Тема 1. Теоретико-методичні засади цифровізації аудиторської діяльності

1. Сутність, завдання та напрями цифрової трансформації аудиту.
2. Міжнародні стандарти аудиту в умовах використання цифрових технологій.
3. Цифрове аудиторське середовище та інформаційні джерела аудиту.
4. IT-ризики, ризик-орієнтований підхід і професійне судження аудитора.
5. Організація аудиту в умовах автоматизованого обліку та електронного документообігу.

1. Сутність, завдання та напрями цифрової трансформації аудиту

Розвиток інформаційних технологій, поширення електронного документообігу, інтегрованих систем управління підприємством та автоматизованої обробки фінансових даних істотно змінюють умови здійснення аудиторської діяльності. Якщо традиційний аудит значною мірою ґрунтувався на дослідженні паперових первинних документів, облікових регістрів і фінансової звітності, то сучасне аудиторське середовище передбачає роботу з електронними документами, цифровими журналами операцій, базами даних та результатами автоматизованих контрольних процедур.

Цифровізація аудиту є складовою загальної цифрової трансформації економіки. Вона охоплює не тільки впровадження програмних засобів у роботу аудитора, а й зміну методів отримання, обробки, перевірки, узагальнення та документування аудиторської інформації.

Важливо розмежовувати поняття *автоматизації* та *цифрової трансформації* аудиту.

Автоматизація аудиту передбачає використання технічних і програмних засобів для виконання окремих аудиторських процедур, які раніше здійснювалися вручну. Наприклад, автоматизований розрахунок вибірки, перевірка арифметичної точності реєстру, зіставлення сум у різних інформаційних масивах.

Цифровізація аудиту характеризується систематичним використанням цифрових технологій для виконання аудиторських завдань, формування доказової бази та підтримки професійного судження аудитора.

Цифрова трансформація аудиту є ширшим процесом, що передбачає перебудову організації аудиторської діяльності, інформаційних потоків, методичних підходів і взаємодії між аудитором, клієнтом та іншими учасниками аудиторського процесу на основі цифрових технологій.

Отже, автоматизація є одним з інструментів цифровізації, тоді як цифрова трансформація передбачає комплексну зміну способів організації та виконання аудиторської роботи.

Передумови цифровізації аудиторської діяльності

Основними передумовами цифровізації аудиту є:

1. Зростання обсягів фінансово-господарської інформації. Підприємства здійснюють значну кількість операцій, інформація про які накопичується в електронних облікових системах. Ручне опрацювання всіх даних потребує значних трудових витрат і збільшує ймовірність технічних помилок.

2. Поширення інтегрованих інформаційних систем. ERP-системи об'єднують бухгалтерський облік, управління запасами, продажами, закупівлями, розрахунками, виробництвом та іншими бізнес-процесами. Відповідно, аудитор має оцінювати не лише правильність окремих записів, а й логіку формування даних у межах інтегрованої системи.

3. Розвиток електронного документообігу. Первинні документи, договори, рахунки, акти та інші підтвердження операцій можуть створюватися, підписуватися, передаватися й зберігатися в електронній формі. Це змінює процедури перевірки їхньої автентичності, цілісності та зв'язку з відповідними господарськими операціями.

4. Ускладнення господарських процесів. Електронна комерція, дистанційні розрахунки, автоматизоване управління запасами, цифрові платіжні інструменти та транскордонні операції створюють нові об'єкти й ризики аудиторського дослідження.

5. Підвищення вимог до своєчасності інформації. Керівництво підприємств, власники, інвестори та інші користувачі потребують достовірної інформації для прийняття управлінських рішень. Це стимулює розвиток аналітичних процедур і можливостей оперативного виявлення відхилень.

6. Посилення вимог до інформаційної безпеки. Несанкціоновані зміни даних, компрометація облікових записів, втрата інформації або порушення роботи систем можуть впливати на достовірність фінансової звітності та надійність аудиторських доказів.

Основні напрями цифровізації аудиту

Цифровізація аудиторської діяльності охоплює кілька взаємопов'язаних напрямів (табл. 1).

Таблиця 1 – Напрями цифровізації аудиту

Напрям	Зміст застосування	Приклад
Автоматизація аудиторської документації	Планування, формування та зберігання робочих документів	Створення електронного файлу аудиту
Аналітика даних	Опрацювання великих масивів облікових операцій	Виявлення повторних платежів
Автоматизовані контрольні процедури	Перевірка заданих правил і критеріїв	Пошук проводок із нетиповими параметрами
Візуалізація інформації	Графічне подання результатів перевірки	Панель індикаторів аудиторського ризику
Штучний інтелект	Допомога в класифікації, пошуку закономірностей та опрацюванні текстів	Визначення договорів із незвичайними умовами
Дистанційна взаємодія	Обмін документами та координація роботи аудиторської групи	Захищений електронний обмін інформацією
Безперервний моніторинг	Повторне або постійне виконання визначених контрольних процедур	Регулярне виявлення нетипових операцій

Використання кожного напряму має бути обґрунтоване характером аудиторського завдання, доступністю даних, рівнем ризику та можливістю перевірити отримані результати.

При цьому цифрові інструменти не усувають потреби в професійному судженні. Наприклад, автоматизований алгоритм може визначити операції, що відрізняються від типових, але сам факт такого відхилення ще не доводить наявності помилки, шахрайства або порушення законодавства.

Вплив цифровізації на якість та ефективність аудиту

Використання цифрових систем може забезпечувати:

- скорочення часу на виконання повторюваних процедур;
- підвищення повноти охоплення інформаційних масивів;
- оперативність виявлення нетипових операцій;
- відтворюваність результатів автоматизованих перевірок;
- покращення документування аудиторських процедур;
- можливість зосередити увагу на операціях із підвищеним ризиком.

Однак цифровізація породжує й нові обмеження. Результати перевірки залежать від повноти та якості вихідних даних, правильності налаштування

алгоритмів, надійності інформаційної системи та компетентності особи, яка використовує програмний інструмент.

Наприклад, якщо аудитор отримав реєстр господарських операцій, з якого помилково виключено частину записів, навіть правильно налаштований алгоритм не виявить порушень у відсутніх даних. Отже, перевірка повноти та достовірності інформаційного масиву є необхідною передумовою використання аналітичних інструментів.

Цифрові технології підвищують потенційні можливості аудиту, але не гарантують достовірності його результатів автоматично.

2. Міжнародні стандарти аудиту в умовах використання цифрових технологій

Міжнародні стандарти аудиту визначають основні принципи, вимоги та процедури, яких має дотримуватися аудитор під час виконання завдань з аудиту фінансової звітності. Застосування цифрових технологій змінює інструменти виконання аудиторських процедур, але не скасовує необхідності досягнення цілей відповідних стандартів.

Цифровий інструмент не є самостійною гарантією якості аудиту. Його використання повинно забезпечувати належне виконання конкретної процедури, отримання достатніх і прийнятних аудиторських доказів та формування обґрунтованих висновків.

У цифровому середовищі особливого значення набувають стандарти, що регулюють оцінювання ризиків, отримання доказів, використання вибіркових методів, документування роботи та використання роботи експертів.

<u>Основні стандарти, пов'язані з цифровізацією аудиту:</u>

МСА 315 «Ідентифікація та оцінювання ризиків суттєвого викривлення».

Стандарт передбачає розуміння суб'єкта господарювання, його середовища, системи внутрішнього контролю та інформаційних процесів з метою ідентифікації й оцінювання ризиків суттєвого викривлення фінансової звітності.

У цифровому середовищі аудитор досліджує, зокрема:

- інформаційні системи, що використовуються для формування фінансової звітності;

- процеси ініціювання, реєстрації, обробки та відображення господарських операцій;
- автоматизовані й ручні контрольні процедури;
- ризики, пов'язані з правами доступу та змінами програмних налаштувань;
- залежність облікової інформації від зовнішніх інформаційних систем і сервісів.

МСА 330 «Дії аудитора у відповідь на оцінені ризики».

Після оцінювання ризиків аудитор визначає характер, час і обсяг подальших аудиторських процедур. Цифрові інструменти можуть застосовуватися для розширення охоплення операцій, відбору об'єктів перевірки та виконання процедур по суті.

Наприклад, якщо встановлено ризик подвійного відображення витрат, аудитор може перевірити записи за однаковими сумами, датами, номерами рахунків та ідентифікаторами контрагентів. Проте виявлені збіги потребують подальшого дослідження первинних документів і економічного змісту операцій.

МСА 500 «Аудиторські докази».

Стандарт визначає вимоги до отримання достатніх і прийнятних аудиторських доказів. У цифровому середовищі це означає необхідність оцінювати не лише зміст інформації, а й джерело її отримання, повноту, точність та надійність.

Якщо аудитор використовує електронний реєстр операцій, сформований клієнтом, потрібно встановити, чи відповідає він даним облікової системи, чи охоплює визначений період і чи не зазнав необґрунтованих змін.

МСА 530 «Аудиторська вибірка».

Використання програмних засобів дає змогу автоматизувати формування вибірок, здійснювати випадковий відбір, стратифікацію сукупності та аналіз результатів перевірки.

Водночас застосування програми не звільняє аудитора від необхідності визначити генеральну сукупність, мету тестування, параметри вибірки та спосіб оцінювання виявлених відхилень.

МСА 230 «Аудиторська документація».

Документування цифрових процедур має забезпечувати можливість зрозуміти, які дії виконав аудитор, які дані використав, які результати отримав і на яких підставах сформував висновки.

До робочих документів можуть включатися опис інформаційного масиву, критерії відбору операцій, параметри застосованих процедур, результати аналітичних тестів, пояснення суттєвих відхилень і посилання на підтвердні документи.

МСА 240 «Відповідальність аудитора щодо шахрайства під час аудиту фінансової звітності».

Цифрові інструменти можуть сприяти виявленню незвичайних операцій, повторних платежів, нетипових бухгалтерських проведень або операцій, здійснених у незвичний час.

Однак автоматизоване виявлення аномалії не є доказом шахрайства. Аудитор має дослідити обставини, перевірити підтвердні документи, оцінити пояснення відповідальних осіб та інші доступні докази.

МСА 220 (переглянутий) «Управління якістю аудиту фінансової звітності».

Застосування цифрових інструментів має відбуватися в межах системи управління якістю аудиторського завдання. Важливими є належна компетентність персоналу, керівництво роботою, перевірка виконаних процедур і відповідальність за якість отриманих результатів.

У разі використання спеціалізованих програм необхідно враховувати можливості інструмента, його обмеження та потребу в перевірці коректності отриманих результатів.

Загальний принцип застосування стандартів у цифровому середовищі

Цифровізація змінює передусім **спосіб виконання аудиторських процедур**, а не фундаментальну мету аудиту.

Наприклад, перевірка правильності відображення витрат може виконуватися шляхом ручного дослідження документів або автоматизованого зіставлення реєстрів. В обох випадках аудитор повинен отримати достатні й прийнятні докази, оцінити виявлені відхилення та задокументувати висновки.

Отже, вибір програмного засобу має визначатися метою процедури, властивостями досліджуваної інформації та оціненими ризиками, а не самим фактом доступності певної технології.

3. Цифрове аудиторське середовище та інформаційні джерела аудиту

Цифрове аудиторське середовище – це сукупність інформаційних систем, електронних даних, програмних засобів, цифрових документів, каналів обміну інформацією та процедур контролю, у межах яких аудитор отримує й перевіряє інформацію про діяльність суб'єкта господарювання.

До основних складових такого середовища належать:

1. Системи бухгалтерського та управлінського обліку.
2. ERP-системи й галузеві інформаційні платформи.
3. Електронний документообіг і системи електронного підпису.
4. Банківські, платіжні та інші зовнішні інформаційні системи.
5. Бази даних, електронні реєстри та сховища документів.
6. Засоби аналітики, візуалізації та автоматизації аудиторських процедур.
7. Системи інформаційної безпеки, управління доступом і журналювання подій.

Аудитор повинен розуміти, як формується інформація, яким чином вона передається між системами та які контрольні механізми забезпечують її повноту, точність і захищеність.

Основні категорії цифрових джерел аудиторської інформації

Внутрішні електронні джерела формуються безпосередньо в межах підприємства. До них належать бухгалтерські проведення, оборотно-сальдові відомості, реєстри продажів і закупівель, електронні накладні, дані про рух запасів, платіжні реєстри, договори та управлінські звіти.

Зовнішні електронні джерела формуються незалежно від підприємства або іншими учасниками господарських відносин. Це можуть бути банківські виписки, відповіді контрагентів, інформація з офіційних реєстрів, підтвердження третіх сторін та інші зовнішні відомості.

Технічні джерела відображають функціонування інформаційної системи. До них належать журнали системних подій, історія змін записів, журнали доступу користувачів, параметри налаштування системи та відомості про виконання автоматизованих процесів.

Аналітичні джерела формуються внаслідок опрацювання первинних даних за допомогою програмних засобів. Це результати перевірки дублікатів,

звіти про аномальні операції, візуалізації, статистичні показники та результати застосування аналітичних моделей.

Результат аналітичної обробки не слід автоматично ототожнювати з незалежним аудиторським доказом. Його надійність залежить від вихідних даних, правильності алгоритму та можливості підтвердити виявлені обставини іншими доказами.

Оцінювання якості цифрової інформації

Для використання електронних даних аудитор має оцінити кілька характеристик.

Повнота – чи охоплює інформаційний масив усі операції, що відповідають визначеним критеріям, за відповідний період.

Точність – чи правильно відображені суми, дати, ідентифікатори, рахунки та інші реквізити.

Актуальність – чи відповідає інформація періоду, який перевіряється, та чи враховано необхідні оновлення.

Цілісність – чи не було необґрунтованих змін даних під час їх створення, передавання, зберігання або експортування.

Походження та простежуваність – чи можна встановити джерело даних, час їх формування, відповідальну особу та зв'язок із відповідною господарською операцією.

Доречність і надійність – чи придатні дані для виконання конкретної аудиторської процедури та наскільки обґрунтовано можна покладатися на них.

Наприклад, аудитор отримав електронний реєстр закупівель підприємства за рік. Перед пошуком подвійних платежів необхідно з'ясувати, чи включено до реєстру всі закупівлі, чи відповідають суми бухгалтерським записам, чи охоплено необхідні періоди та чи не виключено частину операцій під час експортування.

Лише після перевірки придатності вихідної інформації результати автоматизованого аналізу можуть використовуватися як належна основа для подальших аудиторських процедур.

Простежуваність цифрової операції

Простежуваність означає можливість встановити зв'язок між господарською операцією, первинним документом, бухгалтерським записом, відображенням у фінансовій звітності та результатом аудиторської перевірки.

Наприклад, для перевірки придбання матеріалів аудитор може простежити такий інформаційний ланцюг:

договір → замовлення на закупівлю → накладна або акт приймання → запис у системі обліку → розрахунок із постачальником → відображення запасів і кредиторської заборгованості у звітності.

Якщо певна ланка відсутня або її неможливо підтвердити, аудитор має з'ясувати причини та оцінити вплив на достовірність відповідних показників.

Цифрові системи можуть полегшувати таке простежування за допомогою унікальних ідентифікаторів, посилань між документами та журналів операцій. Проте наявність технічного зв'язку між записами не доводить сама по собі економічної обґрунтованості операції.

4. IT-ризики, ризик-орієнтований підхід і професійне судження аудитора

IT-ризики в аудиті – це ризики, пов'язані з використанням інформаційних систем, технологій обробки даних і цифрової інфраструктури, які можуть впливати на формування фінансової звітності, надійність інформації або виконання аудиторських процедур.

Основні групи IT-ризиків:

1. Ризики доступу. Виникають унаслідок неналежного розподілу прав користувачів, використання спільних облікових записів або надання надмірних повноважень.

2. Ризики змін програм і даних. Пов'язані з неконтрольованим коригуванням налаштувань системи, довідників, алгоритмів розрахунку чи бухгалтерських записів.

3. Ризики обробки інформації. Виникають через помилки алгоритмів, некоректні параметри автоматизованих операцій або порушення логіки обробки даних.

4. Ризики інтеграції систем. Пов'язані з неповним або помилковим передаванням інформації між обліковими модулями, платіжними сервісами, складськими системами та іншими платформами.

5. Ризики втрати або пошкодження даних. Виникають через технічні збої, неналежне резервне копіювання, кібератаки чи інші події.

6. Ризики недостатньої надійності цифрових доказів. Пов'язані з неможливістю встановити походження інформації, перевірити її повноту або підтвердити незмінність.

7. Ризики використання аналітичних алгоритмів. Виникають унаслідок помилок у правилах аналізу, некоректного визначення критеріїв відбору або хибної інтерпретації отриманих результатів.

Не кожний ІТ-ризик автоматично означає ризик суттєвого викривлення фінансової звітності. Аудитор повинен оцінити, яким чином відповідна технологічна проблема може впливати на конкретні показники, операції та твердження керівництва щодо фінансової звітності.

Зв'язок ІТ-ризиків із твердженнями фінансової звітності

Під час аудиту фінансової звітності перевіряються твердження керівництва щодо операцій, залишків рахунків і розкриття інформації.

Наприклад:

- **існування** – чи дійсно актив, відображений у системі, існує;
- **повнота** – чи всі операції, які мали бути відображені, включені до обліку;
- **точність** – чи правильно визначено суми й інші параметри;
- **відсічення** – чи відображено операції в належному звітному періоді;
- **права та зобов'язання** – чи належать підприємству відповідні активи та чи має воно відповідні зобов'язання;
- **класифікація та подання** – чи правильно класифіковано й представлено операції у звітності.

Наприклад, у системі обліку складських запасів доступ до коригування кількості матеріалів мають користувачі, які не здійснюють фактичного приймання або відпуску запасів. Це створює ризик необґрунтованих змін залишків.

Такий ризик може впливати на твердження щодо існування, повноти та точності запасів, а також на достовірність собівартості реалізації.

Аудитор має дослідити розподіл прав доступу, історію змін, первинні документи руху запасів і результати інвентаризації. За необхідності він розширює процедури перевірки відповідно до оціненого ризику.

Реалізація ризик-орієнтованого підходу в цифровому середовищі

Ризик-орієнтований підхід передбачає зосередження аудиторських ресурсів на тих ділянках, де ймовірність суттєвого викривлення та потенційні наслідки є найбільш значущими.

У цифровому середовищі цей підхід може реалізовуватися за такими етапами:

1. Визначення об'єктів аудиту та суттєвих показників фінансової звітності.
2. Дослідження інформаційних систем і бізнес-процесів, що формують відповідні показники.
3. Ідентифікація ризиків, включно з ризиками автоматизованої обробки даних.
4. Оцінювання ризиків суттєвого викривлення.
5. Визначення аудиторських процедур у відповідь на оцінені ризики.
6. Виконання автоматизованих і традиційних процедур.
7. Оцінювання виявлених відхилень та отриманих доказів.
8. Документування результатів і формування висновків.

Наприклад, якщо підприємство здійснює значну кількість платежів, аудитор може проаналізувати весь доступний реєстр платежів для виявлення повторів, незвичних сум, платежів у нетипові дати або операцій із контрагентами, що потребують додаткової уваги.

Після автоматизованого відбору аудитор перевіряє відібрані операції за первинними документами, банківськими виписками, договорами та іншими доказами. Таким чином, цифрова аналітика допомагає визначити напрями поглибленого дослідження, але не замінює оцінювання доказів.

Професійне судження аудитора

Професійне судження – це застосування аудитором відповідних знань, досвіду та професійних стандартів під час прийняття обґрунтованих рішень у конкретних обставинах аудиторського завдання.

У цифровому середовищі професійне судження необхідне для:

- визначення доцільності використання конкретного програмного інструмента;
- оцінювання придатності вихідних даних;
- вибору параметрів автоматизованих процедур;
- інтерпретації незвичайних результатів;
- визначення потреби в додаткових доказах;
- оцінювання суттєвості виявлених відхилень;
- формування обґрунтованих висновків.

Особливо важливим є критичне ставлення до результатів роботи штучного інтелекту. Згенеровані пояснення, класифікації або рекомендації можуть містити

неточності. Аудитор повинен перевіряти їхню відповідність фактичним даним і не перекладати відповідальність за професійні рішення на алгоритм.

Наприклад, система може позначити платіж як підозрілий через його незвично велику суму. Проте платіж може стосуватися законної закупівлі обладнання, передбаченої договором. Завдання аудитора – встановити економічний зміст операції, перевірити підтвердні документи та визначити, чи існує реальний ризик викривлення.

Отже, цифрова компетентність аудитора має поєднувати технічні навички з розумінням обліку, аудиторської методики, внутрішнього контролю та професійної етики.

5. Організація аудиту в умовах автоматизованого обліку та електронного документообігу

Планування аудиту в цифровому середовищі передбачає врахування інформаційної архітектури підприємства, джерел формування фінансових показників, доступності електронних документів і надійності інформаційних систем.

На етапі планування аудитор визначає:

1. Які інформаційні системи використовуються для ведення обліку та формування звітності.
2. Які бізнес-процеси автоматизовані.
3. Які дані потрібні для виконання аудиторських процедур.
4. Яким чином буде отримано та перевірено ці дані.
5. Які IT-ризики можуть впливати на достовірність інформації.
6. Які цифрові інструменти доцільно застосувати.
7. Які ресурси, компетентності та строки необхідні для виконання завдання.

План цифрового аудиту має передбачати не лише використання програмного забезпечення, а й процедури перевірки придатності отриманих даних, контролю доступу до них та належного зберігання робочих документів.

Використання ERP-систем у процесі аудиту

ERP-системи забезпечують інтегроване управління ресурсами підприємства та об'єднують інформацію про основні господарські процеси.

Для аудитора важливими є такі функціональні компоненти:

- фінанси та бухгалтерський облік;
- закупівлі й розрахунки з постачальниками;
- продажі й розрахунки з покупцями;
- складський облік і рух запасів;
- основні засоби;
- виробництво та калькулювання витрат;
- управління персоналом і нарахування заробітної плати, якщо відповідний функціонал використовується.

Інтеграція даних дозволяє простежувати зв'язок між господарською операцією та її відображенням у фінансовій звітності. Водночас аудитор має оцінювати правильність налаштувань, повноту даних, розмежування повноважень та контроль за змінами.

Наприклад, під час аудиту закупівель можна дослідити зв'язок між замовленням, фактичним отриманням товарів, документом постачальника, бухгалтерським записом і платежем. Відсутність належного узгодження між цими елементами може свідчити про недоліки контролю або потребу в додаткових процедурах.

Електронний документообіг і перевірка цифрових документів

Електронний документообіг дає змогу створювати, підписувати, передавати та зберігати документи без обов'язкового використання паперових носіїв.

Під час аудиту електронних документів важливо оцінювати:

- наявність необхідних реквізитів;
- можливість ідентифікувати автора або підписувача;
- чинність і перевірюваність електронного підпису, якщо він застосовується;
- цілісність документа;
- дату створення, підписання та передавання;
- зв'язок документа з відповідною господарською операцією;
- відповідність вимогам законодавства, що застосовуються до конкретного виду документа.

Необхідно розрізняти автентичність електронного документа та економічну обґрунтованість операції. Навіть належно підписаний документ не доводить автоматично фактичного постачання товарів, реального виконання робіт або правильності визначення вартості.

Для підтвердження господарської операції аудитор може зіставляти електронні документи з інформацією про фактичне отримання активів, даними складського обліку, платіжними документами, зовнішніми підтвердженнями та іншими доказами.

Контроль доступу та розмежування повноважень

У цифровому середовищі система внутрішнього контролю значною мірою залежить від організації прав користувачів.

Важливим є принцип розподілу несумісних функцій. Наприклад, особа, яка створює нового постачальника в інформаційній системі, не повинна без належного контролю одноосібно змінювати його платіжні реквізити та здійснювати оплату.

Аудитор може перевірити:

- перелік активних користувачів;
- відповідність прав доступу посадовим обов'язкам;
- наявність спільних облікових записів;
- повноваження адміністраторів;
- процедури надання та скасування доступу;
- журналювання критичних операцій;
- контроль за змінами довідників і налаштувань.

Виявлення надмірних прав доступу не завжди означає наявність викривлення звітності. Проте така обставина може свідчити про підвищення ризику несанкціонованих змін і потребу в додаткових аудиторських процедурах.

Документування цифрових аудиторських процедур

Результати застосування цифрових інструментів повинні бути належно задокументовані. Робочі документи мають містити інформацію, достатню для розуміння виконаних процедур, отриманих результатів та обґрунтування висновків аудитора.

Доцільно фіксувати:

1. Мету аудиторської процедури.
2. Джерело та період охоплення вихідних даних.
3. Спосіб отримання інформаційного масиву.
4. Критерії відбору й параметри перевірки.
5. Використаний програмний засіб.
6. Отримані результати та виявлені відхилення.
7. Додаткові процедури, виконані для перевірки відхилень.

8. Висновки аудитора та посилання на підтвердні докази.

Наприклад, якщо під час аналізу платежів виявлено повторні операції, до робочого документа потрібно включити критерії виявлення повторів, перелік відібраних операцій, результати перевірки підтвердних документів і висновок щодо характеру встановлених обставин.

Самого скриншота аналітичної панелі або переліку позначених програмою операцій може бути недостатньо, якщо з нього неможливо встановити джерело даних, логіку перевірки та підстави для висновків.

Захист інформації під час виконання аудиторських завдань

Під час роботи з цифровими даними аудитор повинен дотримуватися вимог конфіденційності, захисту інформації та умов доступу до даних клієнта.

Основними організаційними заходами є:

- використання авторизованих каналів передавання інформації;
- обмеження доступу до даних відповідно до робочих повноважень;
- захищене зберігання робочих документів;
- резервне копіювання та контроль цілісності інформації;
- дотримання правил зберігання й видалення даних;
- перевірка умов використання хмарних сервісів та інструментів штучного інтелекту;
- недопущення передавання конфіденційної інформації до непогоджених зовнішніх сервісів.

Якщо аудитор використовує зовнішню аналітичну платформу або інструмент штучного інтелекту, необхідно врахувати, які дані передаються сервісу, як вони зберігаються, хто може отримати до них доступ і чи відповідає таке використання вимогам договору та законодавства.

Таким чином, організація цифрового аудиту повинна забезпечувати одночасно ефективність процедур, надійність доказів і належний захист інформації.

Таким чином, цифровізація аудиторської діяльності є закономірним результатом розвитку інформаційних технологій та ускладнення інформаційного середовища підприємств. Вона змінює способи отримання, обробки й аналізу аудиторської інформації, розширює можливості автоматизованої перевірки та сприяє підвищенню ефективності аудиторських процедур.

Водночас використання цифрових систем не усуває фундаментальних вимог аудиту щодо достатності й прийнятності доказів, професійного

скептицизму, незалежності, належного документування та відповідальності аудитора.

Особливого значення набувають оцінювання надійності вихідних даних, розуміння інформаційних систем клієнта, ідентифікація ІТ-ризиків і перевірка результатів автоматизованих процедур.

Ефективний цифровий аудит передбачає інтеграцію трьох складових: *професійних знань з аудиту, розуміння бізнес-процесів та компетентності у використанні цифрових технологій*. Саме їх поєднання дає змогу перетворювати великі масиви електронних даних на належні аудиторські докази й обґрунтовані висновки.

Питання для самоконтролю

1. У чому полягають відмінності між автоматизацією, цифровізацією та цифровою трансформацією аудиту?
2. Які основні передумови зумовлюють цифрову трансформацію аудиторської діяльності?
3. Які переваги та обмеження має застосування цифрових технологій у процесі аудиту?
4. Які міжнародні стандарти аудиту мають особливе значення для використання цифрових інструментів?
5. Які категорії цифрових джерел аудиторської інформації можна виділити?
6. За якими характеристиками аудитор оцінює придатність електронних даних?
7. Які основні групи ІТ-ризиків можуть впливати на достовірність фінансової звітності?
8. Як ІТ-ризики пов'язані з твердженнями керівництва щодо фінансової звітності?
9. У чому полягає роль професійного судження під час використання аналітичних алгоритмів?
10. Які вимоги висуваються до документування цифрових аудиторських процедур?
11. Як ERP-системи впливають на організацію аудиту?
12. Яких заходів необхідно вживати для захисту цифрової аудиторської інформації?

Рекомендована література та нормативні джерела

1. Міжнародні стандарти аудиту та інші міжнародні стандарти, видані Радою з міжнародних стандартів аудиту та надання впевненості (IAASB).
2. Закон України «Про аудит фінансової звітності та аудиторську діяльність».
3. Закон України «Про бухгалтерський облік та фінансову звітність в Україні».
4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги».
5. Закон України «Про електронні документи та електронний документообіг».
6. Професійні матеріали IAASB та IFAC щодо використання технологій у проведенні аудиту, управління якістю та застосування професійного судження.