

УДК 657.6: 658. 87

Л. О. ГЕЛЕЙ,

к. е. н., старший викладач
кафедри обліку і фінансів,

Львівський інститут економіки і туризму

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ОПЕРАЦІЙНОГО АУДИТУ В СЕРЕДОВИЩІ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

***Анотація.** У статті досліджено можливості використання комп'ютерних інформаційних систем в системі операційного аудиту. Проаналізовано переваги та недоліки їх застосування. Встановлено основні процедури перевірки доказовості використовуваної інформації та її суттєвості для формування повноцінного аудиторського висновку.*

Ключові слова: автоматизовані інформаційні системи, інформаційна безпека, контроль, критичний елемент контролю.

***Аннотация.** В статье исследованы возможности использования компьютерных информационных систем в системе операционного аудита. Проанализированы преимущества и недостатки их применения. Установлены основные процедуры проверки доказуемости использованной информации и ее существенности для формирования полноценного аудиторского заключения.*

Ключевые слова: автоматизированные информационные системы, информационная безопасность, контроль, критический элемент контроля.

***Summary.** The article explored the possibility of using computer information systems in the system of operational audit. The advantages and disadvantages of their use have been analyzed. The basic procedures of verification of evidence of used information and its materiality of forming a full auditory opinion have been established.*

Keywords: computerized information systems, information security, control, critical component of control.

Постановка проблеми. Комп'ютеризація є однією з найважливіших стадій інноваційних технологій. Комп'ютеризацію пройшли найбільш розвинені країни Заходу, держави Східної Європи, включаючи Україну. Інтенсивний розвиток електронно-обчислювальної техніки і технологій дав значний вплив на ефективність операційного аудиту і вдосконалення його методів.

Аналіз останніх досліджень і публікацій. Вивченню ефективності комп'ютеризації аудиторських перевірок присвячені праці багатьох вітчизняних та зарубіжних учених і фахівців, зокрема таких як С. Івахненко, С. Суворова, Н. Парушіна, Є. Галкіна, Л. Терещенко, Б. Кудрицький, Г. Федорова та інші. Проте питання визначення теоретико-методичних підходів, які б застосовували аудитори під час

комп'ютеризації своєї роботи та формулювання основних вимог щодо автоматизації операційного аудиту на основі вітчизняних та міжнародних стандартів, все ще залишаються відкритими.

Метою статті є обґрунтування методичних підходів до комп'ютеризації такої важливої складової економічної роботи як операційний аудит та визначення його місця в сучасних інформаційних системах.

Виклад основного матеріалу дослідження. Протягом останніх років практично всі торговельні підприємства перейшли на використання сучасних автоматизованих інформаційних систем (АІС). Серед багатьох проблем, які супроводжують цей процес, однією з головних є забезпечення надійного операційного аудиту в умовах АІС і напрацювання методик його проведення під час періодичних внутрішніх ревізій та тематичних перевірок.

За організацію контролю у середовищі АІС завжди відповідає керівництво компанії, яке повинно забезпечити необхідні умови для придбання комп'ютерної техніки і відповідного програмного забезпечення, визначити вимоги і пріоритети контролю та аудиту в АІС, розподілити обов'язки щодо автоматизованого оброблення даних між різними відповідальними працівниками, налагодити нагляд за роботою обчислювального центру (відділу комп'ютерного оброблення) та здійснити цілу низку інших заходів, спрямованих на довгострокову перспективу.

На жаль, у вітчизняній економічній літературі з питань контролю протягом останніх років майже немає праць, присвячених організації та методиці проведення контролю та операційного аудиту в середовищі АІС. Щоправда, у 80-х – середині 90-х років ХХ ст. проблеми контролю і ревізії в умовах автоматизації обліку досліджували такі відомі вчені як М. Білуха, В. Завгородній, Р. Криницький, А. Савицький [5–8], але ці дослідження на сьогоднішній день дещо втратили актуальність через швидкі зміни у сфері новітніх інформаційних технологій.

Разом із тим, цікавий досвід проведення внутрішнього (операційного) аудиту у середовищі АІС існує у зарубіжних країнах, передусім США, Канаді, Великій Британії. На нашу думку, розробки зарубіжних професійних аудиторських організацій та установ можуть бути успішно адаптовані і використані у вітчизняній практиці операційного аудиту [2, с. 23–142].

Ми вважаємо можливим використовувати аналогічний підхід у діяльності служб внутрішнього аудиту вітчизняних торговельних компаній і пропонуємо власну систему оцінки надійності контролю у середовищі АІС за критичними елементами та їх групами. Критичні

елементи контролю інформаційних систем торговельної компанії можуть бути згруповані таким чином (рис. 1):

- 1) КЕ (№№ 1–6) – загальний контроль;
- 2) КД (№№ 1–4) – контроль доступу;
- 3) КП (№№ 1–3) – контроль прикладного програмного забезпечення;
- 4) КС (№№ 1–3) – контроль системного програмного забезпечення;
- 5) КР (№№ 1–3) – контроль розподілу обов’язків та повноважень;
- 6) КФ (№№ 1–4) – контроль безперервності функціонування.

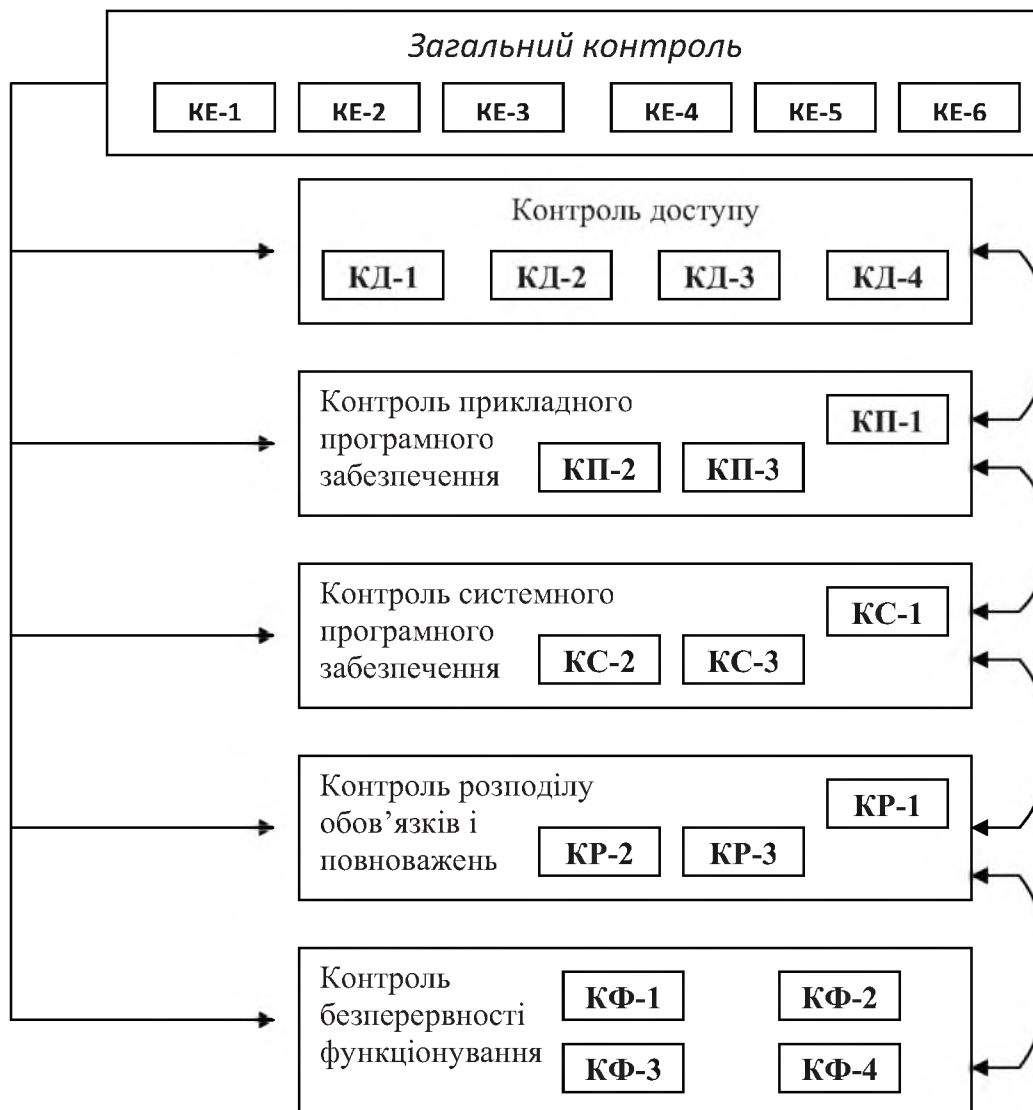


Рис. 1. Загальна схема групування і взаємозв’язку критичних елементів контролю АІС торговельної компанії
Джерело: побудовано автором

Критичні елементи стосуються факторів, які є істотними для декількох складових частин загальної структури внутрішнього контролю компанії, включаючи середовище контролю. Саме тому практичне

використання критичних елементів допомагає гарантувати ефективність і надійність системи внутрішнього контролю.

Оцінка програми інформаційної безпеки – це, фактично, оцінка заходів забезпечення існування і функціонування кожного з перерахованих нижче критичних елементів:

- КЕ-1 «Періодична оцінка ризику»;
- КЕ-2 «Планування і розробка програми інформаційної безпеки»;
- КЕ-3 «Визначення структури і підтримка управління інформаційною безпекою»;
- КЕ-4 «Визначення обов'язків по забезпеченню інформаційної безпеки»;
- КЕ-5 «Виконання обов'язків, пов'язаних з інформаційною безпекою, персоналом підприємства»;
- КЕ-6 «Нагляд і контроль за ефективністю програм інформаційної безпеки».

Наступна група критичних елементів належить до категорії «Контроль доступу».

Контроль доступу повинен забезпечити обґрунтовану впевненість у тому, що комп'ютерні ресурси (файли даних, прикладні програми і комп'ютерне обладнання) захищені від неправомірної модифікації, викрадення або втрати.

Критичними елементами контролю доступу, які підлягають оцінюванню, можуть бути:

- КД-1 «Класифікація інформаційних ресурсів за ознаками їхньої чутливості до змін і важливості»;
- КД-2 «Забезпечення актуального переліку уповноважених користувачів та їхніх повноважень щодо доступу до даних»;
- КД-3 «Запровадження засобів фізичного і логічного контролю для попередження або виявлення випадків несанкціонованого доступу»;
- КД-4 «Нагляд і контроль за доступом до інформаційних ресурсів, дослідження очевидних порушень правил забезпечення цілісності даних, здійснення відповідних коригуючих процедур».

Далі йдуть дві категорії, пов'язані з контрольною оцінкою програмного забезпечення: «Контроль прикладного програмного забезпечення» і «Контроль системного програмного забезпечення».

Оцінювання засобів контролю прикладного програмного забезпечення здійснюється у розрізі таких критичних елементів:

- КП-1 «Санкціонування режимів оброблення даних, придбання та модифікації програмного забезпечення, змін у форматах представлення даних»;
- КП-2 «Перевірка нового і модифікованого програмного забезпечення»;

- КП-3 «Періодичний контроль бібліотек прикладних програм».

Для того, щоб зменшити ризик втрати або неналежного використання даних в АІС, потрібен добре продуманий розподіл обов'язків і повноважень. Наприклад, функції написання програми, її тестування і схвалення для практичного використання повинні бути розподілені між різними особами. Часто розподіл обов'язків і повноважень здійснюють не між окремими особами, а між декількома групами працівників, але як у першому, так і у другому випадку мета залишається однаковою – зменшення ризику здійснення вчасно непомічених помилкових операцій або шахрайства.

В цілому до категорії «Контроль розподілу обов'язків і повноважень» пропонується включити такі критичні елементи:

- КР-1 «Розподіл несумісних обов'язків щодо обслуговування інформаційної системи між різними особами або підрозділами»;

- КР-2 «Визначення регламенту доступу для практичного розподілу обов'язків і повноважень»;

- КР-3 «Контроль діяльності і взаємодії персоналу шляхом диспетчерського управління і нагляду».

Втрата здатності обробляти, відновлювати і захищати інформацію в комп'ютерному середовищі суттєво впливає на нормальний режим роботи компанії. Тому потрібно використовувати всі можливості захисту інформаційних ресурсів і мінімізації незапланованих збоїв, для чого доцільно розробити план ліквідації непередбачених ситуацій (так звані плани відновлення), призначити відповідальних осіб і регулярно контролювати виконання всіх превентивних заходів.

Отже, контроль безперервності функціонування комп'ютерної системи є однією з найважливіших ділянок внутрішнього контролю компанії. Для оцінки надійності контролю у цій категорії доцільно виділити такі критичні елементи:

- КФ-1 «Оцінка чутливості комп'ютерних операцій до різноманітних негативних впливів»;

- КФ-2 «Вжиття заходів щодо запобігання і мінімізації ризику пошкодження технічного обладнання і переривання обробки даних»;

- КФ-3 «Розроблення схеми взаємодії компонентів автоматизованої системи і плану вирішення можливих неузгодженостей»;

- КФ-4 «Періодична перевірка наявності неузгодженостей та помилок, відповідне коригування і відновлення робочого стану системи».

Здійснення контролю за визначеними вище групами контрольних елементів дозволяє правильно спланувати операційну перевірку в умовах АІС і раціонально розподілити зусилля перевіряючих.

Перевагою запропонованої методики є також те, що вона може бути використана для будь-якого типу АІС. У разі проведення перевірок у середовищі різних АІС відмінності будуть стосуватися конкретних процедур контролю і дій аудитора, але не загальної схеми критичних елементів.

Розглянемо можливості використання сховищ даних у діяльності з виконання завдань операційного аудиту в АІС.

У технологічному плані СХД, організовані на найвищому рівні, беруть дані з різних систем (пакетів прикладних програм), «очищують» їх і зберігають таким чином, щоб забезпечити найлегший доступ до них з боку користувачів, які беруть зі сховища даних потрібну інформацію. Детальніше цей процес зображено на рис. 2.

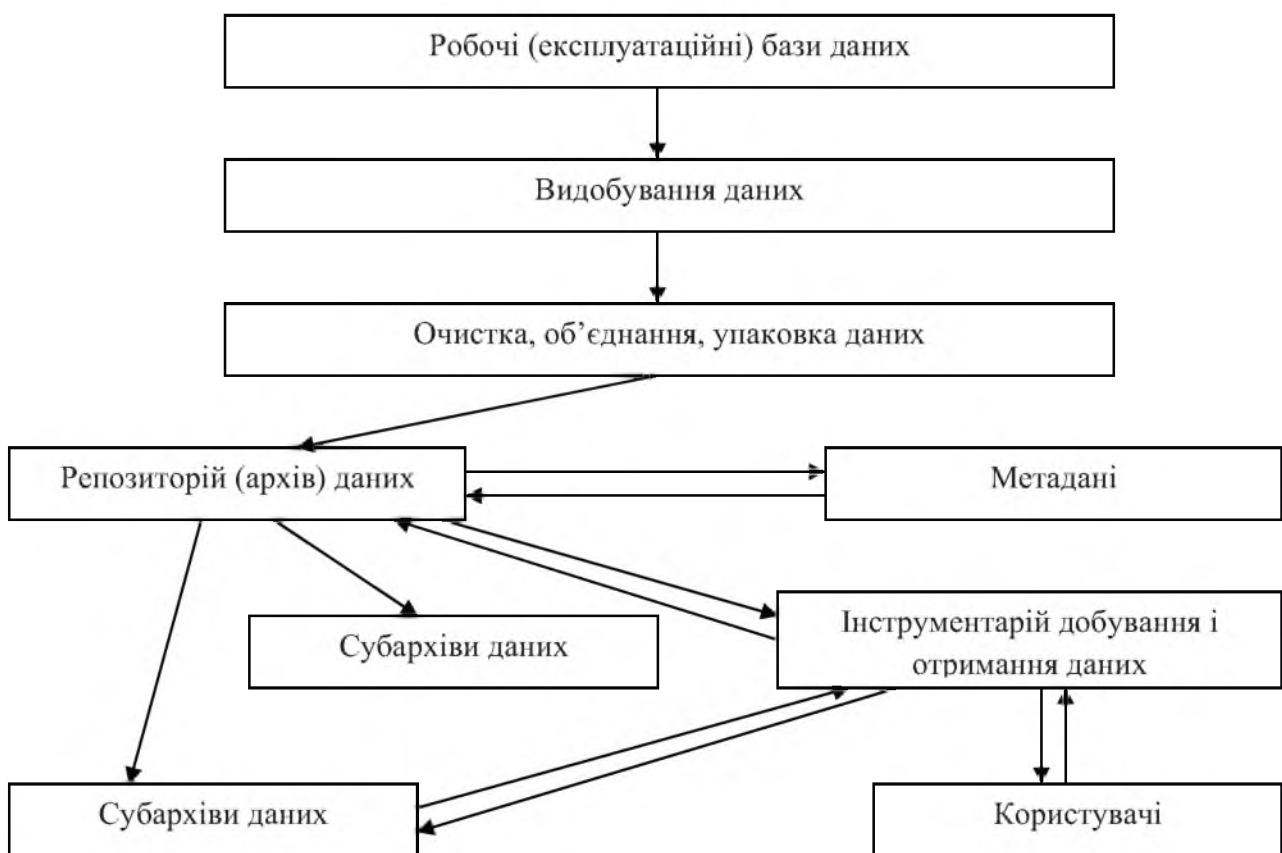


Рис. 2. Загальна схема функціонування сховища даних [4, с. 14]

Дані, які використовуються прикладними програмами, збираються прикладними засобами СХД з робочих (експлуатаційних) баз даних. Тоді вони «очищуються» та об'єднуються з іншими даними, які є важливими і цінними для користувачів сховища даних [1, с. 60–61].

Для контролю цілісності даних, знаходження необхідної інформації, перевірки порушень користування даними використовуються спеціальні програмні засоби.

Внутрішній контроль з боку адміністратора СХД забезпечується з допомогою SAS/Warehouse Administrator, що дозволяє здійснити наступні контрольні процедури:

- ідентифікувати об'єкти СХД, їхні атрибути і взаємозв'язки;
- контролювати доступ до зовнішніх джерел інформації;
- визначати фізичну модель СХД;
- представляти структуру СХД у зручній графічній формі для візуального контролю;
- регламентувати виконання процедур завантаження тощо.

З точки зору аудиторів, які здійснюють операційні перевірки в середовищі АІС компанії, СХД може розглядатися як об'єкт першочергової уваги. Це пов'язано з тим, що СХД містять багато інформації, розташованої в одному місці і пов'язаної з цілою низкою інструментальних засобів для отримання і маніпулювання цією інформацією.

Висновки. Відповіді на наведені питання дають можливість оцінити надійність середовища збереження даних в компанії. Успішність і тривалість операційної перевірки, у ході якої збирається доказова інформація у середовищі АІС згідно з поставленим завданням, значною мірою залежить від того, наскільки добре аудитор знає методологію дослідження даних, що зберігаються в електронному вигляді, та особливості організації та методики контролю.

Список використаних джерел

1. Бритов П. А., Липчинский Е.А. Опыт создания хранилищ: система SAS / П. А. Бритов, Е. А. Липчинский // Корпоративные системы. – 1999. – № 3. – С. 58–68.
2. Federal Information System Controls Audit Manual. Volum I – Financial Statement Audits. – Washington, USA: GAO, Accounting and Information Management Diviusion, 1999. – 276 p.
3. Mansour C. Data Warehousing – Part II / C. Mansour // Datawatch. – 1999. – No. 41 (Summer). – P. 14–15.
4. Дорош Н. І. Операційний аудит та аудит на відповідність. Досвід США // Фінансово-кредитне регулювання ділової активності господарюючих суб'єктів : Наук. збірник. Спец. Випуск 11 «Формування ринкової економіки в Україні» / За ред. Є. М. Мниха. – Львів : Інтереко, 2005. – С. 228–235.
5. Завгородній В. П. Автоматизація бухгалтерського обліку, контролю, аналізу та аудиту / В. П. Завгородній. – К. : А. С. К., 1998.
6. Криницький Р. І. Контроль и ревизия в условиях автоматизации бухгалтерского учета / Р. И. Криницький – М. : Финансы и статистика, 1990. – 120 с.
7. Редченко К. И. Новые аспекты управленческого контроля / К. И. Редченко // Менеджмент сегодня. – 2003. – № 4(16). – С. 2–10.