ЛЕКЦІЯ 4

МЕТОДИ ТА ОЦІНКА РИЗИКУ ПРИ ПРОВЕДЕНІ КОМП′ЮТЕРНОГО АУДИТУ

ЗМІСТ

1. Сутність аудиторського ризику.
2. Методика визначення загального ризику.
3. Ознаки визначення характеру ризику в умовах КІСП
4. Аспекти підвищення аудиторського ризику при застосуванні комп’ютерних технологій
5. Особливості визначення додаткового аудиторського ризику в умовах КІСП.

I.

Відповідно до МСА, аудиторський ризик – це ризик того, що аудитор зробить неправильний висновок щодо фінансової звітності після виконання ним аудиторських процедур

<u>Об’єктами</u> аудиторського ризику є ймовірні суттєві помилки у фінансовій звітності та бухгалтерському, статистичному і податковому обліку.

<u>Суб’єктами</u> є аудиторські фірми, приватні аудитори, які перевіряють звітність на достовірність і, які зацікавлені у зниженні рівня аудиторського ризику.

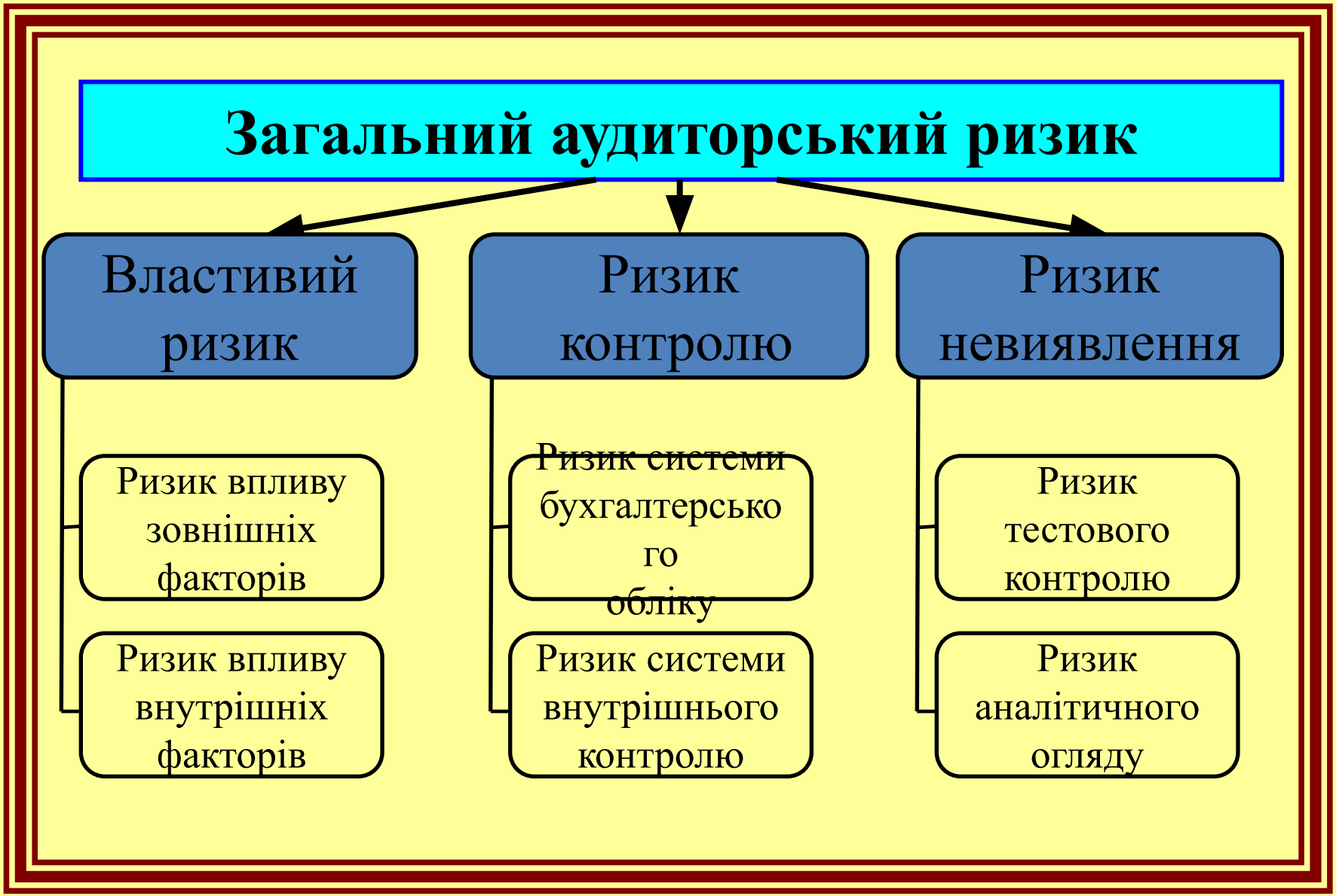
II.

Зарубіжні вчені (Ф.Л. Дефліз, Г.Р. Дженік, В.М. Рейллі, М.Б. Хірш) розглядають загальний аудиторський ризик як сукупність двох видів:

1) **ризик від наявних фальсифікованих фінансових документів;**

2) **ризик того, що аудитор не зможе виявити фальсифікації.**

Українські фахівці вважають, що загальний аудиторський ризик складається з *властивого ризику*, *ризику контролю* та *ризику невиявлення*.


Загальний аудиторський ризик
Властивий ризик
Ризик контролю
Ризик невиявлення
Ризик впливу зовнішніх факторів
Ризик впливу внутрішніх факторів
Ризик системи бухгалтерського обліку
Ризик системи внутрішнього контролю
Ризик тестового контролю
Ризик аналітичного огляду

Міжнародними стандартами аудиту передбачено, що модель аудиторського ризику повинна мати такий вигляд:

ЗАР = ВР * РК * РН,

де ЗАР – загальний аудиторський ризик;

ВР – властивий ризик;

РК – ризик контролю;

РН – ризик невиявлення.

III.

Аудитор повинен врахувати вплив ризиків використання КІС для того, щоб оптимально виконати процедури контролю і максимально понизити вірогідність складання неправильного висновку

Характер ризику в середовищі КІСП визначають такі ознаки:

1) **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 може існувати тільки протягом короткого періоду або тільки у форматі, що читається на комп'ютері.

2) **єдина обробка операцій** - при комп'ютерній обробці подібних операцій застосовуються однакові інструкції. Таким чином, фактично усувається можливість помилок, що властиві ручній обробці. І, навпаки, помилки програмування (помилки в технічних засобах або програмному забезпеченні) призводять до неправильної обробки всіх без винятку операцій

3) **відсутність поділу функцій** - декілька процедур управління можуть бути сконцентровані в руках одного бухгалтера, тоді як при веденні бухгалтерського обліку вручну вони були б звичайно розподілені між декількома працівниками. Таким чином, цей бухгалтер, маючи
вплив на всі розділи обліку, контролює сам себе

4) **можливість помилок і порушень** - можливість здійснення помилок, властивих людині, при розробці, технічному обслуговуванні й експлуатації КІС може бути більша, ніж у системах ручної обробки.

5) **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.

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 КІСП:

1) апаратного забезпечення;
2) програмного забезпечення;
3) обчислювальних потужностей;
4) даних.

IV.

Кожній КІСП притаманний ризик виникнення помилок в роботі, зокрема і у бухгалтерському обліку через порушення їх безпеки

Аудиторський ризик в умовах КІСП може бути як нижчий, так і вищий порівняно з паперовою бухгалтерією (залежно від дотримання або недотримання певних умов).

Підвищення аудиторського ризику спричиняють порушення безпеки в **технічному, програмному, інформаційному** та **організаційному** аспектах, а також **ризики, повязані з кваліфікацією аудитора**.

Технічні аспекти стосуються ризиків, викликаних поганою роботою апаратних засобів, браком належного технічного обслуговування і контролю.

Такі ризики зменшуються 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:

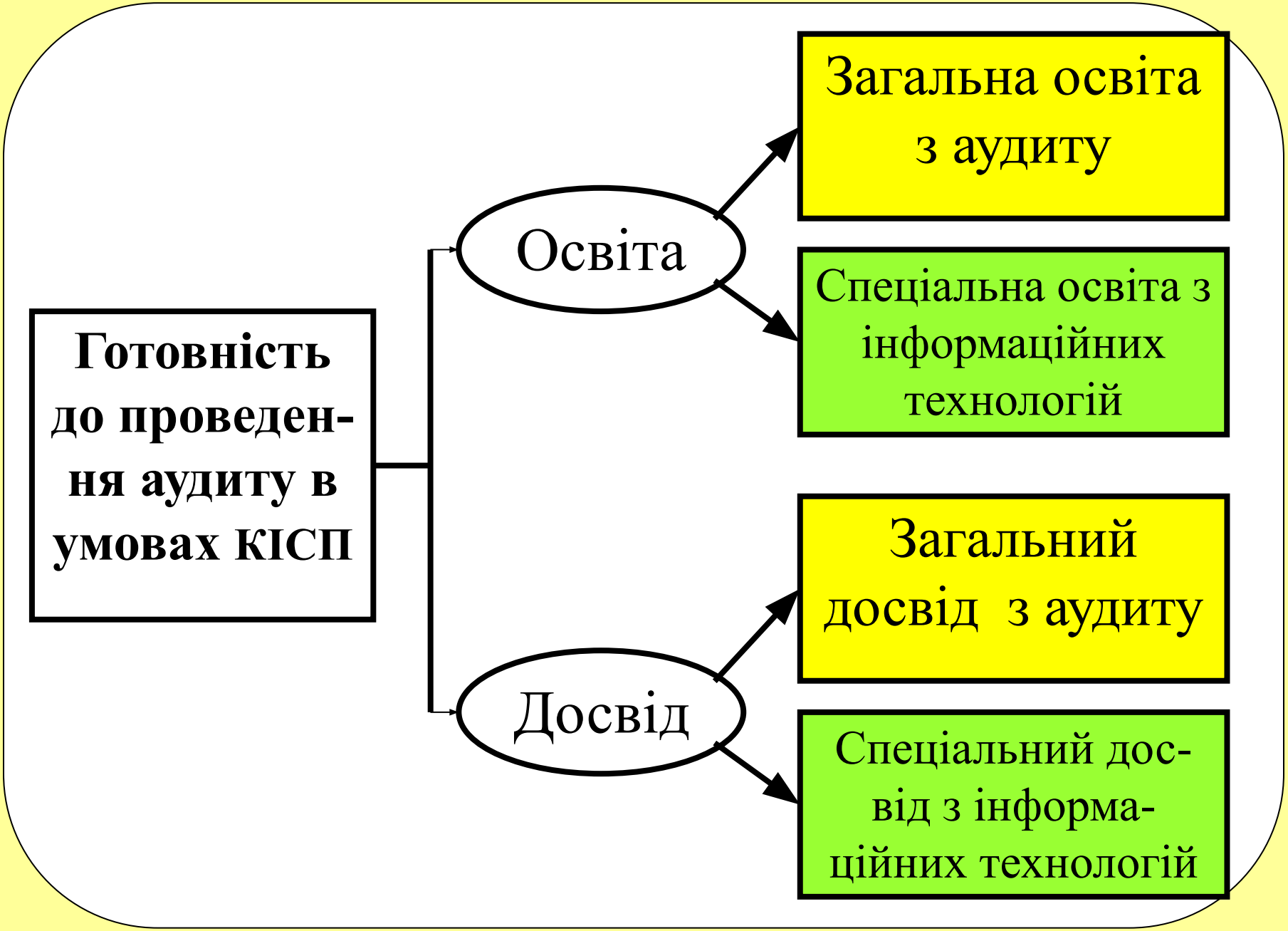
1) пов'язані з використанням нелегального програмного забезпечення;

2) викликані помилками в алгоритмі програми, її малим тиражем, поганою технічною підтримкою

Такі ризики зменшуються за наявності спеціальних програмних засобів (архіватор WinRar або антивірус Doctor Web), які можуть перевіряти цілісність і незмінність програмного забезпечення

Інформаційні аспекти аудиторських ризиків полягають у можливих помилках в інформації, тобто таких порушень її цілісності, які можуть бути результатом випадкових помилок у вихідних даних або навмисного їх викривлення.

Організаційні аспекти аудиторських ризиків викликані недостатньою підготовкою персоналу клієнта до роботи з системою обробки даних обліку, браком чіткого розмежування обов'язків і відповідальності персоналу клієнта, утратою даних.



Складові вимог до освіти та досвіду аудитора в середовищі ІТ

Якщо в аудитора немає достатніх знань, МСА 401 зобов'язує його запрошувати експерта в галузі інформаційних технологій.

v.

Rдод = Rт * Rп * Ri * Ro * Rк

де Rт — ризики, пов'язані з технічними аспектами;

Rп — ризики, пов'язані з програмними аспектами;

Ri — ризики, пов'язані з інформаційними аспектами;

Ro — ризики, пов'язані з організацією обліку;

Rк — ризики, пов'язані з кваліфікацією аудитора.

Rт складається з добутку ризиків:

1) ризики, пов'язані із придбанням
2) дешевого обладнання або у ненадійних постачальників;
2) ризики, викликані браком технічного обслуговування і контролю;
3) ризики, викликані браком оновлення апаратних засобів;
4) ризики, викликані браком фізичного захисту від крадіжок;
5) ризики, викликані браком системи протидії перепадам живлення.

Rп складається з добутку ризиків:

1) ризики, викликані браком або застарілістю антивірусних програм;
2) ризики, викликані браком останніх оновлень в операційних системах;
3) ризики, викликані використанням неліцензійного програмного забезпечення;
4) ризики, викликані використанням малотиражного програмного забезпечення;
5) ризики, викликані помилками в алгоритмі програми.

Ri складається з добутку ризиків:

1) ризики, викликані відсутністю шифрування інформації при зберіганні та передачі;
2) ризики, викликані відсутністю паролів;
3) ризики, викликані браком контролю правильності вхідної інформації;
4) ризики, викликані відсутністю архівації інфор¬мації.

Ro складається з добутку ризиків:

1) ризики, викликані слабкою підготовкою персоналу клієнта до роботи з КІСП;
2) ризики, викликані браком чіткого розподілу обов'язків і відповідальності клієнта;
3) ризики, викликані слабкою організацією систе¬ми внутрішнього контролю.

Rк складається з добутку ризиків:

1) ризик неправильної оцінки КІСП;

2) ризик некоректної побудови тестів КІСП;

3) ризик помилкового тлумачення результатів тестів.

ЛЕКЦІЯ ЗАКІНЧЕНА.

ДЯКУЮ ЗА УВАГУ!