

МІЖРЕГІОНАЛЬНА  
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



МАУП

**М. М. Матюха**

# **КОМП'ЮТЕРНИЙ АУДИТ**

(для студентів економічних спеціальностей  
дистанційної форми навчання)

*Опорний курс лекцій*

Київ  
ДП «Видавничий дім «Персонал»  
2018

Рецензенти: *В. В. Сотко*, д-р екон. наук, проф.  
*Б. П. Ткач*, д-р фіз.-мат. наук, проф.  
*О. П. Колумбет*, канд. екон. наук, проф.

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 9 від 26.10.11)*

**Матюха М. М.** Комп'ютерний аудит: опор. курс лекцій для студ. екон. спец. дистанційної форми навчання / М. М. Матюха. — К.: ДП «Вид. дім «Персонал», 2018. — 228 с. — Бібліогр.: с. 226–227.

ISBN 978-617-02-0191-1

Конспект лекцій включає пояснювальну записку, навчально-тематичний план, програмний матеріал до вивчення дисципліни “Комп'ютерний аудит”, список рекомендованої літератури.

Для студентів вищих навчальних закладів.

© М. М. Матюха, 2018

© Міжрегіональна Академія управління персоналом (МАУП), 2018

© ДП «Видавничий дім «Персонал», 2018

ISBN 978-617-02-0191-1

# Зміст

<b>Вступна частина</b> .....	5
<b>Модуль I. ТЕОРЕТИЧНІ АСПЕКТИ КОМП'ЮТЕРНОГО КОНТРОЛЮ ТА АУДИТУ</b> .....	9
<i>Тема 1. Інформаційні технології у бізнесі та бухгалтерському обліку</i> .....	9
1.1. Поняття інформаційних технологій .....	9
1.2. Застосування комп'ютерної інформаційної системи підприємства (КІСП) .....	10
1.3. Технологічний процес обробки інформації при комп'ютерній системі бухгалтерського обліку.....	13
1.4. Електронний обліковий реєстр та його застосування .....	15
<i>Тестові завдання до теми 1</i> .....	23
<i>Тема 2. Поняття комп'ютерного контролю та аудиту</i> .....	25
2.1. Економічний зміст контролю .....	25
2.2. Необхідність аудиту в ринковій економіці .....	25
2.3. Аудит як форма контролю.....	26
2.4. Завдання аудиту .....	32
<i>Тестові завдання до теми 2</i> .....	36
<i>Тема 3. Застосування комп'ютерів в аудиті</i> .....	38
3.1. Варіанти застосування та регламентація комп'ютерних технологій в аудиті .....	38
3.2. Види аудиту із застосуванням обчислювальної техніки.....	41
3.3. Варіанти проведення аудиту із застосуванням комп'ютерної техніки.....	46
<i>Тестові завдання до теми 3</i> .....	53
<i>Тема 4. Методологія комп'ютерного аудиту</i> .....	55
4.1. Поняття методології комп'ютерного аудиту .....	55
4.2. Елементи аудиту при автоматизованих технологіях.....	59
4.3. Послідовність проведення аудиту в комп'ютерному середовищі .....	63
4.4. Аудиторський ризик при комп'ютерному аудиті .....	66
<i>Тестові завдання до теми 4</i> .....	88

<i>Тема 5. Аналітичні процедури в комп'ютерному аудиті</i> .....	91
5.1. Визначення та необхідність аналітичних процедур аудиту .....	91
5.2. Мета та цілі аналітичних процедур .....	93
5.3. Види аналітичних процедур .....	96
<i>Тестові завдання до теми 5</i> .....	106
<b>Модуль II. МЕТОДИКА І ПРАКТИКА КОМП'ЮТЕРНОГО АУДИТУ</b> .....	108
<i>Тема 6. Аудит в умовах застосування комп'ютерних облікових систем</i> .....	108
6.1. Аудит середовища КІСП.....	108
6.2. Фактори, що впливають на проведення аудиту .....	111
6.3. Тестування програмного забезпечення при комп'ютерному аудиті .....	128
<i>Тестові завдання до теми 6</i> .....	135
<i>Тема 7. Методи аудиту із застосуванням комп'ютерів</i> .....	137
7.1. Переваги та необхідність проведення аудиту в комп'ютерному середовищі .....	137
7.2. Типи аудиторських програмних систем .....	139
7.3. Структура аудиторської системи.....	140
7.4. Програмні продукти для проведення аудиту .....	141
7.5. Принципи застосування аудиторських програм .....	156
<i>Тестові завдання до теми 7</i> .....	171
<i>Тема 8. Автоматизація аналітичних процедур</i> .....	173
8.1. Загальні підходи до автоматизації аудиторських аналітичних процедур .....	173
8.2. Приклад застосування аналітичних процедур.....	182
<i>Тестові завдання до теми 8</i> .....	199
<i>Тема 9. Аудит інформаційної безпеки підприємства</i> .....	201
9.1. Класифікація загроз та вимоги до інформаційної безпеки підприємства .....	202
9.2. Етапи аналізу ризиків, пов'язаних із безпекою інформаційної системи .....	204
9.3. Оцінка системи внутрішніх засобів контролю.....	208
<i>Тестові завдання до теми 9</i> .....	223
<b>Список літератури</b> .....	226

## **Вступна частина**

Дисципліна “Комп’ютерний аудит” призначена для студентів бакалаврської підготовки спеціальності 6106 “Облік і аудит”.

Мета опанування дисципліни в контексті підготовки фахівців спеціальності “Облік і аудит” — формування необхідних теоретичних знань і практичних навичок, які дають змогу ефективно використовувати на практиці сучасні інформаційні системи і технології в аудиті на рівні, що відповідав би вимогам підготовки висококваліфікованих фахівців.

### **Взаємозв’язок з іншими дисциплінами навчального плану**

Дисципліна “Комп’ютерний аудит” пов’язана з такими дисциплінами, як “Інформаційні системи і технології в обліку”, “Бухгалтерський облік”, “Фінансовий облік”, “Управлінський облік”, “Економічний аналіз”, “Аудит”, “Державний фінансовий контроль”, “Організація і методика аудиту” та іншими базовими дисциплінами, що становлять основу спеціальності “Облік і аудит”.

Опанування дисципліни дасть змогу студенту:

- оволодіти теоретичними знаннями та набути практичних навичок проведення аудиту в комп’ютерному середовищі;
- засвоїти методи і прийоми організації комп’ютерних систем в аудиті за їх видами, рівнями та функціональним призначенням;
- удосконалювати, поглиблювати і розробляти форми і конфігурації інформаційних систем у напрямку максимального охоплення і рішення задач аудиту;
- створювати постановки і моделювати окремі задачі та комплекси задач з аудиту для прийняття управлінських рішень;

- адаптувати “Спеціалізовані програмні системи з аудиту” для практичного використання в аудиторській діяльності та управлінських процесах підприємств.

Вивчення дисципліни допоможе майбутнім фахівцям оволодіти сучасними методами обробки задач з аудиту, застосовуючи програмні засоби.

Методика засвоєння дисципліни передбачає практичну роботу в комп’ютерній системі, яка направлена на рішення задач аудиту.

### **Сфера реалізації набутих знань у майбутній професії**

Діяльність аудиторських фірм, приватних аудиторів, внутрішніх аудиторів, керівників підприємств, функціональних підрозділів та працівників державних контролюючих органів.

### **Як користуватися підручником**

Дисципліна “Комп’ютерний аудит” представляє опис принципів побудови автоматизованої форми проведення аудиту на підприємствах різних форм власності; висвітлює проблеми автоматизації аудиторської роботи відповідно до етапів проведення аудиту процесів, кругообігу коштів і цінних паперів, формування ресурсів і витрат, доходів, складання бухгалтерської звітності в комп’ютерних програмах при автоматизації обліку.

Програма розрахована на студентів, які мають певний рівень знань з таких дисциплін: “Теорія бухгалтерського обліку”, “Бухгалтерський облік”, “Фінансовий облік”, “Управлінський облік”, що базуються на національних положеннях (стандартах) бухгалтерського обліку.

Мета дисципліни — засвоєння студентами теоретичних знань, набуття практичних навичок організації ведення бухгалтерського обліку, вивчення теоретичних основ організації роботи бухгалтерів на підприємстві.

Завдання дисципліни “Комп’ютерний аудит” — засвоєння методики та засобів здійснення господарського контролю у сучасних умовах розвитку економіки, здійснення контрольної діяльності із застосуванням інформаційних технологій.

Рекомендується такий порядок роботи з посібником для дистанційного навчання. Насамперед, необхідно звернутися до навчальної програми — ознайомитись із її навчальними елементами. Курс складається із двох модулів, після яких наведені тестові завдання. Студенти мають дати відповіді на ці тести.

### **Критерії оцінювання тестових завдань**

Поточне оцінювання контролю знань проводиться на підставі тестових завдань, передбачених для кожного модуля. Кожне тестове завдання складається із 10 тестів. За правильну відповідь студент отримує:

- на 9–10 тестів — 90–100 балів (“A”);
- на 8 тестів — 82–89 балів (“B”);
- на 7 тестів — 75–81 бал (“C”);
- на 6 тестів — 68–74 бали (“D”);
- на 5 тестів — 60–67 балів (“E”);
- на 4 тести — 35–59 балів (“FX”);
- на 3 тести — 1–34 бали (“F”).

Для проведення контрольного опитування передбачене тестування 20 тестових завдань. Оцінювання контрольних тестових завдань проводиться у певному порядку.

Правильна відповідь на:

- 19–20 тестів — оцінюється у 90–100 балів (“A”);
- 17–18 тестів — 82–89 балів (“B”);
- 15–16 тестів — 75–81 бал (“C”);
- 13–14 тестів — 68–74 бали (“D”);
- 11–12 тестів — 68–67 балів (“E”);
- на 5 тестів — 10–59 балів (“FX”);
- на 4 тести — 1–34 бали (“F”).

При виставленні кінцевої оцінки за курс враховуються всі поточні оцінки та оцінка, отримана на іспиті.

### **5 (оцінка — відмінно)**

Студент повинен чітко і вільно володіти термінологією, логічно, вмотивовано виконувати теоретичні завдання, вміти знаходити основне у навчальному матеріалі, технічно грамотно і послідовно виконувати практичні завдання.

#### **4 (оцінка — добре)**

Студент повинен чітко і вільно володіти термінологією, технічно грамотно і послідовно виконувати практичні завдання, перелік яких наводиться у практичному розділі.

#### **3 (оцінка — задовільно)**

Студент не завжди чітко володіє термінологією, допускає змішування понять, не зовсім правильно виконує практичні завдання (проте виконане завдання досягає своєї мети).

#### **2 (оцінка — незадовільно)**

Студент не дав певних відповідей на поставлені тестові завдання.

Вивчаючи цей курс, студентам рекомендується використовувати наведену літературу. Але з огляду на те, що відбуваються часті зміни нормативно-законодавчих актів, програмних продуктів з автоматизації облікової роботи, їм потрібно самостійно вибирати додаткову літературу. Особливо це стосується законів, постанов. Також для вивчення дисципліни необхідно використовувати матеріали, що друкуються у періодичних виданнях: “Бухгалтерський облік і аудит”, “Дебет і кредит”, “Все про бухгалтерський облік”, “Бухгалтерія” та ін.



---

## **ТЕОРЕТИЧНІ АСПЕКТИ КОМП'ЮТЕРНОГО КОНТРОЛЮ ТА АУДИТУ**

---

### **Тема 1. Інформаційні технології у бізнесі та бухгалтерському обліку**

#### **1.1. Поняття інформаційних технологій**

Нині одним із найважливіших показників і передумов успішного ведення бізнесу є використання сучасних інформаційних технологій. Їх застосування надає нові можливості для розвитку і оптимізації бізнес-процесів, сприяє розширенню ринків збуту, скороченню витрат, підвищенню продуктивності праці, ефективному використанню ресурсів, підвищенню якості управління бізнесом і надання послуг. Таким чином, інформаційні технології слід розглядати як потужний засіб вирішення бізнес-завдань і досягнення бізнес-цілей. Більше того, часто без використання сучасних комп'ютерів і програм сама бізнесова діяльність стає неможливою.

Зазначимо, що ґрунтовно питання, пов'язані з теорією та практикою застосування інформаційних технологій у бізнесі, розглянуті у попередніх роботах автора. У цьому розділі ми лише коротко викладемо основні положення з автоматизації бізнесу і бухгалтерського обліку, необхідні для подальшого розкриття методик комп'ютерного контролю.

На сучасному підприємстві інформація є важливим виробничим ресурсом, без якого неможлива управлінська діяльність. Тому великого значення набувають методи обробки та використання інформації, а також технічні засоби, завдяки яким стало можливим перетворення даних в інформаційний ресурс. Таким чином, інформаційна система підприємства є

сьогодні важливим інструментом для здійснення управлінських функцій.

Будь-яка інформаційна система характеризується наявністю технології перетворення вихідних даних у результатну інформацію. Такі технології прийнято називати інформаційними. Інформаційна технологія не може існувати окремо від технічного і програмного середовища. Термін “інформаційні технології” відображає величезну кількість різноманітних технологій у різних комп’ютерних середовищах і предметних галузях. В інформаційній технології можна виділити дві частини: здатність генерувати за запитом інформаційний продукт і засоби доставки цього інформаційного продукту в зручний час і в зручній для користувача формі.

## **1.2. Застосування комп’ютерної інформаційної системи підприємства (КІСП)**

При застосуванні комп’ютерів обробку економічної інформації на підприємстві здійснює КІСП — комп’ютерна інформаційна система підприємства. Вона є сукупністю інформації, методів, моделей, технічних, програмних, технологічних засобів та рішень, що характеризується наявністю спеціалістів, які займаються обробкою інформації і прийняттям управлінських рішень у межах підприємства. За допомогою комп’ютерних інформаційних систем формується інформація щодо процесу роботи підприємства, зіставляються фактичні й нормативні показники, плануються глобальні й локальні напрями діяльності, розроблюються пропозиції з установаження причин відхилень і коригування результатів, здійснюється прогнозування ефективності управління підприємством.

Ядром економічної інформації підприємства є облікова інформація, що відрізняється великим обсягом та різноманітністю, складністю логічної та відносною простотою арифметичної обробки. Зокрема, аудит фінансової звітності, який є важливою складовою господарського контролю, має справу саме з інформацією, яку формує бухгалтерській облік.

Розглянемо детальніше особливості здійснення бухгалтерського обліку в умовах комп'ютерної обробки даних. Сучасний підхід до характеристики бухгалтерського обліку має дві своєрідні риси: а) необхідність обліку для інформаційного забезпечення управлінських рішень; б) системність у розумінні поняття обліку.

У Законі України “Про бухгалтерський облік та фінансову звітність в Україні”, який визначає правові засади регулювання, організації, ведення бухгалтерського обліку та складання фінансової звітності в Україні, надається таке визначення: “Бухгалтерський облік — процес виявлення, вимірювання, реєстрації, накопичення, узагальнення, зберігання та передачі інформації про діяльність підприємства зовнішнім та внутрішнім користувачам для прийняття рішень”. У цьому Законі метою ведення бухгалтерського обліку і складання фінансової звітності вважається “надання користувачам для прийняття рішень повної, правдивої та неупередженої інформації про фінансове становище, результати діяльності та рух грошових коштів підприємства”. Це узгоджується з визначенням, яке надала бухгалтерському обліку у 1978 р. американська асоціація бухгалтерів: “Бухгалтерський облік повинен відображати господарську діяльність підприємства, допускаючи мінімальні відхилення від реального стану справ. Форма відображення повинна бути зрозумілою кожному користувачу”. Йдеться про відображення господарської діяльності загалом, а не її складових — фактів господарського життя.

Розглядаючи бухгалтерський облік як систему, ми виходимо з того, що на конкретному підприємстві він здійснюється за допомогою засобів праці (обчислювальної та організаційної техніки) і “живої” праці працівників бухгалтерії, які зайняті обробкою специфічних предметів праці (бухгалтерських документів) з метою одержання проміжної та результатної інформації. Бухгалтерський облік можна схарактеризувати як систему, оскільки він має властивості системи — наявність зв'язків (у тому числі зворотних), структуру (упорядкованих елементів), поділ на частини, цілеспрямованість, збереження певної

структури у заданих межах під впливом зовнішніх факторів та багатоаспектність.

Бухгалтерський облік є великою системою, що не вивчається одночасно із позиції одного спостерігача в часі або просторі. Це складна система, створена для розв'язання багатоцільових завдань. Система бухгалтерського обліку є підсистемою більш складної системи — системи управління. Це документальна система, оскільки бухгалтерський облік не може функціонувати без документів.

Система бухгалтерського обліку має три рівні: методичний, технічний (рівень форми обліку) і організаційний. На методичному, базовому рівні систему бухгалтерського обліку утворюють факти господарської діяльності, що реєструються та узагальнюються на бухгалтерських рахунках. Обробка та реєстрація фактів господарської діяльності приводять до створення різних форм обліку (другий рівень системи бухгалтерського обліку). Взаємодія облікових працівників у процесі ведення обліку потребує управління і бухгалтерії, що відбувається на третьому, організаційному рівні системи бухгалтерського обліку.

Бухгалтерський облік входить у систему функцій менеджменту, серед яких планування, організація, мотивація, контроль, координація, а також інформування та прийняття рішень, а конкретніше — до функції інформування. При цьому фактично він є системою методик одержання необхідної економічної інформації на підприємстві, яка включає в себе як управлінський, так і фінансовий облік. Взаємозв'язок інформаційної системи та системи бухгалтерського обліку підприємства може бути проілюстрований за допомогою такої схеми (див. рис. 1.1).

Комп'ютерна система бухгалтерського обліку (КСБО) є центральною ланкою КІСП, де систематично, у хронологічному порядку накопичуються й обробляються дані, пов'язані з обліком, контролем, плануванням та аналізом. Головна мета функціонування КСБО (складової КІСП) — забезпечити керівництво підприємства фінансовою інформацією для при-



**Рис. 1.1. Місце комп'ютерних інформаційних систем в інформаційній системі підприємства:**

ІСП — інформаційна система підприємства;

КІСП — комп'ютерна інформаційна система підприємства;

КІОС — комп'ютерна інформаційна облікова система;

КСБО — комп'ютерна система бухгалтерського обліку

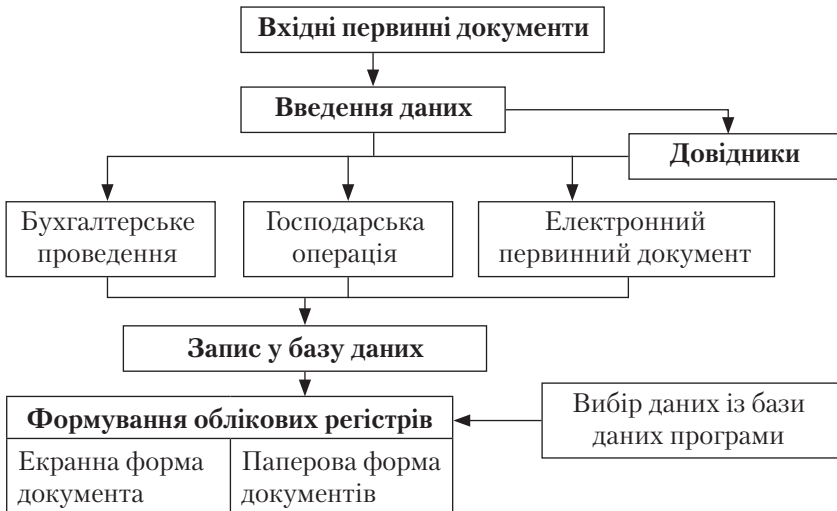
йняття обґрунтованих рішень при виборі альтернативних варіантів використання обмежених ресурсів.

### **1.3. Технологічний процес обробки інформації при комп'ютерній системі бухгалтерського обліку**

Технологічний процес обробки інформації при комп'ютерній системі бухгалтерського обліку показано на рис. 1.2.

Комп'ютерна система бухгалтерського обліку функціонує за такими принципами.

Основою комп'ютерної системи бухгалтерського обліку є електронні облікові реєстри, які представлені: а) базою даних на технічних носіях інформації, яка призначена для накопичення та зберігання облікової інформації; б) змінними величинами, що тимчасово створюються в пам'яті комп'ютера для систематизації та узагальнення облікових даних; в) екранними і друкованими формами, призначеними для візуального відображення результатної інформації.



**Рис. 1.2. Технологія обробки облікової інформації при застосуванні комп'ютерних систем бухгалтерського обліку**

Основним способом здійснення документування господарських операцій є бездокументний збір первинних даних за допомогою периферійних пристроїв та їх передача за допомогою мережових засобів комунікації.

Інформацію, що відображає відхилення за тими або іншими господарськими операціями (наприклад, відхилення від встановлених нормативів, планових завдань тощо), можна отримати автоматично за запитом.

На підставі вхідних первинних даних, одноразово зафіксованих на електронних носіях інформації, здійснюється інтегрована обробка облікових даних з необхідним рівнем деталізації та оперативності. При цьому використовується єдина інформаційна база даних, що накопичує всю потрібну для системи обліку інформацію.

Одноразове введення даних — обліковий запис перетворюється на облікову фразу (набір реквізитів даних), що призначена для перенесення даних на електронні носії та їх обробки у комп'ютеризованій системі обліку.

1. Один журнал хронологічного запису — багато реєстрів систематичного запису. За обліковими фразами формується електронний обліковий реєстр — журнал господарських операцій, хоча більшість програм для комп'ютеризації бухгалтерського обліку дозволяють перегляд інформації у вигляді традиційних для бухгалтерів журналів-ордерів, відомостей тощо.

2. Один синтетичний рахунок — багато аналітичних рахунків. Кількість рахунків аналітичного обліку залежить від мети, що поставлена перед обліком, і ніяк не обмежується.

3. Звітна інформація надається у визначений термін, а робоча (довідки, звіти для управлінців) у будь-який момент може бути одержана за запитом.

Ланцюжок облікових робіт (первинні бухгалтерські документи — паперові облікові реєстри — фінансова звітність) в КСБО реалізується за допомогою відповідних програмних алгоритмів, а накопичення, систематизація та узагальнення облікової інформації в умовах застосування сучасної обчислювальної техніки здійснюються в автоматичному режимі.

#### **1.4. Електронний обліковий реєстр та його застосування**

В умовах застосування комп'ютерів змінилося традиційне розуміння самого поняття “реєстр бухгалтерського обліку”. При паперових формах бухгалтерського обліку система відображення облікових даних у реєстрах об'єднана із системою їх узагальнення та повністю залежить від неї. Якщо при безкомп'ютерному способі обробки бухгалтерських даних під реєстром бухгалтерського обліку розуміють засіб, призначений для фіксації, накопичення, систематизації, узагальнення і відображення облікової інформації, то в умовах комп'ютеризації бухгалтерського обліку стадія відображення облікової інформації, тобто надання систематизованих облікових даних у зручному для користувача вигляді, як правило, є самостійним процесом, що не пов'язаний зі стадіями накопичення, узагальнення та систематизації.

Накопичення, систематизація та узагальнення облікової інформації в умовах застосування сучасної обчислювальної техніки здійснюються в автоматичному режимі. Первинна бухгалтерська інформація накопичується в базі даних комп'ютерної системи, а узагальнюється та систематизується на рахунках, що представлені окремими комірками пам'яті комп'ютера та є ідеальними, з погляду теорії бухгалтерського обліку, носіями ознак її групування. Побудова структури комп'ютерних баз даних може бути найрізноманітнішою; табличний принцип, за яким будуються паперові регістри, не є єдиним при побудові комп'ютерних баз даних. Базы даних є також ієрархічні, мережеві, реляційні. При комп'ютеризованому обліку будь-який матеріальний носій даних бухгалтерського обліку з теоретичного погляду можна розглядати як регістр, а отже, будь-які електронні носії, за допомогою яких накопичується облікова інформація, можна вважати регістрами обліку. Стосовно традиційних паперових облікових регістрів можна погодитись із думкою професора Д. В. Чистова, що при комп'ютеризованому обліку їх призначення та зміст принципово змінюються — із засобів узагальнення та групування інформації вони перетворюються на вихідні форми аналітичної спрямованості.

Таким чином, при застосуванні комп'ютерів обліковий регістр поєднує три складові: а) комп'ютерну базу даних з певною структурою, призначеною для накопичення та зберігання облікової інформації на технічних носіях; б) змінні величини, тимчасово створені в пам'яті комп'ютера для систематизації та узагальнення облікових даних — бухгалтерські рахунки; в) відеограми та машинограми, призначені для відображення згрупованої та систематизованої облікової інформації (рис. 1.3).

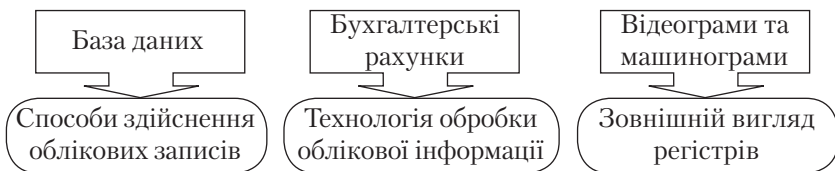


Рис. 1.3. Структура електронного облікового регістру



Первинна бухгалтерська інформація в КСБО вводиться на окремих автоматизованих робочих місцях (АРМ), накопичується в базі даних комп'ютерної системи, звідки може бути у будь-який момент отримана за запитом у зручній для користувача формі.

Визначення документа у бухгалтерському обліку і в теорії автоматизованої обробки інформації відрізняються. Поняття електронного документа в інформатиці або документа, представленого в комп'ютері, дуже широке. Всі екрани, екранні форми і дані, представлені в комп'ютері, можуть бути розглянуті як документи. Спочатку інформація фіксується на магнітному або оптичному диску, потім подається у форматі комп'ютерної програми і, нарешті, використовується у подальшій діяльності.

При комп'ютеризованому обліку первинний документ може складатися або в бухгалтерії, або на робочих місцях облікових працівників — у підрозділах підприємства — за допомогою комп'ютерів, що підключені до локальних та глобальних обчислювальних мереж, причому документи, що зберігаються на електронних носіях інформації, можуть не мати паперових аналогів. Електронний документ реєструється в комп'ютерному журналі реєстрації первинних документів, а проводки, що за ним створюються (облікова фраза), додаються до електронного журналу операцій.

Таким чином, у первинному обліку, який є важливою (а на думку професора Г. Г. Кірейцева, головною) частиною обліку, при застосуванні КСБО відбуваються значні зміни. Т. А. Краєва наводить такі відмінності технології первинного документування у комп'ютеризованих системах: а) накопичення і первинна обробка облікових даних базуються на використанні персональних комп'ютерів, які встановлюють безпосередньо на робочих місцях облікових працівників (у цехах, на складі, в бухгалтерії). При цьому скорочується потік паперових документів та здійснюється перехід до безпаперової технології обліку; б) обробка даних первинного обліку здійснюється за принципом об'єднання процесів складання первинного документа та введення його до комп'ютерної бази даних.

Іншою характерною відмінністю комп'ютеризованого документування є можливість автоматичної реєстрації первинної інформації за допомогою таких засобів, як технологічні датчики, сканери штрихових кодів (для обліку товарно-матеріальних цінностей), касові апарати (для обліку виручки від реалізації у роздрібній торгівлі), смарт-картки (для обліку праці і заробітної плати), ваги, годинники, лічильники, вимірювальна тара тощо. Така технологія первинного обліку дає змогу без будь-якої попередньої реєстрації облікових даних та їх накопичення отримати всі необхідні звітні дані безпосередньо на підставі первинної інформації. При цьому зведені первинні документи створюються періодично після здійснення господарських операцій.

Однак зазначимо, що при безпаперовій технології бухгалтерського обліку залишається дуже важлива проблема, про яку писав ще у 1988 р. професор В. Б. Івашкевич, — забезпечення юридичної обґрунтованості облікових даних та юридичної доказовості електронних первинних документів. Тільки нещодавно прийняті Закони України “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг” зрівняли в правах паперові та електронні документи, підписані електронним цифровим підписом. Проте такі електронні документи використовуються частіше для певних внутрішніх документів підприємства (накази, регламенти, листи), а також звітних бухгалтерських документів, і набагато рідше — для первинних.

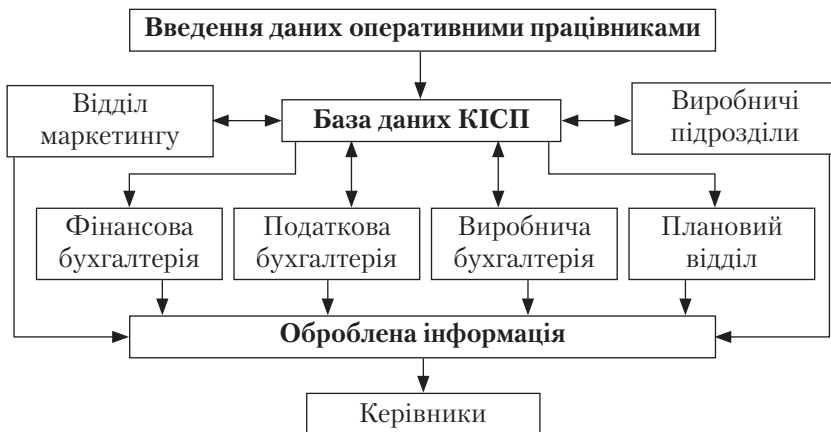
На великих та багатопрофільних підприємствах, які не обмежуються комп'ютеризацією бухгалтерського обліку, а проводять комплексну автоматизацію господарської діяльності, дані оперативного (або, іншими словами, первинного) обліку безпосередньо використовуються всіма економічними службами. За умови коректної побудови бази даних первинних документів, яка дає змогу будувати та обробляти міждокументні та міжреквізитні зв'язки, можна не формувати бухгалтерські проводки під час введення документів. До того ж, технічно це може забирати значну частину ресурсів обчислювальних систем. Доціль-

ніше в кінці звітнього періоду формувати зведені проводки із синтетичного обліку для складання фінансової звітності, а для потреб управління користуватись спеціальними аналітичними механізмами.

З цього погляду бухгалтерські проводки в комп'ютерній системі є вторинною інформацією, результатом застосування набору специфічних запитів до сукупності первинних документів, які зберігаються в базі даних, і не більше того. При розгляді питання під цим кутом зору, рахунки і проводки як основна інформаційна компонента бухгалтерського контуру автоматизованої системи управління можуть бути звільнені від невластивного їм технологічного навантаження, яке існує в системах автоматизації господарської діяльності, побудованих на основі принципу подвійного запису.

Отже, під час комп'ютерної обробки даних у КІСП відбувається інтеграція обробки різних видів первинної економічної інформації, яка використовується окремими функціями управління, тобто облікової, планової, технологічної тощо. Це приводить до створення єдиної інформаційної бази (результат інтегрування обробки), дані з якої потім можуть багаторазово використовуватися всіма службами та підрозділами підприємства. Якщо в умовах ручної обробки даних різні служби створювали й обробляли необхідну інформацію, що зумовлювало різнобій, то в КІСП така обробка є одночасним і єдиним технологічним процесом, який призводить до скасування паралелізму і дублювання, до принципу однократної фіксації, а також єдності та уніфікації (форм документів, показників, класифікації інформації, системи кодування тощо) (див. рис. І.4).

Таким чином, інтегрованою виявляється низка операцій технологічного процесу обробки первинних даних і створення їх інформаційної бази. Наступні стадії і фази групування та узагальнення даних відбуваються з використанням методів та прийомів характерних і специфічних для кожного виду економічної діяльності на підприємстві. При цьому подвійний запис, система рахунків, синтетичний та аналітичний облік не зника-



*Рис. 1.4. Потік інформації в КІСП*

ють, а перетворюються лише в один з методів отримання зведеної інформації з єдиної бази первинних даних КІСП.

Інтеграція обліку полягає в тому, що вся облікова інформація централізовано накопичується в комп'ютерних базах даних і використовується для реалізації функцій управління. У США, наприклад, бухгалтерський облік став настільки органічною частиною системи управління, що облікова інформаційна підсистема становить важливу основу інтегрованої системи економічної інформації. Такий підхід виявився досить перспективним з погляду створення і функціонування загальної інформаційної системи підприємства, оскільки призначення системи обробки даних підприємства ширше, ніж того потребує фінансовий облік, який базується на принципі подвійного запису. Наприклад, якщо облікова система дає змогу робити бюджетні прогнози, в неї можна вводити інформацію про майбутні операції та оцінювати їх вплив на стан підприємства. Як короткотермінові, так і довгострокові бюджети забезпечують керівництво життєво необхідною фінансовою інформацією. Такі облікові системи, призначені переважно для використання всередині підприємства, становлять інформаційну систему управлінського обліку.

Звітні документи бухгалтерського обліку в комп'ютерній системі бухгалтерського обліку складаються з використанням всієї наявної в базі даних інформації незалежно від того, хто персонально — бухгалтер, економіст або інший працівник — здійснив первинну обробку інформації і ввів її в систему. Завдяки цій особливості вся інформація з господарської діяльності може бути отримана як у традиційній “бухгалтерській” формі, так і без прив'язки до рахунків бухгалтерського обліку. Іншими словами, на перше місце виходить оперативний облік бізнесів-процесів, а на друге — їх відображення в бухгалтерському обліку. У результаті аналітичне навантаження блоку бухгалтерського фінансового обліку може бути зведено до мінімуму. Так, наприклад, у фінансовому обліку зовсім необов'язково організовувати облік розрахунків з контрагентами з точністю до договорів, рахунків, накладних. Ці дані можуть бути отримані з відповідних блоків оперативного (управлінського) обліку і деталізовані за всіма актуальними чинниками — контрагентами, договорами й етапами договорів, рахунками, термінами, сумами, предметами постачання тощо.

Отже, інформаційні системи сьогодні є важливим інструментом для здійснення управлінських функцій. Для деяких видів бізнесу, наприклад, для банків, систем мобільного зв'язку тощо, діяльність без комп'ютерної інформаційної системи практично неможлива. Крім того, без застосування інформаційних технологій, які дають можливість користувачу генерувати за запитом інформаційний продукт і доставляти його у зручний час і в зручній для користувача формі, була б неможливою жодна із сучасних концепцій організації бізнесу, наприклад: демократична корпорація, внутрішні ринки корпорацій, домашнє бюро, асоціативні форми організації управління, мережеві організації тощо.

Основою сучасних інформаційних систем підприємств у розвинених країнах є системи планування ресурсів (Enterprise Resource Planning — ERP). В основі ERP-систем лежить принцип створення єдиного сховища даних, що містить усю ділову інформацію, накопичену підприємством у процесі здійснення

господарських операцій, включаючи фінансову інформацію, дані, пов'язані з виробництвом, управлінням персоналом та інші відомості. Часто КСБО використовується як органічна складова ERP-систем. Завдання бухгалтерського обліку при цьому вирішуються в ERP-системах інтегровано із завданнями планування виробництва.

Облік є настільки важливою складовою управлінської функції інформування, що багато нових концепцій менеджменту побудовані саме навколо комп'ютерних інформаційних облікових систем, які відіграють значну роль на сучасних підприємствах. Вони безпосередньо обслуговують процеси планування і прийняття рішень, допомагають розробити номенклатуру і технологію виготовлення та реалізації товарів і послуг. Так, на думку відомого фахівця у галузі менеджменту Пітера Дракера, в розвинених країнах саме бухгалтери найбільшим чином сприяли впровадженню комп'ютерних технологій в господарську практику. Це дозволило П. Дракеру висунути тезу про те, що “сьогодні революційні зміни відбуваються не в технології, механіці, техніці, комп'ютерних програмах або швидкості. Революційні зміни відбуваються в концепціях. Революція йде не у сфері революційних технологій і не в адміністративній інформаційній системі, і очолюють її не менеджери з інформації. Очолюють її ті, на кого інформаційна сфера звичайно дивиться згори донизу, — бухгалтери”.

Зазначимо також, що принципове значення для побудови комп'ютерних інформаційних облікових систем і для перевірки правильності їх функціонування та оцінки вірогідності фінансової звітності має програмне забезпечення. Порядок введення, спосіб і послідовність обробки облікових даних комп'ютерами, формування зведених облікових показників повністю залежать від програми, що використовується. Таким чином, технологічний процес комп'ютеризованого обліку визначається загальними принципами програмування, і в зв'язку з цим технологічні елементи обліку знаходять своє конкретне втілення у спеціалізованих комп'ютерних програмах.

## Тестові завдання до теми 1

1. Інформація для підприємства — це:
  - а) виробничий ресурс;
  - б) незалежна структура;
  - в) комбінована обробка.
2. Інформаційна технологія — це складова:
  - а) інформаційних систем;
  - б) бази даних;
  - в) функцій управління.
3. Комп'ютерна інформаційна система підприємства — це:
  - а) сукупність інформації, методів, моделей, технічних, програмних, технологічних засобів та рішень;
  - б) сукупність управлінців та функцій управління;
  - в) сукупність організаційних заходів, що забезпечують ефективне прийняття управлінських рішень.
4. Основою економічної інформації є:
  - а) облікова інформація;
  - б) функції управління;
  - в) робочі документи аудитора.
5. Система бухгалтерського обліку має три рівні:
  - а) методичний, технічний і організаційний;
  - б) класичний, сучасний і перспективний;
  - в) обліковий, управлінський і фінансовий.
6. Основою комп'ютерної системи бухгалтерського обліку є:
  - а) електронні облікові реєстри;
  - б) первинні документи;
  - в) облікові журнали та записи.
7. Бухгалтерські проведення в електронному документо-обігу є:
  - а) первинними;
  - б) вторинними;
  - в) не використовуються.

8. Звітні документи в інформаційній системі можуть складатися:
  - а) будь-яким працівником, який має доступ до системи;
  - б) тільки обліковим працівником;
  - в) тільки аудитором.
  
9. Звітні документи в інформаційній системі формуються у вигляді:
  - а) комбінованих форм;
  - б) довільних форм;
  - в) бухгалтерських форм.
  
10. В основі ERP-систем лежить принцип:
  - а) єдиного сховища даних;
  - б) розподілення доступу за функціональною ознакою;
  - в) функції управління.



## **Тема 2. Поняття комп'ютерного контролю та аудиту**

### **2.1. Економічний зміст контролю**

Під терміном “контроль” розуміють багато понять: контроль як один із головних принципів управління, контроль як стадія процесу (циклу) управління і, нарешті, контроль як функція управління. У підходах до визначення поняття “господарський контроль” ніколи не існувало єдиних поглядів. Такі вчені, як професори В. Д. Андреев, Ф. Ф. Бутинець, М. І. Карауш, Л. М. Крамаровський, В. К. Радостовець, В. С. Рудницький та багато інших, у своїх працях господарський контроль розглядали і як принцип, і як метод та форму, і як вид діяльності. Ми поділяємо думку Ф. Ф. Бутинця, С. В. Бардаша, Й. С. Завадського і вважаємо, що під господарським контролем слід розуміти процес спостереження і перевірки відповідності функціонування підприємств встановленим стандартам та іншим нормативам, прийнятим планам, програмам і оперативним управлінським рішенням, що здійснюється суб'єктами управління, які мають відповідні повноваження, з метою виявлення відхилень від встановлених параметрів цієї діяльності, прийнятих принципів організації і ведення бізнесу, усунення та попередження негативних явищ і тенденцій.

Сутність контролю як однієї з функцій управління можна визначити як спостереження і перевірку процесу функціонування та фактичного стану об'єкта, яким керують з метою визначення обґрунтованості й ефективності прийнятих управлінських рішень та результатів їх виконання, виявлення відхилень від вимог цих рішень, усунення негативних ситуацій та інформування про це органи управління.

### **2.2. Необхідність аудиту в ринковій економіці**

Становлення ринкової економіки і поява багатьох юридично відокремлених суб'єктів господарювання, в яких перетина-

ються інтереси багатьох зацікавлених сторін, зумовили необхідність незалежного фінансового контролю. Такий різновид зовнішнього контролю у світовій практиці має назву незалежного аудиту. Бухгалтерський облік та його організація належать до різних функцій управління: бухгалтерський облік — до інформування, а організація бухгалтерського обліку — до організації. Аудит як складова контролю належить до іншої функції управління — контрольної.

Необхідність аудиту в ринковій економіці зумовлена такими об'єктивними факторами:

- складність і заплутаність бухгалтерської інформації про економічні процеси;
- віддаленість джерел економічної інформації від осіб, що приймають управлінські рішення;
- неспівпадіння інтересів працівників, які складають інформацію, і осіб, яким ця інформація потрібна;
- тісний взаємозв'язок різноманітних сфер економіки, які потребують об'єктивної інформації.

Аудиторський контроль широко застосовується у світовій практиці. В його основі лежить насамперед зацікавленість власників підприємств у достовірності інформації про господарську діяльність цих підприємств.

У конкретних умовах розвитку ринкових відносин в Україні необхідність проведення аудиту була викликана також і низькою кваліфікацією бухгалтерських кадрів, особливо головних бухгалтерів, на переважній більшості малих підприємств, складною системою чинного законодавства і частими його змінами, слабкою роз'яснювальною і консультативною роботою державних контролюючих органів щодо чинного законодавства, що змушувало підприємства звертатися з цього приводу до незалежних спеціалістів.

### **2.3. Аудит як форма контролю**

Визначень аудиту є багато, і в кожному з них викладається сутність, призначення і мета проведення аудиту. Зазначимо, що

єдиної думки про поняття аудиту і його завдань у вітчизняних і зарубіжних вчених немає.

Деякі визначення аудиту з нормативних актів і підручників наведені в табл. І.1.

*Таблиця І.1*

**Визначення аудиту у працях вітчизняних і зарубіжних авторів**

№ пор.	Визначення	Джерело
1	2	3
1	Аудит — це перевірка публічної бухгалтерської звітності, обліку, первинних документів та іншої інформації щодо фінансово-господарської діяльності суб'єктів господарювання з метою визначення достовірності їх звітності, обліку, його повноти і відповідності чинному законодавству та встановленим нормативам	Закон України “Про аудиторську діяльність” із змін та допов., внесеними Законами України від 14 березня 1995 р. № 18195-ВР, від 20 лютого 1996 р. № 54196-ВР
2	Аудит — це систематичний процес отримання об'єктивних доказів достовірності й оцінки свідчень про економічні процеси для з'ясування міри відповідності цих даних встановленим критеріям ведення бухгалтерського обліку та донесення отриманої інформації до зацікавлених осіб	Пушкин В. А., Поникаров Б. Д., Ялдин И. В., Ачкасов А. Е. Аудит: Учеб. пособие / Американська асоціація бухгалтерів. — Житомир, 1999. — С. 32
3	Аудит — це перевірка публічної бухгалтерської звітності в обліку первинних документів щодо фінансово-господарської діяльності суб'єктів господарювання з метою визначення достовірності їх звітності, обліку його повноти та відповідно чинного законодавства і встановленим нормативам. Якщо говорити простіше, то аудит — це незалежний економічний контроль	Дерій В. А., Кізіма А. Я. Аудит: Курс лекцій. — Тернопіль: Джура, 2002. — С. 4

1	2	3
4	Аудит — це підприємницька діяльність, що полягає у виконанні комплексу заходів, необхідних для формування та висловлення думки аудитора про достовірність фінансової звітності суб'єкта господарювання	Бутинець Ф. Ф., Малюга Н. М., Петренко Н. І. Аудит: стан і тенденції розвитку в Україні та світі. — Житомир: ЖДТУ, 2004. — С. 32
5	Аудит — це незалежне дослідження фінансових звітів та іншої інформації про фінансово-господарську діяльність суб'єкта господарювання з метою формування висновків про реальний фінансовий стан цього суб'єкта	Лутикин В. А., Поникаров В. Д., Ялдин И. В., Ачкасов А. Е. Аудит: Учеб. пособие. — Житомир, 1999. — С. 35
6	Аудит визначається як незалежна перевірка фінансових звітів підприємства і висловлення думки про них аудитором відповідно до чинного законодавства. Аудит не затверджує фінансові звіти і не дає гарантії їх правильності, він лише висловлює думку	Аудит: Конспект лекцій / Уклад. О. А. Петрик. — К.: МИТУ, 1995. — С. 5
7	Аудиторська діяльність (аудит) — це підприємницька діяльність аудиторів (аудиторських фірм) зі здійснення позавідомчих перевірок бухгалтерської (фінансової) звітності, документів бухгалтерського обліку, податкових декларацій та інших фінансових зобов'язань і вимог економічних суб'єктів, а також надання інших аудиторських послуг	Данилевский Ю. Л. Общий аудит в вопросах и ответах. — М.: Бух. учет, 1995. — С. 6
8	Аудит — це діяльність, спрямована на зменшення підприємницького ризику. Аудит сприяє зменшенню інформаційного ризику для користувачів фінансової звітності до прийняттого рівня	Робертсон Дж. Аудит: Пер. с. англ. — М.: КРМГ: аудиторская фирма “Контакт”, 1993. — С. 12

1	2	3
9	Аудит як незалежний вид контролю зводиться врешті-решт до виявлення різного роду помилок у бухгалтерському і податковому обліку і оцінки їх істотності	Подольский В. И., Щербакова Н. С., Комиссаров В. Л. Компьютерный аудит: Практик. пособие / Под ред. В. И. Подольского. — М.: ЮНИТИ-ДАНА, 2004. — С. 37

Кожне з наведених у табл. І.1 визначень аудиту наголошує на різних аспектах аудиторської діяльності. Згідно з визначенням, поданим у Законі України “Про аудиторську діяльність”, аудит зводиться власне до перевірки відповідності законодавству інформації про фінансово-господарську діяльність підприємства. Наголосимо, що набагато ширшим є визначення, надане Комітетом з основних положень аудиту Американської асоціації бухгалтерів. По-перше, воно не обмежує сферу діяльності аудиту до перевірки фінансово-господарської діяльності підприємства. Фактично будь-яка інформація, що піддається кількісному визначенню та перевірці, може бути піддана аудиту, якщо тільки аудитор та клієнт домовляться про критерії як основу для визначення ступеня відповідності. Наприклад, Головне бухгалтерське управління Сполучених Штатів (державна установа) може отримати завдання на аудит ефективності використання конкретного літака. Критерії вимірювання ефективності, які слід обговорити до початку аудиту, скоріш за все стосуватимуться швидкості, прискорення, висоти польоту тощо (в українській практиці можна говорити в цьому випадку про “перевірку” або “ревізію”). Жоден з перелічених критеріїв не пов’язаний з обліковими даними. Комітет Американської асоціації бухгалтерів зазначає, що навмисне надав аудиту настільки широке визначення, яке дає можливість відобразити “всю різноманітність цілей, які може ставити аудит, і всю різноманітність предметів дослідження, на яких може

бути зосереджена увага в процесі конкретної аудиторської перевірки”.

Загалом, основні погляди на поняття аудиту можна згрупувати таким чином (рис. І.5).

Цей перелік визначень аудиту, а також наведені чотири основні тенденції у визначенні аудиту, не є чимось вичерпним. Так, у ґрунтовній монографії за редакцією професора Ф. Ф. Бутинця “Аудит: стан і тенденції розвитку в Україні та світі” наведено визначення аудиту з десятків різних джерел і згруповано їх у сім груп. На нашу думку, це кращий аналіз теоретичних проблем з аудиту на сьогодні в Україні.

Якщо ж вести мову про базову термінологію аудиту, то можна загалом погодитися з авторами цієї монографії, але з одним застереженням. Автори доводять, що аудит — це лише незначна частина контролю. Проте це справедливо лише у тому випадку, якщо казати про незалежний аудит фінансової звітності (independent auditing). Автори монографії справедливо стверджують, що все інше, відоме на Заході під терміном “auditing”, може і має бути назване терміном “господарський контроль”. З цим можна погодитись. Світова економічна думка в галузі аудиту свідчить про наявність розвиненої системи англійської термінології в галузі економічного і бізнесового контролю, де

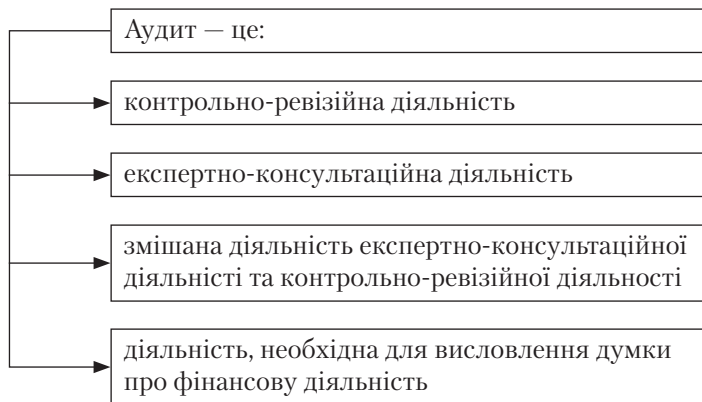


Рис. І.5. Основні погляди на поняття аудиту

за загальне поняття прийнято термін “auditing”, а далі — похідні від цього терміну: governmental auditing — державний аудит (ревізія), independent auditing — незалежний аудит. Цікаво, наприклад, що автор сучасного “Англо-українського тлумачного словника економічної лексики” А. Шимків визначає “audit” таким чином: “1. аудит; ревізія; аудиторська перевірка; перевірка фінансових операцій; аналіз господарсько-фінансової діяльності; 2. аудиторська перевірка; ревізія; аудит; аудиторський; ревізійний; ревізувати”, тобто фактично зрівнює терміни “аудит” і “ревізія”.

Чому в англійській мові саме термін “audit” означає діяльність, пов’язану з контролем господарської діяльності? Можливо, тому що значення слова “control” в англійській мові ще більш неоднозначне, ніж в українській. А. Райс виділяє 57 значень терміна “control” в англійській мові — від “заборони” до “маніпулювання”. Тлумачний словник Вебстера визначає контроль (control) як “...застосування методів та процедур для керування, регулювання та координування виробництва, систем управління та інших видів бізнесової діяльності на шляху досягнення цілей підприємства”, що знову-таки дуже схоже на визначення господарського контролю.

Таким чином, постає питання: яку систему термінології обрати? Автори згаданої монографії пропонують взяти за основу термінологію науки про господарський контроль, детально розроблену професорами Ф. Ф. Бутинцем, Л. М. Крамаровським, М. Ю. Штейнманом, аргументуючи це тим, що в Радянському Союзі була ефективна і прозора система бухгалтерського обліку і господарського контролю. Однак Радянський Союз програв глобальні змагання двох соціально-економічних систем: соціалістичної і капіталістичної. Причому програв насамперед в економічній сфері. Це свідчить також і про те, що потенціал систем бухгалтерського обліку і господарського контролю в Радянському Союзі не використовувався належним чином, а отже, справді великі наукові надбання не пройшли належного випробування практикою.

## 2.4. Завдання аудиту

Основною метою сучасного аудитора-контролера є висловлення думки стосовно відповідності фінансової звітності (і не тільки звітності) підприємства встановленим критеріям. Думка аудитора визначає, до якої міри перевірені факти відповідають встановленим критеріям і стандартам. Важливо знати, що то за критерії та стандарти, оскільки від того, в якій мірі чітко вони визначені, залежить ступінь відповідності і, як наслідок, ризикованості стосовно наслідків перевіреної інформації. Якщо проаналізувати наведені в табл. І.1 визначення, то ми побачимо, що жорсткість встановлених критеріїв як бази для порівняння є різною. Наприклад, у Законі України “Про аудиторську діяльність” чітко визначено, що цими критеріями є “чинне законодавство та встановлені нормативи”. Комітет з основних положень аудиту Американської асоціації бухгалтерів (українські автори в основному цитують Закон) посиляється на “встановлені критерії”, не специфікуючи, які саме. Таке широке визначення дає змогу розширити поле діяльності аудиторів, виводячи її за межі перевірки документів, що стосуються фінансово-економічного стану підприємства (фінансова звітність, первинні документи, облікові реєстри тощо). Проте, як погоджуються й іноземні фахівці, аудит здебільшого має справу саме з обліковими даними, що містяться у бухгалтерських документах та фінансових звітах підприємства. При цьому брак чітко визначених критеріїв їх перевірки надає можливість для неоднозначного трактування результатів фінансово-економічної діяльності підприємства. Міжнародні стандарти аудиту теж не регламентують однозначно цих критеріїв, називаючи їх “встановленими основами фінансової звітності”. Підручники з аудиту, щоправда, зазначають, що в аудиті фінансової звітності критеріями є загальноприйняті принципи бухгалтерського обліку (GAAP, IAS). Встановленими критеріями, на основі яких формулюються висновки про податки, є податкове законодавство, правила і положення, що стосуються конкретного податку. В інших же випадках, таких



як аудит ефективності, критерії є значно менш точними і, як правило, погано визначеними. У таких ситуаціях аудитор і клієнт повинні домовлятися стосовно критеріїв і точно визначити їх в аудиторському висновку. Можливість клієнта вибрати критерії оцінки має значний вплив на об'єктивність та неупередженість аудиторського висновку, що також може поставити під сумнів роль аудитора як незалежного посередника між постачальниками і споживачами фінансової інформації, які мають різні інтереси. Проте міжнародні стандарти аудиту зазначають, що відповідальність за фінансову звітність лежить на управлінському апараті суб'єкта, що перевіряється. Аудитор не затверджує фінансові звіти: він тільки висловлює думку. Тому аудитор несе відповідальність тільки за свою думку; він не відповідає за саму надану підприємством інформацію.

Іноді в роботах українських дослідників трапляється думка, що одним із завдань аудиторських служб є складання фінансової звітності підприємства. Треба зазначити, що тут має місце певне змішування функцій бухгалтерського обліку (або аудиторських послуг) та власне “незалежного” аудиту. Як зазначає відомий американський фахівець у галузі теорії і практики аудиту професор Дж. Робертсон на перших сторінках своєї праці, аудит не включає складання фінансової звітності. Часто аудитори забезпечують не тільки перевірку вірогідності фінансових показників, а й, що не менш важливо, розробку пропозицій з оптимізації господарської діяльності з метою раціоналізації витрат і збільшення прибутку. Однак, згідно із законом Сарбейнса–Окслі, який був прийнятий у 2002 р. у США, аудиторам заборонено одночасно надавати одному і тому самому клієнту аудиторські й консультативні послуги. Прямо українських аудиторів цей закон не стосується, хоча й охоплює де-факто найбільші світові корпорації та аудиторські фірми.

Дж. Робертсон підкреслює, що аудит — це діяльність, спрямована на зменшення підприємницького ризику. І далі стверджує, що аудит сприяє зменшенню до прийняттого рівня інформаційного ризику для користувачів фінансових звітів.

Можна приблизно підрахувати (спрогнозувати) цей ризик і визначити імовірність сприятливих подій. Водночас підприємницький ризик компанії (фірми, організації) прямого впливу на аудиторів не робить. Інакше кажучи, аудит — це система збирання й обробки інформації, мета якої є оцінювання ефективності інформаційної системи бухгалтерського обліку економічного суб'єкта, що перевіряється. Як правильно зазначає П. І. Камишанов, аудит можна визначити як своєрідну експертизу бізнесу.

Відповідно до цього найважливішими цілями аудиту є:

- встановлення вірогідності бухгалтерської (фінансової) звітності економічних суб'єктів і відповідності здійснених ними фінансових і господарських операцій нормативним актам;
- своєчасне виявлення потенційного банкрутства, тобто визначення життєздатності підприємства, що важливо для суб'єкта, якого перевіряють, його контрагентів і суспільства загалом.

Етапи сукупної оцінки аудитором фінансової звітності наведено на рис. 1.6.

Основна мета аудиту також доповнюється зумовленими договором із клієнтом завданнями виявлення резервів кращого використання фінансових ресурсів, аналізом правильності розрахунку податків, розробкою заходів щодо покращення фінансового становища підприємства, оптимізації витрат і результатів діяльності, доходів і витрат. Таким чином, мету аудиту

#### Етапи

Укладення угоди і планування перевірки	Перевірка (тестування) засобів контролю	Перевірка (тестування) господарських операцій	Перевірка (тестування) залишків рахунків	Завершення аудиту і складання висновків
----------------------------------------	-----------------------------------------	-----------------------------------------------	------------------------------------------	-----------------------------------------

Формування думки аудитора

*Рис. 1.6. Етапи сукупної оцінки аудитором фінансової звітності*

ту як діяльності в широкому сенсі можна сформулювати як вирішення конкретного завдання, що визначається законодавством, системою нормативного регулювання аудиторської діяльності, договірними зобов'язаннями аудитора і клієнта.

Підсумковим результатом роботи аудитора є аудиторський звіт. У ньому може міститись будь-яка інформація, що цікавить клієнта — замовника аудиту, і форма подання якої регламентована у договорі на проведення аудиту. Крім того, аудиторські послуги у вигляді консультацій можуть надаватись усно або письмово з оформленням довідки та інших офіційних документів.

Якщо мета аудиту — надати свою думку про вірогідність інформації, що наведена у річній фінансовій звітності, то обов'язковою частиною звіту аудитора є аудиторський висновок, базові вимоги до якого наведені у Законі України “Про аудиторську діяльність” (ст. 7.1). Відповідно до ст. 7 і 21 Закону України “Про аудиторську діяльність” аудитор має провести перевірку бухгалтерської річної звітності суб'єкта господарювання з метою надання висновку про достовірність і реальність представленої інформації та її підтвердження або не підтвердження.

Аудиторський висновок — це офіційний документ, засвідчений підписом та печаткою аудитора (аудиторської фірми), який складається у встановленому порядку за наслідками проведення аудиту і містить висновок стосовно достовірності звітності, повноти і відповідності чинному законодавству та встановленим нормативам бухгалтерського обліку фінансово-господарської діяльності. Аудиторський висновок має містити чітке уявлення аудитора щодо перевіреної ділянки. Він складається з дотриманням відповідних норм та стандартів і має включати підтвердження або аргументовану відмову від підтвердження достовірності, повноти та відповідності певним критеріям.

Висновок щодо фінансової звітності може бути позитивним, умовно-позитивним, негативним, або дається відмова від надання висновку. У двох останніх випадках в аудиторському

висновку може наводитися короткий перелік аргументів, які підштовхнули аудитора зробити такий висновок.

## **Тестові завдання до теми 2**

1. Вкажіть найбільш точне визначення поняття “контроль”:
  - а) функція управління;
  - б) аудиторський цикл;
  - в) мета обліку.
2. Аудит — це складова:
  - а) контролю;
  - б) обліку;
  - в) управління.
3. Одна із необхідностей проведення аудиту — це:
  - а) віддаленість джерел економічної інформації від осіб, які приймають управлінські рішення;
  - б) введення обліку для задоволення потреб управлінців;
  - в) невизначеність державної політики у сфері контролю.
4. Вкажіть найбільш точне визначення поняття “аудит”:
  - а) перевірка публічної бухгалтерської звітності;
  - б) функція управління;
  - в) мета облікової політики.
5. Основною метою сучасного аудитора-контролера є:
  - а) висловлення думки щодо відповідності фінансової звітності підприємства встановленим критеріям;
  - б) дотримання чинного законодавства щодо ведення обліку;
  - в) проведення аналітичних розрахунків підприємства з метою надання рекомендацій щодо діяльності підприємства.
6. Аудиторський висновок — це:
  - а) документ, що містить висновок стосовно достовірності звітності;
  - б) документ, що містить аналітичні розрахунки щодо діяльності підприємства;

- в) документ, що містить ряд контрольних заходів, проведених на підприємстві.
7. Аудиторський висновок має містити:
    - а) чітке уявлення аудитора щодо перевіреної ділянки;
    - б) документи, що перевірялися;
    - в) робочі документи аудитора.
  8. Етапами аудиту є:
    - а) укладення угоди і планування перевірки;
    - б) оформлення аудиторських робочих документів;
    - в) рекламна діяльність аудиторської фірми.
  9. Мета аудиту може бути доповнена:
    - а) договором із клієнтом;
    - б) умовами, що склалися під час перевірки;
    - в) вирішенням нормативних завдань із клієнтом.
  10. Аудит розуміють як:
    - а) зменшення підприємницького ризику;
    - б) продовження аналітичної роботи менеджменту;
    - в) збільшення відповідальності перед замовником аудиту.

## Тема 3. Застосування комп'ютерів в аудиті

### 3.1. Варіанти застосування та регламентація комп'ютерних технологій в аудиті

Комп'ютеризація принципово не змінює методологію бухгалтерського обліку. Найбільші зміни відбуваються у технології обробки облікової інформації, що насамперед втілюється в порядку побудови комп'ютерних форм бухгалтерського обліку. Цікаво, що використання комп'ютерів для ведення бухгалтерського обліку фактично не регламентується нормативними актами (будь-якими стандартами з автоматизації бухгалтерського обліку). Не дуже вдалим винятком може бути, наприклад, спроба Державного казначейства України регламентувати вигляд електронних форм меморіальних ордерів. Натомість методика аудиту фінансової звітності підприємств, на яких використовуються комплексні КІСП та КСБО, зазнає значних і суттєвих змін, хоча, звичайно, загальна мета аудиту не змінюється.

В аудиторських фірмах персональні комп'ютери можуть використовуватися і активно застосовуються як для проведення аудиту економічних суб'єктів, так і для автоматизації управлінських робіт самої аудиторської організації. При цьому використання комп'ютерів в аудиті навіть без використання спеціалізованого програмного забезпечення може включати такі види робіт (табл. I.2).

Таблиця I.2

Варіанти застосування комп'ютерів в аудиті

№ пор.	Види виконуваних робіт з використанням комп'ютера
1	2
1	Виконання нескладних розрахунків, друк типових форм аудиторських документів, анкет, тестів тощо
2	Використання нормативно-правової довідкової бази в електронному вигляді

1	2
3	Виконання запитів до електронної бази даних, сформованої в КСБО
4	Перевірка окремих розрахунків, виконуваних на різних ділянках обліку КСБО
5	Формування реєстрів бухгалтерського обліку й альтернативного балансу з використанням електронної бази даних клієнта
6	Проведення комплексного аналізу фінансового стану економічного суб'єкта

У зв'язку з широким застосуванням обчислювальної техніки і комп'ютерних інформаційних мереж та систем у бізнесі та бухгалтерському обліку перед аудиторами постало завдання пристосування технології своєї роботи або навіть значної її зміни з використанням спеціальних методів і комп'ютерних програм при проведенні аудиту фінансової звітності підприємств, які застосовують автоматизовані фінансово-облікові системи. На жаль, як ми вже зазначали, незважаючи на беззаперечну актуальність проблем, пов'язаних із застосуванням комп'ютерів в аудиті, українські автори не приділяють їм належної уваги. Чи не єдиною ґрунтовною працею з цих питань є навчальний посібник професора В. П. Завгороднього «Автоматизація бухгалтерського обліку, контролю, аналізу та аудиту». Окремі питання автоматизації контролю висвітлені в монографіях С. В. Бардаша. Натомість, у світовій практиці аудиту питанням застосування інформаційних технологій приділяють значну увагу, зокрема, професійні організації. Про це свідчить, наприклад, постійне оновлення (з інтервалом в 1–2 роки) фактично всіх Міжнародних стандартів аудиту, що видаються Міжнародною федерацією бухгалтерів, в яких найбільших змін зазнають саме стандарт і положення про Міжнародну аудиторську практику, що стосуються комп'ютеризації аудиту. В офіційному українському виданні Міжнародних стандартів аудиту 2004 р., яке діє на території України і сьогодні, містяться положення, що стосуються інформаційних технологій (див. табл. І.3).

**Перелік положень про міжнародну аудиторську практику  
щодо комп'ютеризації аудиту**

<b>№ пор.</b>	<b>Назва</b>
401	Аудит у середовищі комп'ютерних інформаційних систем (стандарт)
1001	Середовище ІТ: автономні персональні комп'ютери
1002	Середовище ІТ: онлайніві комп'ютерні системи
1003	Середовище ІТ: системи баз даних
1008	Оцінювання ризиків та внутрішній контроль — характеристики та особливості в КІС
1009	Комп'ютеризовані методи аудиту
1013	Електронна комерція — вплив на аудит фінансових звітів

Однак у новій англomовній редакції Стандартів 2005 р. всіх цих розділів (за винятком Положення 1013) немає. І не тільки їх. Фактично, ідеологія і структура стандартів значно перебудовані. Наприклад, стандарти 310 “Знання бізнесу”, 400 “Оцінка ризику і внутрішній контроль”, 401 “Аудит у середовищі комп'ютерних інформаційних систем” і Положення про Міжнародну аудиторську практику 1008 “Оцінювання ризиків та внутрішній контроль — характеристики та особливості в КІС” втратили свою чинність у грудні 2004 р., коли вступили в дію стандарти 315 “Розуміння господарюючого суб'єкта та оцінювання ризику суттєвого відхилення” та 330 “Аудиторські процедури стосовно оцінених ризиків”. Основною ідеєю, яка, як нам здається, лежала в основі цієї перебудови, було те, що тепер фактично весь аудит розглядається як комп'ютерний, тобто в умовах застосування бізнесових і бухгалтерських комп'ютерних інформаційних систем (КІС) і з використанням комп'ютерних методів аудиту. Саме тому коментарі та вказівки з цих питань тепер містяться майже в кожному стандарті аудиту.

У низці робіт, опублікованих в різний час у Росії, розглядалися питання комп'ютеризації аудиту, теорії і методичних під-



ходів, вживаних аудиторами у середовищі комп'ютерної обробки даних. Досить відомими посібниками є роботи професорів А. Н. Романова і Б. Е. Одінцева “Автоматизація аудиту” (1999 р.) та “Комп'ютеризація аудиторської діяльності” (1996 р.), що сформулювали загальні вимоги до автоматизованих систем проведення аудиту та запропонували ряд практичних рекомендацій щодо їх створення.

### 3.2. Види аудиту із застосуванням обчислювальної техніки

Як у літературі західних авторів, так і в російських джерелах термінологія щодо комп'ютеризації аудиту та аудиту інформаційних систем не є сталою, а підходи до визначення методик значно відрізняються (табл. І.4).

Таблиця І.4

Види аудиту із застосуванням обчислювальної техніки

№ пор.	Термін	Визначення	Джерело
1	2	3	4
1	Audit automation (автоматизація аудиту)	Використання інформаційної технології у плануванні, контролюванні та документуванні аудиторської роботи	Manson S., McCartney Sc., Sherer M. Audit Automation: Improving Quality or Keeping up Appearances? // Current issues in auditing. — 3rd ed. — London: Chapman Publishing Ltd, 1997. — 342 p. — P. 254
2	Audit automation (автоматизація аудиту)	Процес застосування будь-яких інформаційних технологій для допомоги аудитору у плануванні, проведенні, контролюванні,	Williamson A. L. Audit Automation, Accountants Digest. — 1994. — № 318. — London: ICAEW. — P. 1

1	2	3	4
		завершенні та адмініструванні аудиторської роботи	
3	Комп'ютерний аудит	Означає використання комп'ютерів і сучасних інформаційних технологій для організації аудиторської діяльності, включаючи аудиторські перевірки фінансової звітності і підготовку аудиторського висновку, а також надання супутніх аудиту послуг	Подольский В. И., Щербакова Н. С., Комиссаров В. Л. Компьютерный аудит: Практическое пособие / Под ред. проф. В. И. Подольского. — М.: ЮНИТИ-ДАНА, 2004. — 128 с.
4	Audit approach to computers (аудиторський підхід до комп'ютерів)	Аудит інформаційних систем, який полягає у визначенні аудиторської стратегії, у розумінні та описі комп'ютерної системи, в оцінюванні внутрішніх засобів контролю, у тестуванні цих контролів та виявленні їх слабких місць та у детальному тестуванні	Jenkins B., Cooke P., Quest P. An audit approach to computers. — London: Coopers&Lybrand Deloitte (United Kingdom). — 1992. — 572 p.
5	Information systems auditing (аудит інформаційних систем)	Процес збирання та оцінювання доказів для того, щоб визначити, чи комп'ютерна система зберігає цілісність даних, забезпечує ефективне виконання цілей	Weber R. Information systems control and audit. — Upper Saddle River, Prentice-Hall, Inc, 1999. — 1013 p.

1	2	3	4
		організації та ефективне використання ресурсів	
6	Аудит інформаційних систем	Аудит — це процес перевірки інформаційної системи на відповідність певним критеріям за розробленими методиками. У результаті аудит дає змогу оцінити реальний стан інформаційної системи підприємства	Псалтыра Е. Для чего необходим аудит ИС // <a href="http://www.optim.ru/comp/20_03/3/TMUConsulting/TMUConsulting.asp">http://www.optim.ru/comp/20_03/3/TMUConsulting/TMUConsulting.asp</a>
7	Комп'ютерний аудит	Оцінка поточного стану комп'ютерної системи на відповідність деякому стандарту чи запропонованим вимогам	О выборе компании для анализа защиты информационной системы // <a href="http://www.vit.ru/vit/security/press/press8.html">http://www.vit.ru/vit/security/press/press8.html</a>
8	Ревізія системи автоматизованої обробки економічної (облікової) інформації	Перевірка спеціалістами (ревізорами) засобів і методів контролю (програмних, організаційних) і захисту інформації від можливих зловживань з метою розробки заходів з їх попередження	Криницкий Р. И. Контроль и ревизия в условиях автоматизации бухгалтерского учета. — М.: Финансы и статистика, 1990. — 118 с.
9	Computer-Assisted Audit Techniques — СААТs (комп'ютеризовані методи аудиту)	Будь-які комп'ютерні програми, які використовуються для збільшення ефективності аудиторського процесу через автома-	Champlain J. Auditing information systems: a comprehensive reference guide. — N. Y.: John

1	2	3	4
		тизацію процесів, які раніше виконувались вручну, збільшення аудиторської вибірки та створення нових аудиторських процедур	Wiley&Sons, Inc., 1998. — 422 p. — P. 298
10	Computer-Assisted Audit Techniques — СААТs (комп'ютеризовані методи аудиту)	Методика аудиту, яка полягає у використанні комп'ютерної техніки аудитором, коли облік ведуть за допомогою спеціальних програм, а інформацію зберігають у файлах даних	Додж Р. Краткое руководство по стандартам и нормам аудита: Пер. с англ. — М.: Финансы и статистика; ЮНИТИ, 1992. — 240 с.
11	Computer-Assisted Audit Techniques — СААТs (комп'ютеризовані методи аудиту)	Застосування аудиторських процедур із використанням комп'ютера як аудиторського інструмента	Handbook of International Auditing, Assurance, and Ethics Pronouncements. 2005 Edition — P. 103 // www.ifact.org
12	End-user computing in auditing (обчислення, що здійснює кінцевий користувач під час аудиту)	Використання комп'ютера і його програмного забезпечення для збирання та аналізу великої кількості інформації для того, щоб дати висновок про коректність цих даних і правильність фінансової звітності	Titanen Anne M. The Role of End-User Computing Support in Auditing // http://www.helsinki.fi/~tiitane/isd97.htm

У наведених визначеннях чітко спостерігаються три аспекти:

- використання комп'ютерів для організації роботи аудиторської фірми (№ 1–3);
- перевірка та оцінювання комп'ютерних інформаційних систем (№ 4–8);
- використання комп'ютерів і програм як специфічних інструментів для проведення аудиту (№ 9–12).

Саме в організаційному аспекті професор В. І. Подольський розуміє комп'ютерний аудит як використання комп'ютерів і сучасних інформаційних технологій для організації аудиторської діяльності, включаючи аудиторські перевірки фінансової звітності й підготовку аудиторського висновку, а також надання супутніх аудиту послуг. А. С. Менсон і С. Мак-Картні під автоматизацією аудиту (*audit automation*) мають на увазі використання інформаційної технології у плануванні, контролі та документуванні аудиторської роботи:

- у плануванні: створення бюджетів часу та розподіл функцій між учасниками (*creation of time budgets, allocation of staff to functions*), розрахунок фінансових та статистичних показників при здійсненні аналітичних процедур (*icalculation of financial ratios for analytical review*);
- у контролі: підготовка стандартної документації (*standard documentation*), підсумовування результатів (*summary of results*), складання блок-схем (*flowcharting*);
- у документуванні: облік часу та витрат, потрачених на аудиторський проект (*recording of time and costs*).

Щодо другого аспекту, Р. Вебер каже про аудит власне інформаційних систем (*information systems auditing*), який ним визначається як процес збирання та оцінювання доказів для того, щоб визначити, чи комп'ютерна система зберігає цілісність даних, забезпечує ефективне виконання цілей організації та ефективне використання її ресурсів. Такий підхід він пояснює тим, що з переходом від ручних до комп'ютерних інформаційних систем, внутрішні засоби контролю, на які здебільшого спирається у своїй роботі аудитор, стають комплекснішими, а тому процес їх оцінювання — складнішим. Тестування

комп'ютерних систем клієнта він розглядає як важливий і необхідний процес при проведенні аудиту фінансової звітності. Цю думку поділяють Б. Дженкінс і П. Кук і визначають, що аудиторський підхід до комп'ютерів (audit approach to computers) полягає у визначенні аудиторської стратегії; розумінні та описанні системи; оцінюванні вбудованих засобів контролю; тестуванні засобів контролю та виявленні слабких місць; детальному тестуванні.

### **3.3. Варіанти проведення аудиту із застосуванням комп'ютерної техніки**

Надалі розглянемо окремі практичні аспекти автоматизації аудиту, маючи на увазі, що вести мову про застосування комп'ютерних інформаційних технологій в аудиті можна, коли: а) проводиться аудит фінансової звітності підприємств, що використовують комп'ютерні облікові системи; б) аудиторі в своїй діяльності використовують комп'ютери і певне програмне забезпечення.

Причому в першому випадку аудит може здійснюватись як із застосуванням інформаційних технологій, так і без них, а в другому випадку може проводитись аудит як паперових, так і автоматизованих облікових систем.

В умовах функціонування автоматизованих інформаційних систем зазнають деяких змін основні принципи аудиту. Відповідно, застосування КІСП може вплинути на:

- процедури, яких дотримується аудитор у процесі одержання достатнього уявлення про системи бухгалтерського обліку і внутрішнього контролю;
- аналіз властивого ризику і ризику системи контролю, за допомогою чого аудитор проводить оцінювання ризику;
- розробку і здійснення аудитором тестів системи контролю і процедур перевірки по суті, необхідних для досягнення цілей аудиту.

Зазначимо, що на відміну від ручних облікових систем, де записи здійснюються на папері і аудитор розглядає можливість

знищення, підробки, заміни паперових документів, в умовах використання КІСП аудитор доводиться мати справу з питаннями безпеки та надійності комп'ютерних облікових систем. Отже, аудитор перевіряє низку суто технічних питань, які не мають прямого відношення до бухгалтерського обліку, але безпосередньо впливають на оцінювання аудитором ризику системи контролю. Подібні заходи передбачало Положення про міжнародну аудиторську практику 1008 “Оцінювання ризиків та внутрішній контроль: характеристики та особливості в КІС”.

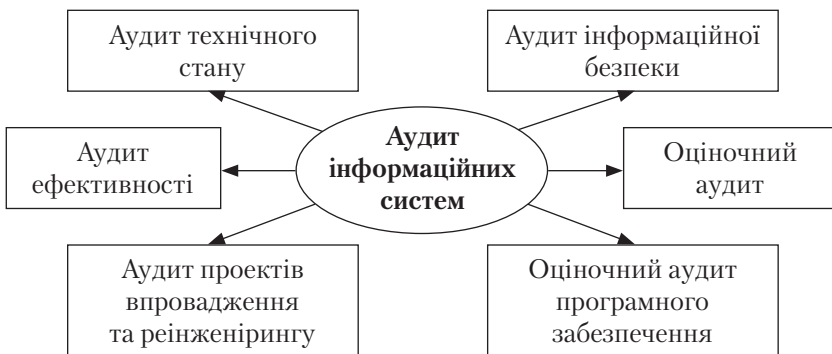
Таке поєднання різних, здавалося б, за змістом видів діяльності (технічних і фінансових), якими доводиться займатися у сучасних умовах аудиту, можна легко сприйняти та пояснити, якщо погодитись із думкою відомого американського фахівця у галузі менеджменту П. Дракера стосовно того, що застосування комп'ютерних інформаційних технологій привносить в наше життя такі масштабні зміни, які можна порівняти зі змінами, що свого часу спричинили винайдення писемності та технології друкування книг. Саме тому в умовах застосування КІСП відбувається взаємне проникнення різних за своїм змістом та суб'єктами видів контрольної та організаційної діяльності (рис. 1.7).



*Рис. 1.7. Складові аудиту в умовах застосування КІСП*

Для перевірок ефективності й безпечності інформаційної системи як такої здійснюють комп'ютерний аудит інформаційної системи. Під ним мається на увазі оцінювання поточного стану комп'ютерної системи на відповідність деякому стандарту або запропонованим вимогам. Цей термін використовується насамперед спеціалістами із загальної безпеки комп'ютерних інформаційних систем і у вузькому значенні не стосується аудиту фінансової звітності. Такий аудит не направлений на пропонування конкретного рішення, він дає можливість поглянути на інформаційну систему комплексно, виявити проблемні місця, сформувані обґрунтовані рекомендації для ухвалення рішення з усунення недоліків. Він включає кілька напрямів (рис. 1.8).

Аудит технічного стану інформаційної системи спрямований на зменшення втрат, викликаних системними збоями. Збої можуть стати причиною відчутних втрат підприємств. Враховуючи, що в інформаційних системах, в яких не налагоджені належні процеси контролю і попередження можливих причин збоїв, вони виникають у найвідповідальніші, а отже, і найнапруженіші моменти, втрати можуть вилитися у величезні суми. Скорочення таких втрат можна досягти шляхом комплексного дослідження технічного стану всіх компонентів інформаційної системи. Аудит технічного стану інформаційної системи насамперед призначений для оцінювання поточного



*Рис. 1.8. Напрями аудиту інформаційних систем*



стану інформаційної системи з метою реконструкції і модернізації, щоб підготуватися до розширення інформаційної системи і впровадження нових технологій. Його проведення дає змогу також організувати і налагодити підтримку інформаційної системи та розробити корпоративні стандарти підтримки інформаційної системи.

Аудит технічного стану інформаційної системи включає проведення таких заходів, як облік наявних на підприємстві апаратних засобів, програмного забезпечення, периферійних пристроїв і аналіз побудови структурованої кабельної системи, мереж передачі даних, функціонування ІТ-служби підприємства, технічних параметрів ефективності роботи інформаційної системи, її надійності та безпеки.

За наслідками аудиту клієнту надається звітність за такими напрямками:

- стан кабельної системи;
- реалізація резервного копіювання;
- наявність незахищених дискових ресурсів;
- безпека інформаційної системи для виявлення існування потенційних загроз несанкціонованого доступу до інформаційної системи;
- інвентаризація програмних і апаратних засобів;
- завантаженість каналів зв'язку для визначення і локалізації критичних ділянок інфраструктури мережі.

Аудит ефективності інформаційної системи дає можливість підприємству:

- оцінити сукупну вартість володіння інформаційною системою і порівняти показники досліджуваної системи з лідером у цій галузі;
- оцінити терміни повернення інвестицій при вкладенні коштів в інформаційну систему;
- розробити оптимальну схему вкладень, здійснити ефективне витрачання коштів на обслуговування і підтримку, понизити виробничі витрати.

Цей вид аудиту включає такі складові інформаційної системи підприємства, як апаратні засоби, програмне забезпечення,

периферійні пристрої, IT-персонал компанії, а також документи, бізнес-процеси, інформаційні потоки та ін. Також до методів проведення аудиту можна зарахувати:

- комплексне дослідження бізнес-процесів;
- оцінювання вартості обладнання;
- оцінювання якості наявної кабельної системи;
- оцінювання вартості впроваджених технологій;
- оцінювання витрат на утримання інформаційної системи;
- оцінювання якості технічної підтримки користувачів;
- оцінювання вартості налагоджених процесів управління;
- оцінювання сукупної вартості володіння інформаційної системи.

У результаті проведення такого аудиту підприємству-клієнту надається перелік звітності, що включає підсумковий звіт з рекомендаціями щодо оптимізації інформаційної системи і звіт за наслідками розрахунку сукупної вартості володіння.

Результати аудиту інформаційної безпеки дають змогу побудувати оптимальну за ефективністю і витратами корпоративну систему захисту інформації, адекватну завданням і меті бізнесу. Аудит інформаційної безпеки не обмежується перевіркою тільки фізичної безпеки, наявні методики дають можливість проаналізувати бізнес-процеси і визначити основні інформаційні потоки компанії, які мають бути захищені.

При проведенні аудиту інформаційної безпеки виявляється поточний стан системи безпеки і визначаються найкритичніші ділянки системи, перевіряється відповідність наявної в компанії системи захисту інформації, вимогам інформаційної безпеки, що висуваються до неї, оцінюється ефективність вкладень у корпоративну систему захисту інформації. Аудит включає такі етапи, як:

- комплексна перевірка рівнів забезпечення інформаційної безпеки;
- аналіз інформаційних ризиків;
- аналіз системи захисту зовнішніх мереж;
- аналіз системи контролю інформації, що передається по телефонних з'єднаннях і електронною поштою;

- визначення можливих каналів просочування конфіденційної інформації.

У перелік матеріалів, що надаються за підсумками аудиту, входять також звіт про поточний стан системи інформаційної безпеки й ефективність вкладень у систему інформаційної безпеки, а також рекомендації щодо політики безпеки і плану інформаційного захисту.

Якщо підприємство починає великі проекти модернізації своєї інформаційної системи, воно використовує послуги системних інтеграторів з метою визначення реальних термінів і вартості проектів перед початком робіт або ставить перед собою мету контролю проектів впровадження у своїх філіях і дочірніх компаніях, застосовується аудит проектів впровадження реінжинірингу. Він дає змогу оцінити ризики впровадження або реінжинірингу інформаційної системи, терміни і плановані ресурси на розробку і впровадження рішень, правильність вибору методів і технологій, а також завчасно виявити можливі помилки і отримати рекомендації, направлені на підвищення ефективності проекту. У проведенні аудиту проектів впровадження і реінжинірингу входить перевірка проекту і складеного технічного завдання (ТЗ) на відповідність реальним вимогам підприємства і стандартам, перевірка виконаних робіт на відповідність технічному завданню, а також здійснюється оцінювання ефективності виконаних робіт.

Оціночний аудит інформаційних систем державні органи, а також зарубіжні партнери компанії можуть зажадати сертифікації інформаційної системи підприємства з метою відповідності послуг необхідному рівню якості. Для цього проводиться оціночний аудит інформаційних систем. У рамках оціночного аудиту інформаційної системи, як правило, виявляються відхилення від наявних стандартів і формуються рекомендації, що дозволяють усунути знайдені невідповідності.

Програмне забезпечення посідає важливе місце в інформаційній системі будь-якого підприємства. Оціночний аудит програмного забезпечення дає можливість визначити економічну ефективність від впровадження і експлуатації як певного виду

програм, так і комплексу програмних продуктів. Результати, отримані після його проведення, допоможуть підвищити економічну ефективність використання програмного забезпечення, визначити функціональність його використання й оптимальну схему впровадження, здійснити вибір найдешевшого варіанта переходу до ліцензійного програмного забезпечення, отримати рекомендації з оптимізації програмної інфраструктури.

У перелік звітності, що надається, входять опис результатів аналізу програмної інфраструктури, рекомендації із сумісності й коректності настройок програмного забезпечення та з підвищення ефективності й функціональності його використання.

Таким чином, після виконання комп'ютерного аудиту інформаційної системи аудитор отримує змогу з різних боків оцінити реальний стан комп'ютерної інформаційної системи підприємства. А це безпосередньо впливає на оцінювання аудитором системи внутрішнього контролю на підприємстві.

Загалом проведення комп'ютерного аудиту таким чином впливає на удосконалення КІСП (рис. 1.9).

Здебільшого комп'ютерний аудит інформаційних систем потрібний, коли автоматизована система призначена для обробки конфіденційної чи секретної інформації. Саме до таких належать комп'ютерні системи бухгалтерського обліку. Проведення комп'ютерного аудиту корисно також після побудови автоматизованої системи і її підсистеми безпеки на етапі приймання в експлуатацію для оцінювання ступеня дотримання висунутих до неї вимог.

Комп'ютерний аудит підприємства поліпшення
-----------------------------------------------

- засобів захисту КІСП;
- цілісності даних у КІСП;
- ефективності КІСП;
- продуктивності КІСП

*Рис. 1.9. Вплив комп'ютерного аудиту на вдосконалення КІСП*

### Тестові завдання до теми 3

1. Зазначте, які нормативні документи регламентують автоматизацію аудиту:
  - а) міжнародні стандарти аудиту;
  - б) міжнародні стандарти фінансової звітності;
  - в) положення бухгалтерського обліку.
2. Використання комп'ютерної техніки в аудиторських фірмах використовується за такими напрямками:
  - а) організаційний, контролюючий, документування;
  - б) технічний, інвестиційний, фінансовий;
  - в) контролюючий, стандартизація, нормування.
3. В умовах використання КІСП аудитор найчастіше стикається із:
  - а) безпекою даних;
  - б) організацією даних;
  - в) фінансовими питаннями.
4. Аудит технічного стану інформаційної системи спрямований на:
  - а) зменшення втрат, викликаних системними збоями;
  - б) збільшення швидкодії системи;
  - в) збільшення витрат на систему.
5. Аудит ефективності інформаційної системи дає можливість підприємству оцінити:
  - а) окупність витрат на її запровадження;
  - б) рентабельність підприємства;
  - в) витрати на систему.
6. Аудит інформаційних систем включає дослідження таких частин:
  - а) апаратних засобів;
  - б) нормативної бази;
  - в) облікової політики.

7. При аудиті інформаційних систем в аудиторську звітність включають:
  - а) аналіз програмної інфраструктури;
  - б) фінансову звітність;
  - в) податкову звітність.
8. Комп'ютерний аудит сприяє удосконаленню КІСП:
  - а) засобів захисту;
  - б) облікової політики;
  - в) програмного забезпечення.
9. Аудит інформаційних систем включає один із таких елементів:
  - а) оціночний аудит;
  - б) облікову політику;
  - в) оперативний аудит.
10. Одним із складових аудиту в умовах застосування КІСП є:
  - а) аудит інформаційної безпеки;
  - б) аудит інформаційної інформації;
  - в) аудит оперативного спрямування.

## **Тема 4. Методологія комп'ютерного аудиту**

### **4.1. Поняття методології комп'ютерного аудиту**

Впровадження комп'ютерів в обліковий процес суттєво вплинуло на проведення аудиту. При цьому велике значення мають власні характеристики системи обробки даних, тому що вони впливають на характеристику внутрішнього контролю, вибір виду перевірок, на основі яких можна визначити характер, тривалість і обсяги аудиторських процедур.

Питання зміни методології аудиту при застосуванні комп'ютерної техніки досліджувалося багатьма авторами. Професор В. П. Завгородній, зокрема, зазначав, що “в умовах функціонування інформаційних систем основні принципи аудиту зазнають деяких змін”. Професор Ф. Ф. Бутинець дещо конкретизував це питання, зазначаючи, що аудитору необхідно визначити, як саме впливають на організацію та проведення аудиту використання системи комп'ютерної обробки даних у суб'єкта господарюючого. При цьому всі автори єдині в тому, що сама мета аудиту не змінюється.

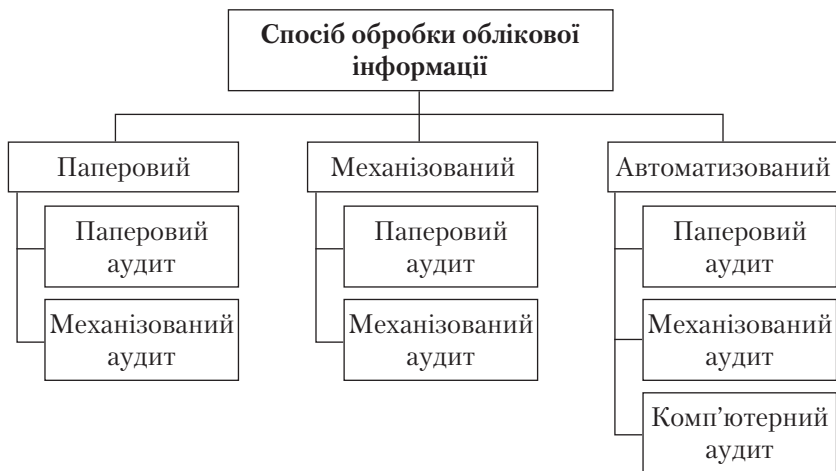
Методологія аудиту значною мірою залежить від способу обробки облікової інформації. Всі способи обробки облікової інформації в системі бухгалтерського обліку можна поділити на три види: паперовий, механізований, комп'ютеризований (автоматизований) залежно від виду обчислювальної техніки, що застосовується. При цьому перші два методи (паперовий та механізований) можна об'єднати під загальною назвою “безкомп'ютерний спосіб”, маючи на увазі не перелік технічних засобів, а саме спосіб їх використання.

При “механізації” обчислювальна техніка є допоміжним засобом для обробки інформації, а при комп'ютеризації технічні засоби стають основним засобом ведення обліку: суттєві зміни відбуваються в процесі збирання, накопичення облікової інформації, її передачі та одержання підсумкових даних. На відміну від “механізації” комп'ютеризація обліку базується на системному вирішенні облікових завдань за допомогою комп'ютерів.

Відповідно до способів обробки облікової інформації аудит теж можна умовно поділити на паперовий, механізований та комп'ютерний. При цьому спосіб обробки облікової інформації суттєво впливає на вид аудиту, який проводиться чи міг би проводитися в процесі перевірки фінансової звітності підприємства (рис. I.10).

Безкомп'ютерний спосіб обробки облікової інформації (паперовий та механізований) пов'язаний з відображенням даних про об'єкти аудиту в первинних документах та облікових регістрах, що отримуються в результаті ручної обробки інформації або обробки за допомогою певної техніки. При цьому дані фіксуються на певних носіях, а інформація, що зафіксована в документах, сприймається візуально.

В умовах паперового обліку при перевірці операцій аудитор проводить суцільну або вибіркочну перевірку. Для цього дані з первинних документів порівнюються із записами у звітах, залишки на кінець попереднього періоду – із залишками на початок наступного. Тут аудитор проводить так званий “паперовий” аудит, де комп'ютерна техніка не використовується взагалі.



*Рис. I.10. Види аудиту, що використовуються за різних способів обробки облікової інформації*



Під механізованим аудитом будемо розуміти використання аудитором комп'ютера винятково як допоміжного інструмента — наприклад, для оформлення текстів та таблиць у стандартних текстових і табличних редакторах. Як видно з рис. І.10, паперовий та механізований аудит є характерними для безкомп'ютерного способу обробки облікової інформації, тоді як комп'ютерний аудит — для автоматизованого.

Для виявлення можливих відхилень аудитор складає різні групувальні таблиці, на що витрачає багато часу. Це потребує застосування комп'ютерної техніки та програмного забезпечення для полегшення роботи аудитора. У такому випадку аудитор проводить механізований аудит, у процесі якого обчислювальна техніка є допоміжним засобом для обробки інформації.

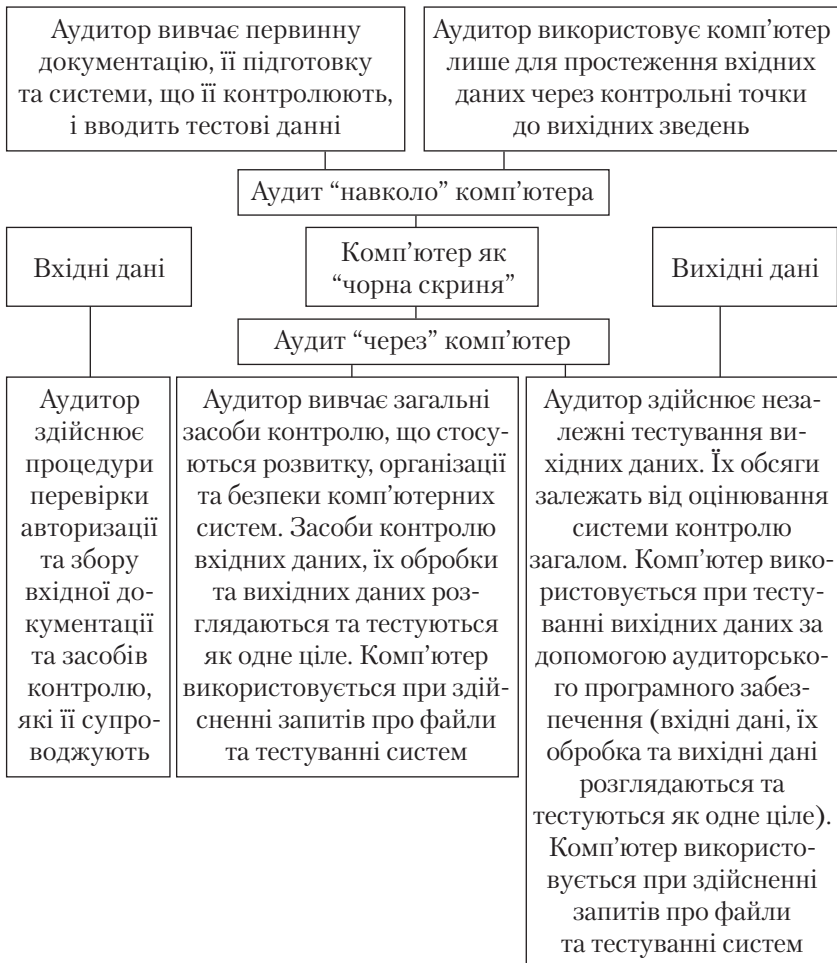
У зарубіжній літературі аудит в умовах автоматизованої обробки облікової інформації поділяють на три типи: аудит “навколо” комп'ютера (auditing around the computer), аудит “через” комп'ютер (auditing through the coputer) і аудит з використанням комп'ютера (auditing with the computer) (див. рис. І.11).

Паперовий аудит, механізований аудит і аудит “навколо” комп'ютера певною мірою ігнорують факт використання комп'ютера для обробки облікової інформації. Проте, оскільки аудиторські методи передбачають простеження шляху формування підсумкової (звітної) облікової інформації від первинних документів до залишків на рахунках і звітів і навпаки, то таке “обминання” комп'ютера можливе без втрати ефективності перевірки тільки за таких умов:

- 1) наявність очевидних аудиторських слідів (audit trail), тобто якщо для кожної господарської операції наявні належним чином оформлені паперові первинні документи, а також є роздруковані детальні журнали операцій з чіткими посиланнями на первинні документи і на відповідні показники у звітах;

- 2) операції, які обробляються, достатньо зрозумілі, прості, і взагалі обсяг оброблюваних даних порівняно невеликий;

- 3) до комп'ютерних програм є детальна документація, в якій є чіткі схеми документообігу і формування підсумкової інформації.



*Рис. 1.11. Аудит “навколо” та “через” комп’ютер*

Звичайно ці умови можуть виконуватись, коли бухгалтерський облік ведеться за допомогою окремих автоматизованих робочих місць (АРМ) за ділянками обліку, не з’єднаними між собою (механізований облік). В умовах використання комплексних КІСП усі наведені моменти не є такими очевидними.

## 4.2. Елементи аудиту при автоматизованих технологіях

Як зазначалося раніше, в умовах комп'ютерної обробки даних зберігається мета та основні елементи методології аудиту. Проте середовище комп'ютерної обробки інформації суттєво впливає на процес вивчення аудитором системи обліку та засобів внутрішнього контролю суб'єкта господарювання. Тому аудитору слід визначити, як впливають на організацію та проведення аудиту використання системи комп'ютерної обробки даних у суб'єкта господарювання, в тому числі на вивчення системи бухгалтерського обліку та внутрішнього контролю.

Щоб скласти висновок щодо фінансової звітності або інших аспектів діяльності клієнта, аудитор повинен визначити конкретні цілі проведення аудиту, досягнення яких дасть йому можливість підтвердити або спростувати (виявити неузгодженість) у фінансових документах клієнта. Встановивши конкретні цілі аудиту, аудитор прагне одержати докази на користь кожної конкретної мети перевірки або всупереч їй. Таким чином, аудитор визначає процедури, які дають йому можливість досягти конкретних цілей перевірки і підготувати позитивний висновок або виявити неузгодженість фінансових документів.

Основна мета аудиторських процедур — зібрати достатню кількість підтверджень (аудиторських доказів) на користь формування того чи іншого типу аудиторського висновку.

Термін “аудиторські докази” означає інформацію, одержану аудитором для вироблення і підтвердження думок, на яких ґрунтується підготовка аудиторського висновку та звіту. Аудиторські докази складаються з первинних документів та облікових записів, що кладуться в основу фінансової звітності, а також підтверджувальної інформації з інших джерел. Поняття аудиторських доказів та основні шляхи їх отримання наводяться у Міжнародному стандарті № 500 “Аудиторські докази”.

Цікаво, що професор Ф. Ф. Бутинець зі співавторами вважають недоцільним використання терміна “докази” в аудиті, стверджуючи, що докази — це суто юридична категорія. Можна з цим погодитися, оскільки аудитор справді не здійснює зби-

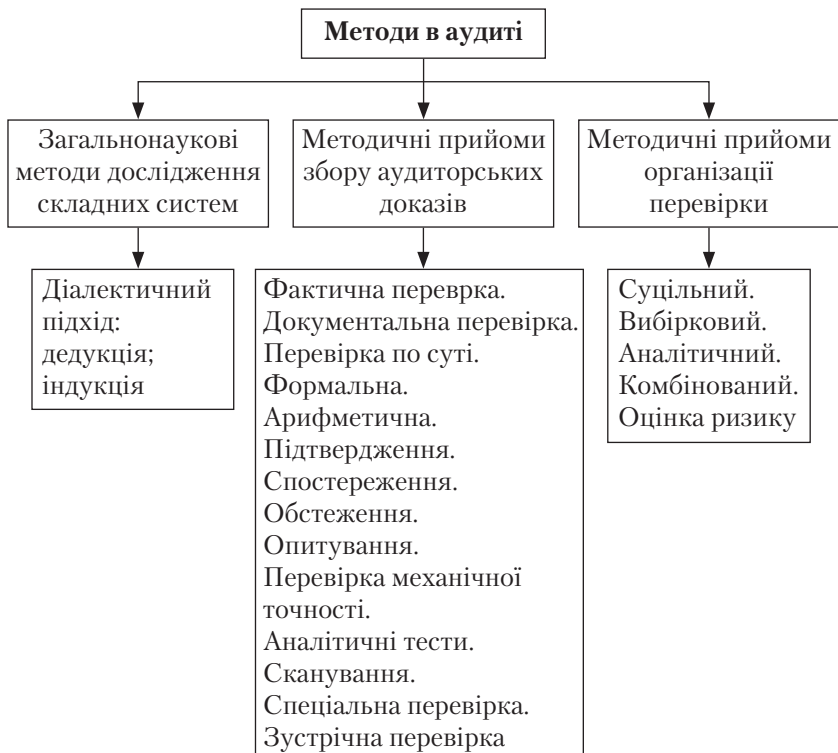
рання певної оформленої належним чином інформації, яка може бути використана в суді. Англійський термін “evidence” має кілька перекладів — може українською перекладатись не тільки як доказ, а й як свідчення. Втім, як перший, так і другий переклад мають як юридичне, так і загальне значення. Можливо, найкращим варіантом перекладу було б “підтвердження”, проте термін “докази” в російській та українській науковій літературі з аудиту вже набув значного поширення і використаний в офіційному перекладі міжнародних стандартів аудиту. Ті самі автори зазначають: “Якщо аудитор сумнівається у достовірності даних, то замовник аудиту повинен надати аудитору докази того, що такі факти відображені у фінансовій звітності відповідно до вимог, а аудитор на підставі наданої інформації формулює власну думку про достовірність фінансової звітності”. Знову йдеться про “докази”, але які має надавати аудитору замовник. Тут вже, напевно, автори монографії не мали на увазі юридично значимих доказів для подання в суді.

Аудиторські докази одержуються в результаті належного поєднання тестів систем контролю та процедур перевірки по суті, які складаються з перевірок докладної інформації про операції і залишки та аналітичних процедур.

Тести систем контролю — це перевірки, що виконуються для одержання аудиторських доказів щодо відповідності структури та ефективності функціонування систем обліку та внутрішнього контролю. Проте за деяких обставин докази можуть бути одержані тільки в результаті процедур перевірки по суті.

При плануванні та проведенні аудиторських процедур аудитор використовує певні методи (рис. І.12).

Кажучи про методи в аудиті, необхідно розрізняти застосування методів у різних площинах та класифікувати їх відповідно до цього, оскільки кожен підручник з аудиту дає свою класифікацію методів аудиту, при цьому не завжди уточнюється, про які саме методи йдеться. Наприклад, Л. П. Кулаковська називає такі загальнонаукові методи, як індукція та дедукція. Вони використовуються як діалектичний підхід дослідження складних систем, до яких належить аудит. Саме тому можна



*Рис. 1.12. Класифікація методів аудиту*

розглядати застосування дедуктивних та індуктивних прийомів в аудиті. При першому — дослідження здійснюють від загального до конкретного, при другому — від конкретного до загального. В аудиті мають значення обидва прийоми. Дедуктивний використовують при вивченні фінансово-господарської діяльності підприємства, оцінюванні напряму та ефективності системи управління, в межах якої діє об'єкт. Його також застосовують для характеристики системи внутрішнього контролю, яка включає систему внутрішнього обліку, процедури внутрішнього контролю, середовище контролю тощо. Індуктивний метод дає змогу зосередити всю увагу на окремих групах процесів, як правило, з найбільшим ступенем ризику. Вивчивши не-

доліки окремих процесів та проаналізувавши частоту їх виникнення, можна перенести результати цієї перевірки на загальну сукупність інформації, побачити цілісну проблему і сформулювати об'єктивні висновки щодо вибудованої інформації. Окрім цього, можна виділити методичні прийоми проведення збору аудиторських доказів. Їх класифікацію можна знайти у роботах Ф. Ф. Бутинця, Н. М. Малюги, Б. Ф. Усача, Л. П. Кулаковської. Методичні прийоми збору аудиторських доказів в англійських джерелах мають назву *audit procedures*, тобто аудиторських процедур.

Найповніший перелік методичних прийомів збирання аудиторських доказів наводять Ф. Ф. Бутинець та Н. М. Малюга. До них належать: фактична перевірка, підтвердження, документальна перевірка, спостереження, опитування, перевірка арифметичної точності, аналітичні процедури, сканування, обстеження, спеціальна перевірка, зустрічна перевірка тощо.

Під фактичною перевіркою розуміють огляд або підрахунок аудитором матеріальних активів (виробничих запасів, грошових коштів, цінних паперів, основних засобів тощо), тобто інвентаризацію.

Підтвердження — отримання письмової відповіді від клієнта або третіх осіб для підтвердження точності інформації (наприклад, за дебіторською заборгованістю).

Документальна перевірка — перевірка документів та записів. У практиці аудиторів використовуються такі методи документальної перевірки:

- формальна перевірка документів (правильність заповнення всіх реквізитів, наявність необумовлених виправлень, підчищень, справжність підписів посадових та матеріально відповідальних осіб);
- арифметична перевірка (правильність підрахунків у документах, облікових регістрах та звітних формах);
- перевірка документів за змістом (законність та доцільність господарської операції, правильність зарахування операції на рахунки та включення до статей звітів).

Спостереження — отримання загального уявлення про можливість клієнта на основі візуального спостереження.

Опитування — отримання письмової або усної інформації від клієнта.

Аналітичні процедури — метод порівнянь, індексів, коефіцієнтів.

Сканування — безперервний перегляд інформації за елементами (наприклад, бухгалтерськими первинними документами) з метою знайти будь-що нетипове.

Обстеження — особисте ознайомлення з проблемою.

Спеціальна перевірка — залучення спеціалістів з вузької спеціалізації.

#### **4.3. Послідовність проведення аудиту в комп'ютерному середовищі**

З метою ідентифікації і відбору бухгалтерських проводок для тестування, а також для вибору належного методу перевірки документів-підстав для цих вибраних елементів, аудитор розглядає процес складання фінансової звітності суб'єкта господарювання і тип доказів, які можуть бути одержані. Для багатьох підприємств порядок обробки операцій включає комбінацію ручних і автоматизованих етапів та процедур. Так само, обробка бухгалтерських проводок може включати як ручні, так і автоматизовані процедури і засоби контролю. Як зазначається у Міжнародному стандарті № 240, "...коли інформаційна технологія використовується в процесі складання фінансової звітності, облікові записи можуть існувати лише в електронній формі".

Детально послідовність проведення аудиту в комп'ютерному середовищі наведена на рис. І.13.

При плануванні аудиторських процедур, на які може вплинути середовище КІСП суб'єкта, аудитор повинен отримати уявлення про значимість і складність процесів функціонування КІСП, а також про доступність даних для використання при аудиті. Це уявлення охоплює такі аспекти: значимість, складність, організаційна структура, доступність даних.

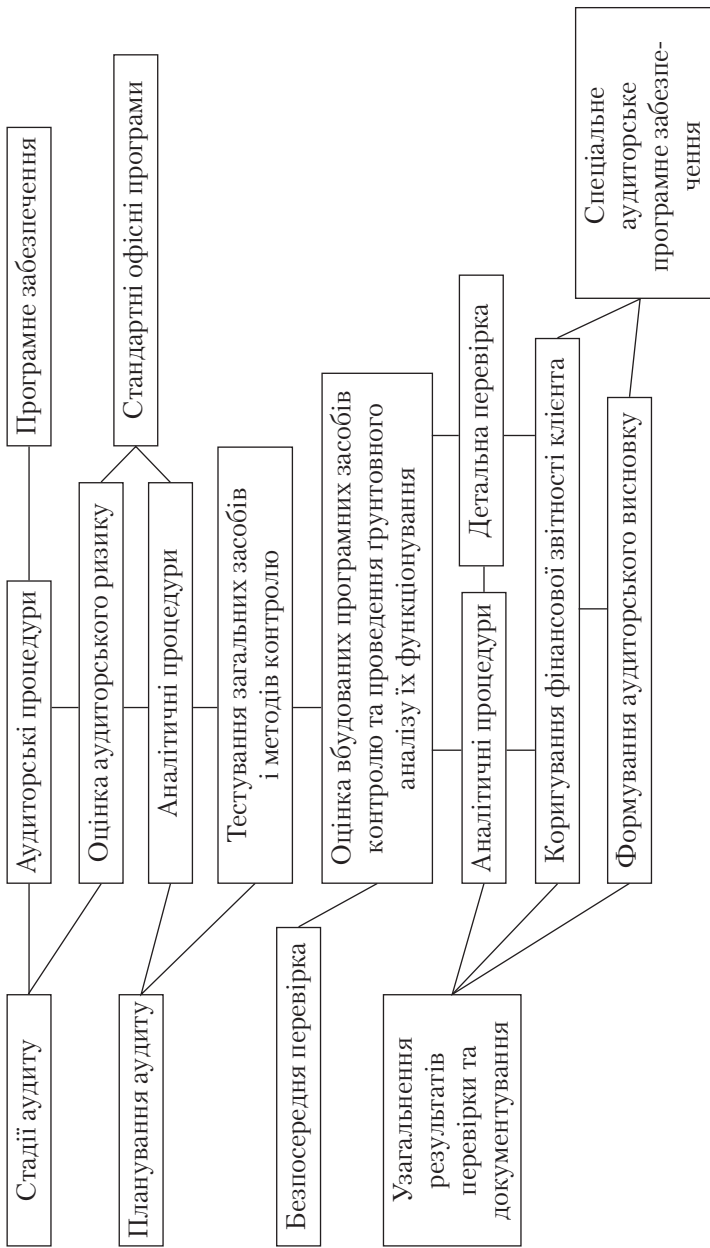


Рис. 1.13.



Значимість стосується змісту тверджень, що містяться у фінансовій звітності і підлягають комп'ютерній обробці.

Складність комп'ютерної обробки — у кожній значній прикладній бухгалтерській програмі. Прикладна програма вважається складною, якщо:

- обсяг операцій такий, що користувачам важко виявити і виправити помилки, допущені в процесі обробки;
- комп'ютер автоматично генерує суттєві операції або проводки безпосередньо в іншій прикладній програмі;
- комп'ютер виконує складні розрахунки за фінансовою інформацією і (або) автоматично генерує операції або проводки, що не можуть бути підтвержені чи не підтверджуються окремо;
- обмін операціями з іншими організаціями здійснюється електронним способом (як у системах електронного обміну інформацією), і при цьому не проводиться фізична перевірка на предмет правдивості або прийнятності.

Організаційна структура КІСП клієнта, а також ступінь концентрації або розподілу комп'ютерної обробки в рамках суб'єкта, зокрема, те, як вони можуть впливати на розподіл обов'язків.

Доступність даних. Первинні документи, деякі комп'ютерні файли й інший доказовий матеріал, що може знадобитися аудиторю, можуть існувати тільки протягом короткого періоду або у форматі, доступному для перегляду тільки на комп'ютері.

Важливу роль при плануванні аудиторської перевірки відіграє рівень автоматизації облікових задач. При оцінюванні складності автоматизованої обробки бухгалтерських даних необхідно враховувати як ступінь інтеграції інформаційних систем, так і ступінь спільного використання різними системами однієї і тієї самої облікової бази даних.

При використанні методів аудиту треба враховувати технічну структуру програмного забезпечення КСБО (див. рис. І.14).

Є дві основні причини використання такої структури. По-перше, це спрощена розробка та налагодження прикладних програм. Концептуально розробник в одному рівні має спрощене завдання, оскільки він може не вивчати деталей роботи



*Рис. 1.14. Трирівнева архітектура програмного забезпечення КСБО*

розташованого нижче шару. По-друге, це підвищена безпека і захист. Кожен рівень може створюватись і налагоджуватись різними фірмами та групами спеціалістів із застосуванням різних мов програмування, причому конкретний розробник одного рівня не може контролювати розташований нижче рівень. Отже, така структура побудови програмного забезпечення в принципі може підвищити безпеку і секретність КСБО.

#### **4.4. Аудиторський ризик при комп'ютерному аудиті**

Важливим елементом при плануванні та проведенні аудиту є оцінка аудиторського ризику. Він залежить від особливостей господарської діяльності підприємства, якості функціонування системи внутрішнього контролю підприємства. Аудиторський ризик полягає в тому, що аудитор може висловити неадекватну думку в тих випадках, коли в документах бухгалтерської звіт-

ності є значні перекручення, інакше кажучи, за неправильно підготовленою звітністю буде представлено аудиторський висновок без зауважень.

Згідно з вимогами Міжнародного стандарту № 400 “Оцінка ризиків та внутрішній контроль” аудитор повинен оцінити властивий (притаманний) ризик і ризик невідповідності внутрішньої системи контролю і управління.

Найважливішим у цьому випадку є оцінювання аудитором ризику внутрішнього контролю – ефективності системи внутрішньогосподарського контролю підприємства, тобто її спроможності попереджати і виявляти помилки на підприємстві, оцінка розміру аудиторського ризику невиявлення суттєвих помилок у звітності підприємства, який існує під час проведення аудитором аудиторських процедур, і визначення на підставі цього найважливіших напрямів аудиту.

Аудиторський ризик визначається за формулою:

$$AP = BP \cdot PK \cdot PH,$$

де AP – аудиторський ризик; BP – внутрішньогосподарський ризик (також притаманний або властивий); PK – ризик контролю; PH – ризик невиявлення.

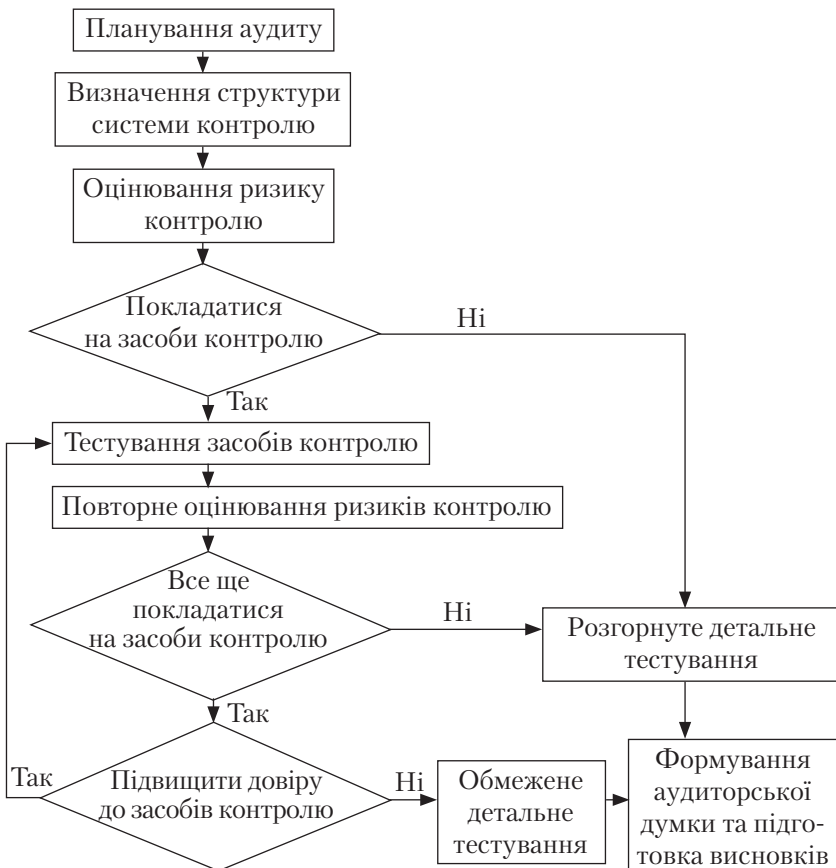
Ризик контролю виражає міру очікування аудитором імовірності пропуску помилок, що перевищують припустиму величину, системою внутрішньогосподарського контролю, тобто ризик наявності помилок в обліку після перевірки системою внутрішнього контролю. Звичайно це значення лежить у межах від 0,3 до 0,5.

Ризик невиявлення виражає міру готовності аудитора визнати імовірність невиявлення в процесі проведення аудиту помилок, що перевищують припустиму величину. Відповідно до статистики, цей ризик становить приблизно 0,1 (10 %).

Одержавши значення величини аудиторського ризику, необхідно врахувати, що він має бути прийнятним. Прийнятний аудиторський ризик виражає міру готовності аудитора визнати прийнятною імовірність наявності у фінансовій звітності суттєвих помилок після завершення аудиту і видачі клієнту аудиторського висновку. Більшість аудиторів вважають, що величи-

на прийнятний аудиторський ризик не повинна перевищувати 5 %, хоча яких-небудь офіційних норм граничного значення аудиторського ризику не встановлено.

Оцінювання ризику – складний ітераційний процес. Аудитор оцінює ризик перед проведенням аудиту. Однак якщо в процесі перевірки він виявив певні проблеми, пов’язані з функціонуванням системи контролю, то повинен скоригувати свою оцінку ризику і програму аудиту (рис. І.15).



*Рис. І.15. Циклічний алгоритм проведення аудиторської перевірки при переоцінюванні ризику системи контролю*

Комп'ютерна обробка економічних даних впливає, перш за все, на процес вивчення аудитором системи обліку і внутрішнього контролю підприємства, що перевіряється. Відповідно до вимог Міжнародного стандарту № 400 “Оцінка ризиків і внутрішній контроль” аудитор повинен оцінити властивий ризик (inherent risk) на підприємстві і ризик засобів контролю (control risk).

Відповідно до Положення про міжнародну аудиторську практику № 1008 “Оцінка ризику та внутрішній контроль: характеристики та особливості в КІС” аудитор повинен врахувати вплив ризиків використання КІС для того, щоб оптимально виконати процедури контролю і максимально понизити вірогідність надання неправильних висновків і рекомендацій. Особливості оцінювання ризиків при застосуванні КІСП і КСБО також наведені у Міжнародному стандарті 401 “Аудит у середовищі комп'ютерних інформаційних систем”.

Аудитор повинен зрозуміти, які заходи вживає суб'єкт господарювання щодо ризиків, які випливають із використання інформаційних технологій (ІТ). Використання ІТ впливає на спосіб здійснення контрольної діяльності. Аудитор розглядає, чи суб'єкт господарювання належним чином компенсував ризики, пов'язані з ІТ за допомогою створення ефективних загальних засобів контролю ІТ (Jgeneral controls) і засобів контролю прикладних програм (application controls). З погляду аудитора, засоби контролю над ІТ-системами є ефективними, коли вони підтримують цілісність інформації і безпеку даних, які ця система обробляє.

Характер ризику і характеристики внутрішнього контролю у середовищі КІСП включають:

- відсутність слідів операцій — незрозумілість шляху перетворення вхідної інформації з первинних облікових документів у підсумкові показники. Деякі КІСП спроектовані таким чином, що повний обсяг інформації про операцію, що використовується з метою аудиту, може існувати тільки протягом короткого періоду або тільки у форматі, що прочитується на комп'ютері. Якщо складна програма передбачає велику кіль-

кість етапів обробки, то повного обсягу інформації може і не бути. Побічна інформація може бути корисна для завдань контролю, але часто є можливість прочитання інформації тільки на електронних носіях, оскільки там, де складна система виконує більшу кількість кроків та завдань, неможливо простежити наявності повного набору дій. Саме тому помилки, які існують у самому алгоритмі програми, дуже складно виявити без використання спеціальних програм;

- єдину обробку операцій. При комп'ютерній обробці таких операцій застосовуються однакові інструкції. Таким чином, фактично усувається можливість помилок, що властиві ручній обробці. І, навпаки, помилки програмування (та інші помилки в технічних засобах або програмному забезпеченні) призводять до неправильної обробки всіх без винятку операцій. Зменшення участі людини у процесах обробки інформації призводить до того, що помилки і недоліки через зміни прикладних програм або системного програмного забезпечення можуть залишатися невиявленими ними тривалий час;

- відсутність поділу функцій. Багато процедур контролю, які зазвичай виконуються окремими особами вручну, можуть бути сконцентровані в КІСП. Таким чином, особа, яка має доступ до комп'ютерних програм, процесу обробки або даних, може виконувати несумісні функції. Декілька процедур управління можуть бути сконцентровані в руках одного бухгалтера, тоді як при веденні бухгалтерського обліку вручну вони були б розподілені між кількома працівниками. Таким чином, цей бухгалтер, маючи вплив на всі розділи обліку, контролює сам себе;

- можливість помилок і порушень. Можливість здійснення помилок, властивих людині, при розробці, технічному обслуговуванні й експлуатації КІС може бути більша, ніж у системах ручної обробки, частково через ступінь деталізації, властивій такій діяльності. Крім того, можливість несанкціонованого доступу до даних або зміни даних без очевидних доказів може бути більшою при використанні КІСП, ніж у системах ручної обробки даних. Менший ступінь участі людей у процесі здійснення операцій може зменшити імовірність виявлення поми-

лок і порушень. Помилки або порушення, що мають місце при розробці або модифікації прикладних програм або системного програмного забезпечення, можуть залишатися невиявленими протягом тривалого часу. Властивий (притаманний) ризик і ризик внутрішнього контролю в середовищі КІСП мають свої особливості: ризик може виникнути через неточності при розробці програми, супроводженні й підтримці програмного забезпечення системи, операцій, безпеки системи і контролю доступу до спеціальних програм управління. Розмір ризику може збільшуватися через помилки або шахрайство як у програмних модулях, так і в базах даних. Наприклад, слід вжити необхідних заходів, що попереджають виникнення помилок у системах, в яких виконується складний алгоритм розрахунків, оскільки виявити такі помилки дуже важко;

- ініціювання або здійснення операцій. КІС можуть мати здатність автоматично ініціювати або здійснювати визначені види операцій. Дозвіл на виконання таких операцій або процедур не обов'язково документально оформляється таким самим чином, як і при ручній обробці;

- можливості удосконалення управлінського контролю. КІСП може надати керівництву багато аналітичних засобів, які можна застосовувати при аналізі операцій і контролю за діяльністю суб'єкта. Наявність таких додаткових засобів контролю, у випадку їх використання, допомагає покращити структуру внутрішнього контролю загалом.

Часто масові господарські операції здійснюються у повністю автоматизованому режимі або з мінімальним втручанням людини. У таких умовах виконання тільки процедур по суті буде досить ризикованим. Наприклад, в умовах, коли суттєва кількість інформації суб'єкта господарювання ініційована, записана, оброблена або надана електронним способом, аудитор може з'ясувати, що розробка ефективних процедур по суті, які самі по собі могли б забезпечити достатні аудиторські докази щодо відсутності суттєвих відхилень в операціях або залишках на рахунках, не є можливою. У таких випадках аудиторські докази можуть бути доступними тільки в електронній

формі. Їх достатність і відповідність звичайно залежать від ефективності вбудованих у програмне забезпечення засобів контролю, їх точності й повноти. До того ж, потенціальна можливість випадків некоректного ініціювання або зміни інформації, які відбулися і не були виявлені, може бути більшою, якщо інформація ініційована, записана, оброблена або надана тільки в електронній формі й відповідні засоби контролю не діють ефективно.

Наприклад, КІСП може використовуватися для ініціювання замовлень на придбання та постачання товарів, яке базується на заздалегідь заданих правилах щодо того, що саме замовляти і в якій кількості. Потім КІСП автоматично приймає рішення щодо сплати відповідних рахунків постачальників, на підставі підтвердженого факту отримання товарів. При цьому ніяке інше документування щодо розміщених замовлень або отриманих товарів не здійснюється, окрім як через КІСП.

Суб'єкт господарювання, який надає послуги замовникам через електронні засоби (наприклад, інтернет-провайдер або телекомунікаційна компанія), також використовує КІСП для автоматичної реєстрації послуг, наданих замовникам, ініціювання бухгалтерських записів і обчислення вартості послуг.

Таким чином, використання КІСП на підприємстві створює специфічні аудиторські ризики, які тісно пов'язані з поняттям інформаційної безпеки КІСП. Інформаційна безпека досягається шляхом задоволення вимог до чотирьох груп специфічних ресурсів комп'ютерної інформаційної системи підприємства: апаратного забезпечення, програмного забезпечення, обчислювальних потужностей (наприклад, процесорного часу або місця на твердому диску) і даних.

До апаратного забезпечення у безпечній системі висувається вимога забезпечити безперервну і безпомилкову роботу програмного забезпечення (*continuity of operations*). Вимоги до програмного забезпечення аналогічні — забезпечити безперервне і безпомилкове виконання передбачених функцій (збір даних, обробка, автоматичне обчислення показників, надання даних користувачу тощо). Обчислювальні потужності мають



використовуватися тільки правомірно — для вирішення поставлених завдань.

З одного боку, найбільш цінним ресурсом інформаційної системи є інформація. Тому до інформації, що міститься в системі, висувають такі специфічні вимоги:

- конфіденційність — забезпечення надання доступу до інформації тільки уповноваженим на це користувачам;
- цілісність — гарантування точності та повноти інформації та методів обробки;
- доступність — забезпечення того, що уповноважені користувачі на свою вимогу отримають доступ до інформації і пов'язаних з нею ресурсів.

З іншого боку, інформаційну безпеку можна визначити як відсутність порушень в роботі інформаційної системи. Тому інколи вимоги до інформації визначаються як відсутність порушень в роботі системи:

- конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність — властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- доступність — властивість інформації бути захищеною від несанкціонованого блокування.

Згідно із Законом України “Про захист інформації в автоматизованих системах” порушення роботи автоматизованої (інформаційної) системи — дії або обставини, які призводять до спотворення процесу обробки інформації. Згідно з цим Законом до порушень роботи автоматизованої інформаційної системи зараховують такі загрози:

- витік інформації — результат дій порушника, внаслідок яких інформація стає відомою суб'єктам, які не мають права доступу до неї;
- втрату інформації — дії, внаслідок яких інформація перестає існувати для фізичних або юридичних осіб, які мають право власності на неї у повному чи обмеженому обсязі;

- підробку інформації — навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в автоматизованій системі;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи автоматизованої системи — дії або обставини, які призводять до спотворення процесу обробки інформації.

Як бачимо, перша загроза порушує конфіденційність інформації, друга і третя — її цілісність, четверта — доступність. Натомість п'ятий клас загроз стосується не тільки інформації, а й апаратної і програмної частин системи, її інфраструктури.

В англomовній літературі замість безпосередніх порушень роботи КІСП найчастіше розглядають можливі загрози її роботі, намагаються протидіяти саме загрозам, а не порушенням, які вже відбулись і оцінюють ризики того, що загроза матиме місце в реальності.

Під загрозою (threat) розуміють певний вчинок або подію, що може призвести до збитків. Загрозу прийнято поділяти на випадкову, або ненавмисну, і навмисну (табл. І.5).

Таблиця І.5

**Класи загроз безпеці інформації**

<b>Ненавмисний (accidental)</b>	<b>Навмисний (deliberate)</b>	
	<b>пасивний</b>	<b>активний</b>
Помилки у вхідній інформації. Порушення інфраструктури (коротке замикання, стихійні лиха, перепади струму)	Використання ресурсів не за призначенням. Несанкціонований перегляд інформації (підслуховування, шпигунство)	Крадіжка обладнання. Саботаж. Порушення апаратної або програмної інфраструктури (диверсія). Навмисний злом системи безпеки (підбір паролю). Порушення роботи веб-сайту (Denial of Service — DoS). Шкідливі програми (віруси, трояни, черв'яки)

Джерелом ненавмисних загроз (accidental threats) можуть бути некваліфіковані дії, неуважність користувачів або адміністрації, вихід з ладу апаратних засобів, помилки в програмному забезпеченні, стихійні катаклізми, бруд, пил тощо. Навмисні загрози (deliberate threats), на відміну від випадкових, мають на меті завдання збитку користувачам інформаційної системи і, в свою чергу, поділяються на активні й пасивні.

Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів системи, не порушуючи при цьому її функціонування. Пасивною загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах, за допомогою їх прослуховування. Джерелом пасивних загроз можуть бути як внутрішні користувачі системи, які не мають злого умислу, так і зловмисники ззовні, мета яких — не бути поміченими.

Активні загрози мають на меті порушення нормального процесу функціонування шляхом цілеспрямованого впливу на апаратні, програмні та інформаційні ресурси. До активних загроз належать, наприклад, руйнація або радіоелектронне придушення ліній зв'язку, виведення із ладу апаратних або програмних засобів системи, блокування обчислювальних потужностей (наприклад, мільйонами фальшивих запитів на надання інформації), внесення несанкціонованих змін до процедур обробки інформації, спотворення інформації тощо. Джерелами активних загроз можуть бути або безпосередньо зловмисники, або несумлінні чи ображені працівники, або комп'ютерні віруси та інші шкідливі програми (трояни, інтернет-черв'яки тощо).

Для зменшення рівня загроз у комп'ютерній інформаційній системі підприємства впроваджують засоби забезпечення безпеки інформаційної системи. Всі засоби безпеки можна розділити на три групи: засоби попередження порушень безпеки, засоби виявлення порушень безпеки і засоби зменшення збитків і відновлення системи після інциденту (див. табл. І.6).

## Класифікація засобів інформаційної безпеки

Тип засобу захисту	Приклад
1	2
Профілактичний	<p><i>Апаратне забезпечення:</i>  регулярні технічні огляди і профілактика апаратного забезпечення;  регулярне оновлення парку апаратних засобів;  придбання апаратних засобів у постачальника, що гарантує їх якість і технічне обслуговування;  фізичний захист від крадіжки — замок на дверях, сигналізація, прикріплення комп'ютера до столу тощо;  засоби протидії стихії або перепадам напруги: засоби пожежегасіння; герметичний, тугоплавкий або ударостійкий корпус; блок безперебійного живлення тощо.</p> <p><i>Програмне забезпечення:</i>  встановлення останніх оновлень до операційних систем (servicerepacks and hot fixes);  встановлення і підтримання в належному стані антивірусних програм;  підтримка ліцензійної чистоти програмного забезпечення.</p> <p><i>Обчислювальні потужності:</i>  визначення відповідальності за використання обчислювальних потужностей не за призначенням.</p> <p><i>Інформація:</i>  система розподілення доступу;  шифрування даних, особливо при переданні інформації;  програмний контроль інформації “на вході”, відстеження помилок одразу при введенні;  “дружній” інтерфейс програмного забезпечення, який підказує, як без помилок ввести дані;  призначення відповідальності за помилки у введених даних та за помилкове знищення даних</p>

1	2
Моніторинговий	<p><i>Апаратне забезпечення:</i>  ведення журналів роботи обладнання;  ведення журналів технічних оглядів;  сигналізація;  автоматизація обробки надзвичайних ситуацій (виклик системного адміністратора, поліції).</p> <p><i>Програмне забезпечення:</i>  ведення журналів операційних систем і прикладних програм;  регулярна перевірка цілісності програмного забезпечення за допомогою спеціалізованого програмного забезпечення.</p> <p><i>Обчислювальні потужності:</i>  ведення журналів обліку використання обчислювальних потужностей.</p> <p><i>Інформація:</i>  регулярна перевірка цілісності інформації за допомогою спеціалізованого програмного забезпечення</p>
Коригувальний	<p><i>Апаратне забезпечення:</i>  страхування апаратного забезпечення;  передбачення додаткових потужностей на випадок виходу з ладу основних.</p> <p><i>Програмне забезпечення:</i>  регулярне резервне копіювання системи;  детальне документування всіх змін алгоритмів обробки даних.</p> <p><i>Обчислювальні потужності:</i>  передбачення в інфраструктурі запасних вузлів на випадок виходу з ладу основних.</p> <p><i>Інформація:</i>  регулярна архівація</p>

Профілактичні засоби забезпечення безпеки призначені для зменшення ризику настання порушення безпеки інформаційної системи.

Моніторингові засоби призначені для виявлення фактів порушення системи безпеки. Сьогодні це є однією з найбільших проблем у забезпеченні інформаційної безпеки підприємства. Особливо складно відстежувати реалізацію пасивних загроз, які не порушують функціонування системи. Зокрема, Міністерством оборони США було проведено дослідження, в якому намагалися “зламати” 38000 власних комп’ютерів. У 65 % спроб “зламу” до комп’ютерів вдалось проникнути. При цьому було викрито лише 4 % проникнень, а зафіксовано лише 1 %. Гірше того, більшість порушень виявляють через тривалий час після самого факту порушення. А оскільки даними в інформаційних системах легко маніпулювати як до, так і після вчинення порушення, виникають складнощі з отриманням доказів того, що порушення справді відбулось.

Впорядкувати засоби захисту і полегшити управління системою інформаційної безпеки підприємства покликані аудит інформаційних систем та політика інформаційної безпеки підприємства. Аудит інформаційних систем розглянутий у параграфі 1.2. Зупинимось більш детально на політиці безпеки.

Політика безпеки є підґрунтям програми інформаційної безпеки і засобом документування та розповсюдження важливих рішень, які стосуються безпеки. У Міжнародних стандартах аудиту наводиться багато в чому аналогічне поняття “середовище контролю” (control environment). Поняття політики безпеки є неоднозначним, і дуже часто під цим розуміють тільки документацію, яка містить положення щодо безпеки певної організації. На нашу думку, політика безпеки — це набір правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію. Зокрема, правила встановлюють, в яких випадках користувач має право працювати з визначеними наборами даних. Чим надійніша система, тим більш суворою, детальною та всеохоплюючою має бути політика безпеки. Залежно від сформульованої політики можна вибирати конкретні механізми, що забезпечують безпеку системи. Політика безпеки — це активний компонент захисту, що включає в себе аналіз можливих погроз і вибір заходів протидії.

До політики безпеки входять:

- планування непередбачуваних ситуацій та стихійних лих — ненавмисних порушень безпеки (contingency planning);
- опрацювання інцидентів — навмисних порушень безпеки (incident handling);
- встановлення відповідальності за безпеку інформаційної системи.

Планування непередбачуваних ситуацій призначене для ліквідації наслідків стихійних лих; підтримання функціонування критичних процесів організації у випадку краху. Планування непередбачуваних ситуацій виконується поетапно (рис. I.16).



Основні етапи планування непередбачуваних ситуацій.  
Допоміжні цілі планування непередбачуваних ситуацій.  
Ресурси, критичні для безпеки системи.

Рис. I.16. Планування непередбачуваних ситуацій

Як бачимо, при плануванні непередбачуваних ситуацій досягається низка побічних цілей. При передбаченні випадковостей і стихійних лих збирають і обробляють інформацію, яка стосується безпеки інформаційної системи.

Опрацювання інцидентів має за мету ліквідувати та проаналізувати наслідки інциденту, а також попередження майбутніх інцидентів. Згідно з довідником Національного інституту стандартів і технологій США (National Institute of Standards and Technology – NIST) успішна система опрацювання інцидентів має задовольняти такі вимоги: чітко визначені групи людей, які вживають заходів з опрацювання інцидентів; всі члени груп обізнані з порядком дій при виникненні інциденту; наявні засоби централізованого повідомлення про інцидент; організовані експертиза та відповідні служби з опрацювання інциденту; налагоджений зв'язок з іншими групами, які можуть допомогти у випадку виникнення інциденту.

Важливим кроком у формуванні політики безпеки є визначення відповідальності за безпеку системи. Розрізняють чотири рівні відповідальності. Найвищий рівень відповідальності у керівника підприємства. Він визначає загальні положення безпеки інформаційної системи, а також розробляє нормативні документи з політики безпеки на підприємстві. Менеджер з безпеки та функціональні менеджери перебувають на другому рівні відповідальності. Перший відповідає за щоденне безпечне функціонування інформаційної системи, за впровадження на підприємстві політики безпеки; другі відповідають за безпеку системи під час виконання поточних проектів. Постачальники технологій та супровідні організації відповідають за забезпечення технологічної, інформаційної або іншої підтримки інформаційної системи. І нарешті, користувачі системи і користувачі інформації системи мають найнижчий рівень відповідальності і відповідають тільки за наслідки своїх дій при роботі з інформаційною системою.

Кожній КІСП у тому або іншому ступені притаманний ризик виникнення помилок у роботі, зокрема і у бухгалтерському обліку, через порушення їх безпеки. Для кожної системи, за-



лежно від її масштабів, структури і управління, цей ризик різний. Однак, зважаючи на сказане, можна вести мову про додаткові аудиторські ризики, пов'язані з КІСП.

При загальному розгляді аудиторських ризиків, пов'язаних із використанням підприємством-клієнтом КІСП, треба мати на увазі таке. По-перше, такі додаткові ризики можуть входити як складова до ризику контролю, якщо ми маємо на увазі КСБО. Якщо ж суттєва частина безпосередньо господарської діяльності підприємства базується на використанні модулів КІСП з оперативного обліку, тоді такі ризики є складовою і властивою ризику. По-друге, аудиторський ризик в умовах КІСП може бути як нижчий, так і вищий порівняно з паперовою бухгалтерією (залежно від дотримання або недотримання певних умов, див. рис. І.17).

Всі ризики, пов'язані з використанням комп'ютерної інформаційної системи, можна було б звести до ризиків неналежного аудиту інформаційної системи та ризиків неефективної політики інформаційної безпеки підприємства. Оскільки ці поняття є досить абстрактними і широкими, а отже, передбачають, з одного боку, дуже багато конкретних втілень і найрізноманітніших рекомендацій, а з іншого — незрозуміло, як оцінювати ризики на підприємстві, де немає першого або другого. Ми пропонуємо ризики, пов'язані з браком або неналежним функціонуванням засобів безпеки КІСП, розглядати в таких аспектах: технічному, програмному, інформаційному та організаційному.

Підвищення аудиторського ризику спричиняють порушення безпеки в кожному з цих аспектів. У таких порушень, у свою чергу, є певні передумови.

Технічні аспекти стосуються ризиків, викликаних поганою роботою апаратних засобів, браком належного технічного обслуговування і контролю. Ризик збільшується за відсутності засобів фізичної безпеки (сигналізація, замок на комп'ютері) та засобів протидії стихії (пожежна сигналізація, система пожежегасіння). Якщо комп'ютерна система децентралізована, є географічне рознесення комп'ютерних пристроїв, то ризик



*Рис. 1.17. Фактори впливу на рівень аудиторського ризику*

аудиту підвищується за рахунок введення в систему додаткової ланки — ліній зв'язку, а також за рахунок ускладнення технічного обслуговування. Ризик виникнення помилок, у свою чергу, зменшується за наявності ведення автоматичних журналів роботи системи, регулярних технічних оглядів та передбачення додаткових апаратних вузлів, які б взяли на себе функції замість пошкодженого вузла.

Програмні аспекти аудиторських ризиків можуть стосуватися двох типів. Ризики першого типу пов'язані з використан-

ням нелегального програмного забезпечення. Відомо, що законний власник ліцензії на використання програмного забезпечення бухгалтерського обліку має право одержувати допомогу і підтримку в розробника програмного продукту. Оскільки фірми-розробники ретельно відстежують всі зміни у законодавстві й нормативних актах, то вони вчасно вносять виправлення в свої програми, і часто безкоштовно або за незначну доплату надають їх своїм користувачам. Крім того, розробники операційних систем безкоштовно надають ліцензованим користувачам останні оновлення та виправлення, що часто стосуються безпеки і стійкої роботи операційних систем. Ця допомога і підтримка сприяють підвищенню надійності роботи з такою програмою, знижують аудиторський ризик. Використання ж незаконно придбаної програми підвищує аудиторський ризик, оскільки такі програми часто є застарілими версіями; у них своєчасно не коригуються алгоритми розрахунків, форми звітності й документів, користувач не має супровідної документації і не може правильно використовувати можливості програми.

Ризики другого типу можуть бути викликані помилками в алгоритмі програми, її малим тиражем, використанням не за призначенням, поганою технічною підтримкою.

Поширені програми, застосовані на сотнях підприємств і в різних умовах, як правило, не мають помилок, оскільки вони були виявлені в процесі впровадження на багатьох об'єктах і виправлені. Аудиторський ризик у цьому випадку знижується. І навпаки, в системі, створеній в одиничному екземплярі програмістом, який не має економічної підготовки, скоріше за все, є багато помилок. Природно, у такому разі підвищується ризик при аудиторській перевірці.

Аудиторський ризик збільшується, коли ненаявні або погано налагоджені організаційна політика і програмна система розподілення доступу, зокрема, у випадку, коли доступ до алгоритмів може отримати людина, яка не має на це повноважень (наприклад, програміст фірми-розробника після закінчення впровадження КІСП на підприємстві). Аудиторський ризик зменшу-

ється за наявності спеціальних програмних засобів (найпростіший приклад — архіватор WinRar або антивірус Doctor Web), які можуть перевіряти цілісність і незмінність програмного забезпечення (наприклад, за контрольною сумою).

Інформаційні аспекти аудиторських ризиків полягають у можливих помилках в інформації, тобто порушенні її цілісності. Таке порушення може бути результатом випадкових помилок у вихідних даних або навмисного їх викривлення. Цілісність може бути порушена в результаті ненавмисної зміни даних уповноваженим користувачем або як результат навмисної її підробки зловмисником-хакером. Крім того, джерелом можливих помилок може бути просто вчасно не помічене зникнення даних, які не можливо відновити. Отже, аудиторський ризик підвищують брак контролю вхідних даних, регулярних перевірок інформації на цілісність, наявність або погана робота організаційної політики і систем розподілу доступу, нерегулярна архівація інформації або її відсутність.

Крім аудиторських ризиків, що прямо впливають із використання КІСП на підприємстві, є ризики, пов'язані з персоналом, який працює з комп'ютерною інформаційною системою.

Організаційні аспекти аудиторських ризиків пов'язані з організацією обліку і контролю при використанні КІСП, викликані недостатньою підготовкою персоналу клієнта до роботи із системою обробки даних обліку, браком чіткого розмежування обов'язків і відповідальності персоналу клієнта, незадовільною організацією системи внутрішнього контролю, слабкою системою захисту від несанкціонованого доступу до бази даних або її відсутністю, утратою даних.

Оцінюючи ризики, пов'язані з використанням КІСП, слід пам'ятати, що у сучасних умовах погано навчений персонал є однією з найуразливіших ланок системи обробки даних. Аудитор повинен оцінити кваліфікацію облікового персоналу у сфері комп'ютерної підготовки, інформаційних технологій і конкретної облікової системи. Йому необхідно звернути увагу і на відношення персоналу до системи, ступінь довіри до неї. Бухгалтер, який вважає, що він швидше виконає роботу без вико-

ристання програми, очевидно погано знайомий з її можливостями і, ймовірно, робить багато помилок при обробці даних на комп'ютері.

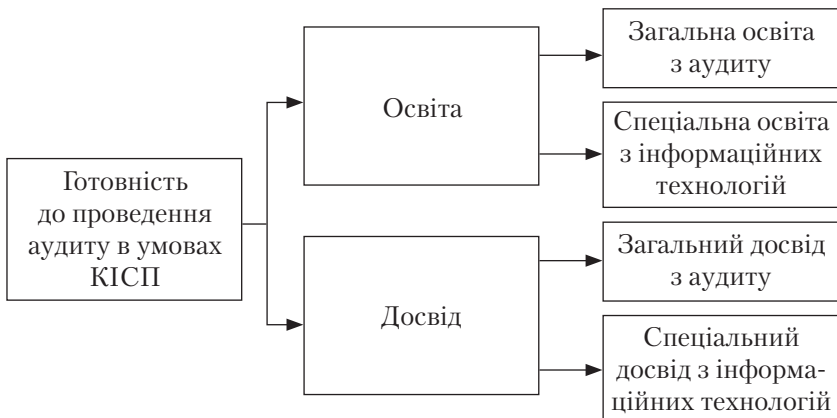
Ризики, пов'язані з кваліфікацією аудитора, можливі у зв'язку з неправильною оцінкою системи обробки облікових даних, некоректністю побудови тестів, помилковим тлумаченням результатів власне аудитором.

Застосування різноманітних комп'ютерних систем на підприємствах приводить до необхідності для аудитора одержання спеціальних знань та досвіду одночасно зі знанням методики та практики, притаманних власне аудиту фінансової Звітності (рис. I.18).

Аудитор повинен добре орієнтуватися у сучасних автоматизованих програмних системах обліку, контролю і аналізу, знати принципи розподілу функцій і взаємного контролю серед працівників, які беруть участь у процесі обробки облікової інформації.

Для проведення аудиту в комп'ютерному середовищі аудитор повинен:

- володіти додатковими знаннями в сфері систем обробки економічної інформації;



*Рис. I.18. Складові вимог до освіти та досвіду аудитора в середовищі ІТ*

- мати уявлення про технічне, програмне, математичне та інші види забезпечення КІСП;
- володіти термінологією в галузі комп'ютеризації; чітко знати особливості технології і послідовність процедур комп'ютерної обробки облікової інформації;
- знати організацію роботи бухгалтерії в умовах КІСП;
- мати практичний досвід роботи з різними системами бухгалтерського обліку, аналізу, з правовими і довідковими системами, зі спеціальними інформаційними системами аудиту.

Враховуючи різноманітність і складність комп'ютерних технологій, аудитору бажано бути першокласним фахівцем з комп'ютерного бухгалтерського обліку. Проте, якщо в аудитора немає достатніх знань, Міжнародний стандарт № 401 зобов'язав його запрошувати експерта в галузі інформаційних технологій (використання послуг сторонніх експертів регламентується Міжнародним стандартом аудиту № 620 “Використання роботи експерта”).

Основні напрями взаємодії аудитора з експертом щодо систем комп'ютерної обробки даних такі:

- оцінка законності придбання і ліцензійної чистоти бухгалтерського програмного забезпечення, яке функціонує в системі комп'ютерної обробки даних;
- оцінка надійності системи комп'ютерної обробки інформації загалом;
- перевірка правильності й надійності алгоритмів розрахунків;
- формування на комп'ютері необхідних аудитору регістрів аналітичного обліку і звітності.

Проте і в цьому випадку аудитор зобов'язаний мати достатнє уявлення про комп'ютерну систему клієнта загалом, щоб правильно планувати, направляти і контролювати роботу експерта. Слід розуміти, що експерт оцінює комп'ютерну систему обробки даних, а аудитор — достовірність інформації, яка міститься у звітності, сформованій за допомогою цієї системи.

Таким чином, використання клієнтом КІСП вносить додатковий аудиторський ризик, який розраховується за формулою:

$$R_{\text{дод}} = R_1 \cdot R_2 \cdot R_3 \cdot R_4 \cdot R_5,$$

де  $R_1$  — ризики, пов'язані з технічними аспектами;  $R_2$  — ризики, пов'язані з програмними аспектами;  $R_3$  — ризики, пов'язані з інформаційними аспектами;  $R_4$  — ризики, пов'язані з організацією обліку і контролю при використанні КІСП;  $R_5$  — ризики, пов'язані з кваліфікацією аудитора.

Ризики, пов'язані з технічними аспектами, можуть бути виражені у вигляді формули:

$$R_1 = R_{1.1} \cdot R_{1.2} \cdot R_{1.3} \cdot R_{1.4} \cdot R_{1.5} \cdot R_{1.6},$$

де  $R_{1.1}$  — ризики, пов'язані із придбанням дешевого обладнання або у ненадійних постачальників;  $R_{1.2}$  — ризики, викликані браком технічного обслуговування і контролю;  $R_{1.3}$  — ризики, викликані браком оновлення апаратних засобів;  $R_{1.4}$  — ризики, викликані браком фізичного захисту від крадіжок;  $R_{1.5}$  — ризики, викликані браком системи протидії стихійним лихам і перепадам живлення;  $R_{1.6}$  — ризики, викликані браком реєстрації роботи апаратного забезпечення.

Ризики, пов'язані з програмними аспектами, розраховуються за формулою:

$$R_2 = R_{2.1} \cdot R_{2.2} \cdot R_{2.3} \cdot R_{2.4} \cdot R_{2.5} \cdot R_{2.6} \cdot R_{2.7},$$

де  $R_{2.1}$  — ризики, викликані браком або застарілістю антивірусних програм;  $R_{2.2}$  — ризики, пов'язані з невиконанням перевірки цілісності програм і даних;  $R_{2.3}$  — ризики, викликані браком останніх оновлень в операційних системах;  $R_{2.4}$  — ризики, викликані браком ведення журналів операційних систем і прикладних програм;  $R_{2.5}$  — ризики, викликані використанням неліцензійного програмного забезпечення;  $R_{2.6}$  — ризики, викликані використанням малотиражного програмного забезпечення або придбання його у сумнівного постачальника;  $R_{2.7}$  — ризики, викликані помилками в алгоритмі програми.

Ризики, пов'язані з інформаційними аспектами:

$$R_3 = R_{3.1} \cdot R_{3.2} \cdot R_{3.3} \cdot R_{3.4} \cdot R_{3.5} \cdot R_{3.6} \cdot R_{3.7},$$

де  $R_{3,1}$  — ризики, викликані ненааявністю або неефективністю організаційної політики розподілу або системи контролю доступу до інформації;  $R_{3,2}$  — ризики, викликані відсутністю або неефективністю шифрування інформації при зберіганні та передачі;  $R_{3,3}$  — ризики, викликані відсутністю або неефективністю призначення паролів;  $R_{3,4}$  — ризики, викликані браком контролю вхідної інформації;  $R_{3,5}$  — ризики, викликані браком перевірки цілісності інформації;  $R_{3,6}$  — ризики, викликані браком контролю правильності вхідної інформації;  $R_{3,7}$  — ризики, викликані відсутністю архівації інформації.

Ризики, пов'язані з організацією обліку і контролю при використанні КІСП:

$$R_4 = R_{4,1} \cdot R_{4,2} \cdot R_{4,3} \cdot R_{4,4},$$

де  $R_{4,1}$  — ризики, викликані слабкою підготовкою персоналу клієнта до роботи з КІСП;  $R_{4,2}$  — ризики, викликані браком чіткого поділу обов'язків і відповідальності клієнта;  $R_{4,3}$  — ризики, викликані ненааявністю або неефективністю політики використання КІСП;  $R_{4,4}$  — ризики, викликані слабкою організацією системи внутрішнього контролю.

Ризики, пов'язані з досвідченістю аудитора, який працює з комп'ютерними інформаційними системами:

$$R_5 = R_{5,1} \cdot R_{5,2} \cdot R_{5,3},$$

де  $R_{5,1}$  — ризик неправильного оцінювання КІСП;  $R_{5,2}$  — ризик некоректної побудови тестів КІСП;  $R_{5,3}$  — ризик помилкового тлумачення результатів тестів.

#### **Тестові завдання до теми 4**

1. Методологія комп'ютерного аудиту значною мірою залежить від:
  - а) способу обробки облікової інформації;
  - б) форм звітності;
  - в) можливостей програмного забезпечення.
2. При механічній системі обробки інформації обчислювальна техніка є:



- а) допоміжним елементом;
  - б) основним елементом;
  - в) комбінованим елементом.
3. Автоматизований спосіб обробки інформації включає:
- а) паперовий аудит, механізований аудит, комп'ютерний аудит;
  - б) паперовий аудит, механізований аудит, внутрішній аудит;
  - в) паперовий аудит, механізований аудит, зовнішній аудит.
4. Середовище комп'ютерної обробки інформації впливає на:
- а) процес вивчення аудитором системи обліку та засобів внутрішнього контролю суб'єкта господарювання;
  - б) процес налаштування облікової політики;
  - в) практику проведення внутрішнього аудиту.
5. Основна мета аудиторських процедур:
- а) зібрати достатню кількість аудиторських доказів;
  - б) перевірити фінансову звітність;
  - в) надати позитивний аудиторський висновок.
6. Додаткові аудиторські ризики при використанні КІСП пов'язані із:
- а) використанням нелегального програмного забезпечення;
  - б) технічними пристроями;
  - в) мовою програмування.
7. Для проведення аудиту в комп'ютерному середовищі аудитор повинен:
- а) володіти додатковими знаннями у сфері обробки економічної інформації;
  - б) знати умови ведення внутрішнього аудиту;
  - в) проаналізувати нормативну базу щодо збереження інформації.

8. При використанні КІСП аудитор може використовувати:
  - а) послуги експерта;
  - б) додаткове програмне забезпечення;
  - в) технічні засоби.
9. Використання КІСП призводить до:
  - а) додаткових аудиторських ризиків;
  - б) розгалуженого внутрішнього аудиту;
  - в) ризиків невідповідності документів.
10. Одним із аспектів ризику, пов'язаних із програмними аспектами, є:
  - а) ризики, викликані браком або застарілістю антивірусних програм;
  - б) ризики невизначеності при перевірці звітності;
  - в) ризики невиявлення помилок документування.

## **Тема 5. Аналітичні процедури в комп'ютерному аудиті**

### **5.1. Визначення та необхідність аналітичних процедур аудиту**

Конкуренція на ринку аудиторських послуг приводить до того, що аудитори намагаються з метою зменшення витрат зменшувати обсяги перевірок (тестів) бухгалтерських документів по суті, застосовуючи певні процедури та методики. Серед таких методик — встановлення прийняттого рівня суттєвості та допустимого ризику невиявлення суттєвих невідповідностей, а також використання різного типу математичних та статистичних методів, зокрема вибірок. При цьому надзвичайно важливого значення для аудитора набуває процес попереднього планування аудиту, визначення витрат на перевірку та встановлення гонорару за послуги.

Аналітичні процедури є одним зі способів отримання аудиторських доказів. Проведення аналітичних процедур дає аудитору великий обсяг необхідної йому інформації і при цьому потребує набагато менше затрат, ніж для проведення детального тестування. В аналітичних процедурах можуть використовуватись, наприклад, дані, отримані з автоматизованих датчиків. Датчики вимірюють фізичний процес, наприклад, об'єм нафти, прокачаний по трубі, кубометри води або число обертів турнікета. Аудитор одержує робочі дані з датчиків і виконує процедури аналітичної перевірки, порівнюючи прогноз і фактичний результат. Скажімо, літри води, фактично використаної на автотомі, множаться на середню виручку за літр. Така процедура ґрунтується на об'єктивно отриманих даних і дає змогу досить точно оцінити валовий прибуток.

У Міжнародних стандартах з аудиту (МСА) визначено, що аналітичні процедури — це аналіз основних співвідношень та трендів, а також дослідження відхилень і зв'язків, що не відповідають сформованим очікуванням. Такий аналіз і дослідження сьогодні проводять на всіх етапах аудиту. Зокрема, на етапі

планування це дає змогу не лише зрозуміти специфіку функціонування підприємства, а й правильно оцінити обсяги аудиту, його основні напрями. Наприклад, цю думку підтримує професор В. С. Рудницький, який зазначає, що “дуже важливо ряд аналітичних процедур здійснювати на початковій стадії аудиту, оскільки це допомагає впровадити дедуктивний метод оцінювання показників Головної книги і фінансової звітності, правильно спланувати різні аспекти майбутньої роботи, виявити факти ризику тощо”.

Міжнародний стандарт МСА № 520 передбачає обов’язкове застосування аналітичних процедур на етапах планування і завершення аудиту. На стадії планування аналітичні процедури слід застосовувати для більш правильного розуміння характеру підприємницької діяльності клієнта і визначення областей потенційного ризику. Виконання аналітичних процедур протягом планування аудиту допомагає краще виявити аспекти підприємницької діяльності клієнта, які аудитору були невідомі, і визначити характер, час і рівень інших аудиторських процедур.

Аудитор повинен виконати аналітичні операції на стадії завершення аудиту, коли він формує висновок про те, чи відповідає фінансова звітність підприємства знанню аудитором його підприємницької діяльності. Висновки, зроблені в результаті таких операцій, використовують для підтвердження висновків, сформованих під час аудиту окремих частин або елементів фінансової звітності підприємства, і допомагають загалом прийти до цілісного та всебічного уявлення про достовірність фінансової звітності підприємства. Проте вони так само можуть визначити напрями та галузі, що потребують проведення додаткових процедур перевірки.

Стандартом МСА № 520 також рекомендовано використання аналітичних процедур при проведенні основних аудиторських перевірок. На цьому етапі можна проводити детальне тестування, аналітичні процедури або їх комбінацію. Характер рішення про те, які процедури використовувати для досягнення конкретних цілей аудиту, залежить від судження аудитора стосовно очікуваної ефективності та продуктивності доступ-

них процедур перевірки з погляду скорочення ризику невиявлення помилок за окремими позиціями фінансової звітності підприємства.

Останнім часом фахівці з аудиту звертають особливу увагу на необхідність оцінки аудитором можливості функціонування підприємства у майбутньому; інакше кажучи, слід оцінити, чи є підприємство потенційним банкрутом. Це пов'язано з тим, що відповідно до міжнародної аудиторської практики, якщо перевірене аудитором підприємство перестане функціонувати протягом року в результаті банкрутства, то аудитор, незалежно від того, який він надав висновок, може бути притягнений до суду. Це яскраво підтверджує припинення аудиторської практики компанією ArthurAndersen. Більше того, експерти Weiss Rating проаналізували інформацію щодо 228 великих компаній, що оголосили себе банкрутами в останні півтора року і пройшли аудиторські перевірки менше ніж за рік до банкрутства. У більшості цих компаній аудиторами були представники “великої п'ятірки” (на той час, нині це “велика четвірка” без компанії ArthurAndersen): KPMG, Ernst&Young, PriceWaterhouseCoopers, Deloitte&Touche та ArthurAndersen. Професор Нью-Йоркського університету Д. Кармайкл зазначає, що “більшість аудиторів схвалюють фінансові звіти компаній без оголошення про майбутнє банкрутство, за винятком випадків, коли важкий фінансовий стан компанії вже зовсім очевидний”. Він пояснює це тим, що “чим важливіший клієнт, тим більший тиск він чинить на аудитора”. Аудитори стверджують, що аудиторський висновок значною мірою залежить від того, яку саме інформацію керівництво компаній надає аудиторам для аналізу. Саме тому застосування аналітичних процедур може допомогти аудитору виявити викривлення або невідповідності у відображенні результатів господарської діяльності компанії.

## **5.2. Мета та цілі аналітичних процедур**

Застосування аналітичних процедур пов'язане, перш за все, з цілями аудиторської діяльності. Як зазначалося раніше, однією з цілей аудиту є визначення життєздатності підприєм-

ства, виявлення резервів кращого використання фінансових ресурсів, розробка заходів з поліпшення фінансового стану підприємства. На основі цього виникає необхідність аудиту з глибоким аналізом фінансового стану суб'єкта господарювання. Окрім цього, аналіз фінансового стану підприємства має величезне значення для аудитора, оскільки дає змогу на його основі зробити важливі висновки для цілей аудиторської перевірки.

Основною метою застосування аналітичних процедур є виявлення наявності чи відсутності незвичайних чи неправильно відображених фактів і результатів господарської діяльності, що визначають сфери потенційного ризику і потребують особливої уваги аудитора. Крім того, фахівці поділяють основну мету застосування аналітичних процедур на конкретніші цілі.

Загальна мета застосування аналітичних процедур — виявлення наявності чи відсутності незвичайних чи неправильно відображених фактів і результатів господарської діяльності, що визначають сфери потенційного ризику і потребують особливої уваги.

Конкретні цілі:

- вивчення діяльності економічного суб'єкта;
- оцінювання фінансового стану економічного суб'єкта та перспектив неперервності його діяльності;
- виявлення фактів викривлення бухгалтерської звітності;
- скорочення деталізованого тестування під час перевірки;
- забезпечення тестування з метою отримання відповідей на нез'ясовані питання.

Аудитору для проведення аналітичних процедур абсолютно необхідне знання характеру бізнесу, яким займається підприємство, галузі промисловості, в якій воно працює, характеристик окремих бухгалтерських рахунків і класів господарських операцій. Звичайно для визначення очікуваного результату аудитор використовує такі джерела інформації:

- статутні документи, рішення зборів акціонерів, результати проведення додаткових емісій акцій;

- фінансова інформація за попередні періоди, відредагована відповідно до поточних змін (наприклад, очікувана сума продаж за поточний рік може бути визначена на основі інформації про продаж минулого року, скоригована на відповідні зміни в ціні та обсягах продажу; цю суму потім порівнюють з фактичними результатами);
- очікувані результати, які можуть бути визначені з використанням планів, прогнозів шляхом екстраполяції проміжних результатів, які потім порівнюють з фактичними результатами;
- співвідношення між показниками фінансової звітності у межах певного періоду;
- галузеві статистичні показники (наприклад, загальна продуктивність може бути визначена на основі статистичних даних щодо конкретних виробничих ліній, що працюють у галузі);
- співвідношення фінансової і нефінансової інформації;
- дані бухгалтерського обліку (перш за все — Головної книги);
- аудиторські висновки за попередні звітні періоди, акти перевірки контролюючих органів, акти інвентаризацій.

Ці дані і є об'єктом, до якого застосовуються аналітичні процедури. Слід зазначити, що в аналітичних процедурах використовують не лише фінансові, а й операційні дані. Так, наприклад, обсяги продажу супермаркету значною мірою будуть залежати від загальної площі приміщень, а промислового підприємства — від потужностей виробничих ліній. Тому визначення аналітичних процедур можна доповнити, якщо зазначити, що вони складаються із порівнянь, обчислень, спостережень, перевірок, проведених для того, щоб сформувані свої очікування щодо взаємозв'язку між фінансовими та операційними даними.

При застосуванні аналітичних процедур слід враховувати ступінь їх надійності. Надійність аудиторських доказів, отриманих у результаті аналітичних процедур, залежить від:

- суттєвості величин, які розглядаються;

- інших процедур перевірки, спрямованих на досягнення тієї самої мети аудиту;
- точності, з якою можуть бути передбачені очікувані результати;
- оцінки властивого ризику та ризику відповідності внутрішнього контролю.

Важливо також зазначити, що аналітичні процедури є ефективними тільки в тому випадку, коли аудитор критично ставиться до пояснень та неочікуваних результатів, отриманих від керівництва компанії, і намагається отримати адекватні та надійні докази на користь таких пояснень.

### 5.3. Види аналітичних процедур

Розглянемо місце аналітичних процедур серед інших аудиторських процедур (рис. І.19). Серед аудиторських процедур виділяють аудиторські процедури по суті (інша назва – незалежні або самостійні аудиторські процедури). Вони належать безпосередньо до перевірки ведення бухгалтерського обліку і достовірності бухгалтерської звітності на відміну, наприклад, від контрольних аудиторських процедур, що полягають у перевірці працездатності й надійності засобів внутрішнього контролю економічного суб'єкта, якого перевіряють.

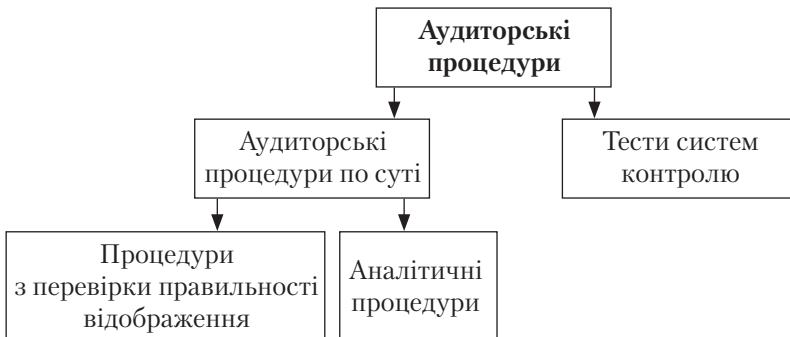


Рис. І.19. Місце аналітичних процедур серед інших аудиторських процедур



У свою чергу, аудиторські процедури по суті підрозділяють на два види. Процедури першого виду пов'язані з детальною перевіркою правильності відображення в бухгалтерській звітності оборотів і сальдо за рахунками, а процедури другого виду — це аналітичні процедури. Вони включають аналіз і оцінювання отриманої аудитором інформації, дослідження важливих фінансових та інших показників (особливо незвичайних відхилень від очікуваних значень), а також з'ясування причин їх викривлень.

Серед аудиторів і користувачів аудиту є думка, що термін “аналітичні процедури” означає лише аналіз фінансово-господарської діяльності економічного суб'єкта, який перевіряють. Проте, як правильно зазначила О. Ю. Попель, “аналітичні процедури використовують уже при оцінці вірогідності бухгалтерської звітності економічного суб'єкта, а аналіз його фінансово-господарської діяльності починається лише після того, як вірогідність встановлена, оскільки аналізувати фінансово-господарську діяльність економічного суб'єкта при невірогідності його бухгалтерської звітності безглуздо”. Інакше кажучи, аналіз фінансово-господарської діяльності економічного суб'єкта починається там, де закінчується його аудит (а отже, і аналітичні процедури). Разом з тим і аналітичні процедури аудиту, і фінансовий аналіз господарської діяльності засновані на методах економічного аналізу, тому фінансовий аналіз (аналіз фінансового стану) можна умовно віднести до заключних аналітичних процедур.

Таким чином, провівши відповідні аналітичні процедури на стадії планування та на стадії безпосереднього проведення аудиту та підтвердивши відповідно фінансову звітність, аудитор може перейти до аналізу фінансового стану підприємства. Такий аналіз дає змогу аудитору оцінити фінансовий стан компанії та тенденції її розвитку. Базою для порівняння можуть стати дані попереднього періоду, бюджетні показники, середньогалузеві дані або дані щодо компанії-аналога. Схему показників для оцінювання фінансової звітності можна подати таким чином (див. рис. І.20).

Аналіз фінансового стану підприємства				
Показники ліквідності	Показники фінансової стійкості	Показники рентабельності	Показники ділової активності	Показники інвестиційної активності
Коефіцієнт покриття. Коефіцієнт швидкої ліквідності. Коефіцієнт абсолютної ліквідності. Робочий капітал	Коефіцієнт автономії. Коефіцієнт фінансової стабільності	Рентабельність залученого капіталу. Рентабельність власного капіталу. Рентабельність активів. Рентабельність продажу. Чиста рентабельність підприємства	Коефіцієнт оборотності активів. Коефіцієнт оборотності основних засобів. Коефіцієнт оборотності виробничих запасів. Тривалість погашення дебіторської заборгованості. Тривалість погашення кредиторської заборгованості	Дохід на акцію. Ціна акції/ дохід. Дивідендний дохід. Дивідендне покриття

*Рис. 1.20. Показники для аналізу фінансового стану підприємства*

Аналіз фінансово-економічної діяльності підприємства-клієнта в процесі проведення аудиту проводять у такому порядку (табл. 1.7).

При виконанні аналітичних процедур можуть використовуватися різні методи: від простого порівняння та аналізу показників фінансово-господарської діяльності підприємства до складних математичних моделей, які включають багато співвідношень між даними за кілька попередніх років.

Такі методи статистики й аналізу, як порівняння, групування, деталізація показників, індекси, метод елімінування, балансовий, сальдовий методи тощо широко використовують при проведенні аналітичних процедур в аудиті.

**Порядок проведення аналізу фінансово-економічного стану підприємства**

<b>Процедура</b>	<b>Захід</b>
Вивчення фінансової звітності підприємства загалом	Зіставлення інформації за минулі періоди. Виявлення і аналіз фінансових співвідношень між показниками звітного періоду
Оцінювання масштабів діяльності підприємства	Визначення структури майна, джерел його утворення. Аналіз дохідності, основних джерел доходу
Виявлення незвичайних показників і сум	Вивчення облікової політики, визначення індивідуальних особливостей порядку формування звітної інформації, її вплив на звітні показники. Розрахунок фінансових коефіцієнтів, їх аналіз і порівняння з галузевими і нормативними показниками

До основних методів аналітичних процедур належать: числові і процентні порівняння; коефіцієнтний аналіз; аналіз, заснований на статистичних методах; регресійний аналіз тощо.

Застосовуючи дані методи, аудитор робить:

- порівняння фактичних показників із плановими (кошторисними; відхилення можуть свідчити про певні виробничі збої, порушення системи постачання, погіршення платіжної культури покупців);
- порівняння показників звітного періоду з показниками попередніх періодів (різкі коливання мають привернути увагу аудитора, вони можуть бути пов'язані зі зміною економічних умов чи з похибками фінансової звітності);
- порівняння фактичних фінансових показників з визначеними аудитором прогнозними показниками;
- обчислення коефіцієнтів фінансового стану організації й аналіз їх динаміки (на основі аналізу аудитор робить важливі висновки про життєздатність клієнта);

- порівняння показників економічного суб'єкта, який перевіряють, із середньогалузевими даними (значні відхилення мають бути вивчені аудитором, однак необхідно враховувати розходження в обліковій політиці підприємств, економічних умовах і можливій специфічності продукції, що її випускають окремі підприємства); у деяких випадках доцільно зробити порівняння з показниками підприємства-аналога;
- порівняння даних про клієнта з очікуваними результатами за допомогою нефінансових даних (кількість реалізованої продукції, відпрацьовані години тощо). Тут важлива впевненість у точності цих нефінансових даних.

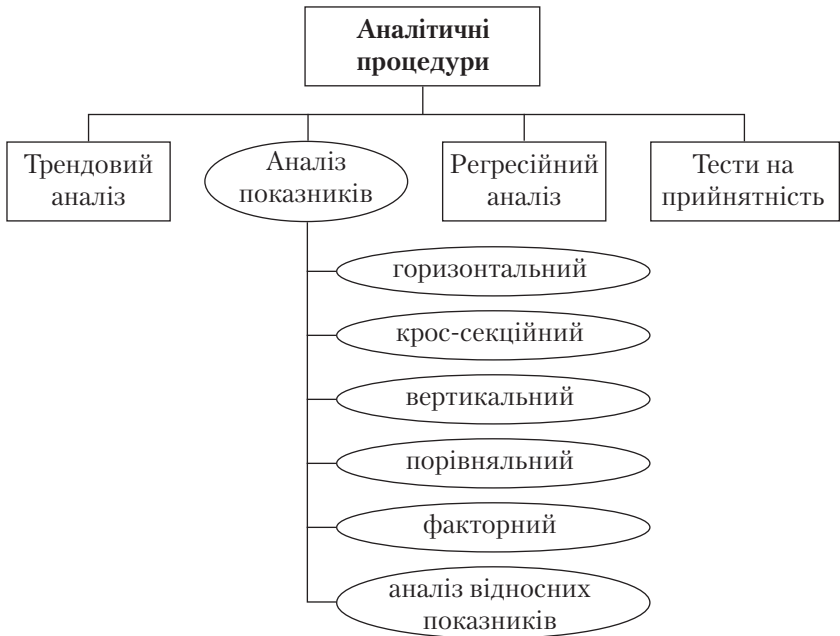
Співвідношення, які використовують в аналітичних процедурах, мають бути правдоподібні і передбачувані. Правдоподібність припускає наявність очевидного причинно-наслідкового зв'язку.

За допомогою спеціальних програмних засобів здійснюють перевірку, моделювання та аналіз облікових даних з метою визначення їх повноти, якості, правомірності й вірогідності. Для цього порівнюють змодельовані облікові дані з реальними даними інформаційної системи, а також здійснюють тестування розрахунків і перерозрахунків, підсумовують, повторно упорядковують і формують звітні дані і порівнюють їх з реальними даними. Професор Б. П. Усач таке моделювання облікових даних називає аналітичною перевіркою і зазначає, що під терміном “аналітична перевірка” слід розуміти набір таких процедур:

- аналіз співвідношень різних фінансових даних;
- порівняння фактичних даних із прогнозними, з аналогічними показниками минулих періодів, із показниками аналогічних підприємств, із середньогалузевими даними.

Процедури можуть варіюватися від простих зіставлень до комп'ютерних програм, які реалізують найновіші статистичні розробки (наприклад, множинний регресійний аналіз).

Загалом методи при застосуванні аналітичних процедур можна подати за допомогою такої схеми (рис. І.21).



*Рис. 1.21. Види аналітичних процедур в аудиті*

Трендовий аналіз (trend analysis) включає відстеження змін у бухгалтерському балансі за певний період. Наприклад, переглядаючи обсяги продажу клієнта за останні три роки, аудитор може виявити, що вони зростали на 7 % щорічно. Ця інформація допоможе сформувати певні очікування аудитора щодо щогорічних обсягів продажу. Необхідно зазначити, що трендовий аналіз варто використовувати лише в стабільному середовищі, коли на підприємстві не відбуваються суттєві поточні зміни. Крім того, такий аналіз буде більш ефективним, якщо працювати з дезагредованими даними. Наприклад, трендовий аналіз за видами продукції і відокремленими підрозділами або за кварталами і місяцями є більш точним і ефективним, ніж за агрегованими даними.

Аналіз показників (ratio analysis) включає порівняння співвідношень між двома або більше статтями фінансової звітності

клієнта (наприклад, собівартість проданої продукції до вартості запасів для визначення коефіцієнта оборотності запасів) або порівняння бухгалтерських балансів з нефінансовими даними (наприклад, дохід від проданої продукції до загальної кількості замовлень). Традиційні фінансові показники звичайно поділяють на показники: ліквідності, фінансової стійкості, прибутковості та ділової активності підприємства (детальніше ми їх розглянемо далі). Саме через те, що аналіз показників включає вивчення співвідношень між двома або більше змінними, він є більш глибокою формою аналізу, ніж трендовий.

Як видно з рис. I.21, аналіз показників поділяють на горизонтальний, крос-секційний, вертикальний, порівняльний, факторний і аналіз відносних показників.

Горизонтальний аналіз охоплює порівняння фінансових показників та змін за статтями бухгалтерського балансу підприємства-клієнта в часі. Горизонтальний аналіз звітності полягає в побудові однієї або кількох аналітичних таблиць, в яких абсолютні показники доповнено відносними — темпами зростання або зниження.

Крос-секційний аналіз передбачає порівняння фінансових показників компанії клієнта із показниками подібних компаній на певний момент, тобто із середніми значеннями по галузі.

Вертикальний аналіз — вивчення структури підсумкових фінансових показників з вивченням впливу кожної позиції звітності на загальний результат. Перевага вертикального аналізу полягає в тому, що в умовах інфляції відносні величини показників бухгалтерського балансу на початок і кінець року легше порівняти, ніж абсолютні величини цих показників.

Порівняльний аналіз — це внутрішньогосподарський аналіз зведених показників звітності за окремими показниками підприємства, дочірніх підприємств, підрозділів, цехів.

Факторний аналіз — аналіз впливу окремих факторів на результативний показник за допомогою детермінованих або стохастичних прийомів дослідження. Факторний аналіз може бути як прямим, тобто розчленуванням результативного показ-

ника на складові, так і зворотним, тобто поєднанням окремих елементів у загальний результативний показник.

Аналіз відносних показників — розрахунок співвідношень між окремими позиціями звіту чи позиціями різних форм звітності, визначення взаємозв'язку показників.

Кожний із наведених показників можна розписати як формулу, що складається з відповідних показників балансу та звіту про фінансові результати. На основі цих формул можна створити комп'ютерну програму, яка надавала б можливість проводити аналіз фінансового стану підприємства, при цьому автоматично б формувала за певним алгоритмом висновки про фінансовий стан.

Тест на прийнятність (reasonableness test) є більш складним аналітичним методом, який застосовує аудитор. Він полягає у використанні статистичних моделей для визначення очікувань аудитора стосовно статей фінансової звітності з використанням фінансової та нефінансової інформації. Наприклад, аудитор може використати середній показник завантаженості готелю та середній показник прибутку з кімнати, щоб оцінити доходи готелю за певний період.

Регресійний аналіз (regression analysis) подібний до тесту на прийнятність у тому, що він полягає в побудові статистичних моделей для визначення очікувань аудитора стосовно статей фінансової звітності. Проте якщо під час тесту на прийнятність можуть будувати моделі у вигляді простих математичних формул, то під час регресійного аналізу використовують складні регресійні методи. Регресійний аналіз має перевагу порівняно з іншими аналітичними методами у тому, що його можна використовувати для прогнозування статей фінансового звіту підприємства, при тому що надійність і правильність очікувань аудитора можуть бути достатньо точно визначені.

Для проведення регресійного аналізу необхідно, насамперед, встановити певний взаємозв'язок між змінними, тобто визначити, які незалежні фактори впливають на залежну змінну, яку необхідно спрогнозувати. Наприклад, на дохід від реалізації певного магазину можуть впливати його місце розташуван-

ня, певні економічні реалії (дохід населення), витрати на рекламу.

Таку розроблену модель називають регресією і оцінюють за допомогою спеціальних методів для того, щоб потім на її основі спрогнозувати залежну змінну на певний заданий період. Потім такі прогнознi дані порівнюють з фактичними, і якщо відхилення будуть незначними, проведені аналітичні процедури можна вважати аудиторським доказом на користь достовірності облікових даних клієнта. Якщо ж відхилення будуть суттєвими, аудитор повинен з'ясувати їх причину і, якщо потрібно, провести детальніші аудиторські процедури. Загалом схему такої аналітичної процедури можна подати таким чином (рис. I.22).

Звичайно ж, регресійне моделювання у таких аналітичних процедурах проводять за допомогою спеціальних програмних засобів, що значно спрощує ці процедури і підвищує ефективність їх виконання.

Важливою відмінністю тесту на прийнятність та регресійного аналізу від трендового аналізу та аналізу показників є те, що їх можна використовувати не лише в стабільному середовищі,

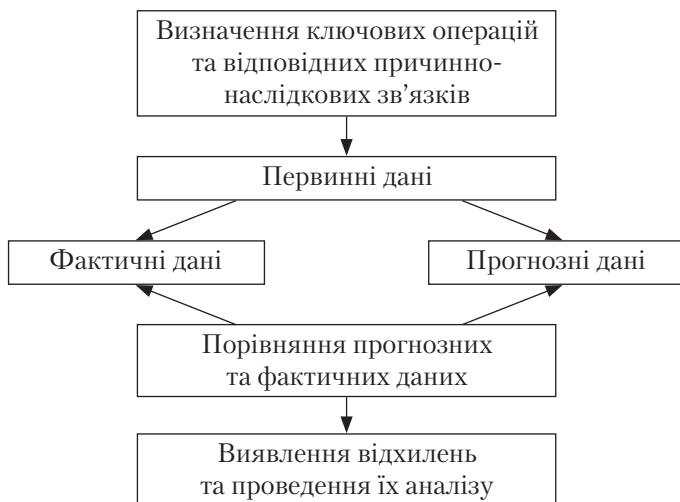


Рис. I.22. Регресійне моделювання в аналітичних процедурах



оскільки тут застосовують певні визначені зв'язки між показниками. Очікування щодо одного показника будують на основі фактичних змін іншого показника, різкі коливання якого вже не є такими критичними.

Ще одним важливим методом аналітичних процедур є аналіз руху грошових коштів (*cash-flow analysis*). Необхідність такого аналізу викликана тим, що не завжди певні операції на підприємстві пов'язані з рухом грошових коштів, але саме ліквідність підприємства є одним із найважливіших показників. Так, наприклад, дохід від продажу продукції може бути значним саме за рахунок високої дебіторської заборгованості, тоді як надходження грошових коштів може просто не відбуватися. Для виявлення такого фактора потенційного ризику варто проаналізувати рух грошових коштів від операційної діяльності до витрат на поповнення обігових коштів та процентних виплат.

Також можна проаналізувати зв'язок між чистим доходом підприємства та його грошовими потоками у часі, а також сформулювати очікування щодо майбутніх грошових потоків підприємства.

Якщо грошовий потік від операційної діяльності є негативним або суттєво відрізняється від чистого доходу, необхідно провести аналіз, щоб зрозуміти, чим викликана така ситуація. Так, у періоди швидкого зростання обсягів бізнесової діяльності дефіцит обігових коштів трапляється досить часто. Проте можлива й інша ситуація, коли брак грошових коштів стає хронічним через погане управління активами і пасивами. Тоді ризик того, що активи переоцінені, а пасиви недооцінені зростає, і аудиторів необхідно проводити додаткові процедури.

Накопичення ділової інформації у КІСП за певний період може дозволити використання аналітичного програмного забезпечення для визначення основних тенденцій, зсувів, відхилень у даних, які відображають зміни в бізнесі, діловому середовищі, складі клієнтів, економічній ситуації, конкурентному середовищі тощо. Такий аудиторський аналіз основних тенденцій в даних може бути орієнтований на пошук відхилень, які

можуть сигналізувати про потребу відкоригувати критерії для відбору господарських операцій для детальної перевірки.

Загалом можна зробити висновок, що аналітичні процедури є надзвичайно ефективним методом аудиту, оскільки вони потребують значно менших затрат часу, ніж, наприклад, детальне тестування, натомість дозволяють отримувати досить чіткі й точні аудиторські докази. Проте тут слід зазначити, що аналітичні методи не можуть замінити собою певні процедури аудиту, такі як отримання підтверджень від третіх осіб щодо дебіторської та кредиторської заборгованостей, інших активів та пасивів, інвентаризації тощо. Тому для отримання повних і достатніх аудиторських доказів варто поєднувати аналітичні процедури з іншими методами аудиту. Головне, щоб таке поєднання було найоптимальнішим з погляду ефективності.

### **Тестові завдання до теми 5**

1. Аналітичні процедури — це:
  - а) один із способів отримання аудиторських доказів;
  - б) підвищення ефективності аудиторських послуг;
  - в) робочі документи аудитора.
2. Проведення аналітичних процедур дає аудитору:
  - а) великий обсяг інформації, отриманий із додаткових технічних засобів;
  - б) масштабні свідчення працівників підприємства клієнта;
  - в) додаткове проведення аудиторських послуг.
3. Аудитор повинен виконати аналітичні операції на стадії:
  - а) завершення аудиту;
  - б) планування аудиту;
  - в) ознайомлення із господарською діяльністю підприємства.
4. Загальна мета застосування аналітичних процедур — це:
  - а) виявлення економічних резервів підприємства;
  - б) виявлення організаційних заходів проведення аудиту;
  - в) невиявлення ризиків аудиту.

5. Аналітичні процедури пов'язані з:
  - а) цілями аудиторської діяльності;
  - б) етапами планування аудиторської діяльності;
  - в) формуванням аудиторського звіту.
6. До показників фінансової стійкості відноситься:
  - а) коефіцієнт автономії, коефіцієнт фінансової стабільності;
  - б) коефіцієнт покриття, коефіцієнт швидкої ліквідності, коефіцієнт абсолютної ліквідності, робочий капітал;
  - в) дохід на акцію, ціна акції (дохід), дивідендний дохід, дивідендне покриття.
7. Горизонтальний аналіз звітності передбачає:
  - а) порівняння показників за часом;
  - б) порівняння показників як структурного відношення;
  - в) розрахунок коефіцієнтів покриття.
8. Вертикальний аналіз звітності передбачає:
  - а) вивчення структури показників;
  - б) порівняння показників за часом;
  - в) розрахунок показників ліквідності.
9. Факторний аналіз є:
  - а) визначенням впливу на результативний показник;
  - б) розрахунком структури фінансових показників;
  - в) елементом вертикального аналізу.
10. Аналіз відносних показників — це:
  - а) розрахунок співвідношень між окремими позиціями звіту;
  - б) елемент вертикального аналізу;
  - в) порівняння показників за часом.

## **МЕТОДИКА І ПРАКТИКА КОМП'ЮТЕРНОГО АУДИТУ**

---

### **Тема 6. Аудит в умовах застосування комп'ютерних облікових систем**

#### **6.1. Аудит середовища КІСП**

Організація аудиту в умовах комп'ютерної обробки даних потребує перевірки функціонування самої автоматизованої інформаційної системи шляхом тестування засобів контролю, які діють у цій системі.

Міжнародні стандарти аудиту виділяють два поняття, пов'язані із використанням інформаційних технологій на підприємствах — середовище комп'ютерних інформаційних систем і середовище комп'ютерних інформаційних технологій.

Середовище комп'ютерних інформаційних систем (Computer information systems (CIS) environment) наявне тоді, коли комп'ютер будь-якого типу або розміру використовується суб'єктом господарювання для обробки фінансової інформації, суттєвої для аудиторської перевірки, незалежно від того, чи цей комп'ютер використовується самим суб'єктом господарювання або третьою стороною. Середовище інформаційних технологій (IT-environment) — це політика і процедури, які застосовує суб'єкт господарювання й IT-інфраструктура (технічні засоби, операційні системи тощо), а також прикладне програмне забезпечення, що він використовує для забезпечення господарської діяльності й досягнення стратегічних цілей бізнесу. Очевидно, перше стосується КСБО, друге — КІСП.

В умовах застосування КІСП і КСБО організація і методика проведення аудиту суттєво змінюється, оскільки здійснення її

за методиками, орієнтованими на паперовий облік, не дає необхідного результату. Застосування КІСП впливає:

- на процедури, які використовує аудитор у процесі отримання достатнього уявлення про системи бухгалтерського обліку і внутрішнього контролю підприємства;
- на процес оцінювання властивого ризику (inherent risk) і ризику системи засобів контролю (control risk);
- на розробку і здійснення аудитором тестів системи контролю і процедур перевірки по суті, необхідних для досягнення мети аудиту — формування аудиторського висновку.

На практиці можуть виникнути такі можливі варіанти застосування комп'ютерів в обліку та аудиті (табл. II.1).

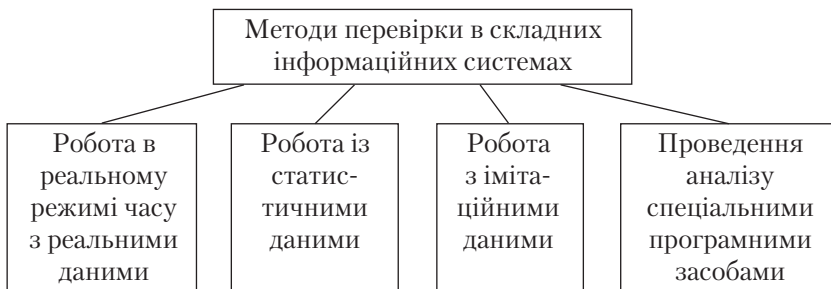
Таблиця II.1

**Можливі ситуації при аудиті**

<b>№ пор.</b>	<b>Варіант</b>	<b>Підприємство-клієнт</b>	<b>Аудитор</b>
1	Використання комп'ютерних інформаційних технологій	Ні	Так
2	Використання комп'ютерних інформаційних технологій	Так	Ні
3	Використання комп'ютерних інформаційних технологій	Так	Так

Проведення аудиту в умовах використання комп'ютерних систем (варіанти 2, 3) регламентується Міжнародним стандартом № 401 “Аудит в середовищі комп'ютерних інформаційних систем” і низкою відповідних Положень про міжнародну аудиторську практику, які розкривають різні аспекти проведення аудиту в середовищі комп'ютерних інформаційних систем, дають оцінку аудиторських ризиків, а також встановлюють вимоги до знань аудиторів про комп'ютерні інформаційні системи. Метою цих нормативів є встановлення стандартів і надання рекомендацій щодо процедур, які необхідно використовувати при проведенні аудиту в умовах комп'ютерних інформаційних систем.

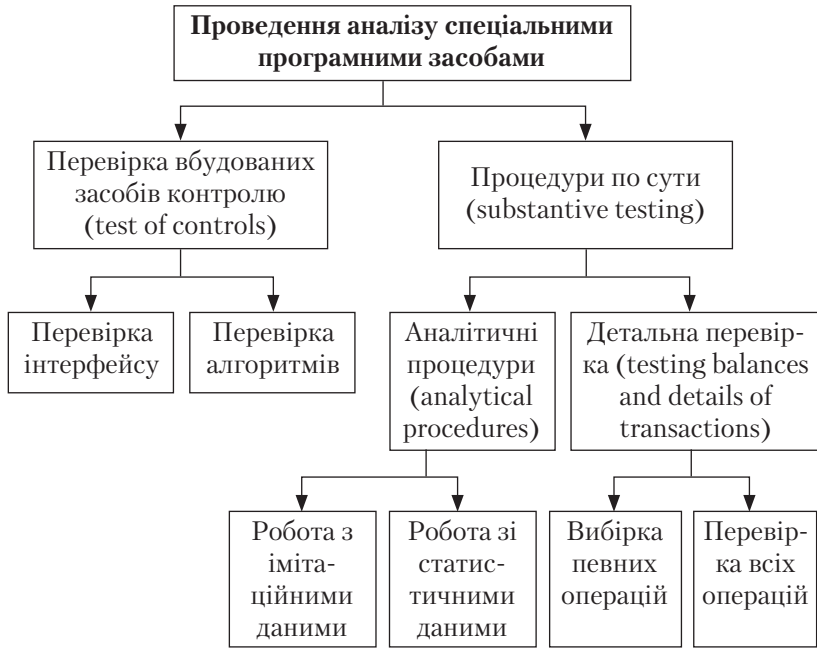
Професор В. П. Завгородній поділяє засоби і методи, що застосовуються для аудиторської перевірки в складних інформаційних системах, на такі групи (рис. II.1).



**Рис. II.1. Групи методів перевірки в складних інформаційних системах**

Цей поділ, по суті, відокремлює механізований аудит від комп'ютерного. За такою схемою нині працюють всі великі світові аудиторські компанії. В Україні комп'ютерна техніка сьогодні є лише допоміжним інструментом під час проведення аудиту і в безпосередньому процесі аудиторської перевірки використовується вкрай рідко. Це пов'язано з багатьма причинами, основними з яких є значні капіталовкладення, необхідність спеціальних знань та велика різноманітність облікових систем обробки даних, що їх використовують підприємства-клієнти. Деталізувати способи і методи використання комп'ютерної техніки у самому процесі проведення аудиторських процедур (тобто використання спеціальних програмних засобів) можна за допомогою такої схеми (рис. II.2).

Процедури аудиторської перевірки поділяються на три великі групи: тестування засобів контролю, аналітичні процедури та детальні перевірки (процедури по суті). При застосуванні двох останніх типів процедур можна використовувати спеціальне програмне забезпечення, що значно збільшує надійність отриманих результатів та ефективність виконуваної роботи.



*Рис. II.2. Методи перевірки в складних інформаційних системах за допомогою спеціальних програмних засобів*

## **6.2. Фактори, що впливають на проведення аудиту**

Проведення аудиту в умовах автоматизованих систем обліку залежить від таких факторів: рівня автоматизації бухгалтерського обліку та контролю, наявності методик проведення автоматизованого аудиту, ступеня доступності облікових даних, складності обробки інформації. При цьому велике значення мають власні характеристики системи обробки даних, тому що вони впливають на ступінь розробки бухгалтерської системи, тип внутрішнього контролю, вибір виду перевірок, на підставі яких можна визначити характер, тривалість і обсяги аудиторських процедур.

Як вже зазначалося, під час планування аудиторських процедур, на які може впливати середовище КІСП підприємства,

що перевіряється, аудитор зобов'язаний розглянути, яким чином використання КІСП впливає на аудит, і оцінити значущість (significance) і складність (complexity) процесів функціонування КІСП, а також доступність даних КІСП для використання в аудиті.

Далі аудитор вивчає структуру КІСП клієнта, зокрема ступінь концентрації або розподілу комп'ютерної обробки даних у рамках суб'єкта господарювання, її вплив на розподіл обов'язків виконавців і доступність комп'ютерних даних для безпосереднього вивчення. Первинні документи, комп'ютерні файли й інша інформація, необхідна для складання аудиторських доказів, можуть існувати тільки протягом короткого періоду або у форматі, доступному тільки для перегляду на комп'ютері. У цьому випадку аудитор застосовує спеціальні методи дослідження інформації.

Під час перевірки аудитор слід вивчити й оцінити систему документообігу економічного об'єкта, порядок формування, реєстрації, збереження, обробки документів і трансформації первинних документів у систему записів на бухгалтерських рахунках. Варто з'ясувати місця виникнення первинної інформації і ступінь автоматизації її збору і реєстрації. При використанні спеціальних засобів автоматизації збору і реєстрації інформації (датчиків, лічильників, ваг, сканерів штрихових кодів тощо) аудитор повинний переконатися в тому, що тестування цих пристроїв фахівцями проводиться регулярно, при виявленні відхилень результати належним чином оформлюють і вживають відповідних заходів.

Перше уявлення про рівень автоматизації складання первинних документів аудитор може отримати і при знайомстві зі схемою розташування автоматизованих робочих місць (АРМ) на підприємстві. АРМ, розташовані в місцях виникнення первинної інформації (на складах, у цехах), дають змогу скласти первинний документ у момент здійснення операції, зафіксувати інформацію на машинному носії, передати документ у бухгалтерію для подальшої обробки. Відсутність АРМ у виробничих підрозділах підприємства свідчить або про ручний спосіб



складання документів з подальшою передачею їх у бухгалтерію, або про те, що документи формуються у самій бухгалтерії, що характерно для підприємств із невеликим обсягом документів.

Аудитор зобов'язаний оцінити, наскільки модель документообігу, реалізована програмним забезпеченням КІСП, раціональна і ефективна для об'єкта, який перевіряють. Великі підприємства звичайно працюють із застосуванням моделі повного документообігу. Для них важливо проаналізувати розподіл функцій між службами оперативного управління і бухгалтерією, інформаційні зв'язки різних підрозділів з бухгалтерією, простежити рух окремих документів і їх взаємозв'язок, зрозуміти, як підтримується система міждокументальних зв'язків, де зберігаються електронні копії документів, і як забезпечений до них доступ облікових працівників.

На підприємствах, які автоматизують тільки бухгалтерський облік, аудитору необхідно звернути увагу на такі моменти:

- дотримання часового інтервалу між виписуванням документа, здійсненням операції і відображенням її в обліку;
- можливість збереження документів у системі після їх роздрукування;
- зв'язок документів і сформованих бухгалтерських проводок.

Аудитор повинен дати характеристику способам введення даних і формування записів про господарські операції. З одного боку, автоматизована й автоматична генерація бухгалтерських записів і проводок на основі типових операцій і електронних форм документів часто дає можливість уникнути багатьох помилок, що неминучі при ручному веденні й формуванні проводок. Слід вивчити організацію збереження інформації про господарські операції, можливість швидкого одержання інформації про господарські операції, документи і виведення її на друк.

З іншого боку, у комп'ютерному обліку ряд операцій, таких як нарахування відсотків, закриття рахунків, визначення фінансового результату може ініціюватися самою програмою. Отже, за такими операціями може не бути будь-яких організа-

ційно-розпорядчих або виправдовувальних документів. У такому разі обов'язок аудитора — ретельно перевірити правильність алгоритмів розрахунків. Помилка, закладена в алгоритм розрахунку і повторена багато разів у повторюваних господарських операціях, може спотворити результат господарської діяльності. У процесі перевірки алгоритмів розрахунку сум при веденні господарських операцій контролюється також правильність формування проводок. Особливо ретельно перевіряються алгоритми операцій, що ініціюються самою програмою.

Аудитору слід перевірити алгоритм на відповідність чинному законодавству і обліковій політиці підприємства і з'ясувати можливість коригування алгоритму у випадку зміни порядку ведення бухгалтерського обліку, податкового або іншого законодавства. Як вже наголошувалося, тестування алгоритмів ставить високі вимоги до комп'ютерної підготовки аудитора. Бажано, щоб він розумів мову програмування (або вбудовану мову для створення облікових алгоритмів — макромову) конкретної програми. Це дасть йому змогу не тільки провести тестування алгоритму на конкретних даних, а й розібратися у правильності його налагодження.

В обов'язки аудитора входить оцінювання можливостей системи, що використовується клієнтом щодо створення і формування нових форм внутрішньої або зовнішньої звітності: розгляд механізмів роботи з первинною інформацією, можливостей її розшифровки, швидкого виявлення і виправлення помилок; проведення тестування результатів обробки, щоб знайти, наприклад, неправильно розраховане сальдо на рахунках; тестування перенесення облікових даних у звітність, особливо в тому випадку, якщо показники форми звітності в системі заповнюються “вручну” перенесенням зі сформованих програмою стандартних звітів (облікових реєстрів).

Особлива увага приділяється перевірці надійності засобів внутрішнього контролю в середовищі комп'ютерної обробки даних. Облікова політика, що орієнтується на автоматизовану інформаційну систему бухгалтерського обліку, має обов'язково передбачати елементи внутрішнього контролю. Аудитор пови-

нен виявити слабкі місця стосовно контролю системи комп'ютерного обліку — розглянути як апаратні, так і програмні засоби контролю, а також організаційні заходи перевірки цілісності даних і відсутності комп'ютерних вірусів.

Засоби і методи контролю в КІСП значно відрізняються один від одного: деякі з них покликані запобігати помилкам (preventive), а призначення інших — виявляти та виправляти їх (detective). К. Кловз розділяє засоби і методи контролю залежно від того, чи аудит проводиться з перевіркою комп'ютерних процесів обробки даних (audit through the computer), чи без нього (audit around the computer). Інші автори поділяють такі засоби контролю відповідно на автоматизовані (automated) або ручні (manual).

Е. Вульф поділяє засоби контролю (controls) на дві основні групи:

1) засоби контролю прикладних програм (application controls). Це засоби контролю всередині прикладної програми, які перевіряють точність вхідних даних, обробки даних та достовірність облікових вхідних даних. Ці засоби становлять комбінацію ручних та комп'ютерних процедур. Вони не є окремими програмними продуктами, а є частинами комп'ютерних програм, які допускають здійснення процедур контролю;

2) загальні засоби контролю (general controls). Ці засоби контролю забезпечують середовище прикладних програм та ефективну діяльність програмних процедур. Загальні засоби контролю, у свою чергу, поділяються на адміністративні засоби (administration controls), які попереджають ризики того, щоб повноваження з обробки інформації не концентрувались в одних руках, дані зберігались децентралізовано і на безпечних носіях інформації; а також на засоби контролю розробки (system development control), які передбачають обов'язкове використання стандартів і стандартних процедур (де це можливо) при творенні комп'ютерних інформаційних систем, створення засобів контролю доступу тощо.

Види засобів контролю інформаційних систем за Дж. Чемп-лейном такі:

- засоби контролю оточення (environmental controls) — це політика, стандарти, організація відділу ІТ, а також фінансове становище сервісних організацій і постачальників, надані ними гарантії, умови сервісних контрактів;
- засоби фізичного контролю (physical security controls) — фізичний захист апаратного забезпечення;
- засоби логічного контролю (logical security controls) — вбудовані в операційну систему та прикладні програмні засоби для перешкоджання нелегальному доступу до даних та навмисному або випадковому їх пошкодженню;
- засоби контролю функціонування інформаційної системи (information system operating controls), які допомагають переконатися, що інформаційна система працює ефективно, тобто належним чином виконує свої функції.

Можуть бути й інші класифікації засобів і методів контролю комп'ютерних систем. Так, наприклад, Сп. Пікетт і Дж. Вінтен поділяють їх на такі, що забезпечують підтримку комп'ютерної системи (support), засоби контролю прикладних програм (applications) та стандарти, яких треба дотримуватись при розробці комп'ютерних систем.

Відповідно до Міжнародних стандартів аудиту, класифікація засобів і методів контролю КІС може бути узагальнена за допомогою такої матриці (рис. II.3).

Відповідно до Міжнародних стандартів аудиту, загальні засоби ІТ-контролю (General IT-controls) — це методики і процедури, які стосуються багатьох прикладних програм і забезпечують ефективне функціонування засобів контролю прикладних програм, допомагаючи гарантувати постійне належне функціонування інформаційних систем. Загальні засоби ІТ-контролю звичайно включають засоби контролю над центрами даних і мережевими операціями; придбання системного програмного забезпечення, його зміну і підтримку; безпеку доступу; а також придбання прикладних програм, їх розвиток і підтримку.

Натомість, засоби контролю прикладних програм (application controls) стосуються алгоритмічно реалізованих механізмів контролю у конкретному програмному забезпеченні.

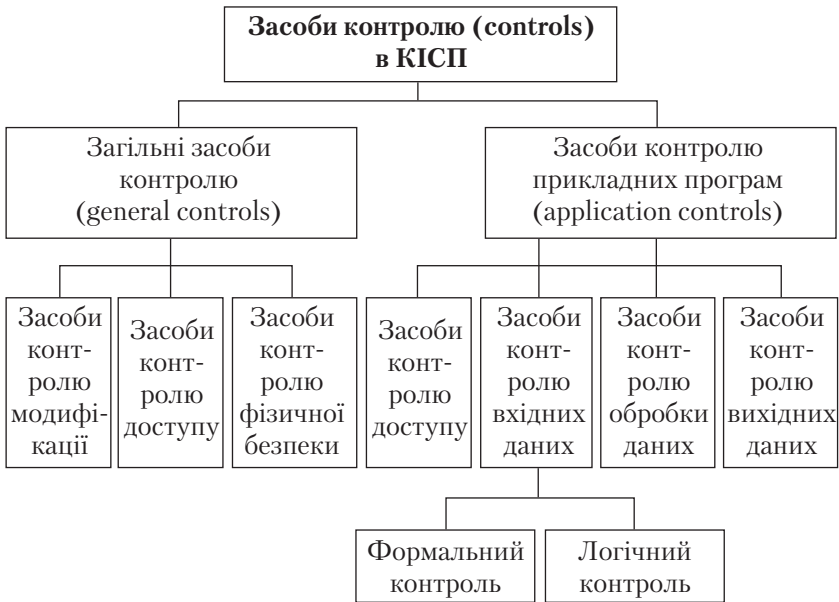
Засоби контролю модифікації	Загальні засоби контролю (general controls)	Засоби контролю прикладних програм (application controls)
Засоби контролю доступу і безпеки	Адміністративні засоби контролю (обмеження фізичного доступу до комп'ютерних засобів, стандарти функціонування комп'ютерних систем, розробка заходів на випадок стихійних лих, пожеж тощо, організація відділу ІТ, організація резервного копіювання інформації)	Засоби контролю доступу (обмеження доступу на рівні паролів, іншої ідентифікації користувача тощо, архівне копіювання даних), контроль цілісності даних
Засоби контролю обробки інформації	Надійність сервісного обслуговування інформаційної системи, засобів контролю розробки і модифікації програм	Засоби контролю функціонування інформаційної системи (контролю введення, контролю обробки та контролю виведення інформації)

**Рис. П.3. Матриця засобів контролю КІС відповідно до Міжнародних стандартів аудиту**

Деталізована класифікація засобів і методів контролю КІСП наведена на рис. П.4.

Засоби контролю модифікації — процедури, розроблені, щоб запобігти або знайти некоректні зміни до комп'ютерних програм. Доступ може обмежуватися такими засобами контролю, як, наприклад, використання окремих програмних бібліотек для реальних операцій та розробки програми і використання спеціалізованих програмних бібліотек. Це є важливим для того, щоб зміни до програм були належним чином відстежені, проконтрольовані і задокументовані.

Засоби контролю доступу — методи і процедури, розроблені для обмеження доступу до онлайн-нових термінальних пристро-



*Рис. II.4. Вбудовані засоби контролю в ІСІП та КСБО*

їв, програм і даних. Засоби контролю доступу складаються з “ідентифікації користувача” і “авторизації користувача”. “Ідентифікація користувача” звичайно намагається ідентифікувати користувача через перевірку його певних унікальних параметрів на початку сеансу роботи (logon) – ім’я доступу, паролі, картки доступу або біометричні дані. “Авторизація користувача” складається з правил доступу, щоб визначити комп’ютерні ресурси, до яких може мати доступ кожний користувач. Зокрема, такі процедури розроблені, щоб запобігти або знайти: несанкціонований доступ до онлайн-ових термінальних пристроїв, програм і даних, введення несанкціонованих операцій, несанкціоновані зміни файлів даних, використання комп’ютерних програм персоналом, якому це заборонено, використання незатверджених комп’ютерних програм. Наприклад, доступ до даних із заробітної плати працівникам може бути наданий лише певним особам.

Засоби контролю фізичної безпеки стосуються фізичної безпеки активів, включаючи відповідні заходи, як, наприклад, забезпечення надійного доступу до активів і записів; авторизація доступу до комп'ютерних програм і файлів даних.

Загальні засоби контролю КІСП перевіряються аудитором як під час проведення аудиту без допомоги комп'ютера, так і з використанням комп'ютерів і комп'ютеризованих методів аудиту.

Традиційний підхід до тестування засобів контролю проявляється під час проведення аудиту без допомоги комп'ютера (auditing around the computer). Цей підхід фокусується на введенні інформації в комп'ютерну систему, отриманні вихідних даних та на ручних процедурах перевірки засобів контролю. Комп'ютерні засоби контролю обробки даних при цьому перевіряються непрямым шляхом через повторне виконання операцій вручну. Тестування входів, виходів інформації та ручної обробки буде включати такі процедури, як підтвердження (vouching), перерахунок (recomputation) та звіряння (tracing). Первинні документи при цьому перевіряються на їх легітимність, авторизацію, точність та повноту запису, а потім звіряються з відповідними вихідними даними. Обчислювальні процеси, які відбуваються в середовищі комп'ютерної системи, перевіряються при цьому вручну шляхом перерахунку, а дані, які використовуються у цих обчисленнях, наприклад, прайс-листи, підтверджуються відповідними затвердженими документами або внутрішніми положеннями.

Цей підхід до тестування бухгалтерських систем може бути достатньо ефективним. Якщо протестувати певну кількість даних, це надасть впевненість у тому, що система працює правильно. Проте питання полягає в тому, що це не є найефективніший метод для отримання такої впевненості. Наприклад, система може мати потужні вбудовані програмні засоби контролю для перевірки та коригування даних (засоби контролю прикладних програм). Замість того, щоб перевіряти велику кількість даних, аудитор просто може перевірити ці засоби контролю, тобто впевнитися в тому, що вони наявні і функціонують.

Аудит за допомогою комп'ютера (auditing with the computer) покликаний насамперед перевіряти засоби контролю прикладних програм, до яких належать засоби контролю вхідних даних, що здійснюють формальний і логічний контроль даних при їх введенні у програму вручну або з інших програм (їх ще називають засобами контролю інтерфейсів); засоби контролю обробки даних, які забезпечують їх цілісність та інтегрованість (наприклад, забезпечують правильність розрахунку залишків або запобігають тому, щоб дані за подібними назвами різних контрагентів додавались); а також засоби контролю вихідних даних (правильність формування звітів і передачі інформації в інші програми).

Після того, як вбудований засіб контролю виявлено, слід протестувати його ефективність. Для цього аудитор спочатку має проглянути технічну документацію на програму. Цей огляд повинен супроводжуватись обговоренням окремих питань з працівниками відділу комп'ютерного забезпечення. Аудитор повинен також впевнитись у тому, що ніяких змін до програмного забезпечення не було внесено, а якщо такі зміни і були проведені, то лише після їх відповідного затвердження.

Програмні засоби контролю можуть інколи бути перевірені шляхом огляду їх функціонування за попередній період. Наприклад, системні звіти (system logs) є доказом того, що цей засіб контролю є і працює ефективно. Приклад такого системного звіту, який фіксує певні проблеми, що трапились під час введення операцій відвантаження продукції, показано у табл. П.2. Цей log-файл містить інформацію про всі випадки, коли операцію почали вводити, але з якихось причин не змогли завершити.

Проте деякі програмні засоби контролю не мають такого “друкованого доказу” і тому необхідно використовувати інші методи перевірки їх функціонування й ефективності. Це можна зробити, наприклад, шляхом введення тестових даних у систему і перевірки правильності отриманого результату (детальніше розглянуто далі).



## Системний звіт скасування спроб відвантаження товару

№ замовлення	Код покупця	Код виробу	№ рядка системного журналу	Код помилки	Повідомлення
32564	354685	0038497	0132	01	Виробу немає в запасі
53627	635497	0004567	0145	02	Неправильний код виробу
32569	465796	0038497	0159	01	Виробу немає в запасі
35626	376444	0023894	0193	06	Перевищення кредитного ліміту покупця
73462	387429	0034782	0234	08	Цьому покупцю товари тимчасово не відпускаються
...	...	...	...	...	...

Іншим способом тестування програмних засобів контролю системи може бути перевірка програмної логіки. Завдання цього тестування — переконатись, що система робить те і тільки те, що закладено в документації і що вона робить це правильно. Проте тестування висуває високі вимоги до комп'ютерної підготовки аудитора. Бажано, щоб він розумів мову програмування конкретної програми. Це дасть йому змогу не тільки протестувати алгоритм на конкретних даних, а й розібратися у правильності його налагодження, наприклад, при використанні шаблонів для введення типових операцій, доступ до зміни яких має непрофесійний користувач — бухгалтер "1С: Бухгалтерія". Процес дещо полегшується, якщо програма правильно розроблена та до неї наявна документація, в якій показано відповідні блок-схеми із зображенням всього процесу обробки даних.

Зазначимо, що деякі поширені програмні продукти для автоматизації бухгалтерського обліку налагоджуються за допомогою специфічних мов програмування, що оперують поняттями бухгалтерського обліку. Це робить алгоритми зрозумілими для бухгалтерів і аудиторів, які не мають спеціальної підготовки. Як приклад наведемо діалогову форму введення документа “Видаткова накладна”, що міститься в українській конфігурації програми “1С: Бухгалтерия 7.7”, що пропонується фірмою АBBYU Software, а також фрагмент алгоритму до цієї накладної, що забезпечує формування проводок (рис. II.5, II.6).

Як бачимо з наведеного прикладу, фахівець з бухгалтерського обліку або аудитор, навіть не маючи спеціальних знань з мови програмування програми, може зрозуміти, що за допомогою цього документа – видаткової накладної, можна формувати бухгалтерські документи з реалізації продукції, товарів або послуг з одночасним розрахунком податку на додану вартість та списанням собівартості товарів.

Расходная накладная - РН-0000001

Основные | Дополнительно

№ **двоори**

Расходная накладная № РН-0000001 от 25.01.05 Админов

Покупатель: Дельта

Место хран.: Основной склад

Гривна Курс: 1.00000 грн за 1 грн

Вид торговли: За наличн Касса: Основная касса

Заказ: Договор ДГ-0000002 (23.01.05)

Примечание:

N	ТМЦ Партия	Кво		Цена -	Сумма б/с Скидка	Сумма - НДС	
		Ед	К			Сумма +	НДС
1	Косметический набор РН-0000004 (13.12.04)	шт.	10.000	55.00	550.00	550.00	110.000
2	Крем для лица Партия по умолчанию	шт.	50.000	6.00	300.00	300.00	60.000
			1.000				360.000

Вид НДС: 20 %

Итого 1250.00  
Итого НДС 250.00  
Всего 1500.00

OK Закрыть Печать Дать скидку > Подбор >

Рис. II.5. Видаткова накладна – діалогова форма документа

```

Процедура ПроводкиШапка ()
    Если СубконтоВалДох <> Константа.НиДоходНиРасход
Тогда
        глПроводка (Контекст,“ВД”, “ВД”, СуммаВалДох,
“Валовые доходы”, Контрагент, ПервыйДок, СубконтоВалДох,
        Контрагент, ПервыйДок, СубконтоВалДох, “НК”);
        КонецЕсли;

    Если глВыделятьЛиАвансыПоСчету(СчетКонтрагента) = 1
Тогда
        // погасим полученный ранее аванс
        Если Валюта=Гривня Тогда
            глПроводка(Контекст, “6811”, СчетКонтр
агента, СуммаПогашенияАванса, “Реализация: погашен авансовый
платеж”, Контрагент, ПервыйДок,,
            Контрагент, ПервыйДок,, “НК”);

```

*Рис. II.6. Видаткова накладна — фрагмент алгоритму формування проводок за документом*

Відстеження комп'ютерної логіки, особливо покрокове, показує, які інструкції виконує комп'ютер і в якій послідовності. Воно дає змогу, наприклад, виявити ділянки коду, не виконані при роботі програми. Такий код здатний стати джерелом зловживань. Наприклад, під час нормальної обробки не виконується ділянка коду в програмі зарплати. Аудитор може припустити, що логіка коду заражає систему вірусом, якщо в поточний період немає трансакцій із зарплати.

Покадрова динаміка документує статус виконання програми, проміжні підсумки або дані трансакцій (операцій) на певний момент. Програмісти часто використовують цю процедуру для налагодження програм. “Зйомка” відбувається при виконанні конкретних умов, з виконання конкретної команди або для якоїсь конкретної трансакції (відміченої позначкою — тегом). Трансакція з тегом (tag) дає змогу вивчати вплив конкретних трансакцій на інші файли. Так, можна виявити проблеми, порівнюючи підсумки відомих даних перевірки на конкрет-

них етапах обробки, скажімо, заробітну плату до і після утримання податків.

Часто закладена в проектну документацію система контролю не відповідає фактичному його здійсненню в процесі обробки облікової інформації. Тому аудиторі слід переконатися у відповідності проекту фактичному обліковому процесу, перевірити правильність обробки інформації. Технологічний процес має забезпечити автоматизацію контролю правильності обробки інформації та виправлення виявлених помилок. Виявлені в період обробки за окремими стадіями технологічного процесу помилки мають відображатися у відповідних актах. За цими актами аудитор може відтворити і документально перевірити процес обробки інформації, з'ясувати, які помилки мають постійний характер, чим це зумовлено.

Прикладом вбудованих засобів контролю вихідних даних може бути приклад обмеження перегляду інформації за рахунками для різних користувачів, впроваджених компанією “ТенТек” у бухгалтерії Києво-Могилянської академії (використовується спеціально розроблена конфігурація для програми “1С: Предприятие 7.7”).

У конфігурації створені особливі довідники “Користувачі” і “Рахунки”. Для кожного користувача адміністратор системи або головний бухгалтер задає перелік бухгалтерських рахунків, з якими йому дозволено працювати. Є довідник “Рахунки”, який заповнюється рахунками для кожного користувача (у цьому випадку — користувач з ім'ям Nagrebelna), до яких доступ дозволений (рис. П.7).

Дані заборонених рахунків блокуються в різних звітах різному. У звітах, в яких передбачена можливість вибору рахунку, за яким цей звіт формується, перевірка здійснюється в момент задання рахунку. Наприклад, у звіті “Оборотно-сальдова відомість за рахунком”, якщо ми спробуємо вибрати заборонений рахунок, програма повідомить про неможливість такого вибору і поверне нас у діалог вибору рахунку.

У звітах, що формуються за переліком рахунків за замовчуванням, дані будуть друкуватися лише за переліком рахунків,

Код	Наименование (укр.)	В.	К.	З.	А.	Субkonto1	Субkonto2
122	Права користування майном		+		А	Места хранения	Необоротные активы
123	Права на комерційні позначення		+		А	Места хранения	Необоротные активы
124	Права на об'єкти промислової власнос		+		А	Места хранения	Необоротные активы
125	Авторське право та суміжні з ним прав		+		А	Места хранения	Необоротные активы
127	Інші нематеріальні активи		+		А	Места хранения	Необоротные активы
13	Знос (амортизація) необоротних активів				П	Необоротные активы	
131	Знос основних засобів				П	Необоротные активы	
132	Знос інших необоротних матеріальних є				П	Необоротные активы	
133	Накопичена амортизація нематеріальні				П	Необоротные активы	
134	Накопичена амортизація довгостроков				П	Необоротные активы	
135	Знос інвестиційної нерухомості				П	Необоротные активы	
14	Довгострокові фінансові інвестиції				А	Инвестиции	
141	Інвестиції пов'язаним сторонам за мет				А	Инвестиции	
142	Інші інвестиції пов'язаним сторонам				А	Инвестиции	
143	Інвестиції непов'язаним сторонам				А	Инвестиции	

*Рис. II.7. Список окремих рахунків для корегування окремим працівником*

доступних даному користувачу. Наприклад, у звіті “Оборотно-сальдова відомість” рядки, в яких виводяться дані за цими рахунками, відображаються не чорним як завжди, а сірим кольором. А замість цифр виводяться символи “х”. У наведеному прикладі відображено, яку інформацію отримує бухгалтер з обліку основних засобів і матеріалів, якщо спробує побудувати оборотно-сальдову відомість загалом за всіма рахунками підприємства (табл. II.3).

*Таблиця II.3*

### Оборотно-сальдова відомість

Рахунок		Сальдо на початок періоду		Обороти за період		Сальдо на кінець періоду	
Код	Найменування	Дебет	Кредит	Дебет	Кредит	Дебет	Кредит
1	2	3	4	5	6	7	8
1.0	Основні засоби	15654 720		357101	285603	15726 218	
1.1	Інші необоротні матеріальні активи	4098 674		168771	85379	4182 066	

Продовження табл. П.3

1	2	3	4	5	6	7	8
1.2	Нематеріальні активи	114502		15720	9260	120962	
1.3	Знос необоротних активів		231703	22355	1064		210412
2.2	Малоцінні та швидкозношувані предмети	79023		7016	12295	73744	
2.3	Матеріали і продукти харчування	1714 991		480902	552029	1643 864	
2.4	Готова продукція	x	x	x	x	x	x
3.0	Каса	x	x	x	x	x	x
3.1	Рахунки в банках	x	x	x	x	x	x
3.2	Рахунки в казначействі	x	x	x	x	x	x
3.3	Інші кошти	x	x	x	x	x	x
3.6	Розрахунки з різними дебіторами	x	x	x	x	x	x
4.0	Фонд у необоротних активах		1636 194	18409	201446		1819 232
4.1	Фонд у малоцінних та швидкозношуваних предметах		79023	5398	119		73744
6.1	Поточна заборгованість за довгостроковими зобов'язаннями	x	x	x	x	x	x

1	2	3	4	5	6	7	8
6.4	Розрахунки із податків та платежів	x	x	x	x	x	x
6.5	Розрахунки із страхування	x	x	x	x	x	x
6.6	Розрахунки з оплати праці	x	x	x	x	x	x
6.7	Розрахунки за іншими операціями і кредиторами	x	x	x	x	x	x
7.0	Доходи загального фонду	x	x	x	x	x	x
7.1	Доходи спеціального фонду	x	x	x	x	x	x
7.2	Доходи від реалізації продукції, виробів і виконаних робіт	x	x	x	x	x	x
8.0	Видатки із загального фонду	x	x	x	x	x	x
8.1	Видатки спеціального фонду	x	x	x	x	x	x
8.2	Виробничі витрати	x	x	x	x	x	x

Крім того, у тих звітах, в яких дані про заборонені рахунки виводяться сірим кольором і позначаються "x", неможливо для цих рядків отримати розшифровку даних.

Таким чином, найточнішим методом оцінки засобів контролю, вбудованих у програмне забезпечення бухгалтерського обліку, є безпосереднє вивчення аудитором програмних алгоритмів.

мів. Проте це завжди потребує значного часу та зусиль, а іноді є зовсім неможливим через, наприклад, брак і в аудитора, і в експерта знань особливостей мови програмування конкретної програмно-апаратної системи. До того ж, багато комп'ютерних програм (“Галактика”, “Парус”) за своєю будовою є жорстко структурованими, зі специфічними алгоритмами, що в принципі не можуть бути переглянуті аудитором, який не має початкового (source) тексту програми.

У цьому випадку аудитори використовують різноманітні способи тестування програмного забезпечення, за яких сукупність програмних алгоритмів розглядається як “чорний ящик”. Окремі такі методи наводяться у Міжнародному положенні про аудиторську практику № 1009 “Комп'ютеризовані методи аудиту” (в англомовній редакції 2005 р. скасоване). У ньому зазначається, що методи тестових даних використовуються під час аудиторської перевірки шляхом введення даних (наприклад, набору господарських операцій) у комп'ютерну систему суб'єкта і порівняння отриманих результатів із заздалегідь визначеними. Аудитор може використовувати тестові дані:

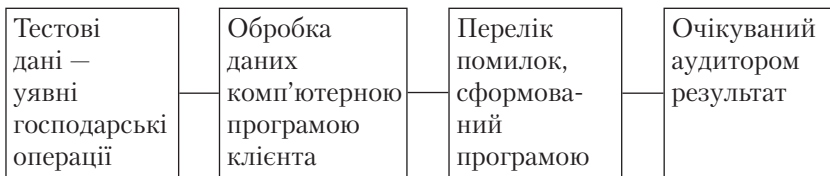
- для тестування конкретних засобів контролю в комп'ютерних програмах, таких як інтерактивний пароль і контроль доступу до даних;
- для тестування господарських операцій, відібраних з раніше оброблених операцій, або сформульованих аудитором для перевірки окремих характеристик процесу обробки, що здійснюється комп'ютерною системою суб'єкта;
- для тестування господарських операцій, що використовуються в інтегрованих тестових підсистемах, де застосовується фіктивний модуль (відділ або службова особа), через який вони проходять під час звичайного циклу обробки.

### **6.3. Тестування програмного забезпечення при комп'ютерному аудиті**

На практиці українські аудитори, спираючись на свій досвід, складають набір облікових задач з різних галузей госпо-



дарської діяльності, що містять десятки певних уявних господарських операцій, які подаються на вхід програмної системи, що перевіряється (рис. П.8).



*Рис. П.8. Схема формування очікуваного результату*

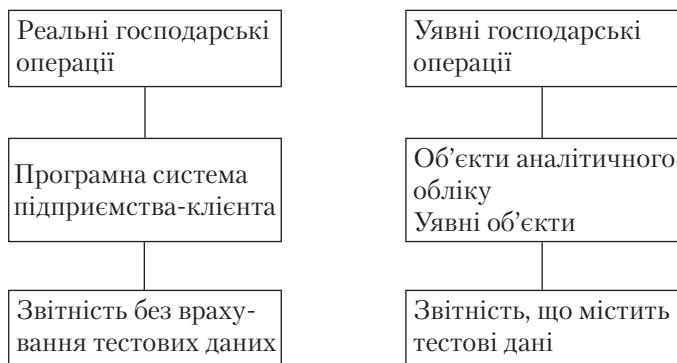
Тестові дані (test data — TD) — це бухгалтерські документи, операції і проводки, що не відображають реальних фактів господарського життя, а спеціально підготовлені аудитором для перевірки програмних алгоритмів, реалізованих в обліковій системі підприємства-клієнта. Тестові дані вводять в КІСП і порівнюють фактичні результати з прогнозом аудитора. Якщо контрольні підсумки дорівнюють фактичним, правильність роботи програми визнається доведеною. Аудитор може застосовувати спеціальне програмне забезпечення, що створює тестові дані (генератор тестових даних). Звичайно частину таких уявних тестових господарських операцій та документів аудитор навмисне робить некоректними з погляду законодавства та загальноприйнятої бухгалтерської практики. При цьому аудитор знає, який саме результат має видати програма. Наприклад, для перевірки правильності нарахування податку з доходів фізичних осіб аудитор може ввести в комп'ютер клієнта значення певної суми заробітної плати та переконатися в правильності отриманого результату. Якщо результат, який на виході надає програмна система клієнта, не збігається з розрахунками аудитора, це є підставою для проведення ретельного дослідження причин та з'ясування можливих наслідків таких розходжень, включно з вивченням алгоритмів щодо конкретної ділянки обліку.

Метод тестових (контрольних) даних може бути ефективним у таких ситуаціях аудиту:

- при тестуванні засобів контролю вхідних даних, включаючи процедури підтвердження даних;
- при тестуванні логіки обробки даних та засобів контролю з метою підтвердження правильності головних файлів;
- при тестуванні розрахунків, здійснених всередині програм, зокрема: визначення відсоткових ставок, знижок, комісій, підрахунків зарплати чи амортизації;
- при тестуванні ручних процедур чи засобів контролю, що стосуються комп'ютерної системи, особливо процедур з вхідними та вихідними даними.

Наведена технологія тестування загалом відповідає методиці, описаній у Міжнародних положеннях про аудиторську практику, хоча у світовій практиці аудиту ширше використовується комплексний підхід до тестування (Integrated test facility approach – ITF), який включає як використання тестових операцій, так і створення певних уявних об'єктів аналітичного обліку (дебіторів, кредиторів, працівників, матеріальних цінностей тощо). При цьому звичайно в програму вводять набір даних, що містить як реальні, так і уявні записи (рис. II.9).

У всіх випадках аудиторські процедури слід проводити не з оригінальними файлами суб'єкта перевірки, а з копіями цих файлів, оскільки будь-які їх зміни, що здійснюються аудито-



**Рис. II.9. Послідовність здійснення комплексного підходу до тестування облікового програмного забезпечення**

ром, та можливе пошкодження не мають впливати на інформацію в системах комп'ютерної обробки даних. У тому випадку, коли контрольні дані обробляються в рамках звичайного процесу обробки інформації суб'єкта, аудитор повинен пересвідчитися в тому, що контрольні господарські операції вилучені з облікових записів підприємства.

Положення про міжнародну аудиторську практику виокремлюють особливості роботи з різними комп'ютерними системами при проведенні аудиту. Це положення № 1001 “Середовище ІТ – автономні персональні комп'ютери”, № 1002 “Середовище ІТ – інтерактивні комп'ютерні системи”, № 1003 “Середовище ІТ – системи баз даних” (в англomовній редакції 2005 р. всі скасовані).

Міжнародне положення № 1001 “Середовище ІТ – автономні персональні комп'ютери” регламентує особливості проведення аудиту на підприємствах, що використовують окремі персональні комп'ютери. Застарілі бухгалтерські системи 70–80-х років ХХ ст. (іноді їх називають успадкованими), як правило, складаються з автономних підсистем (зарплата, постачання), які виводять дані на друк. З підсистем бухгалтери беруть підсумкові цифри для проводок у Головній книзі. Потім система Головної книги готує фінансові звіти. Такі комплекси працюють у пакетному режимі: дані збираються у файлі транзакцій і періодично вводяться у головний файл. Порядок розрахунку і звірки контрольних сум за групами такий: введення – обробка – висновок. Подібна схема досі застосовується на багатьох підприємствах і в бюджетних організаціях. Особливість застосування персональних комп'ютерів і окремих АРМ полягає в тому, що для керівництва підприємства-клієнта може бути неможливим або недоцільним з погляду співвідношення витрат і результатів впровадити належні засоби контролю з метою зменшення ризику невиявлення помилок до мінімального рівня. Тому аудитор вправі припустити, що в таких системах ризик системи контролю високий. Рівень же централізації обробки і збереження даних може бути різним і залежатиме від чисельності бухгалтерії, оснащення її комп'ютерами,

розподілу робіт між персоналом і багатьох інших факторів. На малих підприємствах, де обробка даних виконується одним бухгалтером, програмне забезпечення КСБО й інформаційна база зосереджені на одному комп'ютері. Однак за більш численної бухгалтерії мова йде вже про багатокористувацькі системи, що реалізують роботу кількох користувачів з інформаційною базою обліку.

Загалом КСБО, в яких використовуються тільки окремі персональні комп'ютери, є менш складними, ніж мережеві КСБО. У першому випадку прикладні програми можуть бути легко розроблені користувачами, які володіють основними навичками обробки даних. У таких випадках контроль за процесом системної розробки (наприклад, адекватна документація) і операціями (наприклад, доступ до контрольних процедур), що суттєві для ефективного контролю у великому комп'ютерному середовищі, не може розглядатися розробником, користувачем або керівниками як настільки ж важливий або ефективний з погляду співвідношення витрат і результатів. Оскільки дані були оброблені комп'ютером, користувачі такої інформації можуть без відповідних на те підстав надмірно покладатися на облікову інформацію. Оскільки персональні комп'ютери орієнтовані на індивідуальних кінцевих користувачів, точність і вірогідність підготовленої фінансової інформації залежатиме від засобів внутрішнього контролю, встановлених керівництвом і прийнятих користувачем. Наприклад, якщо комп'ютером користуються кілька людей без належного контролю, то програми і дані одного користувача, що зберігаються на вбудованому носії інформації, можуть стати предметом недозволеного користування, зміни або шахрайства з боку інших користувачів.

Міжнародне положення № 1002 “Середовище ІТ – інтерактивні комп'ютерні системи” регламентує особливості проведення аудиту на підприємствах, що використовують КІСП з модулями оперативного обліку господарських операцій у реальному режимі часу. Це актуально насамперед для таких сфер бізнесу, як банки, мобільна телефонія, електронна комерція тощо.

Особливістю таких систем є розвинені вбудовані засоби контролю (controls) під час здійснення господарських операцій. При введенні даних в інтерактивному режимі вони звичайно піддаються негайній перевірці. Непідтверджені дані не будуть прийняті, і на екрані терміналу висвітиться повідомлення, що дає можливість користувачу виправити дані та відразу ж ввести їх повторно. Наприклад, якщо користувач вводить неправильний порядковий номер товарно-матеріальних цінностей, буде виведено повідомлення про помилку, що надасть користувачу можливість ввести правильний номер.

Аудиторські процедури, виконувані одночасно з інтерактивною обробкою, можуть включати перевірку відповідності засобів контролю за інтерактивними прикладними програмами. Наприклад, це може бути зроблено за допомогою введення тестових операцій через пристрій терміналу або за допомогою аудиторського програмного забезпечення. Аудитор може використовувати такі тести для того, щоб підтвердити своє розуміння системи або для перевірки засобів контролю, таких як паролі та інші засоби контролю доступу.

Є певні особливості систем, що працюють у реальному масштабі часу, які створюють труднощі як для користувача, так і для аудитора. В американських публікаціях зазначається, що із системами, що працюють у реальному часі, пов'язані чотири фактори, що створюють додаткові труднощі для контролю:

- введені дані звичайно не згруповані, тому комп'ютерна система сприймає невпорядковані дані різних видів, що вводяться;
- на комп'ютері здійснюється швидка перевірка документів. Наприклад, засоби контролю обробки даних системи, що працює у реальному масштабі часу, можуть функціонувати без будь-якої документації. Подібно до цього робочі програми, команди можуть бути подані у формі візуального зображення без роздрукування результатів і стандартної форми;
- системи, що працюють у реальному масштабі часу, збільшують і ускладнюють взаємозв'язок секцій системи;

- висока продуктивність систем, що працюють у реальному масштабі часу, значно збільшує швидкість обробки інформації, що ускладнює процес контролю.

Особливості інтерактивних комп'ютерних систем зумовлюють велику ефективність проведення аудитором аналізу нових інтерактивних бухгалтерських прикладних програм до, а не після початку експлуатації. Такий попередній аналіз дасть аудитору можливість перевірити додаткові функції, наприклад, детальні списки операцій або функції контролю в межах самої програми. Це також може дати аудитору достатньо часу для того, щоб розробити і випробувати аудиторські процедури до їх проведення.

У Міжнародному положенні № 1003 “Середовище ІТ — системи баз даних” зазначаються особливості функціонування комплексних КІСП, які ґрунтуються на єдиній базі (сховищі) даних (data warehouse), дані з якої використовуються різними службами підприємства.

База даних є сукупністю даних, що використовуються багатьма користувачами для різних цілей. Кожен користувач може не знати всіх даних, що зберігаються в базі даних, і способів використання даних для різних цілей. Загалом, індивідуальні користувачі знають тільки про дані, якими вони користуються, і можуть розглядати дані як комп'ютерні файли, що використовуються прикладними програмами.

Системи баз даних складаються, переважно, з двох основних компонентів — бази даних і системи управління базою даних (СУБД). Бази даних взаємодіють з іншими технічними і програмними засобами всієї комп'ютерної системи. Системи баз даних відрізняються двома важливими характеристиками: спільним користуванням даними і незалежністю даних. Оскільки інфраструктура безпеки підприємства відіграє важливу роль у забезпеченні цілісності виробленої інформації, аудитору необхідно розглянути цю інфраструктуру перед перевіркою контрольних засобів. Загалом внутрішній контроль у середовищі баз даних потребує ефективної системи контролю за базою даних, СУБД і прикладними програмами. Ефективність системи вну-

трішнього контролю залежить великою мірою від характеру завдань адміністрування бази даних і того, як вони виконуються.

Отже, ми з'ясували, які є засоби контролю КІСП та визначили способи перевірки їх ефективності. Таке тестування засобів контролю проводиться для того, щоб визначити ступінь ризику, який потенційно може виникнути при складанні фінансової звітності. Після тестування засобів контролю ризик може бути оцінений як низький, середній та високий, що матиме значний вплив на проведення детальної перевірки.

### **Тестові завдання до теми 6**

1. Середовище комп'ютерних інформаційних систем — це:
  - а) обробка фінансової інформації;
  - б) політика і процедури, які застосовує суб'єкт господарювання;
  - в) досягнення стратегічних цілей бізнесу.
2. Середовище інформаційних технологій — це:
  - а) політика і процедури, які застосовує суб'єкт господарювання;
  - б) обробка фінансової інформації;
  - в) досягнення стратегічних цілей бізнесу.
3. Одним із факторів, що впливають на спосіб проведення аудиту в умовах автоматизованих систем обліку, є:
  - а) рівень автоматизації бухгалтерського обліку та контролю;
  - б) рівень розвитку нормативної бази з питань регулювання аудиту;
  - в) високий ризик проведення аудиту.
4. Структура КІСП при вивченні аудитором складає:
  - а) розподіл комп'ютерної обробки даних у рамках суб'єкта господарювання;
  - б) наявність спеціального програмного забезпечення для проведення аудиту;
  - в) розподіл первинної документації для аудиту.

5. При аудиті первинної документації аудитор вивчає:
  - а) ступінь автоматизації первинних документів збору і реєстрації;
  - б) потребу автоматизації аудиту;
  - в) наявність спеціального програмного забезпечення для проведення аудиту.
6. При аудиті в комп'ютерному середовищі перевіряється:
  - а) технічна документація програмного забезпечення;
  - б) потреба в автоматизації аудиту;
  - в) ефективність внутрішнього контролю.
7. Методом оцінювання засобів контролю, вбудованих у програмне забезпечення бухгалтерського обліку, є:
  - а) вивчення аудитором програмних алгоритмів;
  - б) вивчення мови програмування;
  - в) вивчення звітів, сформованих програмних продуктів.
8. Тестові дані — це:
  - а) бухгалтерські документи спеціально підготовлені аудитором для перевірки програмних алгоритмів;
  - б) звітні форми для перевірки програмних продуктів;
  - в) алгоритми програмних продуктів з автоматизації проведення аудиту.
9. Аудиторські процедури перевірки бухгалтерського програмного забезпечення слід проводити:
  - а) із копіями файлів;
  - б) із оригіналами файлів;
  - в) змішаним способом.
10. Системи баз даних складаються із:
  - а) бази даних і системи управління базою даних (СУБД);
  - б) бази даних;
  - в) системи управління базою даних (СУБД).



## **Тема 7. Методи аудиту із застосуванням комп'ютерів**

### **7.1. Переваги та необхідність проведення аудиту в комп'ютерному середовищі**

Комп'ютеризація обліку суттєво впливає на проведення аудиту. Однак і сам комп'ютер може стати інструментом аудитора, що дає змогу не тільки скоротити час та заощадити кошти при проведенні аудиту, а й провести більш детальну перевірку і скласти якісний аудиторський висновок.

Обробка економічної інформації клієнта за допомогою комп'ютера має такі переваги перед традиційними методами обробки інформації:

- надає можливість збільшити ефективність аудиторської роботи, зменшивши при цьому витрати;
- зменшує кількість даних, що обробляються вручну, внаслідок чого в аудитора з'являється час для детальнішої перевірки документів;
- надає можливість розширити сферу аудиторської перевірки, збільшити кількість проведених тестів;
- зниження ризику аудитора, пов'язаного з тестами, вибірковою перевіркою;
- зручність користування: можливість одночасно працювати з багатьма документами та спостерігати, як зміна показників одного документа відображається на інформації інших, пов'язаних з ним.

Автоматизація аудиторської діяльності можлива, тому що бухгалтерський облік пов'язаний із застосуванням різних математичних прийомів, регламентованих правил перетворення інформації (математичних формул, відображень одних множин в інші, дій з таблицями). Математичні формули використовують при розрахунках сальдо, оборотів за рахунками, платежів до бюджету і позабюджетних фондів, показників фінансово-господарської діяльності економічного суб'єкта. Прикладом відображення множини господарських операцій у множину бух-

галтерських записів може слугувати будь-який довідник бухгалтерських записів (проводок). Такі довідники орієнтовані звичайно на зміст господарських операцій, що враховуються. Застосування і використання робочих таблиць, класифікаторів і роботу з ними можна проілюструвати описом взаємної відповідності показників різних форм звітності, а також довідником-класифікатором допустимих бухгалтерських проводок.

А. Тіттанен зазначає, що аудит з використанням комп'ютерів (computer-assisted auditing) — це єдиний шлях проведення аудиту в безпаперових бухгалтерських інформаційних системах (paperless accounting information systems). Досліджуючи роль комп'ютерів у аудиті, вона звертає увагу на використання обчислювальної техніки кінцевим користувачем (end-user computing — EUC) у сфері аудиту. Загальним визначенням цього поняття (EUC) є використання комп'ютера і його програмного забезпечення для того, щоб об'єднувати й аналізувати дані з різних джерел. Методику EUC обирають на основі:

- елементів інформаційної системи — загальне та спеціальне тренування користувачів з метою отримання ними відповідних знань (user training);
- елементів бухгалтерської системи — загальне знання бухгалтерських інформаційних систем (accounting information systems — AJS), аудиторського процесу (audit process), наявність аудиторського досвіду (audit experience and expertise), аудиторських технологій (audit firm technologies), систем підтримки прийняття рішень та експертних систем (Decision Support Systems and Expert Systems);
- елементів біхевіористської системи — суб'єктивна думка аудитора (judgement in auditing) і ставлення до комп'ютерних програм (attitudes).

Комп'ютеризовані методи аудиту дають можливість провести більший обсяг перевірки електронних операцій та файлів з обліковою інформацією. Такі методики можуть використовуватися, щоб здійснити вибірку операцій з ключових електронних файлів, відсортувати операції за окремими параметрами або перевірити всю генеральну сукупність замість вибірки.

## 7.2. Типи аудиторських програмних систем

Варто зазначити, що в деяких системах обліку, де використовують комп'ютерну обробку значної частини операцій, можуть виникати складнощі в отриманні чітких результатів без допомоги спеціальних комп'ютерних програм. З іншого боку, при невеликих обсягах даних ефективнішими можуть бути методи обробки даних без використання комп'ютера. До того ж, можна не отримати адекватної технічної допомоги від клієнта, що зробить використання спеціалізованих методів аудиту не ефективним. Але загалом КІСП спонукає аудиторів здійснювати аудиторські перевірки з використанням комп'ютеризованих методів аудиту (Computer-Assisted Audit Techniques – СААТs). Дж. Чемплейн дав найзагальніше визначення комп'ютерним технологіям в аудиті – це будь-які комп'ютерні програми, що їх використовують для підвищення ефективності аудиту через автоматизацію процесів, збільшення розміру аудиторської вибірки та створення нових аудиторських процедур. Є два основні типи СААТs, що їх використовує аудитор (рис II.10):

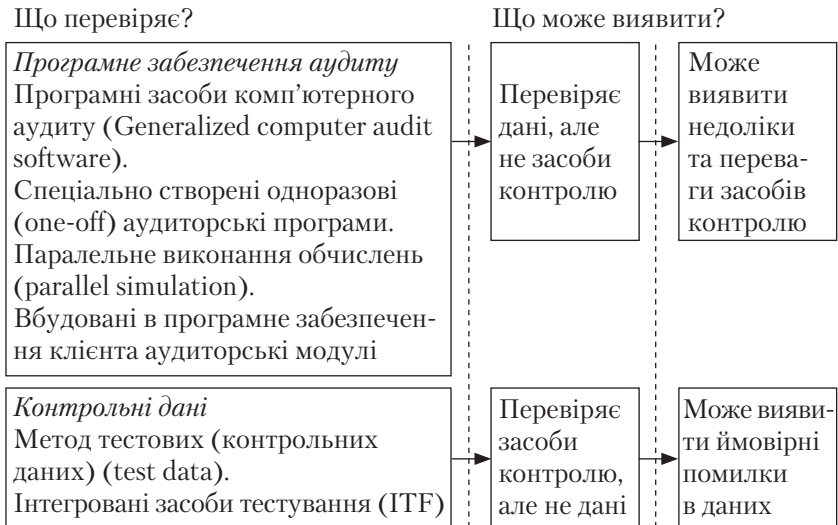


Рис. II.10. Два основні типи комп'ютеризованих методів аудиту

- програмне забезпечення аудиту: комп'ютерні програми, що їх використовують для перевірки змісту файлів клієнта;
- контрольні дані: дані, що їх використовують для комп'ютерної обробки з метою перевірки функціонування комп'ютерних програм клієнта.

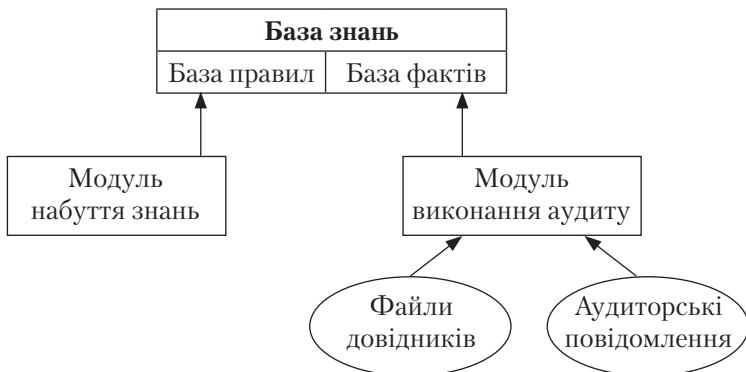
Спеціальні програмні засоби комп'ютерного аудиту призначені для проведення аудиту безпосередньо комп'ютерної системи клієнта шляхом її тестування з використанням різних методів. Результатом є висновок про ефективну роботу процедур контролю і захист даних у системі. Це дає змогу оцінити ризик неефективності контролю і визначити можливість використання бази даних клієнта при проведенні аудиторської перевірки.

### **7.3. Структура аудиторської системи**

Програмні засоби забезпечують роботу з великими масивами даних, які перевіряються при виконанні аудиторських процедур (наприклад, перевірка і аналіз записів, зіставлення даних різних файлів, розмітка і роздруковування вибірок, генерація звітів тощо). Такі програмні засоби підтримки аудиторських процедур припускають виконання певних тестів на фактичних даних. За допомогою таких програмних засобів здійснюють перевірку й аналіз записів на основі визначених критеріїв з метою розкриття їх якості, повноти і правильності. Для цього також використовують різноманітні бази знань, що допомагає визначити невідповідності й прийняти необхідні рішення. Таке програмне забезпечення дає змогу робити тестування розрахунків, виконувати необхідні перерахунки і зіставляти отримані результати з нормативними, кошторисними, попередніми даними.

У літературі з питань комп'ютеризації аудиту модель такої реалізації аудиторської програмної системи має таку структуру (рис. П.11).

Модуль набуття знань призначений для формування бази знань. База знань складається з двох частин: бази правил і бази



*Рис. П.11. Структура аудиторської системи*

фактів. База правил містить процедурні знання у стандартній формі:

ЯКЩО <умова>, ТО <реакція>.

Припустимо, що аудитору необхідно впевнитися у правильності застосування облікової ціни готової продукції. Для цього створюють правило, що може мати вигляд:

ЯКЩО облікова ціна дорівнює сумі, поділеній на одиницю з планів калькуляції собівартості, ТО помилки немає. Наприклад, якщо показник “Обсяг робіт” у “Договорі підряду” збігається з показником “Обсяг виконаних робіт” у “Акті приймання”, то можна перейти до наступного правила. Інакше – сформулювати повне повідомлення.

База фактів відображає типові описи змісту бухгалтерської документації і її взаємозв’язків.

Модуль виконання аудиту призначений для ініціалізації роботи системи, формування аудиторських повідомлень.

#### **7.4. Програмні продукти для проведення аудиту**

Цікаво, що й інші російські автори (за винятком професора В. І. Подольського) здебільшого розглядають процес автоматизації аудиту насамперед як формування за допомогою спеціалізованих програм думки аудитора щодо вірогідності змісту ін-

формації, що міститься у фінансовій звітності клієнта. Фактично, в цьому випадку можна говорити про застосування в аудиті експертних систем та систем штучного інтелекту. Ван Дійк поділяє аудиторські комп'ютерні системи на знаннєві та експертні й зазначає, що саме експертні системи відіграють визначальну роль при проведенні аудиту. Різниця між цими системами полягає в тому, що знаннєва система складається з теоретичних і практичних знань, тоді як експертна система потребує ще й евристичних знань (інтуїтивних), які базуються на досвіді, глибоких теоретичних знаннях та великій кількості інформації, що закладається в комп'ютерну систему. Ван Дійк визначає експертну систему, як комп'ютерну програму, що збирає та зберігає інформацію та дані, визначає взаємозв'язки між певними елементами і робить висновки, виходячи з цих зв'язків, ніби імітуючи при цьому людський розум та здатність мислити. Експертні системи забезпечують можливість додати функціональності в програмні засоби підготовки робочих документів. Наприклад, експертна система може оцінювати відповіді в анкетах для обстеження й автоматично генерувати посилання на додаткові пов'язані питання.

Вибірка (selection) певних операцій для подальшого їх підтвердження є іншим прикладом використання програмного забезпечення аудиту. Залежно від функцій програми сьогодні можна отримати статистичну, систематичну або випадкову вибірку. Проте тут необхідно зазначити, що хоча підбір операцій відбувається автоматично, подальше їх підтвердження звичайно відбувається вручну, оскільки включає процедури, які неможливо автоматизувати: звірку з первинними документами, отримання підтверджень за проведеними операціями від третіх сторін тощо.

Розмір вибірки суттєво залежить від оцінки ризику, яку було дано на етапі тестування засобів внутрішнього контролю підприємства. Це видно із формули розрахунку обсягу вибірки:

$$\eta = \frac{(RA \cdot RF)}{TM},$$

де  $\eta$  — обсяг вибірки, шт.;  $RA$  — загальна бухгалтерська вартість всієї генеральної сукупності, грн.;  $RF$  — фактор ризику;  $TM$  — припустимий рівень помилок (відхилень) у фінансовій звітності, грн.

Результатом проведеного на попередньому етапі тестування засобів контролю є оцінений фактор ризику. Якщо ризик помилки у фінансовій звітності клієнта був оцінений як низький, то фактор дорівнює 1. Якщо ж при тестуванні внутрішніх засобів контролю клієнта аудитором було виявлено певні відхилення, ризик помилки може бути оцінено як помірний. При цьому фактор ризику подвоюється і дорівнюватиме 2. У разі ненаявності засобів внутрішнього контролю на підприємстві або їх невикористання ризик, звичайно, буде оцінений як високий. При цьому фактор ризику знову подвоюється і дорівнюватиме 4.

Іншою важливою складовою цієї формули є припустимий рівень відхилень у фінансовій звітності. Ця величина показує граничний рівень відхилень, за якого фінансову звітність клієнта може бути оцінено аудитором позитивно. Цей припустимий рівень встановлюють суб'єктивно, і він залежить передусім від прибутку підприємства та його сукупних активів.

Після того як було визначено обсяг вибірки, необхідно зробити саму вибірку. Для цього використовують таку формулу:

$$k = \frac{RA}{(n-1)},$$

де  $k$  — інтервал вибірки, грн.

Наприклад, для того щоб перевірити залишок дебіторської заборгованості підприємства на кінець року, необхідно зробити вибірку за дебіторами підприємства і розіслати їм запит на підтвердження залишку їх кредиторської заборгованості. Якщо дебіторська заборгованість на кінець року дорівнює 350000 грн, рівень припустимих різниць — 40000 грн, а ризик помилки у фінансовій звітності був оцінений як помірний, обсяг вибірки дорівнюватиме:

$$n = \frac{350000 \cdot 2}{40000}.$$

При цьому крок вибірки дорівнюватиме: 350,000

$$k = \frac{350000}{18-1}.$$

Тобто для перевірки підтверджень необхідно вибрати 18 дебіторів через кожні 20588 грн дебіторської заборгованості.

У випадку виявлення різниць при тестуванні вибірки такі відхилення екстраполюють на всю популяцію за формулою:

$$\text{Загальна помилка в популяції} = \text{Сума виявлених різниць у вибірці} \times \frac{\text{Загальний обсяг популяції}}{\text{Загальний обсяг вибірки}}.$$

Отже, якщо сумарна заборгованість 18 вибраних дебіторів становить 87460 грн і в цій вибірці сума виявлених різниць становить 2356 грн, а загальна кількість дебіторів підприємства дорівнює 134, то загальна помилка в популяції становитиме 2356 (134 : 18) = 17539 грн. Саме на таку суму аудитор після проведених процедур запропонує проводку: Дт “Сумнівна дебіторська заборгованість” — Кт “Дебіторська заборгованість”, тобто дебіторську заборгованість на цю суму буде зменшено, ймовірно збільшивши при цьому витрати підприємства в майбутньому.

На практиці для цієї процедури використовують спеціальне програмне забезпечення, яке за допомогою цих формул обчислює обсяг вибірки, безпосередньо проводить вибірку та потім екстраполює отримані різниці на всю популяцію. Це значно заощаджує час та дає можливість впевнитись у тому, що для вибірки використовувалися всі операції та проглядалися всі дані.

Прикладом розрахунку обсягу вибірки може слугувати програма E&Y Microstart фірми ErnstsYoung.

У цій програмі обсяг вибірки (Representative Sample Size) розраховується на підставі наперед відомих загальної вартості генеральної сукупності (Population Value), допустимої похибки (Tolerable Error), наперед заданого рівня аудиторського ризику і рівня впевненості щодо інших процедур по суті (Combined



Risk Assesment, Assurance from Other Substantive Procedures). У наведеному прикладі застосовується тип вибірки, за якого кожній гривні або долару надається однакова ймовірність потрапити у вибірку, таким чином при його використанні більше великих за вартістю позицій потрапляє у вибірку для тестування.

З історії відомо, що аудитори покладалися на вибірки господарських операцій, щоб провести свої тести. Але сьогодні аудитор може вирішити, що найбільшим доцільним буде перевірити всю генеральну сукупність, яка формує певний тип операцій або залишок на рахунку (або страту в межах цієї сукупності). Нетиповою для тестування засобів контролю є 100 % перевірка, однак вона більше підходить для тестів по суті. Наприклад, 100 % перевірка може бути доцільна, коли генеральна сукупність складається з невеликого числа елементів з великим числовим значенням, коли є суттєвий ризик та інші засоби не забезпечують достатніх аудиторських доказів, або коли характер обчислення або повторюваного іншого процесу, виконуваного автоматично інформаційною системою, робить 100 % перевірку економічною, наприклад, через використання комп'ютеризованих методів аудиту (СААТs). У цьому випадку аудитори можуть встановити в програмі параметри, за якими господарські операції будуть відібрані за певним критерієм. Такі методи дослідження файлів баз даних клієнта (file interrogation techniques) будуються здебільшого на комп'ютерному аналізі проводок клієнта, взятих з його бухгалтерської програми. За допомогою відповідних програмних засобів перевіряється реальність дат оплати та оприбуткування, вказаного клієнтом у книзі купівель, і, як наслідок, правомірність зарахування ПДВ.

Таким чином, вибірка в умовах КІСП може бути залишена лише в тому випадку, якщо аудитор оцінює працездатність модуля оперативного обліку, який щоденно здійснює мільйони записів, наприклад, системи мобільного зв'язку чи банкомати.

Комп'ютерні програми, які дають змогу проводити такий аналіз, отримали назву аудиторського програмного забезпечення загального призначення (generalized audit software – GAS). Таке програмне забезпечення складається з однієї або кількох

комп'ютерних програм, придатних для аналізу різних аудиторських ситуацій на базі різного облікового програмного забезпечення. На противагу цьому типу програм, іноді використовують спеціальне програмне забезпечення (one-off software) для використання в конкретній аудиторській ситуації. Як правило, створення спеціального програмного забезпечення коштує дорого.

Методи дослідження файлів баз даних клієнта ґрунтуються на тому, що більшість бухгалтерських програмних продуктів зберігає в базі даних інформацію про бухгалтерські проводки. У проводки є обов'язковий набір реквізитів (облікова фраза). Як мінімум, це реквізити: дата, номер, текст, сума, валюта, рахунок дебету, рахунок кредиту, інформація про об'єкти аналітичного обліку за дебетом і кредитом проводки. Сучасні програмні продукти для КСБО також зберігають інформацію про імена користувачів, дату і час проводки. Ця база даних завантажується у спеціалізовану аудиторську програму. Після цього аудитор здійснює над цими даними ряд автоматизованих процедур.

У країнах, де дослідження файлів баз даних у комп'ютерному аудиті є поширеним явищем, аудитори для аналізу файлів даних використовують такі програмні пакети, як ACL або IDEA.

IDEA (Interactive Data Extraction and Analysis) – програмний продукт, який був розроблений у 1987 р. Канадським інститутом присяжних бухгалтерів (Canadian Institute of Chartered Accountants) як інструмент для зовнішніх аудиторів, а нині підтримується і вдосконалюється фірмою CaseWare IDEA. Цікаво, що інший подібний загальноновживаний аудиторський програмний продукт – ACL (Audit Command Language) також був розроблений у Канаді фірмою ACL Services у м. Ванкувері. Це програмне забезпечення дає змогу аудитору здійснювати такі операції з бухгалтерськими проводками:

- знайти проводки, введені у незвичайний час дня, тобто не в робочий час;
- знайти проводки, введені незвичайними користувачами, анонімно або під вигаданим ім'ям, вищим керівництвом або, наприклад, працівниками відділу інформаційних технологій;

- відфільтрувати операції, що є типовими для підприємства, щоб побачити певні разові проводки;
- проаналізувати пари “дебет-кредит” на відповідність законодавству та правилам бухгалтерського обліку;
- розрахувати окремі підсумки за рахунками, які потім звіряються із даними роздрукованих і офіційно завірених журналів і звітів.

Це спеціалізоване аудиторське програмне забезпечення може здійснювати просте підсумовування, перехресне підсумовування, вибірку і аналіз результатів, перевіряти відповідність даних у багатьох різних файлах, імпортувати й експортувати дані, проводити аналітичні процедури та розрахунки над такими “первинними” даними. Аудиторське програмне забезпечення може допомогти відшукати й певні логічні аномалії у файлах даних про виключені трансакції (наприклад, про подвійну оплату за одним номером рахунку-фактури).

Наприклад, перед аудитором поставлене завдання проаналізувати процес продажу продукції покупцям та її оплати за рік. За допомогою програми IDEA бухгалтерська програма клієнта зберігає дані в стандартному текстовому форматі поквартально. Також ми маємо наданий відділом кадрів підприємства-клієнта файл у форматі Microsoft Excel, що містить інформацію про скорочені імена користувачів (авторизацію), яким дозволено здійснювати записи у бухгалтерській програмі (logon — поле Approved Auth), а також максимальні суми операцій, які дозволено проводити цим працівникам, не звертаючись за дозволом до своїх керівників, — поле Limit (див. табл. II.4).

Аудитору необхідно ідентифікувати всі операції, що відбувалися протягом вихідних днів, знайти всі операції з “круглими” сумами (наприклад, всі операції, суми в яких закінчуються двома нулями). Далі аудитор має перевірити, чи всі операції здійснені тими працівниками, яким це дозволено, і чи не перевищений ліміт авторизації.

На початку аудитор послідовно завантажує в програму IDEA кварталні масиви даних, щоб мати суцільну річну базу.

## Інформація про користувачів та їх ліміти авторизації

Approved Auth	Limit
BC	100 000,00
CW	50 000,00
HMV	100 000,00
VST	90 000,00
WJN	85 000,00

Програма за допомогою функції Import Assistant належним чином ідентифікувала файл як текстовий (ASCII Delimited) і запропонувала розглядати перший рядок даних як назви полів даних.

Після цього, використовуючи вбудовані засоби програми IDEA, ми вводимо в базу даних два додаткових службових поля, яких не було в базі даних бухгалтерської програми. Перше з них — NEW\_AUTH нам знадобиться для перевірок з авторизації. А поле DAYOFWEEK буде заповнене програмою значеннями від 1 до 7 (обчислюється на підставі інформації про дату здійснення господарської операції; відповідає дням тижня з неділі — “1” до суботи — “7” послідовно).

У наведеному прикладі база даних операцій з відвантаження продукції має такі поля: INVOICE\_NUMBER — номер накладної, INVDATE — дата накладної, AMOUNT — сума, SKNUMBER — порядковий (контрольний) номер запису, PMTDATE — дата оплати, AUTH та NEW AUTH — ім'я користувачів, під якими вони входять у програму, DAY\_OF\_WEEK — день тижня, в якому здійснена операція.

Для того, щоб ідентифікувати всі операції, які відбувалися протягом вихідних днів, створюємо нову базу даних (пункт Direct Extraction з меню Data), яка і буде містити такі відібрані нами операції. Назвемо її “операції протягом вихідних днів” — Weekend Transactions. Після цього за допомогою редактора логічних виразів (Equation Editor) сформуємо запит, згідно з яким програма відбере всі операції, здійснені у неділю і суботу — DAYOFWEEK = 1. OR. DAY\_OF\_WEEK = 7.

Результат вибірки — нова база даних, яка містить 166 записів (всього операцій за рік), здійснених у вихідні дні із загальної кількості 1017 записів.

Тепер аналогічно віднайдемо всі “заокруглені” за сумою операції. Записувати їх будемо в нову базу даних Round Payments, а логічним виразом буде  $AMOUNT \% 100 = 0$ . Знак “%” відображає функцію, що видає результат у вигляді десяткової частини числа, яке утворюється від ділення суми (amount) на 100. Якщо залишок нульовий, це вказує, що сума закінчується на “00”. Результат виявився досить несподіваним.

Всього відібраними згідно з нашим запитом виявились 3 операції. Причому дві — взагалі з нульовими сумами. Якщо перша відібрана операція на суму 79500 може бути підставою для подальшого розслідування на предмет шахрайства, то наявність операцій з нульовими сумами однозначно свідчить, окрім помилок, допущених виконавцями в обліку, про слабкі засоби контролю прикладної програми щодо введення даних. Програма взагалі не повинна дозволяти вводити операції з нульовими сумами.

Так само просто проаналізувати дані в IDEA шляхом побудови логічного виразу, який визначає прийнятний інтервал значень для одного чи кількох полів у базі даних. Наприклад, для того, щоб відібрати всі накладні з підсумками від 4000 до 5000 грн, це рівняння має виглядати таким чином:

$AMOUNT \geq 4000 \text{ AND } AMOUNT \leq 5000$ .

Аналогічним чином можна відібрати, наприклад, всі матеріальні цінності, що зберігаються на складі, залишок за кількістю яких більший від якогось значення.

Для того щоб перевірити, чи всі операції здійснені тими працівниками, яким це дозволено, і чи не перевищений ліміт сум операцій, у межах якого їм дозволено їх здійснювати, слід до вже відкритої, основної бази даних бізнесових операцій (primary database), завантажити у програму файл Excel Approved Auth’s з інформацією про користувачів, який буде допоміжною базою даних (secondary database) за допомогою команди об’єднання баз і отримаємо третю, об’єднану базу Payments and limits.

Після цього, застосовуючи просту формулу `AMOUNT > LIMIT`, одержуємо базу даних записів операцій `Transactions over Limit`, які здійснені з перевищенням дозволених лімітів. Ця база даних містить 205 записів. Причому з них насправді перевищено ліміт тільки у 35 операціях, а 170 записів попали у базу, тому що інформацію про цих користувачів відділ кадрів нам не надав взагалі, тобто таких користувачів немає у файлі Excel (відповідно, програма вважає цей ліміт таким, що дорівнює нулю). Якщо це не наслідок навмисного зламу системи ззовні, то, скоріше за все, нові працівники просто могли використати для входу в систему ідентифікатори вже звільнених працівників, що знову ж таки свідчить про слабкі вбудовані у бухгалтерську програму засоби контролю доступу або ж про неузгодженість у роботі бухгалтерії і відділу кадрів.

Цікавою для подальшого вивчення аудитором щодо виявлення, наприклад, шахрайства може бути інформація про те, з якими покупцями мали справу наші працівники — продавці або агенти, скільки вони уклали угод з кожним покупцем і на які загальні суми. Для цього використовується функція програми, що дає змогу підсумовувати за ключовими полями.

У результаті отримуємо спеціальну базу даних, яка містить 123 записи (відповідає кількості найнятих підприємством продавців). Тут поле `VENDOR` містить код нашого продавця, поле `PAYEE` — назву покупця, поле `NO_OF_RECS` — кількість угод, поле `AMOUNT` — загальну суму за цими угодами. Тут також можна переглянути і записи за кожною угодою окрема.

Надалі, якщо підозра у шахрайстві пала на когось з наших працівників, то можна, наприклад, за допомогою програми порівняти номери домашніх телефонів продавців та підприємств-покупців, адреси тощо.

Аудитор може використати для аналізу файлів клієнта і досить поширене програмне забезпечення із пакета програм Microsoft Office, наприклад Microsoft Access. Наведений файл `lsentry.dbf` бази даних однієї із типових конфігурацій програми “1С: Бухгалтерія”, відкритий за допомогою Microsoft Access.

Звичайно, у базі даних будь-якої програми дані зберігаються у певному внутрішньому форматі, і для того, щоб над ними здійснювати певні операції, необхідно знати цей формат. Так, з наведеного прикладу є очевидним, що в полях DATE і SUM зберігаються відповідно дата і сума проводки. А от в полях TIME, ACCDTID та ACCKTID – відповідно точний час введення проводки, рахунок дебету і рахунок кредиту у внутрішньому комп'ютерному форматі. Поле CURRID призначене для зберігання інформації про тип валюти суми проводки (у прикладі – “0” – українська гривня, може бути “1” – долар США тощо). Коли відомий формат зберігання даних, аудитор може використовувати для їх обробки засоби власне СУБД Access.

Якщо в КСБО передбачена можливість збереження облікової інформації в одному зі стандартних форматів, наприклад Microsoft Excel, то завдання аналізу таких даних може значно спроститися. Наприклад, така можливість передбачена в конфігурації програми “1С: Бухгалтерія” для автоматизації обліку і планово-фінансової роботи українських університетів – бюджетних установ компанії “Тен-Тек” (Тес™). Тут реалізована можливість формувати журнал операцій з проводками у зручному для перегляду і роздруку вигляді.

Далі можна аналізувати дані або вручну стандартними засобами Excel, або створити програму із застосуванням мови Microsoft Office Visual Basic. Такий набір інструментів фактично дасть змогу аналізувати й перевіряти Головну книгу й оборотно-сальдові відомості, а також, наприклад:

- отримати структуру будь-якого рахунку, тобто з якого дебету склався кредит того чи іншого рахунку з розбиттям за місяцями (у сумарному або відсотковому до загального обороту вираженні) або навпаки;
- отримати вибірку некоректних проводок;
- отримати вибірку значущих проводок (встановивши відсоток значущості до загального обороту);
- отримати вибірку сторнуючих проводок;
- перевірити проводки списання МШП;

- перевірити проводки нарахування амортизації нематеріальних активів;
- перевірити проводки нарахування амортизації основних засобів;
- перевірити проводки нарахування платежів до бюджету;
- розрахувати структуру витрат;
- розрахувати і звірити показники податкових декларацій за ПДВ;
- провести аналіз даних, наприклад, порівняти оборот: певним рахунком з оборотами за іншими рахунками.

Таким чином, програма може відстежити проводки з очевидно неправильною кореспонденцією рахунків (точніше кажучи, кореспонденції рахунків, які неможливі за правилами бухгалтерського обліку); вибрати проводки з великими сумами, сторнуючі тощо. Все це дає можливість скласти подальший план аудиторської перевірки, який буде спрямований на найбільш ризикові зони стосовно помилок.

Насправді не тільки файли баз даних, що містять бухгалтерські проводки, можуть бути досліджені. Можуть бути досліджені, наприклад, бази даних із довідниками аналітичних об'єктів. Багато важливої інформації містять також журнали обліку завдань або системні журнали (log-файли), зокрема дані про використання ресурсів. Досліджуючи такі файли, можна, наприклад, порівняти плановий час роботи програми або працівника з фактичним і виявити всі серйозні розбіжності, що потребують подальшого розслідування.

Іноді аудитор використовує спеціальне програмне забезпечення навіть для управління і контролю змісту програмних файлів з кодом — файлів-бібліотек (dll-файли). Таке програмне забезпечення реєструє всі зміни в коді, модулях і операційних системах. Пошук несанкціонованих змін у цих журналах допоможе розкрити порушення цілісності даних.

В українській практиці поширеним способом тестування облікового програмного забезпечення є його опосередкована перевірка за допомогою спеціальних бухгалтерських програм, підготовлених аудиторською фірмою. Ця методика тестування



передбачає використання тільки реальних даних клієнта, що їх обробляють одночасно в комп'ютерній системі бухгалтерського обліку клієнта та в програмному забезпеченні, яке використовує аудитор. У світовій практиці вона має назву паралельного виконання обчислень (parallel simulation). Таку перевірку здійснюють шляхом рівномірного моделювання облікового циклу з програмною перевіркою всіх можливих параметрів облікового процесу. На основі цих моделей, що відображають особливості господарської діяльності конкретного підприємства, аудитор здійснює імітаційну обробку даних зі структурою, аналогічною структурі реального програмного забезпечення. Отримані вихідні дані порівнюють із реальними даними, і за результатами порівняння виявляють відхилення, що їх фіксують у протоколі перевірки.

Таким чином, за допомогою спеціальних програмних засобів здійснюють перевірку, моделювання й аналіз облікових даних з метою визначення їх повноти, якості, правомірності й вірогідності. Для цього виконують порівняння змодельованих облікових даних з реальними даними інформаційної системи, а також здійснюють тестування розрахунків і перерахунків, підсумовування, повторне упорядкування і формування звітних даних і їх порівняння з реальними даними. Крім цього, здійснюють контроль правильності відновлення даних (рис. II.21).



Рис. II.21. Паралельна обробка облікових даних

Метод паралельного моделювання позбавляє від необхідності готувати тестові дані й дає змогу аудиторю проводити тести неявно і з більшою частотою, не заважаючи роботі операційної системи і не змінюючи файлів КІСП клієнта.

Для підприємств, з якими аудиторська фірма має довгострокові договірні відносини, можуть бути розроблені спеціальні вбудовані аудиторські модулі, які вбудовують у наявні програмні засоби обліку, контролю й аудиту (рис. П.22) і які дають можливість контролювати необхідні параметри облікового процесу. За допомогою цих модулів виконують відбір операцій, що становлять інтерес з погляду аудиторської перевірки. Вбудований аудиторський модуль фільтрує файли операцій та проводок і шукає аномалії в даних або в їх співвідношенні, наприклад, факти використання кредитної картки в дванадцяти країнах у межах двох годин. Відібрані при цьому дані групують за операціями у спеціальну аудиторську базу даних для подальшої обробки.

Вбудовані програмні модулі застосовують такі види контролю даних:

- систематичний контроль, коли тестування облікових даних здійснюють за всіма основними критеріями (діапазон, зіставлення з нормативно-довідковою інформацією тощо);



**Рис. П.22. Збирання аудиторської інформації за допомогою вбудованого контрольного модуля**

- вибірковий контроль, здійснений на деякій вибірці даних (за визначеними операціями, за окремими задачами тощо).

Модулі для безперервного систематичного тестування можна використовувати для систем, в яких вже передбачене ведення журналу помилок та реєстрації нетипових подій (transaction log), наприклад, програм для електронної комерції. Безперервний моніторинг у цьому випадку дасть змогу аудитору оцінити не тільки ризик контролю, а й притаманний (властивий) ризик, оскільки тут саме ведення бізнесу цілковито базується на функціонуванні комп'ютерної системи. Прикладами подій, на які реагують подібні модулі, у цьому випадку можуть бути автоматична відмова від обслуговування у випадку, коли замовлення на товари більше від деякої визначеної суми, або якщо ціна перевищує заданий діапазон.

Вбудовані аудиторські модулі слід застосовувати лише за повної згоди й підтримки з боку керівництва підприємства клієнта і працівників внутрішнього аудиту (якщо така служба є на підприємстві), оскільки таке втручання у схему і реалізацію засобів аудиту може поставити під питання незалежність аудитора.

У принципі, аудитори можуть у своїй діяльності використовувати широкий набір програмних засобів різного призначення, які, як правило, не об'єднані в єдину комплексну систему. На певних стадіях використовують стандартні офісні програми, такі як Word, Excel, що є допоміжними під час проведення аудиту, роблять роботу зручнішою, а подання інформації наочним. На основних етапах, таких як аналітичні процедури, тестування засобів контролю та детальні перевірки на перший план виходить використання спеціального програмного забезпечення, яке безпосередньо дає можливість за його допомогою швидко та ефективно проводити аудит.

Весь процес роботи зі спеціальним аудиторським програмним продуктом можна розділити на такі етапи.

На першому етапі аудитор визначає завдання, які необхідно вирішити під час перевірки за допомогою спеціального програмного забезпечення.

На другому етапі складають план виконання поставлених завдань і роблять оцінку реальності застосування аудиторських програмних засобів. Для цього проводять аналіз форми і методів бухгалтерського обліку на підприємстві, оцінюють можливість застосування спеціального аудиторського програмного забезпечення. При цьому встановлюють обсяг облікової інформації, обсяг роботи аудитора, кількість часу, необхідного для проведення аудиторської перевірки. На цьому етапі визначають потрібну потужність обчислювальної техніки і складають графік виконання аудиторських робіт із зазначенням обсягів виконуваних робіт, термінів виконання, конкретних виконавців і форми завершення.

На третьому етапі здійснюють налагодження стандартних програмних засобів, розробку нових засобів, необхідних для цієї аудиторської перевірки. Наявні програмні засоби адаптуються під фактичні облікові дані.

На четвертому етапі здійснюють перевірку сформованих на електронних носіях даних з метою підтвердження їх незмінності, оцінюють стан підприємства, яке перевіряють, проводять тестування й обробку за графіком, аналіз отриманої інформації, її оцінювання за допомогою бази знань і формують висновок за тими позиціями, які перевіряють.

## **7.5. Принципи застосування аудиторських програм**

Враховуючи специфіку аудиторської діяльності, вимоги до аудиторського програмного забезпечення можуть бути такими.

1. Наявність розвинених засобів контролю операцій. Контроль може здійснюватися не тільки у момент оформлення документа або проводки, як це прийнято в бухгалтерських програмах, а й тоді, коли в цьому виникає потреба.

2. Гнучкість. Оскільки аудиторам доводиться працювати з різними підприємствами, і в кожного з них свої облікова політика, форми звітності й навіть план рахунків, то програма повинна мати можливість швидко переналагоджуватися на специфіку страхової компанії, торгового дому, бюджетної орга-

нізації, виробничої компанії. У комп'ютерних аудиторських системах повинні враховуватися як загальні вимоги і стандарти аудиту, так і особливості обліку фірм-клієнтів.

3. Ергономічність. Це означає наявність засобів для зручного введення великих обсягів інформації, оперативного і простого формування звітів. Інакше кажучи, програма має бути розрахована не на програміста або оператора, а на аудитора, знання якого в галузі комп'ютерної техніки можуть бути обмежені.

4. Зв'язок на рівні баз даних з бухгалтерськими програмами. Необхідні додаткові засоби для введення і виведення даних, представлених у різних форматах.

Крім основних вимог аудиторському програмному забезпеченню (як і будь-яким іншим прикладним програмам) мають бути притаманні простота освоєння, швидкодія, професійна оперативна підтримка з боку розробників.

Ринок аудиторського програмного забезпечення лише починає розвиватися. На світовому ринку представлено використовані у роботі аудиторів програмні засоби різних типів (рис. II.23).



Рис. II.23. Програмні засоби, які використовують у своїй роботі аудитори

Розглянемо деякі з цих класів програмного забезпечення.

Пакети прикладних програм загального і проблемно-орієнтованого призначення. Ця група включає широкий набір готових універсальних програм, з якими повинен уміти працювати аудитор. За функціональним призначенням і застосуванням їх в аудиті виділяють такі підгрупи:

- текстові процесори;
- табличні процесори;
- правові бази даних і довідники;
- бухгалтерські програми та їх окремі модулі;
- спеціалізовані статистичні пакети загального призначення;
- програми фінансового аналізу та їх окремі модулі;
- програми електронного документообігу;
- програми автоматизації управлінських функцій.

Текстові процесори використовують на всіх стадіях аудиту, що потребують створення та якісного оформлення аудиторських документів. Їх застосовують при складанні аудиторських програм і планів; договорів; різних довідок і запитів; робочих документів аудиторської перевірки; при листуванні з клієнтами і третіми особами; підготовці аудиторського висновку і рекомендацій керівництву підприємства тощо. Найчастіше аудиторські фірми використовують Word фірми Microsoft.

Табличні процесори з потужними обчислювальними можливостями, засобами ділової графіки, обробки текстів і ведення баз даних набули широкого застосування при проведенні аудиторських перевірок. Їх використовують при складанні різних аналітичних таблиць; реалізації аналітичних процедур, насамперед пов'язаних з оцінкою фактичних показників бухгалтерської звітності й аналізом фінансового стану економічного об'єкта, що перевіряється; поданні отриманої інформації у графічному вигляді; складанні альтернативних прогнозних балансів; при створенні різних робочих табличних документів, наприклад, кошторисів, фінансової звітності тощо. Вбудовані функції, у тому числі фінансові, статистичні функції, можливість розв'язання задач на кшталт “що буде, якщо” зробили таб-

личні процесори популярними серед аудиторів. Найбільшого поширення набули табличні процесори Excel.

Правові бази даних і довідники забезпечують інформаційно-консультаційне обслуговування аудиторів у процесі проведення перевірок, що дає їм змогу з достатньою впевненістю зробити висновок про відповідність бухгалтерського обліку підприємства документам і вимогам нормативних актів, що регулюють порядок ведення бухгалтерського обліку.

Програми електронного документообігу дають змогу накопичувати документи, зберігати, здійснювати швидкий пошук і доступ до документів в електронних архівах, виконувати їх об'єднання, а також забезпечувати групову роботу при створенні документа. Наприклад, аудиторська фірма Ernst & Young використовує систему DOCS Open, розроблену компанією PC DOCS Inc. Нерідко аудиторські фірми під час перевірки натрапляють на такі системи й у клієнтів. Тоді вони дають оцінку правильності її застосування. Крім того, якщо система електронного документообігу функціонує в клієнта, то це спрощує і прискорює проведення аудиту на об'єкті через швидкий доступ і одержання потрібних документів.

Спеціалізовані статистичні пакети загального призначення аудитори використовують при проведенні досить складних розрахунків. Вони реалізують набір різних статистичних методів, дають змогу здійснювати обмін з найбільш поширеними СУБД, мають можливість графічного подання даних, зручний для користувача інтерфейс. Сьогодні найбільш популярні з них Mathematics, Statistics, Quick, Statgraphics.

Програми фінансового аналізу та їх окремі модулі. Для реалізації процедур аналізу фінансово-господарської діяльності економічних суб'єктів поряд з табличними процесорами аудиторські фірми використовують спеціальні програми фінансового аналізу. Вони орієнтовані на аналіз фінансового стану підприємства, вироблення стратегічних і тактичних рішень управління підприємством.

Програми аналізу дають змогу виконати перевірку фінансової, податкової й іншої звітності завдяки закладеному в них ме-

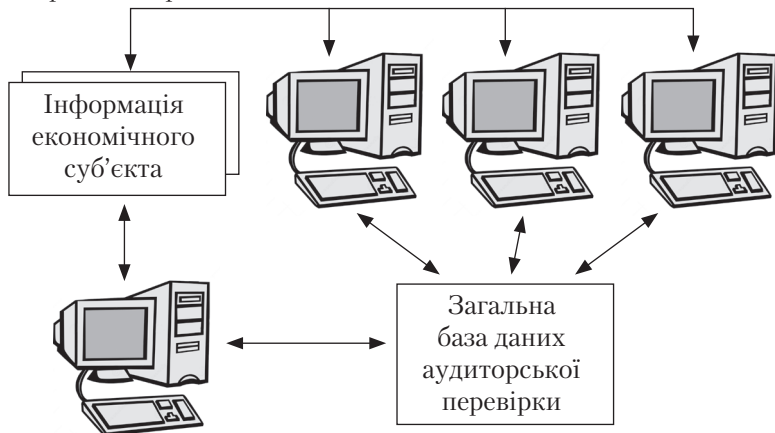
ханізму зв'язання взаємозалежних показників. Вони забезпечують проведення фінансового аналізу за різними методиками і розраховують велику кількість економічних показників, дозволяють складати й аналізувати бізнес-плани. Деякі програми містять можливість трансформації фінансової звітності до міжнародних стандартів МСФЗ, наприклад, Pro-Invest Consulting (Audit Expert, Project Expert). Останнім часом засоби фінансового аналізу часто інтегрують у системи бухгалтерського обліку та управління підприємством, наприклад у розробки фірм “Галактика”, “Інфософт”, “Інтелект-Сервіс”, “R-Style Software Lab” та ін.

Програми автоматизації управління аудитом використовують для автоматизації управлінських процедур самих аудиторських фірм (рис. П.24).

Ці програми дають змогу:

1) щодо фінансів – розрахувати собівартість виконаних робіт на основі погодинної оплати, вести облік виконаних робіт і формувати рахунки за виконані роботи, робити розрахунки і аналіз дебіторської заборгованості;

Аудитори і експерти



*Рис. П.24. Організація командної роботи у програмах організації аудиторської діяльності*



2) стосовно документообігу — формувати довідники і тексти договорів, акти про виконані роботи;

3) щодо управління персоналом — вести облік витрат часу аудиторів з видів робіт стосовно клієнтів та інших робіт;

4) в інформаційно-аналітичній сфері — вести докладні довідники клієнтів, структурних підрозділів компанії та їх співробітників; видів робіт і годинних ставок;

5) щодо статистичного аналізу — виконувати вибірку даних за довільними критеріями, одержувати статистичні форми звітності.

Такі програми використовують протягом всього процесу аудиту: на етапі планування (планування часу та розподілу обов'язків, граничних показників фінансової звітності, показників суттєвості), на етапі організації аудиту (робота з різноманітними електронними документами, їх обробка, групування, аналіз, агрегування), на етапі контролю (внутрішня та зовнішня перевірка роботи аудиторської команди, відповідність внутрішнім стандартам та стандартам аудиту), на етапі підготовки та обґрунтування аудиторського висновку.

У світовій практиці в аудиторській консультативній діяльності використовуються системи підтримки прийняття рішень при наданні послуг з діагностики бізнесу, приватизації, дослідження ринків, оцінюванні бізнесу тощо, а також експертні системи при моніторингу діяльності клієнтів, підготовці фінансової звітності тощо.

На сьогодні аудиторські фірми розробили і використовують спеціальні інформаційні системи, орієнтовані на внутрішню регламентацію аудиторської діяльності із застосуванням внутрішньофірмових стандартів. Прикладами таких програм є системи провідних аудиторських фірм, таких як KPMG, яка використовує програму Vector 6, PricewaterhouseCoopers із системою My Client та Deloitte & Touche, спеціальною інформаційною системою якої є Audit System/2. Розглянемо структуру і функції програмних аудиторських систем на прикладі програми фірми Deloitte & Touche. Система Audit System/2 (AS/2), наприклад, поєднує можливості текстового і табличного

го редакторів і програми для складання оборотно-сальдової відомості. Вона призначена для полегшення комплексної підготовки робочої документації і звітності та проведення їх консолідації. Структура цієї програми наведена на рис. П.25.

Модуль управління документообігом (менеджер документів) забезпечує організацію системи папок, щоб допомогти стежити за масою інформації (її звичайно зберігають в аудиторських файлах), такою як робочі папери, плани аудиту, аудиторські програми і контрольні таблиці, меморандуми, пробні баланси, фінансові звіти, контактні бази даних, а також допомагає керувати цією інформацією й організувати її. Система спрощує процес обміну інформацією між членами аудиторської групи, дозволяючи їм працювати одночасно з високим ступенем безпеки.

Функції пробного балансу AS/2™ містять багаторівневу консолідацію звітів і конвертацію іноземних валют, журнал коригувань і можливість готувати відомості, плани аналітичних оглядів і фінансові звіти. Тісна інтеграція з табличним редактором Excel дає змогу готувати й аналізувати бази пробних балансів. Зручність імпорту дозволяє переносити комп'ютеризований пробний баланс клієнта в електронному вигляді прямо в програму.

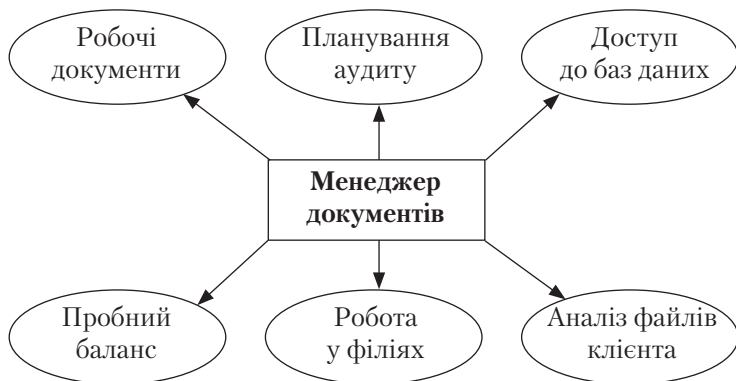


Рис. П.25. Структура програми Deloitte & Touche Audit System/2

Аналіз ринку спеціалізованих аудиторських програмних продуктів у Росії показує його крайню обмеженість (в Україні у продажу такого програмного забезпечення немає). Фактично, пропонується автоматизація окремих процедур і задач, причому, частіше за все, за авторською методикою розробників. В огляді аудиторських програм, опублікованому в російському журналі “Двойная запись”, з цього приводу пишуть: “На відміну від Заходу, де аудиторських програм хоч відбавляй, ситуація на вітчизняному ринку в цій сфері далека від блискучої. Ми нарахували всього п’ять продуктів російського виробництва для аудиторів”. Розглянемо деякі з цих програм.

Система “Асистент Аудитора” фірми “Сервіс-аудит” є професійною інформаційно-довідковою системою. Вона призначена для аудиторських фірм, приватних аудиторів, а також фірм і підприємств, що прагнуть підвищити ефективність роботи служб внутрішнього аудиту і фінансово-економічних служб. “Асистент Аудитора” дає змогу проводити пошук необхідних матеріалів різними методами, що реалізовані у цій системі (тематичний пошук, контекстний пошук, пошук за найменуванням, видом і типом документа тощо). Система “Асистент аудитор” також дає можливість систематизувати виконання аудиторських процедур, починаючи з попереднього вивчення клієнта і закінчуючи оформленням аудиторського висновку, сформуванню ряд робочих документів, необхідних для документування аудиту, що дає змогу здійснювати ефективний контроль якості аудиторських перевірок, а також забезпечити аудитора (бухгалтера, економіста) довідковим матеріалом з широкого спектра питань бухгалтерського обліку, оподаткування і фінансового аналізу.

Система складається з чотирьох умовно незалежних тематичних розділів.

Розділ “Плани і програми аудиту” містить бланки документів, які слід формувати до підписання договору на проведення аудиту, зразки договорів на різні види аудиторських послуг, бланки і зразки документів, які складаються на етапі планування аудиторської перевірки і складання програми аудиту, а та-

кож методичні матеріали, що можуть бути використані для розробки внутрішньофірмових стандартів аудиторської фірми. Анкети (листи опитування), що входять у цей розділ, можуть застосовуватися не тільки аудиторськими фірмами. За їх допомогою служби внутрішнього аудиту або фінансово-економічні служби підприємства можуть провести тестування системи внутрішнього контролю й організації бухгалтерського обліку.

Розділ “Робочі документи аудитора” містить анкети з різних ділянок бухгалтерського обліку. Вони покликані допомогти при виконанні аудиторських процедур і тестуванні окремих ділянок бухгалтерського обліку на підприємстві. У цей розділ також включені методичні матеріали, покликані допомогти в підготовці й оформленні висновку за підсумками аудиторської перевірки.

Розділ “Консультант аудитора” містить довідкові таблиці з питань бухгалтерського обліку, оподаткування, фінансового аналізу діяльності підприємств, а також оформлені у вигляді таблиць нормативи, ставки, індекси, що використовуються для розрахунків показників окремих господарських операцій, сум податків.

Розділ “Основні нормативні документи” має довідковий характер і включає основні законодавчі і нормативні відомчі акти, які регулюють аудиторську діяльність і порядок ведення бухгалтерського обліку.

Бази даних системи “Асистент Аудитора” є набором аудиторських процедур, оформлених у вигляді анкет (листів опитування), бланків, робочих карт, методик, довідкових таблиць. Велика частина документів, включених у бази даних, є оригінальними авторськими розробками, створеними фахівцями з великим практичним досвідом аудиту. Інформаційні ресурси інформаційної системи “Асистент Аудитора” постійно поповнюються, оновлюються, актуалізуються відповідно до змін у законодавчій і нормативній базі з аудиту і бухгалтерського обліку.

Програма “Помощник аудитора”, що створена російською фірмою “Гольдберг-аудит”, є спробою створити аудиторську

систему, спрямовану на розв'язання завдань аудиту на всіх етапах його здійснення.

Структура автоматизованої аудиторської системи складається з чотирьох основних блоків, функції яких відповідають чотирьом етапам проведення аудиту.

Блок підготовчого етапу містить анкету для підприємства, яке перевіряють, і бланки-тексти листів, якими обмінюються аудитор і клієнт перед висновком договору на аудит — лист-пропозиція і лист-зобов'язання. На цьому етапі здійснюють збір даних про клієнта та отриману інформацію вводять у комп'ютер для подальшого використання в інших блоках.

Блок планування містить математичні моделі й алгоритми розрахунків величин аудиторського ризику, рівня суттєвості та вибірки. Через бланки-розрахунки вводять необхідні для розрахунків вихідні дані, що відповідають типу підприємства, яке перевіряють. Введення даних можна здійснювати як вручну, так і автоматично з бухгалтерської бази. Останнє є пріоритетним, тому що розрахунки суттєвості й вибірки для конкретних процедур ґрунтуються на знанні кінцевого сальдо, дебетових і кредитових оборотів за конкретними рахунками. У результаті розрахунків програма визначає всі необхідні для планування величини.

Блок процедур аудиту найбільший і найважливіший. Основним завданням цього блоку є підготовка матеріалів для аналітичної частини аудиторського висновку. Він містить такі елементи: робочі програми аудиту за розділами; бланки-процедури для кожного розділу аудиту; бланки-тести для окремих розділів аудиту; висновки за розділами аудиту. У цьому блоці реалізують стратегію оптимізації обсягу інформації, яку вводять, з мінімізацією ризику аудиторських помилок. Це найбільш складна частина системи, спрямована на встановлення зв'язків між інформацією аудитора, що її вводять, при виконанні процедур, розрахунковими значеннями суттєвості та вибірки і формуванням висновку аудитора за конкретним розділом.

Суттєвою допомогою в роботі аудитора на цьому етапі перевірки можуть бути додаткові засоби довідкового характеру:

виклик довідково-правової системи; коротка довідка із законодавчих документів; перелік типових помилок для цієї процедури; методика виконання процедури тощо.

Блок заключного етапу, який має вступну, аналітичну і заключну частини, містить бланки-шаблони для підготовки офіційного висновку. Форми вступної і заключної частин мають стандартизований вигляд. У блоці є бланк письмової інформації аудитора керівництву економічного суб'єкта.

Іншою подібною програмою є також російська Abacus Professional, яка охоплює практично всі стадії проведення аудиторської перевірки. При першому знайомстві з клієнтом аудитор за допомогою програми може провести експрес-аудит бухгалтерської звітності. Для спрощення цієї процедури в програмі реалізована можливість введення даних з інших бухгалтерських програм у форматах СУБД Vtrieve, Clarion, Clipper, Foxpro тощо. Використання цих прийомів допомагає оперативно знайти ділянки обліку клієнта, де можливий ризик виникнення помилки, й ухвалити рішення про проведення або не проведення аудиторської перевірки. Під помилкою, яку виявляє комп'ютер, розуміють не лише математичне, а й логічне нестикування. Експрес-аудит дає змогу також приблизно оцінити обсяги вибірки, терміни проведення перевірки, суму аудиторського гонорару.

На стадії перевірки правильності оформлення документів і пов'язаних з ними проводок, накопичувальних реєстрів і авітів аудитор може використовувати спосіб дослідження за якою-небудь ознакою, наприклад за сумами або контрагентами, які здаються "підозрілими". Під дослідженням (audit trial) розуміють процедуру, під час якої аудитор перевіряє деякі первинні документи і їх відображення в реєстрах синтетичного і аналітичного обліку. Відповідна заключна кореспонденція рахунків, жорстко прив'язана в програмі до цих документів, дає змогу зробити висновок щодо правильності (або неправильності) відображення цієї господарської операції у бухгалтерському обліку.

Для формування звітів довільної форми є спеціальний конструктор документів і звітів — Abacus Designer, за допомогою

якого розробники доопрацьовують звіти за технічним завданням самих аудиторів. На базі Abacus Designer можна також підготувати контрольні акти звірки розрахунків, спеціальні звіти, в яких інформація може бути представлена в різних розрізах, з різною глибиною аналітики.

Одним з найбільш складних напрямів аудиторської діяльності є оптимізація облікової політики підприємства. Оскільки Abacus Professional підтримує роботу з кількома базами даних, аудитор може моделювати ситуацію зміни облікової політики фірми-клієнта на основі реальних даних. Таким чином, аудитор може обґрунтувати, які прибутки або втрати принесе фірмі-замовнику зміна облікової політики, і дати зважені рекомендації щодо стратегічного планування.

Ще одним прикладом є програмно-апаратний комплекс “ЕкспрессАудит: ПРОФ”, призначений для вирішення повного циклу завдань з проведення аудиторської перевірки фінансово-господарської діяльності комерційного підприємства та організації від етапу підготовки і планування аудиту до етапу формування аудиторського висновку.

Комплекс “ЕкспрессАудит: ПРОФ” складається з двох модулів. Перший модуль – “Єдиний центр планування і проведення аудиту”. Його функції: підготовка і планування аудиту; розробка програми аудиту; розподіл об’єктів аудиту за виконавцями; вивантаження персональних завдань виконавцям на носій даних для проведення аудиту на виїзді; збирання, систематизація й обробка результатів аудиторської перевірки; формування звітної документації у форматі Microsoft Word; зберігання результатів аудиторських перевірок.

Другий модуль – “Мобільне робоче місце аудитора” – призначений для вирішення таких завдань: завантаження персональної програми перевірки за виділеними об’єктами аудиту; проведення аудиту і збирання аудиторських доказів за виділеними об’єктами аудиту відповідно до персональної програми перевірки; систематизація й обробка результатів аудиторської перевірки у межах виділених об’єктів аудиту; зберігання результатів перевірки; передача результатів проведеної

перевірки об'єктів аудиту в модуль планування і проведення аудиту.

У програмному комплексі “ЕкспрессАудит: ПРОФ” етап планування аудиторської перевірки, будучи початковим етапом проведення аудиту, дає змогу вирішувати завдання розробки загального плану і програми аудиту, включаючи розподіл робіт між учасниками аудиторської групи.

На етапі планування аудиторської перевірки керівником робіт проводиться розподіл аудиторської перевірки на окремі об'єкти аудиту відповідно до таких критеріїв: обсяг робіт з перевірки; рівень підготовленості фахівців; територіальна віддаленість тощо.

Для кожного об'єкта аудиту керівник робіт формує індивідуальну програму перевірки і закріплює за ним відповідальних виконавців зі складу аудиторської групи, визначеної на етапі підготовки аудиторської перевірки. Сукупність індивідуальних програм перевірки виділених об'єктів аудиту є підсумковою програмою аудиторської перевірки, на підставі якої формуються загальний план і програма аудиту.

У програмний комплекс “ЕкспрессАудит: ПРОФ” на етапі підготовки до проведення перевірки здійснюється внесення у систему вихідних даних, необхідних для початку робіт з проведення аудиту в організації, що перевіряється (підприємстві). Далі на етапі підготовки до проведення аудиту керівником робіт у систему вносяться такі дані: реквізити організації, що перевіряється (підприємства); період аудиту; кількість людино-годин, необхідна для проведення аудиторської перевірки; планований аудиторський ризик; планований рівень істотності; перелік первинних документів, що підлягають перевірці; склад аудиторської групи.

Далі у систему вводяться планований аудиторський ризик і планований рівень суттєвості, а також визначається склад первинних документів, що підлягають перевірці, вибираються документи, форми бухгалтерської і податкової звітності, які планується перевірити під час проведення перевірки по організації (підприємству) загалом. Для автоматизації процедури створен-



ня індивідуальних програм перевірки об'єктів аудиту в програмному комплексі “ЕкспрессАудит: ПРОФ” реалізований спеціальний “Майстер створення об'єкта аудиту”, який викликається користувачем кожного разу, коли потрібно визначити новий об'єкт аудиту в межах поточної аудиторської перевірки.

У програмному комплексі “ЕкспрессАудит: ПРОФ” передбачено два варіанти проведення аудиторської перевірки сформованих об'єктів аудиту: за повною і за скороченою програмою. Залежно від вибраного варіанта система формує відповідно повний або скорочений перелік питань, що потребують обов'язкового контролю на етапі проведення аудиту. Якщо потрібно провести перевірку за скороченою програмою, то в “Майстрі створення об'єкта аудиту” слід вказати варіант перевірки — Експрес-аудит.

За кожним елементом типового об'єкта аудиту закріплений перелік питань, що підлягають обов'язковому контролю на етапі проведення аудиторської перевірки. Отже, процес формування програми перевірки об'єкта аудиту полягає у послідовному відборі необхідних елементів типових об'єктів аудиту із загального списку. Заключним етапом створення нового об'єкта аудиту в рамках поточної аудиторської перевірки є призначення відповідальних виконавців робіт з перевірки даного об'єкта аудиту зі складу членів аудиторської групи, визначеної на етапі підготовки аудиту.

Результатом роботи із системою на етапі планування аудиторської перевірки є повністю сформовані й готові до виконання загальний план і програма аудиту. На цьому етапі фахівці, які беруть участь в аудиторській перевірці, за допомогою засобів, вбудованих у програмний комплекс “ЕкспрессАудит: ПРОФ”, можуть: детально ознайомитися з повним обсягом робіт; отримати перелік питань, що підлягають аудиту і витягання з нормативних документів, знання яких потрібне при проведенні перевірки закріплених за виконавцем об'єктів аудиту; скласти персональні листи опитування, записати індивідуальну програму перевірки на носій даних для роботи на виїзді.

У програмному комплексі “ЕкспрессАудит: ПРОФ” на етапі здійснення аудиторської перевірки проводиться аудит фінансово-господарської діяльності комерційного підприємства відповідно до програми, розробленої на етапі планування аудиторської перевірки.

Вся методична частина системи реалізована у вигляді повнотекстової бази даних, що містить перелік питань (понад півтори тисячі), що охоплюють бухгалтерський облік і оподаткування фінансово-господарської діяльності підприємств.

У процесі аудиту система в діалоговому режимі послідовно пропонує аудитору питання, що потребують обов'язкового контролю відповідно до персональної програми перевірки закріплених за ним об'єктів аудиту. Якщо під час перевірки фінансово-господарської діяльності організації (підприємства) з контрольних питань, запропонованих системою, аудитор виявляє невідповідність або неповну відповідність вимогам законодавства, він має нагоду зробити про це відмітку у відповідному вікні програми, здійснюючи тим самим систематизоване збирання аудиторських доказів і формуючи послідовно робочі матеріали аудиторської перевірки.

На етапі оформлення результатів аудиторської перевірки програмний комплекс “ЕкспрессАудит: ПРОФ” дає змогу сформувати в автоматичному режимі підсумкові документи за наслідками проведеної перевірки на основі бланків документів, представлених у бібліотеці системи.

Таким чином, програмно-апаратний комплекс “Експресс Аудит: ПРОФ” може використовуватися аудиторськими організаціями для розробки загального плану і програми аудиту; створення робочої документації аудиту; вивчення і оцінювання систем бухгалтерського обліку і внутрішнього контролю економічних суб'єктів, що перевіряються; отримання аудиторських доказів про достовірність бухгалтерської звітності; отримання достовірного уявлення щодо дотримання економічним суб'єктом вимог нормативних актів; організації внутрішньофірмового контролю якості аудиту; проведення первинного аудиту початкових і порівняльних показників бухгалтерської звітності.

ті; підготовки письмової інформації аудитора й аудиторського висновку за наслідками аудиту, а також може розглядатися як помічник на кожному етапі виконання різних аудиторських процедур, починаючи з моменту оформлення договору на надання аудиторських послуг і закінчуючи безпосередньо аудиторською перевіркою.

### **Тестові завдання до теми 7**

1. Однією із переваг обробки економічної інформації клієнта є:
  - а) зниження ризику аудитора, пов'язаного з тестами, вибірковою перевіркою;
  - б) збільшення ризику аудитора при застосуванні аудиторської перевірки;
  - в) збільшення документальних засобів аудиторської перевірки.
2. Можливість автоматизації аудиторської діяльності можлива через:
  - а) застосування математичних прийомів при веденні обліку;
  - б) нормативне регулювання обліку;
  - в) зручність користування довідковими даними.
3. Поняття EUC пов'язано із:
  - а) використанням комп'ютера і його програмного забезпечення для того, щоб об'єднувати й аналізувати дані з різних джерел;
  - б) визначенням ефективності формування аудиторського висновку;
  - в) формуванням первинних документів при обліку.
4. Комп'ютерні технології в аудиті — це:
  - а) будь-які комп'ютерні програми;
  - б) аудиторські процедури;
  - в) засоби визначення аудиторського ризику.

5. Залежно від функцій програмного забезпечення можна отримати такі види вибірок:
  - а) статистичну, систематичну або випадкову;
  - б) математичну, повноцінну, незалежну;
  - в) математичну та статистичну.
6. Програмне забезпечення для проведення аудиту поділяється на:
  - а) загального використання, спеціалізоване;
  - б) математичне, спеціалізоване, економічне;
  - в) статистичне, бухгалтерське.
7. До загального програмного забезпечення відносять:
  - а) програми пакету Microsoft Office;
  - б) “1С: Підприємство”;
  - в) IDEA.
8. Перевагами методу паралельного моделювання аудиторської перевірки є:
  - а) відсутність необхідності підготовки спеціальних тестів;
  - б) підвищення ефективності аудиторських ризиків;
  - в) визначення ризиків при проведенні аудиту.
9. Ергономічність аудиторських програм — це:
  - а) наявність зручного введення великих обсягів інформації;
  - б) пристосованість до організаційних змін підприємства;
  - в) прибутковість системи.
10. Гнучкість — це:
  - а) пристосованість до організаційних змін підприємства;
  - б) прибутковість системи;
  - в) наявність зручного введення великих обсягів інформації.

## **Тема 8. Автоматизація аналітичних процедур**

### **8.1. Загальні підходи до автоматизації аудиторських аналітичних процедур**

Сьогодні аналітичні процедури проводять здебільшого вручну або за допомогою комп'ютерної техніки, яка є допоміжним засобом. Аудитор аналізує місячні коливання продажу, дебіторської та кредиторської заборгованості, запасів тощо. При цьому в програмі Excel будуються відповідні графіки, які дають змогу наочно побачити ті чи інші тренди. Проте в умовах автоматизованого бухгалтерського обліку, коли збирання та обробку обліково-економічної інформації виконують за допомогою електронних обчислювальних машин, аудитору набагато доцільніше та ефективніше використовувати комп'ютер не лише для обробки та подання інформації, а й безпосередньо в процесі аналізу даних та формулювання певних висновків.

Цей абсолютно інший за своєю суттю підхід до комп'ютеризації аналітичних процедур дає можливість, крім підвищення ефективності, значно зменшити ризик невиявлення навмисного чи випадкового викривлення даних або неправильно поставленої системи обліку. Це пояснюють тим, що за інтерфейсом зовнішнього користувача в комп'ютерній обліковій програмі знаходиться інформаційна база, дані якої можуть піддаватися певним маніпуляціям. Так, інформаційна база може бути організована у вигляді набору локальних файлів та у вигляді баз даних. Набір локальних файлів відображає однорідну множину звітних документів, які обробляються стандартними засобами операційних систем і прикладних програм. Бази даних, натомість, відображають первинні документи згідно зі спеціальними критеріями, їх обробляють програмами системи управління базами даних. Такі програми управління базами даних розробляються для кожного підприємства окремо, оскільки вони мають враховувати особливості обліку, розрахунку фінансових та інших показників, які характерні саме для цього підприємства. Це несе в собі ризик виникнення навмисних чи

випадкових помилок, які можуть бути закладені в певну програму, що робить дані, виведені на інтерфейс, некоректними.

Для того щоб мінімізувати цей ризик, аудитор може використовувати інформаційну базу, організовану саме у вигляді набору локальних файлів. Обробляти цю базу можна за допомогою бази правил, що відображає знання аудитора у формі правил і яку обробляють засобами логічного програмування або іншими програмними системами.

Для проведення аналітичних процедур таке використання комп'ютерної техніки можливе на всіх етапах аудиту. Так, на етапі планування за допомогою засобів логічного програмування можна виявити сфери підвищеного ризику, на яких необхідно сконцентрувати особливу увагу. На етапі безпосереднього проведення аудиту комп'ютерне моделювання є надзвичайно ефективним засобом збирання аудиторських доказів, а під час аналізу аудиторських висновків за допомогою заданих алгоритмів автоматично обчислюються різноманітні показники та співвідношення.

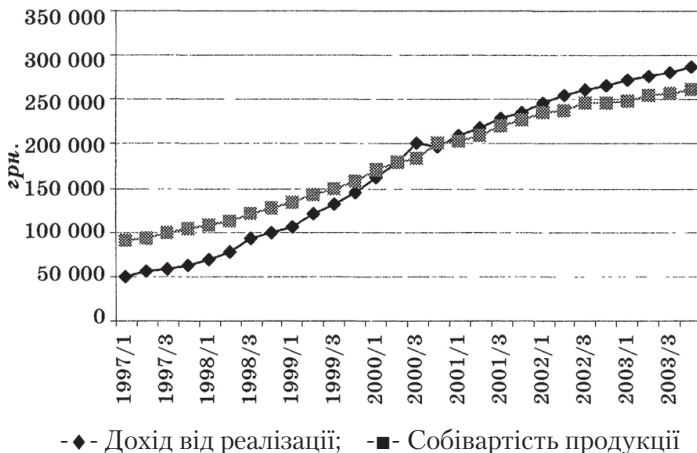
Аналітичні процедури, як уже було зазначено, на стадії планування допомагають визначити ті процеси, ризик випадкової чи навмисної помилки в яких є найбільшим. Це дає змогу аудитору відразу ж приділити особливу увагу проблемним місцям, оскільки детально перевірити всі процеси неможливо.

Розглянемо проведення аналітичних процедур на етапі планування аудиту на прикладі підприємства. Підприємство, утворене на початку 1997 р. як товариство з обмеженою відповідальністю з колективною формою власності, А виробляє та продає заморожену піцу. На початку своєї діяльності підприємство було збитковим, оскільки попит на його продукцію спочатку був невисоким (товар був порівняно новим для українського споживача), а витрати на придбання обладнання, налагодження діяльності підприємства та його збуту були досить високими. Проте, оскільки ніша заморожених продуктів, яку вибрало підприємство А для своєї діяльності, була на той час практично порожньою, попит на продукцію постійно зростав. Підприємство налагодило широку мережу постачання, а висо-

ка якість продукції, продумана рекламна кампанія та пристосування до вимог клієнтів лише розширювало її. Так, у II кварталі 2000 р. підприємство вийшло на беззбитковий рівень діяльності, а згодом почало отримувати прибутки (рис. II.26).

Одним з найважливіших процесів на підприємстві є продаж, тому аудитор під час проведення аналітичних процедур має обов'язково звернути увагу на динаміку доходу зі зміною обсягів продажу. Як видно з наведеного графіка, виручка від обсягів продажу на підприємстві А зростала швидшими темпами, ніж собівартість продукції, тому тут необхідно провести детальніший аналіз.

З процесом продажу завжди пов'язаний ризик, що підприємство завищує свій дохід від реалізації, “роздуваючи” дебіторську заборгованість. З метою покращання показників фінансової звітності підприємство може продавати продукцію в кредит маловідомим покупцям, не перевірявши перед тим належним чином їхню платоспроможність. У цьому випадку, з одного боку, ризик полягає в тому, що така дебіторська заборгованість може бути не сплаченою у майбутньому, що призведе до її списання як безнадійної на витрати підприємства. З іншого боку, збільшення дебіторської заборгованості може бути свідченням



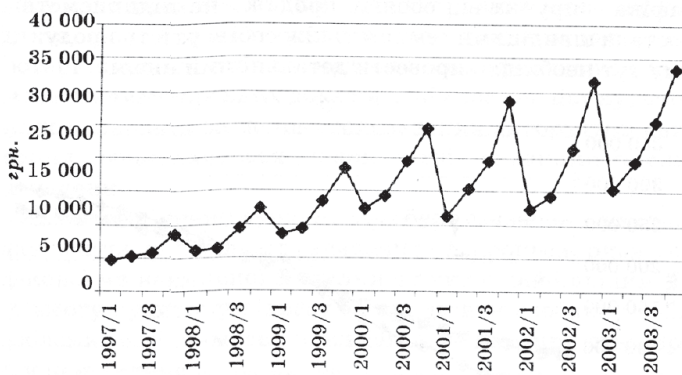
-◆- Дохід від реалізації; -■- Собівартість продукції

Рис. II.26. Динаміка доходу та витрат підприємства А

шахрайства, коли керівництво компанії фактично не продає продукцію, але збільшує обсяги продажу через фіктивних дебіторів. Тому аудитору необхідно проаналізувати динаміку дебіторської заборгованості підприємства (рис. П.27).

З цього графіка видно, що дебіторська заборгованість різко зростала кожного року у III та IV кварталах (проміжні дані). З одного боку, це можна пояснити тим, що попит на заморожену піцу зростає восени та взимку, оскільки піцу традиційно вважають продуктом сезонного характеру. Проте аналіз динаміки доходу зі зміною обсягів продажу не показав цієї сезонності – виручка зростає рівномірно протягом року. З іншого боку, таке нерівномірне збільшення дебіторської заборгованості можна пояснити бажанням керівництва підприємства покращити свою фінансову звітність на кінець року. Отже, у цьому випадку аудитору необхідно на етапі безпосереднього проведення аудиту приділити особливу увагу продажу компанії, перевірити дебіторську заборгованість через підтвердження її третьою стороною (дебітором).

Іншим важливим процесом для підприємства є виробництво продукції. Тут важливо відстежити, як змінюється собівартість продукції, визначити основну динаміку та з'ясувати, чи не було різких змін і чим вони зумовлені. На підприємстві А витрати збільшувалися рівномірно протягом усього періоду



-◆- Дебіторська заборгованість

Рис. 2.27. Динаміка дебіторської заборгованості підприємства А

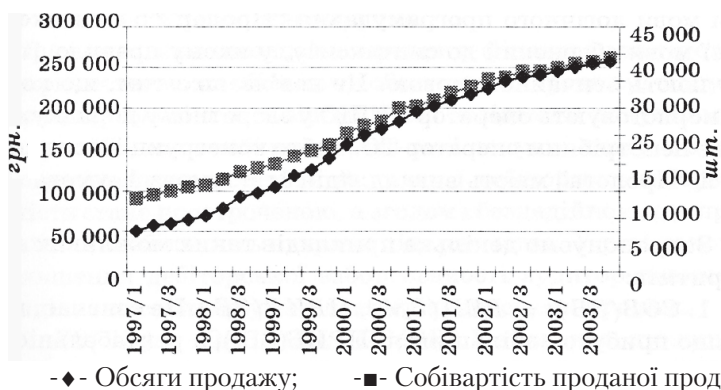


функціонування підприємства і залежали в основному від обсягів виробництва (рис. II.28).

З наведеного графіка видно, що собівартість продукції зростала разом зі збільшенням обсягів продажу, проте темп збільшення собівартості був дещо меншим, ніж темп збільшення обсягів продажу. Така тенденція є цілком закономірною, оскільки при збільшенні обсягів виробництва збільшується лише змінна частина собівартості, а фіксована залишається сталою. Аналіз витрат є надзвичайно важливим, оскільки дає можливість визначити обсяги виробництва, що відповідають точці беззбитковості, а також з'ясувати, наскільки фактичні обсяги виробництва перевищують цю межу.

Отже, на етапі планування аудиту ми проаналізували два найважливіших процеси на підприємстві: продаж та виробництво. Після проведених аналітичних процедур було визначено критичні місця, на які потрібно звернути увагу: для продажу продукції — це детальне тестування дебіторської заборгованості та прогнозування доходів від продажу на рік проведення аудиту з метою виявлення відхилень, а для виробництва продукції — це прогнозування собівартості та виявлення точки беззбитковості.

Алгоритми для проведення аналітичних процедур на цій стадії можна створити за допомогою спеціально розробленої



-♦- Обсяги продажу;      -■- Собівартість проданої продукції

Рис. II.28. Аналіз собівартості продукції підприємства А

мови логічного програмування “Пролог”. Синтаксис цієї мови обернений до синтаксису, в якому правило формулюють звичайною мовою. Це пов’язано з тим, що коли використовують оператор ЯКЩО у зворотному порядку, то стає непотрібним оператор ТО. Тобто конструкції в синтаксисі “Пролога” мають вигляд: “дія 1: — умова 1, умова 2”.

Розглянемо кілька прикладів можливих алгоритмів.

1. СОБ(ЗБ): — РЕН(ЗМ), ПРИБ(ЗБ). Це означає — якщо прибуток збільшився (ПРИБ(ЗБ)), а рентабельність зменшилась (РЕН(ЗМ)), то собівартість (вартість основних засобів та оборотних фондів) зросла (СОБ(ЗБ)). Це впливає із формули:

$$\text{Рентабельність} = \frac{\text{Прибуток}}{\text{Обсяг продажу}}.$$

Якщо прибуток збільшився, а рентабельність зменшилась, то обсяги продажу мали зрости більшою мірою, ніж прибуток, а отже, зросла і собівартість.

Висновок: у цьому випадку необхідно приділити значну увагу таким процесам, як виробництво готової продукції та придбання сировини, щоб виявити причини зростання собівартості продукції.

2. ДЗ(ЗБ): — ОДЗ(ЗБ), ДОХ(ЗБ). Це означає — якщо обороти дебіторської заборгованості збільшились (ОДЗ(ЗБ)) і дохід (виручка) від реалізації продукції зріс (ДОХ(ЗБ)), то дебіторська заборгованість теж зросла (ДЗ(ЗБ)). Це впливає із формули:

$$\text{ОДЗ} = \frac{\text{ДЗ}}{\text{Дохід від реалізації}}.$$

Якщо обороти дебіторської заборгованості і дохід від реалізації зросли, то дебіторська заборгованість мала зрости більшою мірою, ніж виручка.

Висновок: для того щоб покращити фінансову звітність, підприємство може збільшити обсяги свого продажу, відпускаючи продукцію маловідомим або невідомим покупцям у кредит. Це несе в собі ризик, що такі покупці можуть бути неспроможними сплатити за товар і дебіторська заборгованість стане про-

строченою, а згодом і безнадійною, що при її списанні збільшить витрати підприємства. У разі такого збільшення дебіторської заборгованості аудитор повинен приділити особливу увагу такому процесу, як продаж.

3. КЗ(ЗБ): – ОКЗ(ЗБ), СОБ(ЗБ). Це означає – якщо обороти кредиторської заборгованості збільшились (ОКЗ (ЗБ)) і собівартість реалізованої продукції зросла (СОБ(ЗБ)), то кредиторська заборгованість теж зросла (КЗ(ЗБ)). Це впливає із формули:

$$\text{ОКЗ} = \frac{\text{КЗ}}{\text{Собівартість}} \cdot 365.$$

Якщо обороти кредиторської заборгованості та собівартість продукції зросли, то кредиторська заборгованість мала зрости більшою мірою, ніж собівартість.

Висновок: собівартість продукції (обсяг закупівель), звичайно, може зрости. Це пояснюється збільшенням обсягу продажу, виробничими потребами тощо. Проте коли при цьому збільшується кредиторська заборгованість, це вже свідчить про певні проблеми з ліквідністю підприємства, що у майбутньому може призвести до неплатоспроможності суб'єкта господарювання. Тут потрібно приділити особливу увагу процесу придбання.

4. КБ(ЗБ): – ВК(ЗБ), КоЗаб(ЗБ). Це означає – якщо власний капітал компанії збільшився (ВК(ЗБ)), при цьому коефіцієнт заборгованості за банківськими кредитами теж зріс (КоЗаб(ЗБ)), то кредити банків відповідним чином зросли (КБ(ЗБ)). Це впливає з формули:

$$\text{КоЗаб} = \frac{\text{КБ}}{\text{Власний капітал}}.$$

Висновок: у цьому випадку отримані кредити зросли більшою мірою, ніж власний капітал, що може свідчити про певні проблеми з довгостроковою ліквідністю підприємства. У цьому разі особливу увагу потрібно приділити розділу “кредити”.

5. ЗАП(ЗБ): – ВИР(ЗБ), ПРОД(ЗМ). Якщо виробництво зросло (ВИР(ЗБ)), а продаж зменшився (ПРОД(ЗМ)), то запаси мали збільшитись (ЗАП(ЗБ)).

$$\text{ЗАП(ЗБ)} = \frac{\text{ВИР(ЗБ)}}{\text{ПРОД(ЗМ)}}.$$

Висновок: якщо за зростання обсягів виробництва та зменшення продажу запаси зменшуються, це може свідчити про розкрадання запасів продукції зі складу або погані умови зберігання, у результаті чого більша частина продукції псується. Аудитор у такому випадку повинен приділити особливу увагу запасам.

Отже, ми розглянули кілька прикладів проведення аналітичних процедур за допомогою спеціального програмного забезпечення на стадії планування аудиту. Проте слід зазначити, що такі комп'ютерні системи, призначені для зовнішнього аудиту, мають враховувати стандарти і правила тих підприємств, які перевіряються. Тому таке програмне забезпечення потрібно розробляти спеціально для кожного окремого підприємства. Зрозуміло, що витрати на розробку такої програми є досить значними, тому її використання виправдовує себе лише на великих підприємствах зі складною системою бухгалтерського обліку або на підприємствах, з якими аудиторська фірма встановила довгострокові відносини.

Для інших підприємств аудитор може обмежитися перевіркою програмного забезпечення клієнта. З цією метою переглядають відповідну документацію, ліцензії, з'ясовують, як часто вносилися зміни до системи, чи були вони авторизовані. Крім того, аудитор може провести кілька тестів на власних даних для перевірки результатів функціонування програми і їх відповідності встановленим нормативам. Після цього можна використовувати стандартне програмне забезпечення для аналізу конкретних даних.

Виявивши процеси з високим рівнем ризику, аудитор проводить перевірку по суті, одним з методів якої є ті самі аналітичні процедури. На стадії безпосереднього проведення аудиту аналітичні процедури використовують для ефективного отримання аудиторських доказів, тому вони називаються основними аналітичними процедурами (substantive analytical procedures).

Сьогодні аудитори широко використовують такі методи аналітичних процедур, як трендовий аналіз, аналіз показників, тест на прийнятність. Натомість регресійний аналіз, який потребує використання спеціального програмного забезпечення, використовують у край рідко. Однак саме регресійний аналіз дає змогу враховувати вплив багатьох факторів на змінну величину та надає досить високу надійність і правильність очікуванням аудитора.

Першим кроком під час проведення регресійного аналізу є розробка моделі. Для цього визначають фінансові та операційні змінні та встановлюють зв'язок між ними. Наприклад, витрати на заробітну плату можуть залежати від таких факторів, як робочі години, ставка зарплати, кількість працівників. При цьому важливо вибрати оптимальну кількість факторів, щоб отримана модель не була ні занадто простою (отримані аудиторські докази у такому разі будуть недостатніми), ні занадто складною (таку модель досить важко і дорого обчислювати).

Після того як модель розроблено, на її основі аудитор прогнозує залежну змінну. Цей процес важко уявити собі без використання комп'ютера. На сьогодні у світі розроблені кілька програм, які дають змогу розраховувати регресію та придатні для використання на персональних комп'ютерах. На сучасному ринку статистичних програм лідерами за якістю є такі зарубіжні пакети, як Statgraphics, Systat, SPSS, SAS, BMDP, E. Views та вітчизняні пакети “Мезозавр”, “Сани”, “Сигамд” та ін.

Після того як аудитор спрогнозував залежну змінну, він може порівняти її з фактичним значенням, при цьому важливу роль відіграє аудиторське судження в оцінюванні відхилень. Необхідно встановити, яке граничне значення відсотка відхилення вважати допустимим. Для цього оцінюють багато факторів: середовище, в якому функціонує компанія (для більш динамічного та нестабільного середовища припускають більший відсоток відхилень), ризик випадкової чи навмисної помилки, оцінений на етапі планування (для процесів, де оцінений ризик є досить високим, відсоток відхилення має бути мінімальним), природу зв'язку (зв'язок між показниками у звіті

про фінансові результати виявляється звичайно чіткіше, ніж у балансі).

Якщо отриманий відсоток відхилення є мінімальним та обґрунтованим, розраховані прогнознi дані можна вважати достатнім аудиторським доказом для підтвердження певного фінансового показника. Якщо ж відсоток відхилення перевищує припустимі межі та є необґрунтовано високим, аудитору необхідно або переглянути проведені аналітичні процедури (можливо, не було враховано певного важливого зв'язку) або проводити подальше тестування (у вигляді детальної перевірки).

## 8.2. Приклад застосування аналітичних процедур

Розглянемо на прикладі уже відомого нам підприємства А процедуру проведення основних аналітичних процедур на основі регресійного аналізу. На етапі планування ми встановили, що продаж є одним із найважливіших процесів на підприємстві. Для моделювання виручки від реалізації продукції можна скористатися трендовим аналізом, проте він не враховує впливу інших незалежних факторів на змінну величину, тобто є надто спрощеним і не дає вірогідного результату. Для ґрунтовного аналізу та прогнозування пропонуємо скласти багатofакторну регресійну модель, яка б врахувала вплив основних факторів на виручку та дала б змогу спрогнозувати дані під час проведення аудиту.

Загалом виручку підприємства (*REV*) визначають ціна (*P*) та обсяги продажу (*Q*). Обсяги продажу, тобто споживання піци населенням, у свою чергу, залежать від витрат на рекламу (*ADVER*) та доходу населення (*INCOME*).

Кейнсіанська економічна теорія визначає споживання як функцію від доходу, що залишається у розпорядженні домогосподарств. У кейнсіанській функції споживання лінійно залежить від автономного споживання ( $C_0$ ) та доходу в розпорядженні ( $Y$ ):

$$C = C_0 + cY.$$

Проте дослідження в теорії споживання, такі як теорія постійного доходу й гіпотеза життєвого циклу припускають, що поточний дохід у розпорядженні мало впливає на споживання. Основна ідея цих теорій полягає в тому, що домогосподарства вирівнюють своє споживання у часі, тобто формують свої очікування щодо майбутнього доходу і потім споживають (витрачають дохід) на основі цих очікувань. З одного боку, якщо домогосподарства передбачають стабільний (постійний) дохід, вони витратимуть велику частку його, оскільки впевнені, що матимуть цей дохід у наступному періоді. З іншого — мінливий дохід змушує домогосподарства заощаджувати, щоб компенсувати можливі майбутні витрати доходу і споживати приблизно таку саму кількість товарів і послуг. Згідно з теорією споживання з лагом, яке об'єднує всю доступну інформацію (історичну і припущення), є найкращим прогнозом поточного споживання.

Оскільки піца не є товаром першої необхідності, на неї орієнтуються в основному ті, хто мають стабільний дохід, можуть сформувати свої очікування щодо майбутнього доходу і, відповідно, споживати цей товар у поточному періоді. Тому ми в нашу модель включаємо дохід населення з лагом 1, тобто очікуваний дохід у майбутньому, та припускаємо, що чим вищий очікуваний дохід, тим більшим буде споживання у поточному періоді. Крім того, за Р. Холлом, найкращим прогнозом майбутнього споживання є споживання попередніх періодів, тому ми вводимо в нашу модель ще й обсяги продажу попереднього періоду. Введення фактора з лагом 1 тут пояснюється тим, що споживання піци багато в чому визначається смаками та вподобаннями споживачів, а не необхідністю як такою. Тому при збільшенні обсягів продажу в попередньому періоді обсяги поточного періоду теж мають зрости.

Ми вже визначили, що на дохід від реалізації впливатиме ціна продукції, причому цей зв'язок має бути додатним. Крім того, дохід підприємства від реалізації продукції часто залежить від ціни на товар-замінник, причому цей зв'язок теж є прямим. Проте для такого товару, як піца, цей зв'язок немож-

ливо простежити, оскільки яскраво вираженого товару-замінника для неї немає. Тому вводимо до нашої моделі такі фактори, як ціна на продукцію підприємства, витрати на рекламу, очікуваний дохід населення та обсяги продажу в попередньому періоді і припускаємо, що всі ці фактори позитивно впливають на дохід підприємства. Оцінювати багатофакторну регресійну модель будемо за допомогою пакета E. VIEWS version 3.0.

Це програмне забезпечення надає можливість оцінювати однофакторні та багатофакторні моделі за допомогою різних методів: методу найменших квадратів (МНК), методу непрямих найменших квадратів, двокрокового та трикрокового МНК тощо. Отже, оцінимо за допомогою пакета E. VIEWS таку модель:  $REV = f(ADVER, P, INCOME(I), Q(-1))$ . Оцінка цієї моделі за МНК дає такі результати (табл. II.5).

Таблиця II.5

### Функція доходу від реалізації продукції

Залежна змінна: REV

Метод: Найменших квадратів

Дата: 05.03.04 Час: 13:10

Вибірка (оцінена): 1997:2 2002:3

Кількість спостережень: 22

Фактор	Коефіцієнт	Стандартна помилка	t-статистика	Ймовірність
ADVER	1,411799	0,121021	3,402713	0,0034
P	13364,98	5 336,813	2,504301	0,0227
INCOME(I)	0,820090	0,380 708	2,154119	0,0459
Q(-1)	5,523499	0,510510	10,81958	0,0000
C	-88249,65	34165,68	-2,582991	0,0193

R-квадрат	0,998854	Середня залежна змінна	155286,1
Оцінений $R_2$	0,998585	Стандартне відхилення залежної змінної	70877,16
Стандартна помилка регресії	2 666,595	Інформаційний критерій Акаїке	18,81171



Сума квадратів залишків	1,21E+08	Критерій Шварца	19,05967
Логарифмічна ймовірність	-201,9288	F-статистика	3704,759
Стат. Дарбіна-Вотсона	1,854651	Ймовірність JP-статистики	0,000000

Тест RESET			
F-статистика	0,876293	Ймовірність	0,436587
Логарифмічна ймовірність	2,431053	Ймовірність	0,296554

LM-тест Бройша-Годфрея на серійну кореляцію			
F-статистика	0,135509	Ймовірність	0,874328
Спост.*R <sub>2</sub>	0,390439	Ймовірність	0,822654

Тест гетероскедастичності Байта			
F-статистика	1,811 858	Ймовірність	0,163 788
Спост.*R <sub>2</sub>	11,59 806	Ймовірність	0,170 059

Підставимо коефіцієнти

$$REV = 1,411\ 799 \cdot ADVER + 13\ 364,98 \cdot P + 0,820\ 090 \cdot INCOME(I) + 5,523\ 499 \cdot Q(-1) - 88\ 249,65$$

Як бачимо, оцінена нами модель кількісно вимірює зв'язок між незалежними змінними (факторами) та залежною змінною у вигляді коефіцієнтів. Наступні три колонки (стандартна помилка, *t*-статистика та ймовірність) оцінюють статистичну значимість цих коефіцієнтів, а всі наступні коефіцієнти – адекватність моделі загалом.

З оціненої моделі видно, що всі коефіцієнти виявились статистично значимими (це показує значення *t*-статистики, яке за спрощеним *t*-тестом Ст'юдента має бути більше 2). Зв'язок між факторами і залежною змінною, як ми і передбачали, до-

датний. Отже, при збільшенні ціни продукції на 1 грн виручка зростає на 13365 грн, а при збільшенні на 1 грн витрат на рекламу дохід від реалізації продукції збільшується на 1,41 грн, тобто дає 40 коп. прибутку.

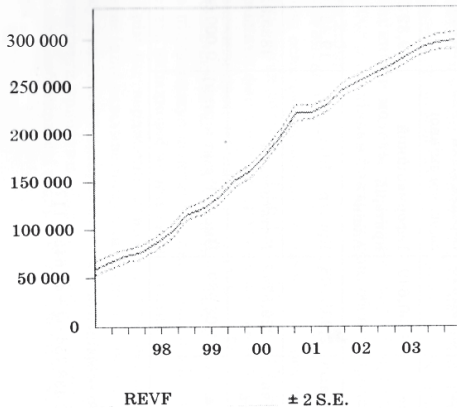
Коефіцієнт при змінній “доходи населення” визначає граничну схильність до споживання як функцію від очікуваного доходу. У цій моделі вона дорівнює 0,82 грн і означає, що з кожної гривні доходу населення витрачає 82 коп., а заощаджує, відповідно, 18 коп.

Вплив попередніх обсягів реалізації на поточну виручку теж виявився значимим: зі збільшенням обсягів продажу на одиницю у попередньому періоді, виручка зростає на 5,52 грн, що є досить вагомим показником.

Загальна якість регресії досить висока: коефіцієнт детермінації ( $R$ -квадрат) показує, що фактори регресії пояснюють близько 99 % варіації залежної змінної. Тест Фішера свідчить, що регресія є загалом адекватною, оскільки  $F$ -статистика =  $3705 > F_{\text{кр}}(4, 19, 5\%) = 2,9$  (граничне значення  $F$ -статистики для цієї кількості факторів та спостережень). Тобто у 95 % випадків наша модель буде статистично значимою. Більше того, тест RESET і тест гетероскедастичності Байта (White heteroscedasticity test) не вказують на помилки специфікації моделі ( $p$ -value  $> 0,1$ ).

Для перевірки моделі на автокореляцію залишків використовуємо тест Дарбіна-Вотсона. Оскільки розраховане значення  $d$ -статистики Дарбіна-Вотсона 1,85 потрапляє в проміжок між  $du = 1,775$  та  $4 - du = 2,225$ , то ми приймаємо гіпотезу про відсутність автокореляції з ризиком помилитись у 5 %. Крім того,  $LM$ -тест також не виявляє автокореляції помилок з імовірністю 10 %.

Отже, ми з'ясували що наша модель адекватна, і тепер можемо використовувати її для прогнозу. Треба зазначити, що для побудови моделі ми використовували квартальні дані за 1997–2002 рр. Тепер для побудови прогнозу залежної змінної, тобто виручки, ми використаємо фактичні дані незалежних змінних (факторів) за 2003 р. (рис. II.29).



Прогнозована зміна: REVF  
 Фактичне значення: REV  
 Вибірка: 1997:2 2003:4  
 Спостережень: 23

Корінь середнього квадрата пом. 2570,988  
 Середня абсолютна пом. 2129,438  
 Середня абсолютна відсоткова пом. 1,742 568  
 Коефіцієнт нерівності Тейла 0,007 336  
 Зміщення оцінки 0,000 000  
 Варіація 0,000 325  
 Коваріація 0,999 675

**Рис. II.29. Прогноз виручки від реалізації підприємства**

Для перевірки точності прогнозу виберемо значення середньої абсолютної відсоткової помилки, оскільки вона є одним із найпоширеніших критеріїв, оскільки її вимірюють у безрозмірних величинах, а саме у відсотках. Як видно з графіка, ми отримали високу точність прогнозу, оскільки значення  $MAPE = 1,74 \% \ll 10 \%$ . Тепер ми можемо порівняти фактичні та прогнозовані дані для виручки та визначити відсоток відхилення (табл. II.6).

*Таблиця II.6*

**Відхилення поквартально**

Квартал	REVF	REV	Відхилення, %
2003/1	268 043	271345	1,23
2003/2	272 773	275 467	0,99
2003/3	278 219	279 857	0,59
2003/4	282 878	286 457	1,27
Разом	1101 913	1113 126	1,02

Оскільки загальне відхилення за рік дорівнює 1,02 %, тобто є незначним, аудитор підтверджує дані клієнта як такі, що не містять випадкової чи навмисної помилки.

Іншим важливим процесом на підприємстві є виробництво, тому аудитору необхідно проаналізувати витрати на вироб-

ництво та вплив, який на них чинять інші фактори. Загалом відомо, що витрати ( $TC$ ) є функцією від обсягу випуску ( $Q$ ):  $TC = f(Q)$ . Відповідну функціональну залежність допоможе встановити однофакторна регресійна модель, яку ми оцінимо за методом МНК (табл. II.7).

Таблиця II.7

### Функція витрат

Залежна змінна:  $TC$

Метод: найменших квадратів

Дата: 05.03.04 Час: 21:26

Вибірка (оцінена): 1997:1 2002:4

Спостережень: 24

Фактор	Коефіцієнт	Стандартна помилка	$t$ -статистика	Ймовірність
$Q$	5,388439	0,077093	69,89511	0,0000
$C$	48645,81	1843,673	26,38527	0,0000
$R$ -квадрат	0,995517	Середня залежна змінна		166514,5
Оцінений $R_2$	0,995313	Середнє відхилення залежної змінної		53324,73
Стандартна помилка регресії	3650,649	Інформаційний критерій Акаїке		19,32285
Сума квадратів залишків	2,93E+08	Критерій Шварца		19,42102
Логарифмічна ймовірність	-229,8742	$f$ -статистика		4885,326
Статистика Дарбіна-Уотсона	1,08980	Ймов. ( $F$ -статистики)		0,000 000

Підставимо коефіцієнти:

$$TC = 5,388\ 438\ 754 \cdot Q + 48\ 645,8\ 117.$$

Як бачимо, всі коефіцієнти нашої моделі виявились статистично значимими ( $t$ -статистика  $> 2,00$ ). Аналізуючи коефіцієнти моделі, ми можемо зробити висновки, що коефіцієнт при  $Q$

свідчить, що зі збільшенням обсягів продажу на одиницю змінні витрати збільшуються на 5,39, а вільний член ( $C$ ) — це фіксовані (умовно-постійні) витрати, і вони становлять 48646.

Проводячи оцінку регресії загалом, ми можемо зробити такі висновки.

$R_2 = 0,99$ . Це означає, що зміна залежної змінної пояснюється змінами незалежних змінних на 99 %. Тобто наша побудована регресійна модель є адекватною реальності.

Оцінений  $R_2 = 0,99$ . Це означає, що ми маємо достатньо спостережень.

$F$ -статистика свідчить про статистичну значущість моделі. Ми маємо  $F = 4885 > F_{\text{Кр}}(1,22) = 4,3$ . Тобто у 95 % випадків наша модель буде статистично значимою.

Оцінивши модель, ми спрогнозуємо витрати на 2003 р., оскільки фактичні дані обсягів продажу в нас є (рис. II.30).

Як видно з графіка, ми отримали високу точність прогнозу, оскільки значення середньої абсолютної відсоткової помилки дорівнює 1,86 %  $\ll$  10 %. Тепер ми можемо порівняти фактичні та прогнозовані дані для витрат і визначити процент відхилення (див. табл. II.8).

Оскільки загальне відхилення за рік є незначним, аудитор підтверджує фактичні дані клієнта як такі, що не містять випадкової чи навмисної помилки.



Рис. II.30. Прогноз витрат підприємства

## Відхилення поквартально

Квартал	ТСФ	ТС	Відхилення, %
2003/1	246 714	249 345	1,07
2003/2	250 442	254 678	1,69
2003/3	254 074	257 465	1,33
2003/4	257 016	261453	1,73
Разом	1 008 246	1 022 941	1,46

Крім підтвердження даних клієнта, перед аудитором постає інше важливе завдання: дати загальну характеристику можливості підприємства функціонувати і надалі та отримувати прибутки. Для цього аудитор може провести аналіз беззбитковості підприємства, скориставшись такою формулою:

$$Q_v = \frac{FC}{P - AVC},$$

де  $Q_v$  – точка беззбитковості, в якій  $TR = 169$  шт.;  $FC$  – фіксовані (умовно-постійні) витрати підприємства, грн.;  $P$  – ціна на продукцію підприємства, грн.;  $AVC$  – середні змінні витрати, які визначаються як  $VC/Q$ , грн.

Точку беззбитковості обчислюємо для ціни  $P = 7,34$ , оскільки протягом 2003 р. ціна не змінювалась і підприємство не планує збільшувати її найближчим часом.

$$Q_v = \frac{48646}{7,34 - 5,39} = 24947.$$

Таким чином, за кварталних обсягів продажу 24947 шт. підприємство виходить на рівень беззбитковості. За четвертий квартал 2003 р. обсяги продажу підприємства досягли 38670 шт., що значно перевищує точку беззбитковості.

Отже, на прикладі моделювання функцій доходу та витрат, прогнозування значень показників та порівняння їх з фактичними відповідними значеннями, ми показали, як аналітичні процедури можна використовувати на етапі безпосереднього проведення аудиту для отримання аудиторських доказів та як спеціальне програмне забезпечення можна використовувати

для проведення цих аналітичних процедур. Тепер перейдемо до наступного етапу аудиторської перевірки: аналізу та узагальнення.

На останній стадії, стадії аналізу аудиторських висновків, узагальнення результатів та документування аудитор проводить аналіз фінансового стану підприємства на основі підтвердженої ним фінансової звітності. Такий аналіз теж належить до різновиду аналітичних процедур і полягає в тому, щоб виявити позитивні та негативні тенденції на рівні фінансової звітності, дати узагальнену оцінку можливості підприємства функціонувати у майбутньому та розраховуватися за своїми боргами.

Загалом аналіз фінансового стану підприємства — досить громіздка і складна процедура. Проте використання комп'ютерної техніки може значно полегшити це завдання, збільшити ефективність і точність розрахунків. Показники фінансової діяльності підприємства поділяються на показники ліквідності, фінансової стійкості, ділової активності, рентабельності та інвестиційної активності. Формули цих показників дають змогу проводити аналіз за допомогою спеціального програмного забезпечення. За допомогою певних алгоритмів програма може надати загальний висновок про фінансовий стан підприємства.

Проведемо аналіз фінансового стану підприємства А на основі його фінансової звітності на 31 грудня 2003 р. Розроблено певний алгоритм дій, де кожному обчисленому показнику та визначеній тенденції присвоюють певну кількість балів на основі граничних значень показників, визначених у методиці інтегральної оцінки інвестиційної привабливості підприємств та організацій. На основі суми цих балів можна визначити загальний фінансовий стан підприємства. Якщо записати цей алгоритм дій мовою логічного програмування, система зможе оцінювати фінансовий стан підприємства автоматично.

### **Показники ліквідності підприємства**

Коефіцієнт покриття:

$$K_{п\ 2003} = \frac{117900}{75000} = 1,57; \quad K_{п\ 2002} = \frac{99900}{58400} = 1,71.$$

Присвоюється: “9” –  $K_{\text{п}} > 2$  і зростає; “6” –  $K_{\text{п}} > 2$  і зменшується; “3” –  $K_{\text{п}} < 2$  і збільшується; “0” –  $K_{\text{п}} < 2$  і зменшується.

Як бачимо, значення коефіцієнта покриття у 2003 та 2002 рр. було нижчим, ніж гранично встановлене значення 2, отже, поточні активи підприємства не покривають достатньою мірою його поточних зобов’язань. Крім того, значення коефіцієнта у 2003 р. зменшилось порівняно з 2002 р., отже, за даним показником присвоюється “0” балів.

Коефіцієнт швидкої ліквідності:

$$K_{\text{ш.л}} 2003 = \frac{33\,400 + 1300 + 3600 + 100 + 2500 + 1200}{75000} = 0,56;$$

$$K_{\text{ш.л}} 2002 = \frac{31500 + 2100 + 1200 + 100 + 1600 + 2900}{58400} = 0,67.$$

Присвоюється: “9” –  $K_{\text{ш.л}} > 1$  і зростає; “6” –  $K_{\text{ш.л}} > 1$  і зменшується; “3” –  $K_{\text{ш.л}} < 1$  і збільшується; “0” –  $K_{\text{ш.л}} < 1$  і зменшується.

Граничне значення коефіцієнта швидкої ліквідності становить 1, оскільки він не враховує таких малоліквідних активів, як запаси. Для підприємства А його значення у 2003 і 2002 рр. нижче від 1, у 2003 р. зменшується. Тому цьому показнику теж присвоюється 0 балів.

Коефіцієнт абсолютної ліквідності:

$$K_{\text{а.л}} 2003 = \frac{1200}{75000} = 0,01; \quad K_{\text{а.л}} 2002 = \frac{2900}{58400} = 0,04.$$

Присвоюється: “9” –  $K_{\text{а.л}} > 0,2$  і зростає; “6” –  $K_{\text{а.л}} > 0,2$  і зменшується; “3” –  $K_{\text{а.л}} < 0,2$  і збільшується; “0” –  $K_{\text{а.л}} < 0,2$  і зменшується.

Коефіцієнт абсолютної ліквідності характеризує негайну готовність підприємства розрахуватися зі своїми короткостроковими зобов’язаннями, його значення має перевищувати 0,2. У цьому випадку значення коефіцієнта значно нижче, ніж граничне, тому ми робимо висновок про те, що грошових коштів підприємства недостатньо для негайних розрахунків. Цьому показнику присвоюється 0 балів.



Робочий капітал:

$$P_{к2003} = 117\,900 - 75\,000 = 42\,900;$$

$$P_{к2002} = 99\,900 - 58\,400 = 41\,500.$$

Присвоюється: “9” –  $P_{к} > 0$  і зростає; “6” –  $P_{к} > 0$  і зменшується; “3” –  $P_{к} < 0$  і збільшується; “0” –  $P_{к} < 0$  і зменшується.

Як бачимо, у 2003 і 2002 рр. робочий капітал підприємства А був позитивний, крім того, у 2003 р. він зріс порівняно з 2002 р., тобто цьому показнику ми можемо присвоїти 9 балів.

### Показники фінансової стійкості

Коефіцієнт автономії:

$$K_{а2003} = \frac{150600}{225600} = 0,66;$$

$$K_{а2002} = \frac{148100}{206500} = 0,71.$$

Присвоюється: “9” –  $K_{а} > 0,5$  і зростає; “6” –  $K_{а} > 0,5$  і зменшується; “3” –  $K_{а} < 0,5$  і збільшується; “0” –  $K_{а} < 0,5$  і зменшується.

У 2003 і 2002 рр. значення показника перевищувало 0,5, тобто залежність підприємства від зовнішніх джерел фінансування є малою. Проте враховуючи, що коефіцієнт автономії у 2003 р. порівняно з 2002 р. зменшився, цьому показнику можемо присвоїти 6 балів.

Коефіцієнт фінансової стабільності:

$$K_{ф.с2003} = \frac{150600}{75000} = 2,00;$$

$$K_{ф.с2002} = \frac{148100}{58400} = 2,53.$$

Присвоюється: “9” –  $K_{ф.с} > 1$  і зростає; “6” –  $K_{ф.с} > 1$  і зменшується; “3” –  $< 1$  і збільшується; “0” –  $K_{ф.с} < 1$  і зменшується.

У 2003 та 2002 рр. власний капітал перевищував залучений вдвічі, тобто фінансова стабільність підприємства є досить високою. Проте значення показника у 2003 р. зменшилося порівняно з 2002 р., тому даному показнику даємо 6 балів.

Коефіцієнт зовнішньої заборгованості:

$$K_{з.з2003} = \frac{20500}{150600} \cdot 100 = 13\%;$$

$$K_{з.з2002} = \frac{31600}{148100} \cdot 100 = 21\%.$$

Присвоюється: “9” –  $K_{з.з} < 50\%$  і зменшується; “6” –  $K_{з.з} < 50\%$  і збільшується; “3” –  $K_{з.з} > 50\%$  і зменшується; “0” –  $K_{з.з} > 50\%$  і збільшується.

Як бачимо, частка позикових коштів у власному капіталі підприємства у 2003 та 2002 рр. незначна і, крім того, у 2003 р. зменшується. Це свідчить про незначний фінансовий ризик для підприємства, тому ми присвоюємо тут 9 балів.

### Показники ділової активності

Коефіцієнт оборотності активів:

$$K_{o.a} 2003 = \frac{1113100}{(206500 + 225600): 2} = 5,15;$$

$$K_{o.a} 2002 = \frac{1029500}{(206500+190600): 2} = 5,18.$$

Присвоюється: “9” –  $K_{o.a} > 5$  і зростає; “6” –  $K_{o.a} > 5$  і зменшується; “3” –  $K_{o.a} < 5$  і збільшується; “0” –  $K_{o.a} < 5$  і зменшується.

Як видно з обчислених коефіцієнтів, активи з погляду реалізації на підприємстві А використовують досить ефективно. Так, на кожну гривню, вкладену в активи підприємства, у 2003 та 2002 рр. припадає майже 5,2 грн реалізації. Тому цьому коефіцієнту присвоюється 9 балів.

Коефіцієнт оборотності основних засобів (фондовіддачі):

$$K_{\phi} 2003 = \frac{1113100}{(107700 + 106600): 2} = 10,38;$$

$$K_{\phi} 2002 = \frac{1029500}{(106600+104400): 2} = 9,75.$$

Присвоюється: “9” –  $K_{\phi} > 12$  і зростає; “6” –  $K_{\phi} > 12$  і зменшується; “3” –  $K_{\phi} < 12$  і збільшується; “0” –  $K_{\phi} < 12$  і зменшується.

Отже, у 2003 р. на кожну гривню, вкладену в основні засоби підприємства, припадає 10,4 грн реалізації. Звідси ми можемо зробити висновок, що основні засоби використовуються досить ефективно, проте тривалість їх обороту менша 30 днів (365/обор.), що є граничним значенням. Зважаючи на те, що коефіцієнт оборотності основних засобів збільшується у 2003 р., у цьому випадку все ж присвоюється 3 бали.

Коефіцієнт оборотності виробничих запасів:

$$K_{o.з} 2003 = \frac{1022900}{(75800 + 60500): 2} = 15,00;$$

$$K_{o.з} 2002 = \frac{965700}{(60500 + 56600): 2} = 16,49.$$

Присвоюється: “9” –  $K_{o.з} > 12$  і зростає; “6” –  $K_{o.з} > 12$  і зменшується; “3” –  $K_{o.з} < 12$  і збільшується; “0” –  $K_{o.з} < 12$  і зменшується.

Значення коефіцієнта за 2003 р. показує, що виробничі запаси протягом звітного року здійснюють 15 оборотів, тобто тривалість їх обороту менша за 30 днів, що є граничним значенням. Але, зважаючи на те, що коефіцієнт оборотності у 2003 р. зменшився порівняно з 2002 р., ми присвоюємо цьому коефіцієнту 6 балів.

Тривалість погашення дебіторської заборгованості в днях:

$$K_{д.з} 2003 = \frac{33400 + 100 + 2500}{1113100} \cdot 365 = 11,80;$$

$$K_{д.з} 2002 = \frac{31500 + 100 + 1600}{1029500} \cdot 365 = 10,95.$$

Присвоюється: “9” –  $K_{д.з} < 30$  і зменшується; “6” –  $K_{д.з} < 30$  і збільшується; “3” –  $K_{д.з} > 30$  і зменшується; “0” –  $K_{д.з} > 30$  і збільшується.

Значення показника за 2003 р. означає, що дебіторська заборгованість покупців перетворюється на грошові кошти приблизно за 12 днів. Загалом, чим менша сума тривалості погашення, тим ефективніше підприємство управляє своєю дебіторською заборгованістю, тож необхідно, щоб значення цього показника зменшувалося. Ми ж маємо деяке збільшення за 2003 р. порівняно з 2002 р. Тому цьому показнику присвоюється 6 балів.

Тривалість погашення кредиторської заборгованості в днях:

$$T_{к.з} 2003 = \frac{42200}{102200} \cdot 365 = 15,05; \quad T_{к.з} 2002 = \frac{16700}{965700} \cdot 365 = 6,31.$$

Присвоюється: “9” –  $T_{к.з} < 30$  і зменшується; “6” –  $T_{к.з} < 30$  і збільшується; “3” –  $T_{к.з} > 30$  і зменшується; “0” –  $T_{к.з} > 30$  і збільшується.

Значення показника за 2003 р. означає, що кредиторська заборгованість перетворюється на грошові кошти приблизно за 15 днів. Загалом, чим менша сума тривалості погашення, тим ефективніше підприємство управляє своєю кредиторською заборгованістю, тож необхідно, щоб значення цього показника зменшувалося. Ми ж маємо значне збільшення за 2003 р. порівняно з 2002 р. Тому цьому показнику присвоюється 6 балів.

### Показники рентабельності підприємства

При обчисленні показників рентабельності вимоги однакові.

Присвоюється: “9” –  $K > 10\%$  і зростає; “6” –  $K > 10\%$  і зменшується; “3” –  $K < 10\%$  і збільшується; “0” –  $K < 10\%$  і зменшується.

Рентабельність залученого капіталу:

$$P_{з.к\ 2003} = \frac{22400}{(150600 + 148100) : 2} 100 = 14,00\%;$$

$$P_{з.к\ 2002} = \frac{21700}{(148100 + 146300) : 2} 100 = 14,74\%.$$

Значення показника за 2003 та 2002 рр. показують, що підприємство досить ефективно використовує власний та залучений капітал: значення коефіцієнта перевищує граничний показник 10 %. Тому цьому показнику присвоюємо 9 балів.

Рентабельність активів:

$$P_{а\ 2003} = \frac{90200}{(225600 + 206500) : 2} 100 = 41,74\%;$$

$$P_{а\ 2002} = \frac{63800}{(206500 + 190600) : 2} 100 = 32,00\%.$$

Цей показник показує величину одержаного прибутку в розрахунку на одну гривню активів. Його значення у 2003 та 2002 рр. значно перевищують 10 %, тобто рентабельність активів підприємства А є надзвичайно високою. Цьому показнику присвоюємо 9 балів.

Рентабельність продажу:

$$P_{п 2003} = \frac{90200}{1113100} 100 = 8,10 \%;$$

$$P_{п 2002} = \frac{63800}{1029500} 100 = 6,19 \%.$$

Цей показник характеризує обсяг прибутку, що надходить на підприємство з кожної гривні від продажу продукції. Як бачимо, у 2003 та 2002 рр. рентабельність продажу підприємства не була високою: вона навіть не перевищувала граничного значення 10 %. Проте значення показника у 2003 р. порівняно з 2002 р. зросло, тому тут присвоюється 3 бали.

Чиста рентабельність підприємства:

$$P_{ч 2003} = \frac{13400}{1113100} 100 = 1,20 \%;$$

$$P_{ч 2002} = \frac{12900}{1029500} 100 = 1,25 \%.$$

Цей показник демонструє загальну рентабельність підприємства після вирахування всіх витрат. Як бачимо, чиста рентабельність підприємства є дуже малою, тому цьому показнику присвоюється 0 балів.

Тепер, коли обчислено основні фінансові показники та надано їм певні бали, можна за загальною кількістю цих балів визначити фінансовий стан підприємства. Зробити це можна за такою шкалою (табл. II.9).

*Таблиця II.9*

#### **Шкала для визначення фінансового стану підприємства**

<b>Сума балів</b>	<b>Значення</b>
>120	Фінансовий стан підприємства дуже стабільний. Підприємство має достатню кількість високоліквідних активів, є фінансово незалежним, має високу оборотність активів і хороші показники рентабельності
72–120	Фінансовий стан загалом стабільний, проте потребує певного покращання. Слід приділити увагу проблемним місцям, окремо оцінити їх важливість для підприємства

24–72	Фінансове становище підприємства погане, основні показники не відповідають граничним значенням. Найвні тенденції погіршення фінансового стану
0–24	Негативна оцінка фінансового стану підприємства. Є великий ризик банкрутства

На основі цих значень комп'ютерна програма може автоматично дати оцінку фінансового стану підприємства, що значно полегшує це громіздке завдання. Для підприємства А оцінка виглядатиме таким чином (табл. II.10).

За сумою балів підприємство А можна віднести до другої групи: його фінансовий стан можна охарактеризувати загалом

*Таблиця II.10*

**Розподіл балів для визначення фінансового стану підприємства А**

<b>Показник фінансового стану підприємства</b>	<b>Бал</b>
Коефіцієнт покриття	0
Коефіцієнт швидкої ліквідності	0
Коефіцієнт абсолютної ліквідності	0
Робочий капітал	9
Коефіцієнт автономії	6
Коефіцієнт фінансової стабільності	6
Коефіцієнт зовнішньої заборгованості	9
Коефіцієнт оборотності активів	9
Коефіцієнт фондівіддачі	3
Коефіцієнт оборотності виробничих запасів	6
Тривалість погашення дебіторської заборгованості	6
Тривалість погашення кредиторської заборгованості	6
Рентабельність залученого капіталу	9
Рентабельність активів	9
Рентабельність продажу	3
Чиста рентабельність підприємства	0
Разом	81

як задовільний, проте такий, що потребує певного покращання. Аудитор повинен у цьому випадку додатково оцінити показники, що не відповідають встановленим нормативам, передбачити наслідки, що можуть виникнути через ці проблемні місця на підприємстві у майбутньому. Крім того, аудитор може запропонувати керівництву компанії своє бачення вирішення проблеми, дати рекомендації, поради. Якщо певне негативне значення показника може мати досить вагомий вплив на функціонування підприємства у майбутньому, це належним чином відображається в аудиторському висновку.

Отже, ми розглянули різні методи аналітичних процедур на різних етапах аудиторської перевірки. При цьому було показано, що за допомогою спеціального програмного забезпечення та комп'ютерної техніки можна значно підвищити ефективність проведення аудиторської перевірки. З одного боку, це виявляється у можливості отримати точніші результати та певніші аудиторські докази, а з другого — в оптимізації витрат, що на ринку аудиторських послуг дає величезну конкурентну перевагу.

### **Тестові завдання до теми 8**

1. Комп'ютеризація аналітичних процедур дає змогу:
  - а) зменшити ризик невиявлення неправильно поставленої системи обліку;
  - б) використовувати автоматизовані аналітичні процедури аудиту;
  - в) подати інформацію у вигляді таблиць.
2. На етапі планування за допомогою засобів логічного програмування можна:
  - а) виявити сфери підвищеного ризику;
  - б) виявити ризик невиявлення неправильно поставленої системи обліку;
  - в) подати інформацію у вигляді таблиць.
3. Найбільш поширені методи аналітичних процедур:
  - а) трендовий аналіз;

- б) вертикальний аналіз звітності;
  - в) горизонтальний аналіз звітності.
4. Регресійний аналіз дає змогу:
- а) виявити вплив багатьох факторів на змінну величину;
  - б) проаналізувати структуру показників;
  - в) визначити елементи аудиторського ризику.
5. Якщо значення коефіцієнта покриття є нижчим гранично встановленого, то:
- а) поточні активи підприємства не покривають достатньою мірою його поточних зобов'язань;
  - б) поточні активи підприємства покривають достатньою мірою його поточних зобов'язань;
  - в) спостерігається низька рентабельність виробництва.
6. Коефіцієнт абсолютної ліквідності характеризує:
- а) негайну готовність підприємства розрахуватися зі своїми короткостроковими зобов'язаннями;
  - б) поточні активи підприємства покривають достатньою мірою його поточних зобов'язань;
  - в) спостерігається низька рентабельність виробництва.
7. Фінансова стабільність підприємства досить висока, якщо:
- а) власний капітал перевищував залучений вдвічі;
  - б) власний капітал менший залученого вдвічі;
  - в) поточні активи підприємства покривають достатньою мірою його поточних зобов'язань.
8. Рентабельність активів показує:
- а) величину одержаного прибутку в розрахунку на одну гривню активів;
  - б) поточні активи підприємства покривають достатньою мірою його поточних зобов'язань;
  - в) ліквідність підприємства.
9. Рентабельність продажу показує:
- а) обсяг прибутку, що надходить на підприємство з кожної гривні від продажу продукції;



- б) величину одержаного прибутку в розрахунку на одну гривню активів;
  - в) поточні активи підприємства покривають достатньою мірою його поточних зобов'язань.
10. Рекомендується для оцінки фінансового стану підприємства використовувати:
- а) шкалу балів;
  - б) фінансові показники;
  - в) показники ліквідності.

## Тема 9. Аудит інформаційної безпеки підприємства

### 9.1. Класифікація загроз та вимоги до інформаційної безпеки підприємства

Виходячи із загального визначення інформаційної системи як системи, що збирає, зберігає, обробляє і надає користувачам інформацію, процес функціонування будь-якої інформаційної системи з погляду загроз її функціонуванню можна подати таким чином (рис. П.31).

Як зазначалося, безпечною є інформаційна система, що задовольняє такі властивості інформації:

- цілісність — відповідає стану системи, коли інформація є вчасною, точною і повною;

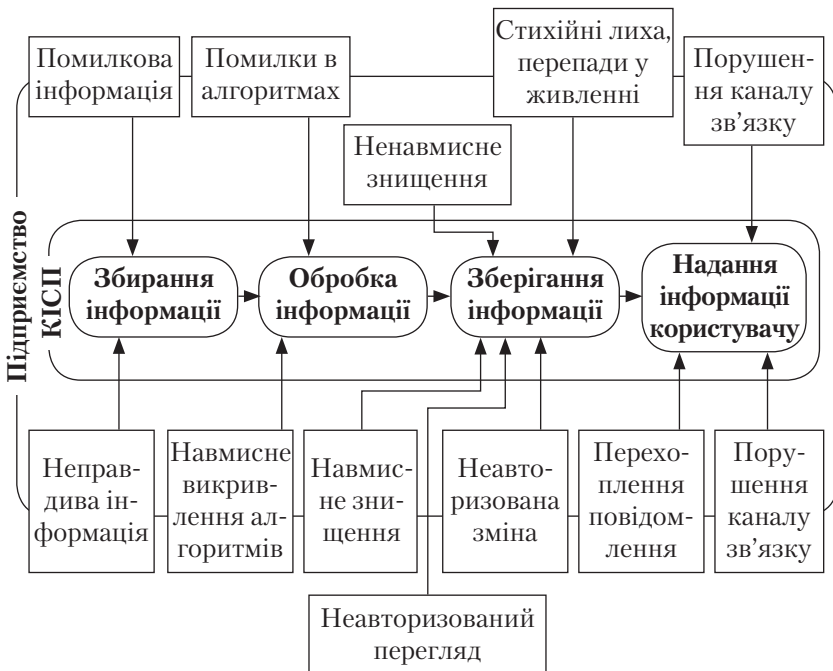


Рис. П.31. Загрози інформаційній безпеці підприємства

- конфіденційність — вимога, щоб до приватної або конфіденційної інформації, що міститься у системі, мали доступ тільки уповноважені користувачі;
- доступність — вимога, щоб система працювала коректно і не відмовляла у доступі легальному користувачу.

Використання КІСП для потреб управління підприємством створює додаткові ризики невиявлення помилок в обліку та винесення аудитором помилкового судження.

Приклади причин помилок в обліковій інформації при застосуванні КІСП наведені у табл. II.11.

*Таблиця II.11*

**Приклади появи можливих помилок в обліковій інформації при застосуванні КІСП**

№ пор.	Найменування	Приклад
1	2	3
1	Зменшення ступеня залучення персоналу	Якщо обліковий персонал чи аудитор не мають можливості безпосереднього візуального спостереження первинної інформації, що вводиться (чи можуть тільки перевірити результати обробки даних у формі звітів), це підвищує ймовірність пропуску помилок і неточностей
2	Помилки в програмних алгоритмах	У спрощених і навіть у складних КСБО іноді (наприклад, при неправильному складанні бухгалтером чи програмістом визначеного алгоритму часто повторюваних розрахунків — скажімо, за ПДВ) підвищується ймовірність системних помилок і неточностей. При цьому, навіть якщо вони несуттєві кожна окремо, їх сукупний накопичений за рік ефект може значно спотворити звітність загалом
3	Порушення конфіденційності	Можливий витік або несанкціонована зміна інформації (у тому числі і конфіденційної), внесення небажаних змін у саму систему, а також матеріальні втрати (розкрадання кош-

1	2	3
		тів, товарно-матеріальних цінностей та інших активів) у результаті шахрайства з використанням комп'ютерів
4	Порушення цілісності	Подання обліково-аналітичної інформації у формі великої бази даних обтяжено потенційним ризиком перекручування чи навіть втрати фрагментів (а іноді — і всього обсягу) цієї інформації, необхідності її термінового відновлення в значних масштабах і як наслідок — у суттєвих за часом перервах при обробці поточної облікової інформації

Крім того, Положення про міжнародну аудиторську практику № 1008 “Оцінка ризиків та внутрішній контроль — характеристика КІС та пов’язані з ними питання” передбачало, зокрема, що в КІСП наявна вразливість засобів зберігання даних і програм, — великі обсяги даних і комп’ютерні програми, що використовуються для обробки інформації, можуть зберігатися на вбудованих або зйомних носіях інформації, таких як магнітні диски і плівка. Такі носії інформації можуть бути украдені, загублені, навмисно або випадково знищені.

## 9.2. Етапи аналізу ризиків, пов’язаних із безпекою інформаційної системи

Аналіз ризиків, пов’язаних із безпекою інформаційної системи, передбачає чотири етапи:

- ідентифікацію засобів захисту на визначеній ділянці інформаційної системи;
- оцінку надійності засобів захисту на цій ділянці;
- оцінку ймовірності, що акт порушення безпеки буде успішний, з огляду на набір засобів захисту на цій ділянці інформаційної системи та їх надійності;

- оцінку втрат, що понесе підприємство, якщо акт порушення безпеки обійде засоби захисту в цьому місці інформаційної системи.

Розглянемо перший етап: ідентифікація засобів захисту на визначеній ділянці інформаційної системи. Напевне, найлегший спосіб це зробити — використати анкетні опитування, розроблені, щоб оцінити безпеку. Вони містять детальні переліки питань щодо засобів захисту, які аудитори можуть використовувати, щоб систематично визначати, чи працює певний засіб. Аудитори можуть використовувати інтерв'ю, спостереження, документацію, щоб одержати інформацію про засоби захисту на визначеній ділянці інформаційної системи.

Для оцінки надійності цих засобів захисту, аудитор повинен їх тестувати. У деяких випадках тести є безпосередніми. Наприклад, легко визначити, чи запобігають замкнені двері неправомірному доступу в приміщення, де розташовані комп'ютери.

Деякі типи засобів захисту, однак, складно перевірити. Наприклад, щоб перевірити, чи працює система пожежегасіння, потрібно було б розпалити пожежу, а потім запустити систему пожежегасіння, щоб оцінити її ефективність. У деяких ситуаціях, пов'язаних із підвищеним ризиком, аудитори можуть періодично моделювати займання у комп'ютерній кімнаті, щоб визначити, чи гасить система вогонь. Зазвичай, аудитори покладаються на звіти технічного обслуговування і гарантії виробника, що система буде працювати ефективно.

Коли всі чотири етапи аналізу ризиків, пов'язаних з безпекою інформаційної системи, пройдені, можуть бути визначені слабкі місця, пов'язані з інформаційною функцією систем. Ризик, пов'язаний з безпекою, — це очікуваний розмір втрат за визначений період з огляду на надійність засобів захисту. Слабкі місця виникають, тому що немає ніякого засобу, щоб запобігти акту порушення безпеки, або є імовірність, що засіб забезпечення безпеки на визначеній ділянці інформаційної системи не спрацює проти специфічного інциденту, що відбудеться.

Запобігти ризикам та забезпечити вимоги до безпеки інформації покликані засоби інформаційної безпеки КІСП. Аудитор

зобов'язаний виявити слабкі місця внутрішніх засобів контролю КІСП – розглянути як апаратні, так і програмні засоби контролю, а також організаційні заходи, які становлять на підприємстві процес управління захистом КІСП (рис. П.32).

Щоб оцінити ймовірність того, що акт порушення безпеки обійде засоби захисту, аудитор:

- 1) розглядає кожний з активів або кожен з груп активів, визначених на другому етапі аналізу ризиків, пов'язаних з безпекою;
- 2) розглядає кожен з можливих загроз, ідентифікованих протягом четвертого етапу аналізу;
- 3) визначає, чи існує засіб захисту, щоб запобігти акту порушення безпеки.

Якщо так, оцінює ймовірність ефективної роботи засобу захисту та ймовірність усунення або пом'якшення ефекту від акту злочину.

Оскільки можливість різних зловживань здебільшого створюється браком необхідних програмних засобів контролю, а система автоматизованого контролю має бути передбачена в проекті автоматизації обліку, то аудитор за будь-якого рівня автоматизації бухгалтерського обліку повинен перевіряти про-

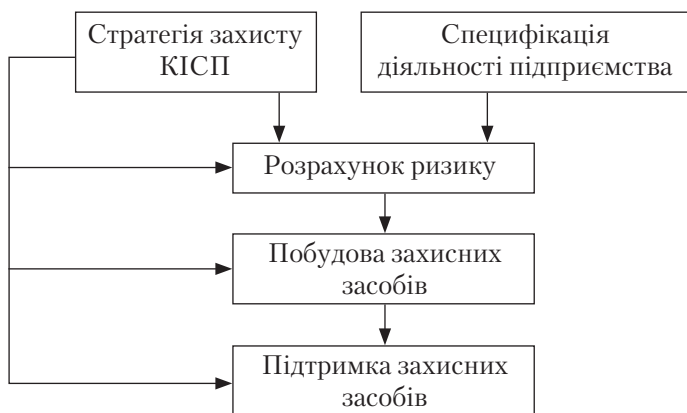


Рис. П.32. Процес управління захистом КІСП

ектну документацію на створення такої підсистеми. Документація перевіряється на наявність у проекті засобів автоматизованого контролю — як для забезпечення достовірності інформації, що обробляється на основних етапах облікового процесу, так і для виявлення різного роду зловживань. У результаті такої перевірки можуть бути виявлені “слабкі” місця (з контрольних позицій) у програмі, що не перешкоджають здійсненню порушень, зловживань. Наприклад, відсутність програмного контролю внутрішнього переміщення матеріальних цінностей і грошових коштів тощо.

Також аудитору слід проаналізувати систему контролю підготовки облікових даних, перевірити, які заходи вжиті в клієнта для запобігання помилкам і фальсифікаціям. Слід зазначити способи організації контролю повноти і правильності введення первинної інформації в інформаційну базу, контролю обробки і висновку даних, дати оцінку їх достатності й ефективності. У багатокористувацьких мережевих системах об’єктом уваги має бути контроль передачі даних.

Якщо внутрішні засоби контролю можуть відмовити з певною ймовірністю, аудиторська оцінка цілісності даних має бути сформульована у термінах імовірнісного розподілу виникнення помилки.

Завжди, якщо можливо, аудитори повинні використовувати аналітичні моделі для підтримки у підготовці аудиторського висновку. Це справедливо, коли проводиться не тільки аудит фінансової звітності, а й спеціалізований аудит інформаційної безпеки. За допомогою аналітичних моделей аудитори, як правило, можуть оцінити значення залежних змінних, які їх цікавлять, з невеликими витратами у широкому діапазоні значень і структури моделі. Наприклад, детерміновані моделі та ймовірнісні моделі здебільшого можуть бути розроблені досить швидко й дешево.

Іноді, однак, аналітичні моделі не можна використати при підготовці висновку щодо інформаційної безпеки. Для початку, аудитор може вирішити, що припущення, які лежать в основі моделей, занадто вузькі і не відображають дійсність досить

добре. Крім того, іноді аналітичні моделі не дозволяють математичні перетворення, тому що відповідні рівняння, використані для моделювання системи, виражені не в явному вигляді, або не мають рішень. У цих випадках аудитор для підтримки складання аудиторського висновку може використати симуляційні моделі.

Коли аудитор формулює висновок, він прагне визначити вплив сильних і слабких сторін окремих внутрішніх засобів контролю на загальну надійність системи. Він робить висновок наприкінці попередньої оцінки внутрішньої системи управління і після того, як закінчені тести засобів контролю і тестування по суті.

### **9.3. Оцінка системи внутрішніх засобів контролю**

Оцінку системи внутрішніх засобів контролю потрібно розглядати в межах структури рентабельності. Аудитор має оцінити потік прибутків і витрат, пов'язаних з розробкою, впровадженням, функціонуванням і обслуговуванням внутрішньої системи захисту. Він повинен також оцінити дисконтну ставку, яку буде використовувати для цього потоку прибутку і витрат. На закінчення аудитор може обчислити чисту приведену вартість системи (net present value), щоб визначити, чи треба робити в неї інвестиції.

Як видно з рис. П.30, найбільшій кількості загроз, і, відповідно, найбільшому ризику виникнення помилок, піддається інформація під час її зберігання. Таким чином, одним із завдань аудитора є оцінка цілісності інформації та збереженості інформаційних активів у системі.

Інформаційні активи системи, які необхідно захистити, можуть бути класифіковані таким чином:

- фізичні активи — включають персонал, апаратні засоби (у тому числі носії даних і периферію), засоби обслуговування, постачання, і документацію;
- логічні активи — включають дані та програмне забезпечення.



Щоб оцінити, наскільки добре захищені активи та забезпечена цілісність даних, аудиторі потрібна певна шкала. Захищеність активів і забезпечення цілісності даних не належать до показників типу “так — ні”, а натомість можуть мати різні ступені захищеності та забезпеченості. Аудитор повинен мати змогу кількісно оцінити ці показники.

З метою визначення втрат, що будуть понесені від актів порушення безпеки, які не були попереджені засобами захисту, необхідно спочатку визначити наслідки цього акту: чи був актив втрачений, пошкоджений, наданий третім особам, вилучений, зруйнований або використаний у неправомірних цілях? Потім ці наслідки необхідно оцінити у грошовому еквіваленті.

Як показник захищеності активів можна використовувати очікувані збитки, які підприємство понесе у випадку знищення, викрадення активу або його використання у неправомірних цілях. Аудитор може призначити різні ймовірності різним видам втрат, які можуть виникнути.

Аудитор повинен визначити, будуть збитки повною чи лише частковою втратою майна. Для всіх активів і видів ризику очікувані збитки можна підрахувати за формулою:

$$EL = Pt \times Pf \times L,$$

де  $EL$  — очікувані збитки, пов'язані з активами;  $Pt$  — ймовірність виникнення інциденту;  $Pf$  — ймовірність помилки засобу контролю;  $L$  — підсумкові збитки.

Наприклад, якщо ймовірність виникнення пожежі ( $Pt$ ) у комп'ютерній кімнаті корпорації становить 0,001, ймовірність невиявлення вогню засобами контролю ( $Pf$ ) — 0,1, а збитки  $L$ , що виникнуть, дорівнюватимуть 4 млн грн, щорічні очікувані збитки  $EL$  становитимуть 400 грн:

$$EL = 0,001 \times 0,1 \times 4000000.$$

Ризик, звідси, становитиме 400 грн.

Показник цілісності даних, який аудитор використовує протягом перевірки, залежить від цілей аудиту та від характеру даних, на яких він зосереджений. Зазвичай, аудитора найбільше турбує міра, на яку система припускає виникнення по-

милки. Увага зовнішнього аудитора прикута до того, чи є суттєві помилки, які стосуються грошових коштів, у фінансових документах. Показником цілісності даних буде розмір грошової помилки, яка, за оцінкою зовнішнього аудитора, наявна у бухгалтерському обліку як результат слабкості внутрішніх процедур. Внутрішній аудитор також приділяє основну увагу грошовим помилкам, які вже могли виникнути або можуть виникнути у майбутньому через певний час. Крім того, вони мають турбуватися про існування, можливий розмір і можливе число кількісних помилок, однак настільки, наскільки вони пов'язані з грошовими помилками у бухгалтерському обліку.

Конфіденційність інформації забезпечується засобами, які Р. Вебер називає засобами контролю перетину границь (boundary controls). Ці засоби забезпечують інтерфейс між потенційним користувачем системи та власне інформаційною системою. Часто використовуються для цього firewall-комп'ютери. Їх визначення можна знайти у Міжнародних стандартах аудиту. Firewall — це комбінація технічних засобів і програмного забезпечення, яке захищає глобальну, локальну мережу або персональний комп'ютер від несанкціонованого доступу через Інтернет і від введення несанкціонованого або шкідливого програмного забезпечення даних або іншого матеріалу в електронній формі.

Для забезпечення наведених вимог до безпечної інформаційної системи використовують такі засоби захисту.

Підзвітність (протоколювання). Мета підзвітності — у кожний момент часу знати, хто працює в системі і що він робить. У безпечній системі обов'язково мають фіксуватися всі події, що стосуються безпеки. До таких подій належать: вхід у систему (успішний або ні); вихід із системи; звернення до віддаленої системи; операції з файлами (відкриття, закриття, перейменування, знищення); зміна привілеїв або інших атрибутів безпеки (режиму доступу, рівня надійності користувача тощо). Ведення протоколів має бути обов'язково доповнене аудитом, тобто аналізом реєстраційної інформації.

До ключових засобів підзвітності належать ідентифікація і аутентифікація. Ідентифікація дає змогу впізнати користувача системи (і визначити, чи користувався він системою раніше). Ідентифікація — це засоби, за допомогою яких користувач надає системі інформацію про себе.

Аутентифікація — це процес достовірної перевірки відповідності когось чи чогось. Вона підтверджує, ким є користувач, а також його права в системі. Інакше кажучи, аутентифікація — це підтвердження правильності ідентифікації. Можливі два види віддаленої аутентифікації: коли комп'ютер аутентифікує інший комп'ютер; коли комп'ютер виконує якісь операції для користувача, якщо той передасть пароль.

Є три основні підходи до аутентифікації:

- використання для аутентифікації чогось, що знає користувач (пароль, ідентифікаційний номер, криптографічний ключ). Цей спосіб аутентифікації є найдешевшим, найпростішим у реалізації і досить надійним. Небезпеки, пов'язані з цим способом аутентифікації, — можливість втрати (забув пароль) або перехоплення інформації;
- використання для аутентифікації чогось, що має користувач, — токен (token — електронний пристрій, який у процесі аутентифікації засвідчує особу власника). Цей спосіб дорожчий, ніж перший. Токен легко загубити або викрасти, проте важко скопіювати або підробити;
- використання для аутентифікації того, ким є користувач, — біометрія. Цей спосіб аутентифікації поки не дуже поширений, але він є найперспективнішим. Біометрія є найдорожчим з трьох перелічених способів аутентифікації, але він позбавлений недоліків перших двох способів (частину тіла, за якою ідентифікують користувача, втратити набагато важче, ніж забути пароль або загубити токен).

Перелічені способи аутентифікації майже завжди використовують не в чистому вигляді, а в комбінації по два або по три (наприклад, пароль і токен).

Ідентифікація й аутентифікація — перший і найважливіший програмно-технічний рубіж інформаційної безпеки. Якщо не є

проблемою одержати доступ до системи під будь-яким ім'ям, то інші механізми безпеки, наприклад, керування доступом, втрачають зміст. Очевидно, що без ідентифікації користувачів неможливе протоколювання їхніх дій (тобто втрачають сенс підзвітність і аудит). Близьким до аутентифікації є поняття авторизації користувача системи. Авторизацією називають процес визначення прав користувача у системі (знову ж таки, на підставі ідентифікації та аутентифікації цього користувача).

У зв'язку з переліченими причинами перевірка істинності має надаватися першочергове значення. Є ціла серія публікацій урядових відомств різних країн з роз'ясненням питань аутентифікації і, зокрема, проблем, пов'язаних із пароллями. Наприклад, декларується, що користувачу має бути дозволено змінювати свій пароль, паролі не мають залишатися незмінними тривалий час, паролі, як правило, мають бути згенерованими комп'ютером (а не вибраними "вручну"), а користувачу варто надавати деяку реєстраційну інформацію (дата і час останнього входу в систему тощо).

Шифрування — процес, у результаті якого інформація змінюється таким чином, що може бути розпізнаною тільки відповідними особами. Шифрування використовують, щоб захистити інформацію від несанкціонованого перегляду та використання, особливо під час передачі даних або коли вона зберігається на переносному магнітному носіїві. Шифрування, як правило, базується на ключах, без яких неможливо розшифрувати інформацію.

Надійність алгоритмів шифрування характеризує такий показник, як кількість ресурсів, необхідна для того, щоб "зламати" зашифроване послання. Найчастіше цей параметр показує час, необхідний для зламу послання, зашифрованого певним алгоритмом, якщо для зламу використовується метод простого перебору. Потрібно зазначити, що цей параметр є не досить об'єктивним через те, що сучасні хакери використовують інші, більш складні методи для "зламу".

Сучасне шифрування базується на використанні спеціально-го математичного апарата і так званих односторонніх перетво-

рень. Зараз найдосконалішою і найпоширенішою системою шифрування є шифрування з відкритим ключем (Public Key Encryption – PKE).

Для сучасних криптографічних систем захисту інформації сформульовані такі загальноприйняті вимоги:

- зашифроване повідомлення має піддаватися читанню тільки за наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифрування інформації шляхом перебирання різноманітних ключів, повинне мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання розподілених обчислень);
- знання алгоритму шифрування не має впливати на надійність захисту;
- незначна зміна ключа має приводити до істотної зміни вигляду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування мають бути незмінними;
- додаткові біти, що вводяться у повідомлення в процесі шифрування, мають бути повністю і надійно сховані у шифрованому тексті;
- довжина шифрованого тексту має дорівнювати довжині вихідного тексту;
- не має бути простих і легко встановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування;
- ключ будь-який з можливих, має забезпечувати надійний захист інформації (не має бути слабких ключів);
- алгоритм має допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Власне, шифрування є настільки потужним засобом забезпечення конфіденційності, що органи влади намагаються регулювати його законодавчо. Яскравим прикладом цього є факт, що національне бюро стандартів США ще у 1971 р. розробило стандарт шифрування DES (Data Encryption Standard), який тривалий час був стандартом у шифруванні інформації у СІЛА. За цим стандартом алгоритм шифрування DES класифікується як зброя, а експорт його за межі Сполучених Штатів карається як карний злочин.

Найпоширенішим способом тестування конфіденційності інформації в системі є тестовий злом системи. При цьому аудитор або фахівець з безпеки намагаються будь-яким способом отримати неавторизований доступ або розшифрувати зашифровані дані. Це може бути метод підбору пароллю або елементи соціальної інженерії, які дають змогу довідатися пароль від легітимних користувачів інформаційної системи. Залежно від складності отримання неавторизованого доступу до інформації і робиться висновок про рівень забезпечення конфіденційності інформації у системі.

Інформаційна система, як і будь-яка інша, не може розвиватися замкнено, вона має взаємодіяти із зовнішнім середовищем. Взаємодію між суб'єктами в полі інформаційної безпеки підприємства можна представити таким чином (рис. II.33).

Головним суб'єктом у цій сфері є, безумовно, підприємство. Воно має у своєму розпорядженні технологічну інформацію про процес виробництва (якщо це виробниче підприємство), дані про ринки збуту, контакти з постачальниками. Інтерес, що виявляється до фірми, прямо пропорційний ступеню її процвітання. У тих сферах промисловості та комерції, де отримують високі доходи і конкуренція особливо сильна, з'являються мотиви для порушення інформаційної безпеки підприємства.

Зловмисники, які з певних причин хочуть порушити безпеку інформаційної системи підприємства чи організації, можуть скористатися послугами так званих хакерів. У хакерів є свої Інтернет-конференції, об'єднання й групи (фактично банди).



*Рис. П.33. Схема взаємодії суб'єктів у полі інформаційної безпеки підприємства*

Щоб зрозуміти ступінь загрози, яку становлять хакерські групи, потрібно розуміти їх мотивацію. М. Кіджер розробив класифікацію мотивацій хакерів, яку назвав МЕЕСЕ: гроші, самоствердження, справа, розвага, входження у соціальні групи, статус (Money, Ego, Entertainment, Cause, Entrance to social groups, and Status).

Оскільки деякі хакери бачать у своїй діяльності джерело доходу, то їх легко може найняти зацікавлена особа (несумлінний конкурент, злочинець, уряд іноземної держави) для атаки на певний об'єкт. Крім того, веб-сайт підприємства або організації може бути атакований і без жодного замовлення, якщо його злом може принести хакеру самоствердження або популярність. Саме тому сайти багатьох державних організацій США, таких як Міністерство оборони, ФБР, НАСА були атаковані й зламані багато разів і надалі, мабуть, теж не зможуть уникнути хакерських атак.

Крім прямої шкоди, якої завдають хакери, зламуючи інформаційні системи, порушуючи їх роботу і виводячи з ладу або викрадаючи й знищуючи інформацію, є непряма погроза, пов'язана з тим, що хакери виявляють слабкі місця (security holes) операційних систем і програмних продуктів і роблять їх надбанням громадськості. Крім того, хакерські групи розробляють спеціальне програмне забезпечення для злому, створюють комп'ютерні віруси й конструктори вірусів, які дають змогу навіть посереднім програмістам створювати нові комп'ютерні віруси.

Однак у нашій країні такий спосіб нечесної конкурентної боротьби поки що непоширений. Причина — у низькому рівні комп'ютерної грамотності населення України та незначному використанні Інтернету в бізнесі. За даними “The World Factbook 2002”, в Україні на 2002 р. Інтернетом користувалось 750 тис. людей, що становить лише 1,5 % населення (у той час, як у країнах “Великої сімки” Інтернет використовують майже 50 % жителів). За абсолютною кількістю користувачів глобальних інформаційних мереж Україна стоїть поряд зі Словачею та Словенією, де чисельність населення у 10 і 20 разів менша.

Як відповідь спільнотам хакерів, які обмінюються знаннями з написання вірусів та методами зламу нових версій програмних продуктів і операційних систем, виникають Інтернет-спільноти фахівців з інформаційної безпеки. Такі спільноти розробляють стандарти інформаційної безпеки для найрізноманітніших інформаційних систем, які вільно доступні в Інтернеті. Крім того, такі спільноти пропонують послуги із сертифікації програмних продуктів на відповідність власним стандартам безпеки.

Яскравий представник таких спільнот — громадська організація “Центр безпеки Інтернету” (Center for the Internet Security — CISt [www.cisecurity.org](http://www.cisecurity.org)). Його місія полягає у тому, щоб допомогти організаціям зменшити ризик банкрутства бізнесу та електронної комерції через неефективні засоби управління безпекою. До складу організації входить велика кількість спеціалістів з інформаційної безпеки, приватних фірм, що працюють у галузі інформаційної безпеки, державні установи, аудиторів.



Основними напрямками діяльності CIS є сертифікація безпечності програмного забезпечення, а також розробка методик дослідження безпечності інформаційних систем, що передбачає розробку методичних рекомендацій у вигляді так званих “еталонних тестів” (benchmarks) та розробку програмного забезпечення (scoring tools), яке автоматично оцінює рівень захищеності системи, порівнює його з еталонним тестом і надає рекомендації з покращання безпеки системи. Еталонні тести розробляються шляхом погодження з усіма членами CIS, і саме тому є, на думку розробників, прийнятним компромісом між захищеністю інформаційної системи і зручністю користувача при роботі з цією системою.

Якщо підприємство, яке було атаковане, хоче посилити свій захист, то може звернутися до державних установ або до приватних фірм, які забезпечують захист інформаційних систем. Крім того, більшість аудиторських компаній надає послуги з дослідження надійності інформаційної системи підприємства. Проте, як свідчить опитування щодо комп’ютерних злочинів і безпеки, проведене ФБР та Інститутом комп’ютерної безпеки у 2004 р., більшість фірм намагаються не передавати функції, пов’язані із забезпеченням комп’ютерної безпеки, третім особам.

Держава представлена у полі інформаційної безпеки двома типами організацій. Організації першого типу — це науково-дослідні установи, які займаються теоретичними і практичними аспектами інформаційної безпеки в організаціях як приватного, так і державного секторів. Результатом діяльності таких організацій є технічні документи — стандарти, рекомендації, довідники, посібники тощо. На державні установи другого типу покладено завдання стежити за дотриманням законодавства у сфері інформаційної безпеки. Зазвичай цим займаються спеціальні підрозділи силових відомств — міністерств внутрішніх справ, спеціальних служб та ін.

У США провідними державними установами другого типу безпеки інформаційних систем є Агентство з національної безпеки (National Security Agency — NSA), Міністерство оборони

(Department of Defence – DAD) та Федеральне бюро розслідувань (Federal Bureau of Investigation – FBI). Методичними ж питаннями захисту інформації в США займається Національний інститут стандартів і технологій (National Institute of Standards and Technology – NIST). NIST – це технічна адміністрація Міністерства торгівлі США (Commerce Department's Technology Administration). Інститут був заснований у 1901 р. як перша національна лабораторія з фізичних досліджень. За роки існування співробітники Інституту зробили чималий внесок у розвиток різних науки і техніки. З 1980 р. NIST займається проблемами безпеки інформації. За 25 років ним було видано більше двохсот посібників і технічних рекомендацій з найрізноманітніших аспектів безпеки інформаційних систем. Найвідомішим з документів Національного інституту стандартів і технологій є, безумовно, документ SP 800–12 “Введення в комп’ютерну безпеку: довідник NIST” (Introduction to Computer Security: The NIST Handbook), виданий у жовтні 1995 р.

“Європейською відповіддю” NIST є Британська організація зі стандартів (British Standards Institution – BSI). Вона була створена у 1902 р. як урядова організація, до якої входили переважно представники промисловості й уряду Великої Британії. Протягом перших 10 років роботи було розроблено більше шістдесяти стандартів, переважно на продукцію важкої промисловості. Наступними роками BSI розробляла стандарти у найрізноманітніших галузях – від стандартів на розмір паперу (A1, A2 та ін.) до стандартів на системи управління компанією. Найвідомішим продуктом BSI у галузі інформаційної безпеки є стандарт з управління інформаційною безпекою ISO 17799 / BS7799, опублікований Міжнародною організацією зі стандартизації (International Organization for Standardisation – ISO) у грудні 2000 р.

В Україні питаннями інформаційної безпеки займається Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (ДСТСЗІ), створений указом Президента України від 6 жовтня 2000 р. № 1120/2000. З одного боку, ДСТСЗІ СБУ виконує науково-методичні функції:

- бере участь у формуванні та реалізації державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечує функціонування державної системи урядового зв'язку;
- формує загальну стратегію і визначає пріоритетні напрями діяльності у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, а також розвитку спеціальних інформаційно-телекомунікаційних систем;
- розробляє і вживає заходи щодо розвитку систем криптографічного та технічного захисту інформації, здійснює державний контроль за їх функціонуванням;
- визначає порядок та вимоги щодо захисту інформації, необхідність охорони якої визначено законодавством, у процесі її оброблення, збирання, зберігання та передавання мережами передачі даних, у тому числі загального користування;
- установлює порядок і вимоги щодо використання мереж передачі даних установам, які обробляють, збирають, зберігають та передають інформацію, що є власністю держави;
- вносить пропозиції щодо стандартизації у сфері криптографічного та технічного захисту інформації, організовує розроблення державних стандартів та забезпечує у встановленому порядку введення їх у дію;
- забезпечує формування та супроводження моделей загроз безпеці інформації.

З іншого боку, на Департамент покладені організаційні, координаційні й контрольно-наглядові функції:

- організація та координація проведення науково-дослідних і дослідно-конструкторських робіт з питань, що належать до його компетенції, та сприяння впровадженню їх результатів;
- організація і здійснення науково-методичного керівництва підготовкою кадрів у сфері криптографічного та технічного захисту інформації;

- у межах своєї компетенції виконання контрольних функцій щодо захисту інформації, необхідність охорони якої визначено законодавством;
- координація діяльності у сфері криптографічного та технічного захисту інформації;
- видання відповідно до законодавства ліцензії на право провадження окремих видів господарської діяльності у сфері криптографічного та технічного захисту інформації та здійснення контролю за виконанням ліцензійних умов;
- координація у межах своєї компетенції діяльності щодо забезпечення протидії технічним розвідкам, оцінка стану та ефективності цієї протидії;
- здійснення державного контролю за станом захисту державних інформаційних ресурсів у мережах передачі даних, виконанням вимог нормативно-правових актів у сфері криптографічного та технічного захисту інформації, необхідність охорони якої визначено законодавством;
- здійснення відповідно до законодавства функції з управління об'єктами державної власності, утворення, реорганізація та ліквідація підприємства, установи та організації;
- здійснення контролю за додержанням вимог безпеки у процесі розроблення, виробництва, розповсюдження, експлуатації, зберігання, використання і знищення криптографічних систем та засобів криптографічного захисту інформації й обладнання спеціального зв'язку.

Таким чином, ДСТСЗІ СБУ поєднує в собі державні організації першого і другого виду. У цьому є певні недоліки, оскільки, на нашу думку, розробка наукових і методологічних засад забезпечення інформаційної безпеки краще могла б бути виконана науково-дослідними установами, як це прийнято в усьому світі, аніж департаментом державної силової служби. Крім того, події останнього часу, зокрема, наявність “тіньового” серверу, що коригував інформацію, яка надходила до Центральної виборчої комісії під час обробки результатів голосування другого туру виборів Президента України 21 листопада 2004 р., і роботі якого ДСТСЗІ СБУ та інші служби ніяк не завадили, дещо

підірвали довіру фахівців до ефективності роботи таких державних установ.

Питанням законодавчого захисту від подібних загроз та безпеки даних в інформаційних комп'ютерних технологіях у розвинених країнах приділяється велика увага. Так, комітет Ради Європи з проблем злочинності у 1990 р. підготував рекомендації з метою визначення правопорушень, пов'язаних із комп'ютерами, і вніс їх до “мінімального” (обов'язкового) та “необов'язкового” списків, рекомендованих всім європейським країнам до внесення у законодавство. В опублікованій у 1983 р. “Помаранчевій книзі” Міністерства оборони США, вперше були визначені основні поняття стосовно надійності програмних інформаційних систем.

Питання безпеки інформаційних систем у Європі регулюються Міжнародним стандартом ISO 17799/BS7799, прийнятим у грудні 2000 р. У Сполучених Штатах Америки головним документом, що регулює питання інформаційної безпеки, є Закон Сарбейнса-Окслі 2002 (Sarbanes-Oxley Act of 2002 — SOX 2002).

Засади інформаційної безпеки в Україні визначають такі Закони: “Про інформацію”, “Про захист інформації в автоматизованих системах”, “Про авторське право та суміжні права”, “Про електронний цифровий підпис”, “Про електронні документи та електронний документообіг”. Крім того, діють “Концепція технічного захисту інформації в Україні”, яка визначає основні загрози безпеці інформації, стан її технічного захисту, його систему та основні напрями державної політики у цій сфері, та “Положення про технічний захист інформації”, яке визначає порядок роботи і повноваження органів, що займаються діяльністю з технічного захисту інформації.

Розділ XVI Кримінального кодексу України передбачає покарання у вигляді штрафів, обмеження або позбавлення волі за такі дії:

- незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення

комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, а так само незаконне втручання в роботу мереж електрозв'язку, що призвело до знищення, перекручення, блокування інформації або до порушення встановленого порядку її маршрутизації;

- викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем;
- порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж.

Конкретні аспекти безпеки інформаційних систем регулюються наказами Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

В Україні також діють Державні стандарти у сфері захисту інформації: ДСТУ 3396.0–96 “Захист інформації. Технічний захист інформації. Основні положення”; ДСТУ 3396.1–96 “Захист інформації. Технічний захист інформації. Порядок проведення робіт”; ДСТУ 3396.1–97 “Захист інформації. Технічний захист інформації. Терміни та визначення”.

Незважаючи на те, що в Україні прийнята і діє низка нормативних актів, проблема захисту і безпеки даних при застосуванні комп'ютерних програм бухгалтерського обліку на підприємствах досі не вирішена. Цими нормативними актами не передбачена обов'язкова сертифікація програмного забезпечення для

ведення бухгалтерського обліку на підприємствах. Відповідного стандарту з бухгалтерського обліку також немає. Винятком є регулювання Національним банком України використання банками та їх клієнтами розрахункових систем “клієнт – банк”. Базові принципи та процедура використання таких програмних систем визначені Інструкцією НБУ № 7, якою встановлюється обов’язкова сертифікація програмних продуктів Національним банком. Для того, щоб отримати сертифікат (дозвіл) НБУ, фірма-розробник має передбачити у своєму програмному продукті виконання таких основних функцій, як передача повідомлень між клієнтом та банком у зашифрованому вигляді за допомогою сертифікованих засобів захисту; автоматичне ведення протоколів роботи; автоматична архівація протоколів роботи наприкінці дня. У галузі захисту і безпеки даних досвід комп’ютеризації банківської системи може бути корисний для розробки стандартів з бухгалтерського програмного забезпечення в Україні.

Таким чином, можна зробити висновок, що в Україні мають місце слабкий розвиток хакерських груп і громадських організацій професіоналів з комп’ютерної безпеки на тлі невисокої комп’ютерної грамотності населення, розвивається ринок послуг з інформаційної безпеки та є достатня нормативна база з питань інформаційної безпеки та державна структура, яка займається цими питаннями. Отже, сукупність зовнішніх факторів сприяє дотриманню інформаційної безпеки окремого підприємства (правильніше, не сприяє його порушенню) і знижує ризик виникнення викривлень в обліку через несприятливі зовнішні впливи на інформаційну систему підприємства.

### **Тестові завдання до теми 9**

1. Цілісність інформаційної системи — це:
  - а) стан системи, коли інформація є вчасною, точною і повною;
  - б) стан системи, коли вона працює коректно і не відмовляє у доступі легальному користувачу;
  - в) стан системи, що відповідає певній структурі.

2. Доступність інформаційної системи — це:
  - а) стан системи, коли вона працює коректно і не відмовляє у доступі легальному користувачу;
  - б) стан системи, коли інформація є вчасною, точною і повною;
  - в) стан системи, в якій забезпечується захист інформації.
3. Прикладом можливих помилок в обліковій інформації при застосуванні КІСП є:
  - а) помилки в програмних алгоритмах;
  - б) помилки в організаційній структурі управління підприємством;
  - в) помилки в показниках розрахунку фінансового стану підприємства.
4. Ризик, пов'язаний з безпекою, — це:
  - а) очікуваний розмір втрат за визначений період, з огляду на надійність засобів захисту;
  - б) бальна оцінка невиявлення помилок підприємства-клієнта;
  - в) імовірність порушення безпеки підприємства.
5. Для забезпечення захисту інформації слід перевірити:
  - а) документацію інформаційної системи;
  - б) первинний облік інформаційної програми;
  - в) звітність підприємства.
6. До фізичних активів, які необхідно захистити, відносять:
  - а) персонал, апаратні засоби, засоби обслуговування, постачання, документацію;
  - б) дані та програмне забезпечення;
  - в) інформаційні дані.
7. Основною метою оцінки системи внутрішніх засобів контролю є:
  - а) визначення очікуваних збитків;
  - б) розрахунок ризиків витрат;
  - в) дослідження інформаційних даних.



8. Мета підзвітності як засіб захисту інформації:
  - а) у кожний момент часу знати, хто працює в системі і що він робить;
  - б) процес, у результаті якого інформація змінюється таким чином, що може бути розпізнаною тільки відповідними особами;
  - в) процес забезпечення документообороту в бухгалтерії.
9. Аутентифікація — це:
  - а) підтвердження права користувача системи;
  - б) засоби, за допомогою яких користувач надає системі інформацію про себе;
  - в) генерація захисних паролів та шифрів.
10. Криптографія систем — це:
  - а) система шифрування даних;
  - б) підтвердження права користувача системи;
  - в) процес забезпечення документообороту в бухгалтерії.

## Список літератури

### *Основна*

1. Закон України “Про бухгалтерський облік і фінансову звітність в Україні: Затв. Постановою Верховної Ради України від 16 липня 1999 р. № 996.
2. Закон України “Про аудиторську діяльність”: Затв. Постановою Верховної Ради України від 22 квітня 1993 р. № 3125-ХІІ.
3. *Стандарти аудиту та етики*. — К.: ТОВ “Паритет-інформ”, 2003.
4. *Бондар М. І. Аудит в АПК: Навч. посіб.* — К.: КНЕУ, 2003.
5. *Савченко В. Я. Аудит: Навч. посіб.* — К.: КНЕУ, 2002.
6. *Білик М. Д. Організація і методика аудиту сільськогосподарських підприємств: Підручник.* — К.: КНЕУ, 2003.
7. *Автоматизированные информационные технологии в экономике: Учебник / Под ред. проф. Г. А. Титоренко.* — М.: Компьютер; ЮНИТИ, 1998.
8. *Ильина О. П. Информационные технологии бухгалтерского учета.* — СПб.: Питер, 2001.
9. *Овчаренко Е. К., Ильина О. П., Балабердин Е. В. Финансово-экономические расчеты в EXCEL.* — М.: Информ.-издат. дом “Филин”, 1999.
10. *Романов А. Н., Одинцов Б. Е. Компьютеризация аудиторской деятельности.* — М.: ЮНИТИ, 1996.
11. *Подольский В. И., Уринцов А. И. Информационные системы бухгалтерского учета.* — М.: Аудит; ЮНИТИ, 1998.
12. *Романов А. Н., Одинцов Б. Е. Автоматизация аудита.* — М.: Аудит; ЮНИТИ, 1999.
13. *Устинова Г. М. Информационные системы менеджмента: Основные аналитические информационные технологии в ППР: Учеб. пособие.* — Ж.: ДиаСофтЮП, 2000.
14. *Шуремов Е. Л. Системы автоматизации бухгалтерского учета.* — М.: Бух. учет, 1996.

15. *Береза А. М.* Основи створення інформаційних систем: Навч. посіб. — К.: КНЕУ, 1998.
16. *Гужва В. М.* Інформаційні системи і технології на підприємствах: Навч. посіб. — К.: КНЕУ, 2001.
17. *Гужва В. М., Постєвой А. Г.* Інформаційні системи в міжнародному бізнесі. — К.: КНЕУ, 1999.
18. *Пономаренко В. С., Пушкар О. І., Коваленко Ю. І.* Проектування автоматизованих економічних інформаційних систем. — К.: ІЗМН, 1996.

*Додаткова*

1. *Давидов Г. М.* Аудит: Навч. посіб. — 2-ге вид., переробл. і допов. — К.: Т-во “Знання”; КОО, 2001.
2. *Кулаковська Л. П., Піча Ю. В.* Основи аудиту: Навч. посіб. для студ. вищ. закл. освіти. — К.: Каравелла; Львів: Новий світ. — 2000, 2002.
3. *Аудит.* Методика документування / Кол. авторів. За заг. ред. акад. АЕНУ, проф. І. І. Пилипенка. — К.: Інформ.-видав. центр Держкомстату України, 2003.
4. *РД 50–34. 698–90.* Комплекс стандартів і керівних документів на автоматизовані системи. Вимоги до змісту документів. — М., 1990.
5. *ГОСТ 19.701–90.* Єдина система програмної документації. Схеми алгоритмів, програм, даних і систем. Умовні позначення і правила виконання.
6. *ГОСТ 34.201–89, ГОСТ 34.602–89, РД 50–682–89.* Комплекс стандартів і керівних документів на автоматизовані системи.
7. *ГОСТ 6.01.1.* — Єдина система класифікації і кодування техніко-економічної інформації. Основні положення.

Конспект лекцій включає пояснювальну записку, навчально-тематичний план, програмний матеріал до вивчення дисципліни “Комп’ютерний аудит”, список рекомендованої літератури.

Для студентів вищих навчальних закладів.

Навчальне видання

**МАТЮХА Микола Миколайович**  
**КОМП’ЮТЕРНИЙ АУДИТ**

*Опорний курс лекцій*

Редактор *Т. К. Валицька*

Коректор *А. А. Тютюнник*

Комп’ютерне верстання *Н. В. Коваленко*

Художнє оформлення *О. О. Стеценко*

Підп. до друку 17.07.15. Формат 60×84/16. Папір офсетний.  
Друк офсетний. Ум. друк. арк. 13,25. Обл.-вид. арк. 8,78. Наклад 1000 пр.

Міжрегіональна Академія управління персоналом (МАУП)  
03039 Київ-39, вул. Фрометівська, 2, МАУП

ДП «Видавничий дім «Персонал»  
03039 Київ-39, просп. Червонозоряний, 119, літ. ХХ

*Свідоцтво про внесення до Державного реєстру  
суб’єктів видавничої справи ДК № 3262 від 26.08.2008 р.*

Надруковано в друкарні ДП «Видавничий дім «Персонал»