснення господарських операцій, ефективності та якості роботи на основі використання даних обліку, звітності та інших джерел
Резервне копіювання	це процес регулярного створення копій критичних даних і конфігурацій з метою їх відновлення після інцидентів втрати, пошкодження або недоступності інформації (backup)
Репрезентативність вибірки	властивість деякої аудиторської вибірки дати можливість аудитору зробити на її основі правильні висновки про властивості всієї сукупності, що перевіряється

Поняття	Зміст
Ризик	це поєднання ймовірності настання небажаної події та тяжкості її наслідків для активів, у кібербезпеці для даних, систем і сервісів
Ризик контролю	ризик невиявлення помилок внутрішньою системою контролю підприємства
Ризик обліку	ризик, що допускає аудитор, як часто у звітності, що перевіряється у звітному періоді, порушувались норми внутрішнього контролю
Ризик суттєвого викривлення	імовірність того, що фінансова інформація містить помилки або викривлення, які можуть суттєво вплинути на рішення користувачів звітності, до проведення аудиту
Ризики фінансової безпеки	сукупність внутрішніх і зовнішніх загроз, які можуть призвести до фінансових втрат, порушення платоспроможності, зниження фінансової стійкості або втрати контролю над фінансовими ресурсами підприємства
Ризик-орієнтований аудит	підхід до проведення аудиту, за якого основна увага зосереджується на ділянках з підвищеним рівнем ризику, у тому числі IT-ризиків та ризиків фінансової безпеки
Ризик-орієнтований підхід	методологія аудиту, за якої обсяг і характер процедур визначаються з урахуванням оцінених аудиторських ризиків
Ризик-скоринг	присвоєння транзакціям або контрагентам балу ризику на основі правил або моделі для пріоритезації перевірок
Рівень опису процесу	ступінь деталізації процесної моделі, що може бути загальним, аналітичним або операційним залежно від мети аналізу
Роботи та автоматизація	використання механічних і програмних систем для автоматичного виконання завдань, які раніше виконували люди, зокрема в сфері виробництва, логістики, медицини та інших галузях
Роботизація бізнес-процесів	впровадження роботів, програмного забезпечення або штучного інтелекту для автоматизації виробничих або управлінських завдань, що дозволяє зменшити витрати, підвищити ефективність і швидкість виконання операцій
Роботизація процесів	використання RPA для автоматизації рутинних дій (збір виписок, вивантаження звітів, оновлення реєстрів)

Поняття	Зміст
Робототехніка	галузь науки та техніки, що займається розробкою роботів для автоматизації різноманітних процесів, включаючи промислове виробництво, медицину, обслуговування і навіть побутові функції
Робочий процес	послідовність кроків від збору даних до аналізу, формування доказів і документування висновків
Розподіл обов'язків	сегрегація функцій, щоб одна особа не могла одноосібно ініціювати, погодити та виконати операцію
Розумні контракти (Smart contracts)	контракти, які автоматично виконуються при досягненні певних умов, без необхідності участі посередників. Вони використовують технологію блокчейн для забезпечення прозорості і безпеки угод
Рольова модель контролю доступу	це модель доступу, за якої права надаються ролям, а користувачі отримують доступ через призначення відповідних ролей (RBAC)
Сегментація мережі	це поділ мережі на ізольовані зони безпеки, який обмежує переміщення атакувальника та радіус ураження у разі компрометації
Система управління фінансовою безпекою	сукупність методів, механізмів, інструментів і процедур, спрямованих на виявлення, оцінку, моніторинг та нейтралізацію фінансових загроз
Системи електронних платежів	платформи або сервіси, що дозволяють здійснювати фінансові транзакції між фізичними або юридичними особами через Інтернет або мобільні пристрої.
Системи управління відносинами з клієнтами (CRM)	програмні рішення, які дозволяють підприємствам зберігати та аналізувати інформацію про своїх клієнтів, щоб покращити взаємодію, підвищити ефективність продажів та маркетингових кампаній
Смарт-контракти	комп'ютерні програми, що автоматично виконують умови контракту при виконанні певних умов, забезпечуючи прозорість, ефективність і безпеку угод без посередників
Соціальна інженерія	це методи психологічного впливу, спрямовані на те, щоб користувач сам розкрив секрети або виконав небезпечну дію
Соціальна інклюзія	залучення всіх груп населення до повноцінної участі в економічному та соціальному житті суспільства, зокрема через доступ до фінансових ресурсів і послуг
Соціальні медіа	онлайн-платформи, що дозволяють користувачам створювати, обмінюватися та взаємодіяти з контентом

Поняття	Зміст
Соціально відповідальний фінансовий сектор	фінансові установи, які у своїй діяльності враховують соціальні наслідки рішень та сприяють фінансовій інклюзії
Спостереження	метод контролю за виконанням іншими особами процедур при безпосередній присутності аудитора для цілеспрямованого та об'єктивного сприйняття інформації
Сталий фінансовий розвиток	розвиток підприємства, за якого забезпечується баланс між прибутковістю, ризиками та довгостроковою фінансовою безпекою
Стійкість домогосподарств	здатність сімей та окремих осіб протистояти фінансовим шокам і зберігати економічну стабільність
Стратегічний інвестор	ставить за мету встановити довгострокові відносини з об'єктом інвестування, при цьому дивіденди не є головною метою, яка може бути різною: від отримання безпосереднього впливу на управління до повного контролю; вихід на нові ринки, отримання доступу до інноваційних, в тому числі цифрових технологій, каналів збуту, бренд, управлінський досвід
Суттєвість в аудиті	можливість інформації вплинути на рішення її користувачів
Суцільний аналіз даних	підхід до аудиту, за якого перевірці підлягає 100 % генеральної сукупності облікових даних без формування вибірки
Схема даних	структура таблиць, полів та зв'язків у базі даних; визначає правила зберігання та інтеграції інформації
Сховище даних	централізоване сховище (DWH) структурованих даних для звітності та аналітики
Табличні процесори	універсальні програмні засоби (Microsoft Excel, Google Sheets), що застосовуються для обробки, структурування та первинного аналізу облікових даних
Таргетинг	процес спрямування рекламних або маркетингових повідомлень на конкретні аудиторії, визначені за демографічними, поведінковими або іншими характеристиками
Тести контролю	тести, які виконуються для одержання аудиторських доказів щодо операційної ефективності заходів контролю стосовно попередження або виявлення та виправлення суттєвих викривлень на рівні тверджень

Поняття	Зміст
Тестування цифрової доступності	комплекс методів оцінювання вебресурсів, електронних форм, цифрових документів і застосунків на відповідність вимогам доступності та безбар'єрності шляхом поєднання автоматизованих інструментів перевірки й експертного (ручного) тестування; результати тестування формують підставу для висновків щодо наявності або відсутності цифрових бар'єрів у комунікації та наданні послуг
Технічний аналіз	метод прогнозування динаміки цін, заснований на математичних, а не на економічних теоріях. Історично склалось так, що технічний аналіз формувався, як певна сукупність різноманітних методів, які існували окремо, один від одного, та розвивались паралельно. По суті, технічний аналіз – це накопичений досвід аналітиків, отриманий емпіричним шляхом. Основою більшості методів є спостереження практикуючих трейдерів, які досліджували ціну або курс активу і користувалися для цього спеціальними графіками
Техноекономіка	галузь економічної науки, що досліджує взаємодію технологій та економічних процесів, зокрема вплив цифрових технологій на ефективність виробництва та розвиток бізнесу
Технології віртуальної реальності (VR)	технологія, що дозволяє користувачам зануритися в повністю віртуальний світ, використовуючи спеціальні пристрої, такі як VR-гарнітури, що створює ілюзію присутності в іншому середовищі
Технології доповненої реальності (AR)	інтеграція віртуальних елементів або інформації в реальний світ за допомогою пристроїв, таких як смартфони або спеціальні окуляри, що дозволяє покращити сприйняття реальності
Технології обробки природної мови (NLP)	технології штучного інтелекту, які дозволяють комп'ютерам «розуміти» та «взаємодіяти» з людською мовою. Це охоплює чат-боти, голосові помічники, автоматичний переклад та інші інструменти для роботи з текстом і мовленням
Технології штучного інтелекту (AI)	програмне забезпечення, яке здатне до самонавчання і виконання завдань, що зазвичай вимагають людського інтелекту, таких як розпізнавання образів, ухвалення рішень, прогнозування тощо

Поняття	Зміст
Технологія 5G	п’яте покоління мобільних мереж, яке забезпечує високошвидкісну передачу даних, низькі затримки та можливість підключення великої кількості пристроїв. Ця технологія дозволяє реалізувати інноваційні рішення в галузях, таких як розумні міста, автономні транспортні засоби, телемедицина та інші
Токенізація	заміна чутливих значень на токени для безпечної обробки та обмеження доступу до оригінальних даних
Тривекторна модель інклюзивного аудиту	концептуальна модель, за якою інклюзивність в організації оцінюється у трьох взаємодоповнювальних векторах: інклюзивність управлінських рішень, інклюзивність процесів та інклюзивність результатів. Вона дає змогу комплексно діагностувати, де саме формуються або відтворюються бар’єри й нерівність можливостей, та пов’язати управлінські причини (рішення), механізми реалізації (процеси) і вимірювані наслідки (результати) в єдину логіку аудиторських висновків і рекомендацій
Фальшиве спрацювання	ситуація, коли тест/модель позначає операцію як ризикову, хоча вона є нормальною
Фальшивий пропуск	ситуація, коли тест/модель не позначає ризикову операцію, хоча вона є проблемною
Фільтрація даних	відбір підмножини даних за умовами (період, тип операції, пороги) для виконання конкретної процедури
Фінансова безпека підприємства	стан захищеності фінансових ресурсів і процесів від внутрішніх та зовнішніх загроз, що оцінюється, зокрема, за результатами аудиту
Фінансова вразливість	підвищена схильність окремих осіб або груп до фінансових ризиків через низькі доходи, обмежений доступ до фінансових інструментів або недостатній рівень фінансової грамотності
Фінансова дискримінація	обмеження або відмова у доступі до фінансових послуг на підставі соціальних, демографічних або фізичних характеристик клієнта
Фінансова етика	сукупність моральних принципів і норм, що регулюють поведінку фінансових установ і учасників ринку щодо клієнтів і суспільства.

Поняття	Зміст
Фінансова інклюзія	процес забезпечення рівного доступу всіх верств населення та суб'єктів господарювання до фінансових послуг і продуктів незалежно від рівня доходів, соціального статусу, фізичних можливостей або місця проживання
Фінансова рівність	рівний доступ до фінансових ресурсів і можливостей незалежно від соціальних або економічних характеристик.
Фінансова стабільність	1) здатність фінансової системи ефективно виконувати свої функції навіть за умов внутрішніх або зовнішніх шоків; 2) здатність підприємства зберігати рівновагу фінансових потоків і показників у змінному економічному середовищі
Фінансова стійкість	здатність підприємства підтримувати збалансовану структуру капіталу, своєчасно виконувати фінансові зобов'язання та протистояти негативним зовнішнім впливам
Фінансова стратегія	довгостроковий план управління фінансовими ресурсами підприємства, спрямований на забезпечення його фінансової безпеки та стійкого розвитку
Фінансовий контроль	система заходів, спрямованих на перевірку законності, доцільності та ефективності використання фінансових ресурсів підприємства
Фінансовий моніторинг	безперервний процес спостереження та аналізу фінансових показників підприємства з метою своєчасного виявлення відхилень і потенційних загроз
Фінансові загрози	сукупність внутрішніх і зовнішніх факторів, які можуть призвести до погіршення фінансового стану підприємства, зниження прибутковості або втрати капіталу
Фінансові ризики	імовірність виникнення фінансових втрат у результаті впливу невизначеності, зумовленої коливанням валютних курсів, процентних ставок, кредитоспроможності контрагентів, ліквідності та інших факторів
Фінансові ризики для населення	імовірність фінансових втрат фізичних осіб унаслідок шахрайства, нестабільності доходів, інфляції або неправильно прийнятих фінансових рішень

Поняття	Зміст
Фінансові технології (FinTech)	технології, що застосовуються для надання фінансових послуг, включаючи мобільні платежі, блокчейн, онлайн-кредитування, краудфандинг та інші інноваційні фінансові рішення
Фішинг	це шахрайські повідомлення електронною поштою або SMS, метою яких є виманювання конфіденційних даних або спонукання до дії на користь зловмисника
Фундаментальний аналіз	всебічний ґрунтовний аналіз, що вивчає рух цін під впливом макроекономічних чинників. Головною його метою є визначення справедливої ціни досліджуваного активу. Порівнюючи отриману оцінку із поточним станом ринку, робиться висновок – переоцінений чи недооцінений цей актив. Фундаментальний аналіз використовується стратегічними інвесторами, що розраховують на реалізацію довгострокових стратегій, заробляючи на багаторічних цінових тенденціях
Функціональний підхід	підхід до організації обліково-аудиторської діяльності, за якого робота будується за функціями або підрозділами, без цілісного уявлення про перебіг процесів
Хешування	обчислення хеш-значення для контролю цілісності та ідентифікації файлів/записів
Хмарні технології	використання віддалених серверів для зберігання даних, обробки інформації та надання різноманітних онлайн-сервісів, що дають змогу користувачам зберігати і обробляти дані без необхідності володіти фізичним обладнанням
Цифрова безпека	комплекс заходів і технологій для захисту цифрових даних, інформаційних систем і інфраструктури від загроз, таких як хакерські атаки, крадіжка даних, вірусні програми та інші небезпеки в цифровому середовищі
Цифрова валюта центрального банку (CBDC)	цифрова форма фіатної валюти, що випускається центральним банком країни, яка має юридичну силу як традиційні гроші, але існує тільки в електронній формі
Цифрова гнучкість	здатність організації або економічної системи адаптуватися до змін і швидко впроваджувати нові цифрові технології, щоб ефективно реагувати на виклики та можливості, що виникають

Поняття	Зміст
Цифрова грамотність	здатність користувачів ефективно використовувати цифрові технології для досягнення своїх цілей, зокрема для отримання, обробки, збереження та передачі інформації
Цифрова економіка	система економічних відносин, яка ґрунтується на використанні цифрових технологій, Інтернету та сучасних інформаційних інструментів для організації та розвитку виробництва, бізнесу, торгівлі та інших економічних процесів
Цифрова інфраструктура підприємства	сукупність технологій, програмного забезпечення, обладнання і процесів, які підприємство використовує для автоматизації своїх операцій, управління даними, комунікацій з клієнтами та іншими зацікавленими сторонами
Цифрова культура	явище, яке виникає в результаті інтеграції цифрових технологій у повсякденне життя та культурні процеси. Вона включає в себе використання цифрових технологій у мистецтві, музиці, літературі, кіно та інших формах творчості
Цифрова платіжна система	система для здійснення фінансових транзакцій через Інтернет або мобільні пристрої, що включає цифрові гаманці, системи мобільних платежів та інші інструменти для переказу грошей онлайн
Цифрова трансформація	процес змін у компанії чи організації, коли традиційні бізнес-процеси, стратегії та моделі управління замінюються новими технологічними рішеннями, що включають використання цифрових інструментів, автоматизацію та інноваційні підходи
Цифрова фінансова інклюзія	розширення доступу до фінансових послуг за допомогою цифрових технологій, зокрема мобільного банкінгу, онлайн-платформ і фінтех-рішень
Цифрове виробництво	застосування цифрових технологій в процесі виробництва, зокрема автоматизації, роботизації, використання 3D-друку, Інтернету речей (IoT) та інших інструментів для підвищення ефективності виробничих процесів
Цифрове державне управління	використання цифрових технологій для поліпшення та оптимізації державних послуг і процесів, включаючи автоматизацію адміністративних процедур, надання електронних послуг громадянам, а також підвищення прозорості та ефективності урядових інститутів

Поняття	Зміст
Цифрове підприємництво	форма підприємницької діяльності, яка повністю або переважно базується на використанні цифрових технологій і інтернет-платформ для здійснення комерційної діяльності
Цифрове підприємство	компанія, що використовує цифрові технології для оптимізації внутрішніх бізнес-процесів, взаємодії з клієнтами та створення нових бізнес-моделей
Цифрове планування ресурсів (ERP)	інтегровані програмні системи для управління ресурсами підприємства, які автоматизують процеси фінансів, обліку, управління персоналом та іншими аспектами бізнесу
Цифрове посвідчення особи	технологія, яка дозволяє верифікувати особистість користувача за допомогою цифрових документів, таких як електронний підпис або біометричні дані, для безпечної взаємодії в Інтернеті
Цифрове право	система норм та принципів, що регулюють взаємодію фізичних і юридичних осіб в цифровому середовищі. Це включає питання безпеки даних, конфіденційності, електронної комерції та авторського права
Цифрове регулювання	нормативно-правова діяльність, спрямована на визначення правил, стандартів і вимог до функціонування цифрових технологій і платформ у межах економіки та суспільства
Цифрове робоче середовище	середовище, в якому здійснюється виконання трудових завдань за допомогою цифрових технологій, включаючи онлайн-співпрацю, використання хмарних сервісів та відеоконференцій
Цифрове управління ланцюгами постачання (Digital Supply Chain Management)	впровадження цифрових інструментів для моніторингу, управління і оптимізації ланцюгів постачання, що дозволяє знижувати витрати, покращувати ефективність і прискорювати процеси
Цифровий аудит-трейл управлінських рішень	сукупність зафіксованих у системах електронного документообігу та корпоративних платформах записів про ініціювання, погодження, зміни, обґрунтування та затвердження управлінських рішень, що забезпечує можливість відстеження управлінського циклу та створює доказову базу для оцінювання прозорості, підзвітності й наявності інклюзивних процедур (залучення, оцінка впливу, врахування потреб різних груп)

Поняття	Зміст
Цифровий банкінг	надання банківських послуг через цифрові канали, зокрема Інтернет-банкінг та мобільні додатки для здійснення фінансових операцій, переведення коштів, погашення кредитів тощо
Цифровий інвестиційний профіль підприємства	поняття, що включає аналітику Big Data і Data Mining, сентимент – аналіз та аналіз соціальних мереж, мережевий аналіз, блокчейн – аналітику, імітаційне моделювання та використання цифрових двійників
Цифровий слід	інформація, що залишається після кожної дії людини в Інтернеті або в цифровому середовищі, включаючи перегляди сайтів, покупки в Інтернеті, коментарі та пости в соціальних мережах
Цифрові активи	активи, що існують лише в цифровому вигляді, включаючи криптовалюти, токени, цифрові права, інтелектуальну власність, а також інші цифрові об’єкти, що мають економічну цінність
Цифрові взаємодії	взаємодія між користувачами, компаніями та технологіями в цифровому середовищі, що включає в себе онлайн-обговорення, покупки, комунікацію через соціальні мережі тощо
Цифрові дані інвестиційного консалтингу	багатовимірний доказовий масив, що доповнює фінансову звітність та управлінську інформацію. Їхня цінність полягає не лише у масштабі (volume), а й у різноманітності (variety), швидкості оновлення (velocity) та достовірності (veracity), що безпосередньо впливає на якість інвестиційних висновків (4V)
Цифрові двійники	віртуальні копії реальних об’єктів, систем або процесів, що використовуються для моделювання і аналізу в реальному часі. Наприклад, цифровий двійник виробничої лінії дозволяє прогнозувати та оптимізувати її роботу
Цифрові інвестиції	інвестиційні стратегії, засновані на цифрових активах, таких як криптовалюти, токени, а також інвестиції в стартапи та інші цифрові ініціативи, що використовують новітні технології для залучення фінансування
Цифрові інновації	використання нових цифрових технологій для створення нових або значно покращених продуктів, послуг, бізнес-моделей та процесів, що допомагають організаціям досягти конкурентних переваг

Поняття	Зміст
Цифрові інструменти управління фінансовою безпекою	програмні та інформаційні системи (ERP, BI, фінансові аналітичні платформи), що забезпечують автоматизацію аналізу, контролю та прогнозування фінансових процесів
Цифрові інфраструктури	технологічні платформи та системи, що забезпечують підтримку цифрових бізнес-процесів, зберігання даних, передачу інформації та комунікацію
Цифрові мікроплатежі	маленькі грошові транзакції, які здійснюються через Інтернет або мобільні платформи для купівлі невеликих товарів і послуг, часто безпосередньо через мобільні додатки або платіжні сервіси
Цифрові підписи	метод верифікації цифрових документів, що використовуються для підтвердження автентичності інформації, здійснення транзакцій, підписання угод тощо, і замінюють традиційні ручні підписи
Цифрові платіжні системи	інфраструктура для обробки електронних платежів, яка дозволяє перевести гроші за допомогою Інтернету або мобільних додатків, таких як PayPal, Apple Pay, Google Pay
Цифрові платформи	онлайн-сервіси або веб-сайти, які сприяють взаємодії між користувачами, постачальниками товарів і послуг, та іншими суб'єктами економіки для здійснення бізнесу, комунікацій чи обміну інформацією
Цифрові платформи для бізнесу	спеціалізовані онлайн-майданчики, які допомагають підприємствам організовувати, автоматизувати та інтегрувати різні аспекти бізнес-процесів, від продажу і маркетингу до управління запасами і взаємодії з постачання і взаємодії з постачальниками
Цифрові платформи для спільної економіки	онлайн-платформи, які дозволяють користувачам обмінюватися товарами, послугами або знаннями, часто в режимі peer-to-peer, без посередників
Цифрові права	юридичні права, пов'язані з використанням цифрових технологій, таких як авторські права на цифровий контент, право на конфіденційність даних, захист персональних даних і цифрові підписи
Цифрові розрахункові системи	системи, що дозволяють здійснювати фінансові операції між суб'єктами господарювання або споживачами за допомогою цифрових інструментів, таких як онлайн-банкінг, мобільні платіжні системи, криптовалюти

Поняття	Зміст
Цифрові стартапи	компанії, що використовують інноваційні цифрові технології для вирішення конкретних проблем або створення нових бізнес-моделей з мінімальними ресурсами і великим потенціалом для масштабування
Цифрові технології	сукупність інструментів та методів, що використовуються для створення, зберігання, обробки і передачі цифрової інформації, включаючи програмне забезпечення, апаратні засоби, інтернет-платформи та інші технічні рішення
Цифрові технології інклюзивного аудиту	цифрові інструменти, що забезпечують збір, перевірку, аналіз і візуалізацію аудиторської інформації для оцінювання інклюзивних наслідків управлінських рішень, процесів і результатів, а також моніторинг виконання рекомендацій
Цифрові товарні потоки	переміщення цифрових товарів (програмне забезпечення, контент, криптовалюта) через Інтернет, що має велике значення для електронної комерції та міжнародної торгівлі
Цифрові торгові платформи	платформи для онлайн-торгівлі, які забезпечують покупцям і продавцям зручні інтерфейси для здійснення транзакцій, включаючи ринки електронної комерції, біржі цифрових товарів та послуг
Цифрові трансформації	процес інтеграції цифрових технологій у всі аспекти діяльності підприємства чи організації, що призводить до змін в бізнес-процесах, продуктах і способах взаємодії з клієнтами
Цифрові трансформації в уряді	впровадження цифрових технологій у державні органи для покращення функціонування урядових інститутів, підвищення прозорості і доступності публічних послуг
Цифрові фінанси	сфера фінансових послуг, що використовують цифрові технології для управління грошовими потоками, інвестиціями, здійснення платежів, кредитування та страхування
Цифровізація аудиту	процес інтеграції цифрових технологій у методологію та практику аудиту з метою підвищення ефективності, точності та аналітичної глибини перевірок
Цілісність	це властивість даних зберігати правильність і повноту та не бути несанкціоновано зміненими, компонент CIA

Поняття	Зміст
Цілісність даних	властивість даних бути точними та незмінними без належної авторизації; підтримується контролями доступу й хешами
Шахрайство	навмисні дії однієї або декількох осіб серед управлінського персоналу та найманих працівників або третьої сторони, при якій застосовується обман для отримання нечесної або незаконної переваги
Шифрування	перетворення даних у нечитабельний вигляд для захисту під час зберігання та передачі
Штучний інтелект (AI)	галузь комп'ютерних наук, що займається розробкою алгоритмів і систем, здатних виконувати завдання, які зазвичай вимагають людського інтелекту, такі як навчання, розпізнавання образів, ухвалення рішень
Якість даних	ступінь придатності даних для аудиту: точність, повнота, актуальність, узгодженість та унікальність
ABAC (Attribute Based Access Control)	це модель контролю доступу, за якої рішення про надання доступу приймається на основі атрибутів користувача, ресурсу та контексту запиту
ACL (Audit Command Language)	спеціалізоване програмне забезпечення для поглибленого аналізу транзакцій, автоматизації аудиторських процедур і безперервного аудиту
API (Application Programming Interface)	набір інструментів і протоколів для створення програмного забезпечення, що дозволяє різним системам взаємодіяти між собою
APT (Advanced Persistent Threat)	це тривала прихована кібератака, у якій зловмисник підтримує стійку присутність у середовищі з метою контролю або викрадення даних
Attack surface	це сукупність усіх точок входу та каналів взаємодії, через які можливе порушення безпеки системи
Backup	це практика створення та зберігання копій даних або конфігурацій для відновлення після втрати, пошкодження або недоступності
BEC (Business Email Compromise)	це шахрайство через компрометацію ділової пошти, коли зловмисник підміняє або захоплює листування, щоб ініціювати несанкціоновані платежі чи отримати дані

Поняття	Зміст
BI-дашборд інклюзивності	інструмент бізнес-аналітики для інтеграції, візуалізації та моніторингу системи індикаторів інклюзивності управлінських рішень, процесів і результатів, що забезпечує можливість зіставлення показників у динаміці, в розрізі структурних підрозділів і комунікативних каналів, а також підтримує управлінську інтерпретацію відхилень від цільових значень і контроль виконання коригувальних заходів
BPMN (Business Process Model and Notation)	стандартизована нотація для моделювання бізнес-процесів, яка дозволяє наочно відобразити послідовність дій, подій, рішень і ролей учасників процесу
CaseWare	програмний комплекс для планування, документування та стандартизованого оформлення результатів аудиторської перевірки
CIA triad (Confidentiality Integrity Availability)	це базова модель інформаційної безпеки, що визначає три цілі захисту конфіденційність цілісність і доступність
Credential stuffing	це автоматизовані спроби входу з використанням баз викрадених логінів і паролів, які експлуатують повторне використання паролів у різних сервісах
DAC (Discretionary Access Control)	це модель доступу, за якої власник ресурсу або уповноважена особа надає чи відкликає дозволи конкретним користувачам
DDoS (Distributed Denial of Service)	це розподілена атака на відмову в обслуговуванні, коли сервіс перевантажується трафіком із багатьох джерел, наприклад ботнетів
DLP (Data Loss Prevention)	це поєднання технологій і політик, що запобігають несанкціонованому винесенню або витоку інформації
DoS (Denial of Service)	це атака, що порушує доступність сервісу шляхом виснаження ресурсів або блокування легітимного доступу
DR (Disaster Recovery)	це процес і спроможність відновити IT-сервіси та дані після інциденту або аварії
DRP (Disaster Recovery Plan)	це документований план, який визначає ролі, процедури та цільові параметри відновлення систем і сервісів після збою
EDR (Endpoint Detection and Response)	це засоби та практики виявлення, розслідування й реагування на загрози на кінцевих пристроях

Поняття	Зміст
EPC (Event-driven Process Chain)	методологія моделювання процесів, у якій діяльність описується через логічний зв’язок подій і функцій
GDPR (General Data Protection Regulation)	це регламент ЄС, який встановлює вимоги до обробки та захисту персональних даних, включно з безпековими заходами та повідомленням про витоки
IDEA (CaseWare IDEA)	аналітична платформа для суцільного аналізу облікових даних, виявлення викривлень і формування відтворюваних аудиторських доказів
IDEF0	методологія функціонального моделювання, що використовується для опису діяльності організації через систему функцій, їхніх входів, виходів, керуючих впливів і ресурсів
IDS (Intrusion Detection System)	це система, що відстежує події та трафік для виявлення підозрілої активності або відомих шаблонів атак
IPS (Intrusion Prevention System)	це система, що виявляє зловмисну активність і активно блокує або пом’якшує атаку в режимі inline
ITDR (Identity Threat Detection and Response)	це підхід до виявлення та реагування на загрози, спрямовані на облікові записи, автентифікацію та зловживання доступом
JIT (Just In Time access)	це практика, за якої підвищені привілеї надаються лише за потреби і на обмежений час
Least Privilege	це принцип безпеки, за яким користувачі або процеси повинні мати лише мінімально необхідні права для виконання задач
MAC (Mandatory Access Control)	це централізована модель доступу, що ґрунтується на правилах класифікації та допуску і не може змінюватися користувачами
MFA (Multi Factor Authentication)	це автентифікація, яка вимагає два або більше незалежних факторів для підтвердження особи
PAM (Privileged Access Management)	це керування привілейованими доступами, яке забезпечує контроль, захист і аудит використання адміністративних облікових записів та їхніх секретів
RBAC (Role Based Access Control)	це рольова модель доступу, за якої дозволи прив’язуються до ролей, а користувачі отримують доступ через призначення ролей
RPO (Recovery Point Objective)	це допустимий обсяг втрати даних у часі, тобто наскільки «назад» можна відкотитися під час відновлення
RTO (Recovery Time Objective)	це цільовий час відновлення, тобто як швидко сервіс має повернутися до роботи після інциденту

Поняття	Зміст
SIEM (Security Information and Event Management)	це платформа, що збирає, корелює та аналізує події безпеки і журнали для виявлення інцидентів та підтримки реагування
SSO (Single Sign On)	це підхід, за якого користувач автентифікується один раз у центральній системі і отримує доступ до багатьох сервісів без повторного введення пароля
TeamMate	інтегрована платформа управління аудиторською діяльністю, що забезпечує планування, моніторинг та контроль виконання аудиторських завдань
TLS (Transport Layer Security)	це криптографічний протокол, що забезпечує конфіденційність і цілісність даних під час передавання мережею
UML (Unified Modeling Language)	стандартизована мова графічного моделювання, що використовується для опису структури та взаємодії елементів інформаційних систем і може застосовуватися як допоміжний інструмент у процесному аналізі
VPN (Virtual Private Network)	це технологія створення шифрованого каналу для передавання трафіку між користувачем або пристроєм і мережевим вузлом
WAF (Web Application Firewall)	це засіб захисту вебдодатків, який фільтрує та блокує шкідливий HTTP або HTTPS трафік
WORM (Write Once Read Many)	це режим або технологія зберігання, що не дозволяє змінювати або видаляти записані дані, забезпечуючи незмінюваність
Zero Trust	підхід, за якого жоден запит не вважається надійним за замовчуванням, а доступ надається лише за умови постійної верифікації та дотримання принципу мінімальних привілеїв.
ZTNA (Zero Trust Network Access)	це підхід доступу, який надає точкове підключення до конкретного сервісу після перевірки ідентичності, стану пристрою та контексту політик

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

Список використаних джерел

1. 25 років інклюзивного поступу: фінансово-економічний та управлінський виміри: кол. моногр. / Нестеренко С. С., Дубас Р. Г., Пшенична М. В. та ін. Київ: Університет «Україна», 2025. 212 с. ISBN 978-966-388-731-9, DOI: 10.36994/978-966-388-731-9-2025-212
2. Крамаренко А. В., Вишневська. М. К. Діджиталізація: теоретичні підходи, виклики та перспективи розвитку. Ефективна економіка. 2024. № 8. DOI: 10.32702/2307-2105.2024.8.49
3. Аналіз консалтингового ринку в Україні. URL: https://blog.youcontrol.market/analiz-konsaltinghovogho-rinku-v-ukrayini/
4. Андрусяк В. М., Хорошилова І. О., Смірнова Н. В. (2025). Вплив цифрових технологій на розвиток системи обліку і аудиту в Україні. Актуальні питання економічних наук. 2025. №7. DOI: 10.5281/zenodo.14697272
5. Анопа, А., Ілляшенко, С. (2025). Особливості ведення інноваційного бізнесу в умовах цифрової трансформації. Економіка та суспільство, (71). DOI: 10.32782/2524-0072/2025-71-85
6. Антоненко, В., Ляшок, Я., Попова, О., Катранжи, Л., & Ляшок, Н. (2024). Інвестиційна привабливість України в контексті її поствоєнного відновлення. Financial and Credit Activity Problems of Theory and Practice, 4(57), 363–380. DOI: 10.55643/fcaptp.4.57.2024.4410
7. Аудит в умовах сталого розвитку: колективна монографія / за заг. ред. проф. О. А. Петрик / О. А. Петрик, Н. В. Гойло, І. І. Матієнко-Зубенко, І. О. Мариніч, Ю. Б. Слободяник ін. Київ : КНЕУ, 2021. 231 с.
8. Бандура З. Л., Кіржнер Д. Д., Шевченко, Я. С. Інноваційні методи внутрішнього аудиту в міжнародних корпораціях. Наукові записки Львівського університету бізнесу та права. 2025. №47. С. 113-121.
9. Бардаш С. В., Грабчук І. Л. Цифрові технології в сфері бухгалтерського обліку: основні можливості та ризики. Ефективна економіка. 2021. № 9. DOI: 10.32702/2307-2105-2021.9.18.

10. Безверхий К., Парасій-Вергуненко І., Гордополов В. Ризики в межах е-аудиту та напрямки їх мінімізації. Збірник наукових праць Державного податкового університету. 2025. № 1. С. 3–10. DOI: 10.32782/2617-5940.1.2025.1
11. Безділь Н., Данилюк М., Дмитришин М. Ідентифікація та мінімізація ризиків фінансового шахрайства під час прийняття управлінських рішень. Економіка та суспільство. 2024. № 64. DOI: 10.32782/2524-0072/2024-64-71
12. Бельдій А.М., Фабіянська В. Ю., Комп'ютерний аудит в Україні в контексті вимог європейського законодавства. Accounting and Finance, № 3 (85)' 2019. С. 129-137
13. Березівська М.Г. Переваги та недоліки використання Internet of things у бухгалтерському обліку. Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. 2024. № 1 (57). С. 3–11.
14. Бойко, Р. В., & Винницький, Т. І. (2025). Внутрішній контроль бізнес процесів у дистрибуційних компаніях: організаційний аспект. Актуальні питання економічних наук, (16). DOI: 10.5281/zenodo.17415189
15. Болдуєв М. В., Болдуєва О. В., Лищенко О. Г. Макроекономічні складові системи електронного документообігу в контексті інституційного забезпечення автоматизованого обліку бізнес-процесів в Україні. Економічний вісник Дніпровської політехніки. 2021. № 1. С. 147-157
16. Бречко, О., Шухманн, В. (2025). Економічна ефективність впровадження гнучких систем штучного інтелекту у цифровізацію великих даних на ринку криптовалют. Acta Academiae Beregsasiensis. Economics, (11), 44-57.
17. Буяк, Л., Пришляк, К., & Семененко, Ю. (2025). Роль моделювання бізнес-процесів в управління ризиками. Modeling the development of the economic systems, (3), 137–143. DOI: 10.31891/mdes/2025-17-19
18. Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи. Вісник економіки. 2021. Вип. 1. С. 97-110

19. Василюк М.М., Вітер С.А., Здирко Н.Г., Гайдучок Д.С. (2025) Аудит фінансової звітності у світлі міжнародних стандартів та принципів сталого розвитку. Сталий Розвиток Економіки. № 4 (55), 2025, С. 5-13, DOI: 10.32782/2308-1988/2025-55-1

Ghosh, S. Financial inclusion and banking stability: Does interest rate repression matter? Finance Research Letters, 2022. Vol. 50. DOI: 10.1016/j.frl.2022.103205.

20. Васиньова Н. С. Автоматизація документообігу як один зі складників процесу діджиталізації публічного управління в Україні. Публічне управління та митне адміністрування. 2020. № 4. С. 39-43

21. Восколович В. ШІ у фінансах: ChatGPT допомагає інвесторам обирати акції. URL: https://mind.ua/news/20295023-shi-u-finansah-chatgpt-dopomagae-investoram-obirati-akciyi

22. Гаврилюк І. О. Розробка та моделювання інформаційної системи для автоматизації фінансового аудиту та оптимізації бізнес-процесів комерційних підприємств : робота на здобуття кваліфікаційного ступеня магістра : спец. 121 - інженерія програмного забезпечення / наук. кер. В. М. Бревус. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2024. 68 с.

23. Гавриш О. А., Омельчук В. І. Глобальні тренди цифровізації в аудиторській діяльності. Економічний вісник Донбасу. 2024. № 3. С. 198-202

24. Гевлич Л. Л. Професія бухгалтера у цифровій економіці. Економіка і організація управління. 2021. № 3 (43). С. 138–146. DOI: 10.31558/23072318.2021.3.13.

25. Герасименко О. М. Порівняльний аналіз методів та програмних методик ідентифікації, аналізу та оцінки ризиків у забезпеченні економічної безпеки підприємства. Економічний вісник Запорізької державної інженерної академії. 2018. Вип. 6. С. 109-113

26. Глобальні Стандарти Внутрішнього Аудиту. Інститут внутрішніх аудиторів, 2024. 129 с.
27. Гнатьєва Т., Яковенко А., Златова М. Особливості використання штучного інтелекту для потреб бухгалтерського обліку та управління підприємством. Економічний вісник Причорномор'я. 2024. № 5. DOI: 10.37000/ebbsl.2024.05.01
28. Голячук Н.В. Переваги та недоліки застосування хмарних технологій в обліку. Екон. науки. Серія: Облік і фінанси. 2015. Вип.12(1). С.80-86
29. Гончар Л. В., Малахова А.В., Невкипіла О.С. Фінансове шахрайство та безпека. Інформаційні технології та економічна безпека. 2021. Вип. 3-4. С. 170–174. DOI: 10.37332/2309-1533.2021.3-4.24
30. Господарський кодекс України. URL: https://zakon.rada.gov.ua/laws/show/436-15
31. Грибіненко О. Діджиталізація економіки в новій парадигмі цифрової трансформації. Міжнародні відносини. Серія «Економічні науки». 2018. № 16. С. 35-37.
32. Грицай О. І., Папіш В. І. Розвиток інформаційних технологій в Україні та їх інтегрування у сфері бухгалтерського обліку. Економіка та суспільство. 2024. Випуск 61. DOI: 10.32782/2524-0072/2024-61-88
33. Гудзь О. Є., Захаржевська А. А. Управління ризиками підприємств в умовах цифровізації: навчальний посібник. Кропивницький: Видавець Лисенко В. Ф., 2023.176 с.
34. Гулей А. І., Язлюк Б. О. та Гулей С. А., 2018. Формування нової цифрової ери на межіреального та віртуального соціально-економічного простору взаємодії. Український журнал прикладної економіки, 3 (2), с. 17-26.
35. Дерев'янко А. Кількість CEO, які вважають вигідними інвестиції в Україну зросла майже вдвічі з 2022 року. Європейська Бізнес-Асоціація. 22.12.2023 URL: https://eba.com.ua/kilkist-seoyaki-vvazhayut-vygidnymy-investytsiyi-v-ukrayinuzrosla-majzhe-vdvichi-z-2022-roku/

36. Державна стратегія цифрової трансформації: Розпорядження КМУ від 17.03.2021 № 232-р. URL: https://thedigital.gov.ua
37. Десятко А., Гамалій В., Ширшов Р. Інформаційні технології та системи для організації внутрішнього аудиту підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. № 1(29). С. 867–876.
38. Десятнюк О. М., Пташенко О. В. Цифрова трансформація фінансового ринку як фактор зміцнення фінансової інклюзивності та розширення доступу до фінансування. Європейський науковий журнал Економічних та Фінансових інновацій, 2025. 4(18), 795-802. URL: https://journal.eae.com.ua/index.php/journal/article/view/688
39. Диба М.І., Гернего Ю.О. DESG в процесі прийняття інвестиційних рішень. Фінанси України. 2024. №3. С.42-58. DOI: 10.33763/finukr2024.03.042
40. Долбнєва Д. В. та Сподарик Т. І. Стан та перспективи використання комп'ютерних технологій в обліково-аналітичній роботі вітчизняних підприємств. Облік і фінанси, 3 (89), 2020. с. 22-29. DOI: 10.33146/2307-9878-2020-3(89)-22-29
41. Дутчак І. Б., Козак О. Р., Ченаш, В. С. Розвиток аудиторських процедур у цифровій економіці. Актуальні питання економічних наук. 2025. №18. DOI: 10.5281/zenodo.18094348
42. Житкевич О. В., Азарова А. О. Аналіз існуючих програмних засобів щодо оцінювання рівня конкурентоспроможності українських підприємств. Молодий вчений. 2015. № 5(1). С. 145-148
43. Журавчак А., Піскозуб А. Аналіз методів машинного навчання для автоматизації тестування на проникнення. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2025. № 3(27). С. 54–62.
44. Захаркін О. О. та ін. Цифрові технології та інструменти забезпечення фінансової безпеки бізнесу. Проблеми сучасних трансформацій. Серія: економіка та управління. 2023. №10. С. 8-17.

45. Захарченко В. І., Меркулов М. М., Балахонова О. В. Економіка підприємства. Теорія : навчальний посібник. Міністерство освіти і науки України, Одеський національний політехнічний університет імені І. Мечникова, Одеський національний політехнічний університет, Вінницький торговельно-економічний інститут КНТЕУ. Львів : Видавництво «Магнолія 2006», 2021. 322 с
46. Заяць О. І., Верна Г. С. Аналіз надходження прямих іноземних інвестицій в Україну: детермінанти та бар'єри 2024 року. Бізнес Інформ. 2024. № 3. С. 87–95. URL: https://www.google.com/search?q=DOI: 10.32983/2222-4459-2024-3-87-95
47. Здирко Н. Г., Мулик Т. О., Мулик Я. І.. Використання штучного інтелекту в аудиторській діяльності: переваги і виклики. Економіка, фінанси, менеджмент: актуальні питання науки і практики. 2024. №3. С. 39–53. DOI: 10.37128/2411-4413-2024-3-3
48. Івахненков С. В. Застосування штучного інтелекту в аудиті. Наукові записки НаУКМА. Економічні науки. 2023. №8(1). С. 4–60. DOI: 10.18523/2519-4739.2023.8.1.54-60
49. Індекс цифрової трансформації регіонів України підсумки 2024 року. URL: https://storage.thedigital.gov.ua/files/a/5a/7be6e4e930076257945a29847c6035a9.pdf
50. Інструменти штучного інтелекту для системного аналізу / О. Г. Трофименко та ін. Вісник Херсонського національного технічного університету. 2024. № 4(91). С. 349–357.
51. Іонін Є. Обліково-аналітичне забезпечення бізнес-процесів в умовах цифрової економіки. Економічний аналіз. 2023. Том 33, № 1. С. 172–191. DOI: 10.35774/econa2023.01.172.
52. Ісайкіна О. Д. Особливості правового забезпечення та практичного втілення електронного документообігу в Україні. Соціум. Документ. Комунікація. 2016. Вип. 1. С. 235-246.

53. Кізима Т. Кізима А. Ідентифікація причин та потенційних наслідків фінансового шахрайства. Вісник економіки. 2019. №. 2. С. 47–56. DOI: 10.35774/visnyk2019.02.047
54. Кізима Т., Хамига Ю. Фінансове шахрайство: теоретична концептуалізація та економічне підґрунтя. Світ фінансів. 2019. Вип. 2. С. 109-123.
55. Клименко К.В. Діджиталізація як інноваційний розвиток підприємств: досвід України. Вісник Хмельницького національного університету. 2020. Т. 3, № 4, С. 13-18. DOI: 10.31891/2307
56. Клочко Т. А. Фінансова безпека як умова фінансової стійкості підприємства. Економіка та суспільство, 2021. Випуск 23. DOI: 10.32782/2524-0072/2021-23-17
57. Коваль О. В., Лишак О. М. Цифровізація бухгалтерського обліку в Україні. Ефективна економіка. 2024. No 2. DOI: http://doi.org/10.32702/23072105.2024.2.67
58. Козуб В., Бобень І., Боярінова Ю. Етичні аспекти використання штучного інтелекту в аналізі даних. Наука і техніка сьогодні. 2024. № 6(34). DOI: 10.52058/2786-6025-2024-6(34)-880-893
59. Коломієць П. Погляди науковців стосовно комплаєнсу як елементу податкової безпеки України. Право і суспільство. 2020. №2. С. 258-263
60. Кондратюк О. М., Руденко О. В., Чернобровкіна А. Є. Можливості та перспективи використання штучного інтелекту в аудиті. Ефективна економіка. 2021. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=8520
61. Кононенко Л. В., Назарова Г. Б., Савченко В. М. Організація обліку та аудиту у контексті використання новітніх цифрових технологій: сучасний стан, проблеми та перспективи. Проблеми сучасних трансформацій. Серія: економіка та управління. 2025. № 18. DOI: 10.54929/2786-5738-2025-18-09-03

62. Концепція розвитку цифрових компетентностей. Розпорядження Кабміну від 3 березня 2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

63. Концепція розвитку цифрової економіки та суспільства в Україні на 2018−2020 роки : Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

64. Коробка С. В. Діджиталізація підприємницької діяльності. Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Економічна. 2021. №100. С. 88-96. URL: http://nbuv.gov.ua/UJRN/VKhE_2021_100_11

65. Король С. Я., Клочко А. О. Цифрові технології в обліку й аудиті. Держава та регіони. Серія: Економіка та підприємництво. 2020. №1(112). С. 170-176.

66. Кравчук І., Лавриненко С., Зелінська А. Діджиталізація бізнеспроцесів: інноваційна складова менеджменту підприємств. Економіка та суспільство. 2023. №58. DOI: 10.32782/2524-0072/2023-58-19

67. Крижановський Є. М., Ящолт А. Р., Жуков С. О., Козачко О. М. Моделювання бізнес-процесів та управління IT-проектами : навчальний посібник. Вінниця : ВНТУ, 2018. 91 с.

68. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14

69. Крисоватий, А. І., Панасюк, В. М., & Мельничук, І. В. (2024). Бухгалтерський облік та оподаткування: підручник / за заг. ред. проф. АІ Крисоватого та проф. ВМ Панасюк. Тернопіль: ЗУНУ. В-во «Економічна думка.

70. Крисоватий, А.І., Панасюк, В.М., Мельничук, І.В. Основи обліку і оподаткування: підручник (е-видання). Тернопіль: ЗУНУ, 2023. 565 с.

71. Крюкова І. О., Рижикова Н. І., Бірченко Н. О., Головко О. В. Професійна етика бухгалтерів у контексті переходу Украї ни до міжнародних

стандартів обліку та фінансової звітності. Український журнал прикладної економіки та техніки. 2025. Том 10. № 3. С. 166 – 169.

72. Лапін А. В., Грінчук І. О., Оленюк Д.О. Діджиталізація економіки в Україні: сучасний стан та перспективи. Електронний журнал «Ефективна економіка». 2022. № 7. DOI: 10.32702/2307-2105.2022.7.22

73. Левицька С. О., Андрєєва А. О. Автоматизація господарського обліку як чинник прискорення процесу діяльності підприємств. Наукові записки [Національного університету «Острозька академія»]. Сер. : Економіка. 2011. Вип. 16. С. 608-614

74. Лепіш Н.Я., Грищук А.Б. Електронний документообіг: приватно-правові та публічно-правові аспекти. Електронне наукове видання «Аналітично-порівняльне правознавство». 2023. С. 353-357

75. Лобас А. О. Використання штучного інтелекту в аудиті: досвід великої четвірки. Міжнародний науковий журнал "Інтернаука" . 2025. № 2. С. 26-31

76. Лучко М. Р. Аудит та не аудиторські послуги: дилема та окремі питання застосування. Економічна експертиза: теорія, методологія та організація: монографія за заг. ред. д.е.н., проф. Михайла Лучка. Тернопіль: ЗУНУ, 2021. С. 257-275

77. Мельник Л. Ю., Аніщенко Г. Ю., Поліщук О. М. Вплив цифрових технологій на трансформацію методології обліку та аудиту управлінської діяльності. Актуальні питання економічних наук. 2025. №12. DOI: 10.5281/zenodo.15771767

78. Мельниченко О. В., Гартінгер Р. О. Роль технології блокчейн у розвитку бухгалтерського обліку та аудиту. European Cooperation. 2016. №7(14). С.9-19.

79. Мельниченко С. Г. Аналіз стратегічного менеджменту та його вплив на успішність організацій. Здобутки економіки: перспективи та інновації. 2024. № 3. URL: https://econp.com.ua/index.php/journal/article/view/19/16

80. Методика проведення оцінки ризиків інформаційної безпеки: Наказ ДССЗЗІ від 19.08.2020 № 105. URL: https://cip.gov.ua
81. Міжнародна інвестиційна діяльність. Підручник [електронне видання] За науковою редакцією д.е.н., професорів Зварича Р.Є. та Сохацької О.М. Тернопіль: ЗУНУ. 2025. 353 с. URL: https://dspace.wunu.edu.ua/handle/316497/55880
82. Міжнародні стандарти аудиту : підручник / А. І. Мілька, В. Я. Плаксієнко, О. В. Артюх-Пасюта, М. О. Любимов. Полтава : ПУЕТ, 2024. 438 с.
83. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг, видання 2021 року, частина І., 2025. 1260 с. URL: https://ifacweb.blob.core.windows.net/publicfiles/2025-06/Ukr_IAASB_HB_2021_Part_%D0%86%20ukr_Secure.pdf
84. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг, видання 2021 року, частина ІІ, 2025. 467 с. URL: https://ifacweb.blob.core.windows.net/publicfiles/2025-06/Ukr_IAASB_HB_2021_%20Part_%D0%86%D0%86%20ukr_Secure.pdf
85. Міжнародні стандарти обліку та звітності: підручник / А. І. Крисоватий, В. М. Панасюк, І. В. Мельничук, Т. Г. Бурденюк ; за заг. ред. А. І. Крисоватого, В. М. Панасюк. - Тернопіль : Економічна думка, 2021. 580 с.
86. Москаленко В. П. . Пластун О. Л. Комплексна оцінка фінансового стану підприємства як основа діагностики його банкрутства. Актуальні проблеми економіки. 2009. № 6. С. 180-192.
87. Найман Е.(2019) Абетка для інвестора: що таке робоедвайзер і чи можна довірити йому управління персональними статками та вкладеннями. URL: https://mind.ua/openmind/20199335-abetka-dlya-investora-shcho-take-roboedvajzer
88. Намлієва Н. В., Грищук Н. В. Діджиталізація – дієвий інструмент переорієнтації та збереження конкурентного статусу підприємства. Економіка. Фінанси. Право. 2025. № 6. С. 65-70

89. Нестеренко О. Форензик аудит як ефективний засіб протидії внутрішньо-корпоративному шахрайству в умовах війни. Acta academiae beregsasiensis. economics. 2024. № 5. С. 392–405. DOI: 10.58423/2786-6742/2024-5-392-405
90. Новіченко Л. С., Ковернінська Ю. В., Шиш А. М. Про впровадження цифрових технологій у бухгалтерському обліку та фінансовому аналізі. Економіка. Фінанси. Право. 2024. № 5. С. 53-58
91. Овчарик Р. Ю. Аудит на базі комп'ютерних програм: продуктивність, рентабельність та тенденції розвитку. Міжнародний науковий журнал "Інтернаука". Серія: Економічні науки. 2017. № 1. 68-72.
92. Олендій О., Назарова К., Нежива М., Мисюк В., Міщенко В., Русин-Гриник Р. Податковий аудит для забезпечення процвітання бізнесу: тенденції та перспективи. Financial and Credit Activity Problems of Theory and Practice. 2023. № 4(51). С. 80–90. DOI: 10.55643/fcaptp.4.51.2023.4069
93. Орлов І. Організація бухгалтерського обліку в умовах цифровізації економіки. Acta Academiae Beregsasiensis. Economics. 2022. №1. С. 264-273.
94. Орлов О. Цифрова етика та алгоритмічна прозорість: виклики та методи забезпечення справедливості автоматизованих рішень у державному управлінні. Аспекти публічного управління. 2025. № 13(2). С. 51-60. DOI: 10.15421/152520
95. Панасюк В. М. Цифровізація вітчизняного аудиту: тренди і перспективи. Інфраструктура ринку. 2021. Вип. 52. С. 190-194
96. Панасюк В. М., Ковальчук Є. К., Мельничук І. В., Мужевич Н. В. Бухгалтерський облік: від знань до компетентностей: навчальний посібник для дистанційного навчання. Тернопіль : 2020. 363 с.
97. Панасюк В., Кулик Р. Інтеграція штучного інтелекту у систему аудиту України: національні особливості та європейський вектор. Економічний аналіз. 2025. Том 35. № 3. С. 11-22. DOI: 10.35774/econa2025.03.011
98. Панасюк В., Монастирськии Г. Цифровізація економічних процесів як чинник розвитку регіонального бізнесу. Український журнал прикладної економіки та техніки. 2025. Том 10. № 2. С. 205-208

99. Панасюк, В. М., & Бєкєтов, О. В. (2025). Цифровізація системи обліку і страхування як чинник адаптації до волатильності цін на міжнародних ринках. Scientific notes of Lviv University of Business and Law, (46), 588-597.

100. Панасюк, В., Мельничук, І., & Мужевич, Н. (2022). Цифрова трансформація обліку в умовах форс-мажорних обставин. Галицький економічний вісник Тернопільського національного технічного університету, 78(5-6), 51-57.

101. Паращич, М.І., Ноджак, Л.С. Діджиталізація та її роль у діяльності українських підприємств. Менеджмент та підприємство в Україні: етапи становлення та проблеми розвитку. 2022. 2 (8), с.192-200.

102. Переверзєва А. В., Губарь О. В. Мікроекономічний аналіз поведінки споживачів із погляду теорії поколінь в умовах цифровізації. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Економіка і управління. 2021. Т. 32(71), № 4. С. 13-19

103. Податковий кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2755-17

104. Приймак Н. Адаптація обліку та аудиту до викликів цифрової економіки: вплив штучного інтелекту. Acta Academiae Beregsasiensis. Economics. 2025. № 10. С. 500–515.

105. Про аудит фінансової звітності та аудиторську діяльність: Закон України від 21.12.2017 № 2258-VIII. URL: https://zakon.rada.gov.ua/laws/show/2258-19

106. Про бухгалтерський облік і фінансову звітність: закон України від 16.07.1999 р. № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996-14#Text

107. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX: станом на 15 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text

108. Про внесення змін до деяких законів України щодо удосконалення правових засад провадження аудиторської діяльності в Україні:Закон України від 01.01.2023. Відомості Верховної Ради України (ВВР), 2023, № 27, ст.94. 2597-IX. URL: https://zakon.rada.gov.ua/laws/show/2597-20#n25

109. Про внесення змін до деяких законодавчих актів України щодо обліку трудової діяльності працівника в електронній формі: Закон України від 05.02.2021 р. № 1217-IX. URL. https://zakon.rada.gov.ua/laws/show/2352-20#Text.

110. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19

111. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15

112. Про затвердження методичних рекомендацій із застосування ризик-орієнтованого підходу: Розпорядження Державної аудиторсько ї служби України № 118 від 10.06.2021. URL: https://www.dkrs.gov.ua

113. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр

114. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

115. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI: станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

116. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

117. Про Національну економічну стратегію на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text

118. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр

119. Про організацію електронної взаємодії з клієнтами банків: Постанова НБУ № 89 від 15.07.2022. URL: https://bank.gov.ua/ua/legislation/Resolution_15072022_89

120. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII . URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

121. Про основні засади здійснення державного фінансового контролю в Україні: Закон України від 26.01.1993 № 2939-XII . URL: https://zakon.rada.gov.ua/laws/show/2939-12#Text

122. Про реалізацію експериментального проєкту із впровадження електронного документообігу в органах влади: Постанова КМУ № 606 від 03.06.2020. URL: https://zakon.rada.gov.ua/laws/show/606-2020-п

123. Про ринки капіталу та організовані товарні ринки: Закон України. Документ 3480-IV, чинний, поточна редакція від 01.01.2026, підстава - 3585-IX, 3981-IX, 4622-IX:URL: https://zakon.rada.gov.ua/laws/show/3480-15#Text

124. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text

125. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації: Постанова Кабінету Міністрів України від URL. https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text.

126. Про схвалення Стратегії цифрової трансформації соціальної сфери: Розпорядження Кабінету Міністрів від 28.10.2020 р. № 1363-р. URL. https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text.

127. Про товарні біржі: Закон України. Відомості Верховної Ради України (ВВР), 1992, № 10, ст.139) Документ 1956-XII, чинний, поточна редакція від 01.01.2026, підстава - 3585-IX URL: https://zakon.rada.gov.ua/laws/show/1956-12#Text

128. Про хмарні послуги: Закон України (законопроєкт №2655 від 20.12.2019, у процесі розгляду). URL: https://itd.rada.gov.ua/billInfo/Bills/Card/2655

129. Рада з міжнародних стандартів бухгалтерського обліку. The International Accounting Standards Board (IASB). URL: https://www.ifrs.org/about-us/who-we-are.

130. Радіонова Н. Й., Войтенко М. В. Методичні засади проведення аудиту основних засобів. Міжнародний науковий журнал "Інтернаука" . 2021. № 15. С. 37-41

131. Разумей Г.Ю., Разумей М.М. Діджиталізація публічного управління як складник цифрової трансформації України. Публічне управління та митне адміністрування. 2020. № 2 (25). С. 139–143.

132. Рєзнік О.М., Болгов Г.О. Фінансове шахрайство: сутність та заходи протидії. Юридичний науковий електронний журнал. 2023. № 11. С. 502–505. DOI: 10.32782/2524-0374/2023-11/122

133. Розіт Т. В., Мурадова К. З. Штучний інтелект в аудиті і бухгалтерському обліку. Ефективна економіка. 2024. № 4. URL: http://nbuv.gov.ua/UJRN/efek_2024_4_78

134. Рябчук О. Г., Ракуть Д .О. Аудит та штучний інтелект: як технології змінюють професію аудитора. Держава та регіони. Серія: Економіка та бізнес. 2025. № 1(135). DOI: 10.32782/1814-1161/2025-1-9

135. Саєнко О. Діджиталізація державного управління та інноваційні технології – найпотужніші інструменти подолання корупції. 2018. URL: https://www.kmu.gov.ua/news/oleksandr-sayenko-didzhitalizaciya-derzhavnogoupravlinnya-ta-innovacijni-tehnologiyi-najpotuzhnishi-instrumenti-podolannya-korupciyi

136. Семененко Ю. С. Оптимізація бізнес-процесів відділу маркетингу за допомогою інформаційних технологій. Бізнес Інформ. 2024. № 1. С. 95-103. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001498092

137. Скачков О., Скачкова І., Калініна О. Моделювання бізнес-процесів впровадження концепції TPM на підприємстві. Проблеми і перспективи розвитку підприємництва. 2021. № 26. С. 122. DOI: 10.30977/ppb.2226-8820.2021.26.122

138. Скіцько О., Складанний П., Ширшов Р., Гуменюк М., Ворохоб М. Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. № 2(22). С. 6–18. DOI: 10.28925/2663-4023.2023.22.618

139. Скрипник М. І., Григоревська О. О. Організація захисту облікової інформації в умовах забезпечення кібербезпеки. Наукові записки Національного університету "Острозька академія". Серія : Економіка. 2020. № 19. С. 95-102

140. Скрипник С., Сливка Я., Музиченко Т. Блокчейн-технології в бухгалтерії: нові підходи до забезпечення прозорості та надійності фінансової звітності. Економіка та суспільство. 2024. № 66. DOI: 10.32782/2524-0072/2024-66-34

141. Скуртол С. Д. Ризики автоматизації обліку. Вісник Київського інституту бізнесу та технологій. 2018. № 2. С. 106-107.

142. Слободяник Ю. Б., Діхтяренко Я. О. Застосування штучного інтелекту в обліку та аудиті: виклики та перспективи. Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки. 2025. № 4(2). С. 63-70

143. Словник Мерріам-Вебстер: веб-сайт. URL: https://www.merriam-webster.com/

144. Сніщенко Р. Г. Індикатори фінансової безпеки як компоненти моніторингу учасників фінансового ринку. Інвестиції: практика та досвід, 2018. № 3. С. 9-13

145. Сохацька О.М. Панасюк В.М., Вінницький С.І., Роговська-Іщук І.В. Фундаментальний та технічний аналізи міжнародних ринків. Підручник. Тернопіль: ЗУНУ. 2022. 307с. URL: http://dspace.wunu.edu.ua/handle/316497/46103

146. Співак С., Дідик І., Скурський Т., Житко О. Роль комп'ютерних програм для аналізу фінансово-господарського стану підприємства. Соціально-економічні проблеми і держава. 2021. Вип. 2. С. 702-707

147. Спіцина, Н. В., Угоднікова, О. І. Цифрові інструменти в аудиті консолідованої звітності: нові можливості для обліку та фінансового менеджменту. Актуальні питання економічних наук, 2025. (13). DOI: 10.5281/zenodo.16737170

148. Технології економічного аналізу. Частина 2. Технології управлінського аналізу: конспект лекцій: навч. посіб. для здобувачів ступеня бакалавр за освіт. програмою «Економічна аналітика» спеціальності 051 «Економіка» / КПІ ім. Ігоря Сікорського ; уклад.: М.М. Дученко, І.В. Шостак. Електрон. текст. дані (1 файл). Київ : КПІ ім. Ігоря Сікорського, 2025. 95 с.

149. Туль С.І. Трансформація світового ринку праці в умовах діджиталізації : автореф. дис. … канд. екон. наук : 08.00.02. Вінниця, 2019. 20 с.

150. Фадєєва, І. Г., Орлова, Н. В., & Макарова, В. В. (2023). Моделювання бізнес-процесів організації: сутність, складові та методологія впровадження в умовах формування глобальної економіки стійкого розвитку. Академічні візії, (17)

151. Фінансовий моніторинг : навч. посібник / укл. Е.О. Юрій, О.М. Грубляк. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2025. 368 с.

152. Харун О., Грицина Л. Вплив діджиталізації на розвиток інноваційних бізнес-моделей логістичної сфери. Вісник Хмельницького національного університету. 2022. Т. 1, № 6. С. 124-129.

153. Хомин П., Плига У., Срога А., Була О. Вплив інформаційних

технологій на обліково-аналітичну систему суб'єктів господарювання. Соціально-економічні проблеми і держава. 2021. № 2 (25). С. 491-499.

154. Цегельник Н. І., Бедер Д. А. Роль внутрішнього аудиту у забезпеченні прозорості інформаційних ресурсів для управління бізнесом в умовах цифровізації. Актуальні питання економічних наук. URL: https://a-economics.com.ua/index.php/home/article/view/278/295

155. Циганова Н. В., Суляєв В. В. Використання штучного інтелекту для оцінки ESG-ризиків та підтримки ухвалення рішень у сфері сталого фінансування. Міжнародний науковий журнал «Інтернаука». Серія: «Економічні науки». 2025. № 3. DOI: 10.25313/2520-2294-2025-3-10844

156. Цифрова економіка: підручник / А. І. Крисоватий, О. М. Десятнюк, О. В. Пташенко [та ін.]; за ред. А. І. Крисоватого, О. М. Десятнюк, О. В. Пташенко. Тернопіль: ЗУНУ, 2024. 520 с.

157. Цифрові технології в системі забезпечення транспарентності корпоративних фінансів / Л. Захаркіна та ін. Herald of Khmelnytskyi National University. Economic sciences. 2023. Т. 320, № 4. С. 298–304. DOI: 10.31891/2307-5740-2023-320-4-44

158. Чернікова Н. М. Аналіз програмних рішень з автоматизації бізнес-процесів підприємств. Підприємництво та інновації. 2021. Вип. 18. С. 57-62

159. Черняк І. О. Аналіз алгоритмів та математичних моделей для автоматизації електронного документообігу. Технічна інженерія. 2023. № 1. С. 178-183

160. Шевцова А. В. Вплив цифрових технологій на конкурентоспроможність країн: порівняльний аналіз країн розвинених економік та країн, економіки яких розвиваються. Міжнародний науковий журнал "Інтернаука". Серія : Економічні науки. 2025. № 5(1). С. 149-156

161. Шестерняк М. М. Контроль і аудит в системі управління. Сталий розвиток економіки, Вип. № 4 (55), 2025. С. 188-196.

162. Що таке діджиталізація – пояснює експерт. Українське радіо. 2019.

URL: http://www.nrcu.gov.ua/news. html?newsID=91042

163. Яковенко А. О., Гнатьєва Т. М., Мельничук В. М. Світові тенденції інтеграції штучного інтелекту в бухгалтерському обліку. Аграрні інновації. 2024. № 23. С. 221–227.

164. Abdul Hamid N.H.A., Masrom M., Mohamed N., et al. Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations. Computers & Security. 2022. DOI: 10.1016/j.cose.2022.102893

165. Accounting Information Systems Security Issues Sheila Shanker September 26, 2017 URL: https://bizfluent.com/ list-6396287-accounting-information-systems-security-issues.html

166. Adamyk O., Chereshnyuk O. Adamyk B., Rylieiev S. Trustworthy AI: a fuzzy-multiple method for evaluating ethical principles in AI regulations. 13th International Conference on Advanced Computer Information Technologies (ACIT). 2023. P. 608-613 DOI: 10.1109/ACIT58437.2023.10275505

167. Alodat A.Y., Salleh Z., Hashim H.A., et al. Board characteristics and cybersecurity disclosures. Review of Quantitative Finance and Accounting. 2024. DOI: 10.1007/s10660-024-09867-w.

168. Beaman C., Emm D., Harding B., et al. Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security. 2021. DOI: 10.1016/j.cose.2021.102490.

169. Boggini M., et al. Reporting cybersecurity to stakeholders: analysis of the EU cybersecurity regulation framework. Computer Law & Security Review. 2024. DOI: 10.1016/j.clsr.2024.105987.

170. Boubaker S, Nguyen DK, Piljak V. Big data analytics and investment. Technol Forecast Soc Change. 2023. URL: https://www.sciencedirect.com/science/article/abs/pii/S0040162523003980

171. Boyer M.M. Cyber insurance: demand, supply, and regulatory issues (editorial introduction). The Geneva Papers on Risk and Insurance – Issues and Practice. 2020. DOI: 10.1057/s41288-020-00188-1.

172. Chaudhari T. Artificial intelligence, its types and application in various fields. International Journal of Commerce and Management Research. 2024. Vol. 10. Issue 6. P. 49–51.

173. Cicala F., Bertino E. Analysis of encryption key generation in modern crypto-ransomware. IEEE Transactions on Dependable and Secure Computing. 2020. DOI: 10.1109/TDSC.2020.3005976.

174. Constantinescu C., Seshadri S. Sentinel: ransomware detection in file storage. Proceedings of the 14th ACM International Conference on Web Search and Data Mining (WSDM). 2021. DOI: 10.1145/3456727.3463834.

175. Deborah Beard, H. Joseph Wen. Reducing the Threat Levels for Accounting Information Systems. Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal. 2017 URL: http://archives.cpajournal. com/2007/507/essentials/p34.htm

176. Desyatnyuk O., Chereshnyuk O., Sachenko S., Liakhovych H. and Brukhanskyi R., Internal Audit of the Sales System: A Fuzzy-Multiple Approach, 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, 2025, pp. 1-6, DOI: 10.1109/IDAACS68557.2025.11322186.

177. Desyatnyuk, O., Krysovatyy, A., Ptashchenko, O., & Kyrylenko, O. (2025). Innovative Approaches to Transformation of Business Processes in Digital Economy: Ensuring Financial Security and Inclusion. Salud, Ciencia Y Tecnología - Serie De Conferencias, 4, 1498. DOI: 10.56294/sctconf20251498, URL: https://conferencias.ageditor.ar/index.php/sctconf/article/view/1498

178. Desyatnyuk, O., Krysovatyy, A., Ptashchenko, O., Kyrylenko, O. (2024). Enhancing financial inclusivity and accessibility of financial services through digital technologies. AD ALTA: Journal of Interdisciplinary Research. pp. 65-69. ISSN 1804-7890 URL: https://www.magnanimitas.cz/ADALTA/140142/papers/A_13.pdf

179. Desyatnyuk, O., Krysovatyy, A., Ptashchenko, O., Kyrylenko, O. (2024). Financial Security in the Conditions of Globalization: Strategies and Mechanisms for the Protection of National Interests. Econ. Aff., 69(Special Issue): 261-268, URL: https://ndpublisher.in/admin/issues/EAv69n1z1.pdf

180. Desyatnyuk, O., Ptashchenko, O., Murenets, I., Oliinyk, K., Kyrylenko, O. (2025). Ensuring Financial Security: Approaches to Risk Management and Protection in the Digital Economy. Data and Metadata, 4, 674. DOI: 10.56294/dm2025674, URL: https://dm.ageditor.ar/index.php/dm/article/view/674

181. Dovbush A.V., Belova I.M. Розвиток бухгалтерського обліку в умовах цифровізації економіки. Інформаційні технології та економічна безпека. 2023. №2(23). С. 176-184.

182. E-Government Development Index. URL: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

183. Eling M., Jung K. Heterogeneity in the severity of cyber losses. Journal of Banking Regulation. 2022. DOI: 10.1057/s41283-022-00095-w.

184. Eling M., McShane M., Nguyen T. Cyber risk management: history and future research directions. Risk Management and Insurance Review. 2021. DOI: 10.1111/rmir.12169.

185. E-Participation Index. E-Government. URL: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

186. European Commission. A European strategy for data. URL: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

187. Fedorov, M., Berko, A., Matseliukh, Y., Schuchmann, V., Budz, I., Garbich-Moshora, O., & Mamchyn, M. (2021). Decision Support System for Formation and Implementing Orders Based on Cross Programming and Cloud Computing. In MoMLeT+ DS (pp. 714-748).

188. Gallego-Losada, M.-J., Montero-Navarro, A., García-Abajo, E., Gallego-Losada, R. Digital financial inclusion. Visualizing the academic literature. Research in International Business and Finance, 2023. Vol. 64. DOI: 10.1016/j.ribaf.2022.101862

189. Gao L., et al. Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems. 2020. DOI: 10.1016/j.accinf.2020.100468.

190. Giboney J.S., Schuetzler R.M., Grimes G.M. Know Your Enemy: Conversational agents for security, education, training, and awareness at scale. Computers & Security. 2023. DOI: 10.1016/j.cose.2023.103207.

191. Gupta J., Cornelissen V., Ros-Tonen M. Inclusive development. Encyclopedia of Global Environmental Governance and Politics. Cheltenham, 2015. P. 35–44.

192. Handbook of the International Code of Ethics for Professional Accountants (including International Independence Standards), 2023 Edition. 402 p.

193. He L., et al. A survey on Zero Trust Architecture. Security and Communication Networks. 2022. DOI: 10.1155/2022/6476274.

194. Hirna O. Assessment of the flexibility of business processes of transport enterprises in the logistics services market under martial law. Economic scope. 2025. No. 198. P. 23–30. DOI: 10.30838/ep.198.23-30

195. Hossain M., et al. Effects of auditor-level cybersecurity breaches on audit quality and audit fees. European Accounting Review. 2024. DOI: 10.1080/09638180.2024.2435389.

196. Huang Y., Murthy U. Cyber risk management strategy disclosure and firm value: evidence from corporate filings. International Journal of Accounting Information Systems. 2024. DOI: 10.1016/j.accinf.2024.100696.

197. Kelton A.S., Yang S. Auditor-contagion effects of cybersecurity incidents. International Journal of Accounting Information Systems. 2024. DOI: 10.1016/j.accinf.2024.100714.

198. Keshvarinia M, MacKenzie CA, Zhao Z. (ScienceDirect landing page). (2026). URL: https://www.sciencedirect.com/science/article/pii/S277266222500102X

199. Koblianska I. Review of scientific literature on BPM concept in social enterprises. Problems and Perspectives in Management. 2023; 21(3). doi:10.21511/ppm.21(3).2023.07

200. Kovalev A. A. International economic security in the modern era of the clash of civilizations: problem of conceptualization. Theoretical and Applied Economics. 2020. № 2. P. 61–74. DOI: 10.25136/2409-8647.2020.2.29842. URL: https://en.nbpublish.com/library_read_article.php?id=29842.

201. Lallie H.S., et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security. 2021. DOI: 10.1016/j.cose.2021.102248.

202. Latysheva O., Antonova V. Features of realization of audit of business processes of cost-accounting and their management. Economic Herald of the Donbas. 2019. No. 1 (55). P. 109–117. DOI: 10.12958/1817-3772-2019-1(55)-109-117

203. Mashkov O., Ivashchenko T., Tupkalo V. Methodological aspects of environmental audit of enterprise management system. Ecological Sciences. 2020. Vol. 33, no. 6. P. 68-78. DOI: 10.32846/2306-9716/2020.eco.6-33.10

204. Masoud N. Cyberattacks and the cost of information processing. Research in International Economics. 2022. DOI: 10.1016/j.rie.2022.07.001.

205. McKinsey & Company. What is digital transformation? 2024. URL: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation

206. Meland P.H., Bayoumy Y.F.F., Sindre G. The Ransomware-as-a-Service economy within the darknet. Computers & Security. 2020. DOI: 10.1016/j.cose.2020.101762.

207. Mensah J. Sustainable development: Meaning, history, principles, pillars, and implications for human action. Literature Review. 2019. URL:

https://www.tandfonline.com/doi/pdf/10.1080/23311886.2019.1653531?needAccess=true

208. Mikalef P, Krogstie J. Big data analytics and firm performance: a review and agenda (journal domain overview). URL: https://gscm.nida.ac.th/wp-content/uploads/2025/10/Jv1nO-1-s2.0-S014829631930061X-main.pdf

209. Modeling organizational activities to create an organization's security policy using business processes / V. V. Radush et al. Informatics and mathematical methods in simulation. 2021. Vol. 11, no. 3. P. 239–246. DOI: 10.15276/imms.v11.no3.239

210. Mollenkamp D. T. Economic security. 2022. August 31. URL: https://www.investopedia.com/economic-security-5213404

211. Mostova A. Digital transformation of business in Ukraine. 2024. URL: https://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/467/12557/26247-1?inline=1

212. Mukhopadhyay A., Jain A. A framework for cyber-risk insurance against ransomware attacks. International Journal of Information Management. 2024. DOI: 10.1016/j.ijinfomgt.2023.102724

213. National Institute of Standards and Technology (NIST). Prioritizing Cybersecurity Risk for Enterprise Risk Management (NISTIR 8286B). 2020. DOI: 10.6028/NIST.IR.8286B.

214. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). 2020. DOI: 10.6028/NIST.SP.800-53r5.

215. National Institute of Standards and Technology (NIST). Zero Trust Architecture (SP 800-207). 2020. DOI: 10.6028/NIST.SP.800-207. DOI: 10.6028/NIST.SP.800-207

216. OECD. Digital transformation (policy issue page). URL: https://www.oecd.org/en/topics/policy-issues/digital-transformation.html

217. OECD. OECD Benchmark Definition of Foreign Direct Investment (4th ed.). (2026). URL: https://www.oecd.org/investment/fdibenchmarkdefinition.htm

218. Ogbanufe O., Baham C. Multi-factor authentication (MFA): adoption and user perspectives on security/usability. Information Systems Frontiers. 2023. DOI: 10.1007/s10796-022-10278-1.

219. Palsson K., Gudmundsson S., Shetty S. Analysis of the impact of cyber events for cyber insurance. The Geneva Papers on Risk and Insurance – Issues and Practice. 2020. DOI: 10.1057/s41288-020-00171-w.

220. Panasyuk, V. (2025). Accounting and audit of consolidated financial statements in the conditions of digital transformation: key principles and advantages. European Science, 5(sge42-05), 202-218. DOI: 10.30890/2709-2313.2025-42-05-045

221. Panasyuk, V. (2025). Cloud technologies and blockchain in auditing: a new stage in the development of control systems. Finanse i Prawo Finansowe, 1 (Sp. Issue), 25-38.

222. Panasyuk, V., & Muzhevych, N. (2024). Osoblyvosti vplyvu tsyfrovizatsii bukhhalterskoho obliku na biznes-protsesy pidpryiemstv [Features of the impact of digitalization of accounting on the business processes of enterprises]. Galician Economic Journal, 89(4), 42-48. TNTU. [in Ukrainian].

223. Radush V. V. Improving the resistance of modern block ciphers using high-quality s-boxes. Informatics and mathematical methods in simulation. 2025. Vol. 15, no. 4. P. 614-624. DOI: 10.15276/imms.v15.no4.614

224. Reijers HA, et al. Business Process Management: The evolution of a discipline. Inf Syst. 2021. URL: https://www.sciencedirect.com/science/article/pii/S0166361521000117

225. Saarikko T, Westergren UH, Blomquist T. Digital transformation: Five recommendations for the digitally conscious firm. Bus Horiz. 2020;63(6):825–839. DOI:10.1016/j.bushor.2020.07.005

226. Schuchmann, V. (2026). Інституційні бар'єри та їхній вплив на впровадження адаптивного ШІ у фінансових технологіях. Європейський науковий журнал Економічних та Фінансових інновацій, 1(19), 124-135. Retrieved із https://journal.eae.com.ua/index.php/journal/article/view/698

227. Skrynkovskyy R., Hladun V., Kramar M. Information technologies in the organization of accounting at the enterprise. Path of science. 2019. Vol. 5, no. 2. P. 3001-3010.

228. Smaili N., et al. Corporate governance. board effectiveness and cybersecurity disclosure. Management and Governance. 2023. DOI: 10.1007/s10997-022-09637-6. DOI: 10.1007/s10997-022-09637-6

229. Syed R., et al. A comprehensive survey of Zero Trust Architecture. IEEE Access. 2022. DOI: 10.1109/ACCESS.2022.3174679.

230. Telukdarie A., Mungar A. The impact of digital financial technology on accelerating financial inclusion in developing economies. Procedia Computer Science. 2023. Vol. 217. P. 670–678. DOI: 10.1016/j.procs.2022.12.263

231. Thathsarani U. S., Jianguo W. Do digital finance and the technology acceptance model strengthen financial inclusion and SME performance? Information. 2022. Vol. 13. P. 390. DOI: 10.3390/info13080390.

232. UNCTAD. Digital Economy Report 2021: Cross-border data flows and development. 2021. URL: https://unctad.org/system/files/official-document/der2021_en.pdf

233. Verhoef PC, Broekhuizen T, Bart Y, et al. Digital transformation: A multidisciplinary reflection and research agenda. J Bus Res. 2021. doi:10.1016/j.jbusres.2019.09.022

234. Wassie F. A., Lakatos L. P. Artificial intelligence and the future of the internal audit function. Humanities and Social Sciences Communications. 2024. pp. 3–11. DOI: 10.1057/s41599-024-02905-w

235. West S, et al. (2026). URL: https://www.mdpi.com/2076-3417/11/9/3750

236. Wheatley S., Hofmann A., Sornette D. Addressing cyber insurance: an analysis of data breach risks. The Geneva Papers on Risk and Insurance. Issues and Practice. 2021. DOI: 10.1057/s41288-020-00163-w.

237. World Bank. World Development Indicators (data portal). (2026). URL: https://databank.worldbank.org/source/world-development-indicators

238. Yazıcılar Sola FG, Güzel D. (2026) URL: https://www.mdpi.com/2071-1050/17/11/5171

Західноукраїнський національний університет

Факультет фінансів та обліку

Цифрові технології в аудиті

Підручник

Підписано е-видання 14.02.2026 р.
Умов. друк. арк. 59,8. Облік.-вид. арк. 58,7

Видавець та виготовлювач
Західноукраїнський національний університет
вул. Львівська, 11, м. Тернопіль 46004

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців ДК № 7284 від 18.03.2021р.