МІНІСТЕРСТВО ОСВІТИ НАУКИ УКРАЇНИ

ПрАТ «ПВНЗ «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Кафедра інформаційних технологій

ДО ЗАХИСТУ ДОПУЩЕНА

Заст зав. кафедри

_____

д.е.н., доц. Н.Р. Полуектова

МАГІСТЕРСЬКА ДИПЛОМНА РОБОТА
УПРАВЛІННЯ АУДИТОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Виконав

ст. гр. ІПЗ – 211м _____ С.І. Левицький

Науковий керівник

к.т.н., доцент _____ Ю.С. Резніченко

Запоріжжя

2023 р.

ПРАТ «ПВНЗ «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»
Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Заст. зав. кафедри
д.е.н., доц.
Н.Р. Полуектова
_____
03.10.2022 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ ДИПЛОМНУ РОБОТУ

Студенту гр. ІПЗ – 211м, спеціальності 121 «Інженерія програмного забезпечення»
Левицькому Станіславу Івановичу

1.Тема: Управління аудитом програмного забезпечення інформаційної системи

затверджена наказом по інституту № 02-16 від 03.10.2022 р.

2. Термін здачі студентом закінченої роботи: 12.01.2023 р.

3. Перелік питань, що підлягають розробці:

1. Визначити предмет, об'єкт та методи управління та аудиту програмного забезпечення інформаційних систем;

2. Виокремити методологічну базу, а також провести порівняльний аналіз існуючих стандартів аудиту;

3. Розробити концептуальну модель аудиту інформаційних систем;

4. Побудувати імітаційну модель проведення процесу аудиту інформаційних систем та провести їх аналіз;

5. Сформувати рекомендації щодо проведення процесу аудиту інформаційних систем.

6. Проаналізувати отримані результати

7. Оформити звіт за результатами роботи

4. Календарний графік підготовки бакалаврської дипломної роботи

№ етапу	Зміст	Терміни виконання	Готовність по графіку %, підпис керівника	Підпис керівника про повну готовність етапу, дата
1.	Формулювання теми магістерської дипломної роботи (збір практичного матеріалу за темою магістерської дипломної роботи)	20.10.22		
2.	I атестація I розділ магістерської дипломної роботи	27.10.22		
3.	II атестація II розділ магістерської дипломної роботи	17.11.22		
4.	III атестація III та IV розділ магістерської дипломної роботи, висновки та рекомендації, додатки, реферат, перевірка програмою «Антиплагіат»	29.12.22		
5.	Доопрацювання магістерської дипломної роботи, підготовка презентації, отримання відгуку керівника і рецензії	10.01.22		
6.	Попередній захист магістерської дипломної роботи	12.01.22		
7.	Подача магістерської дипломної роботи на кафедру	за 3 дні до захисту		
8.	Захист магістерської дипломної роботи	18.01.22		

Дата видачі завдання: 03.10.2022 р.

Керівник магістерської роботи _____ Ю.С. Резніченко
(підпис) (прізвище та ініціали)

Завдання отримав до виконання _____ С.І. Левицький
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Магістерська робота містить 89 сторінок, 6 таблиць, 8 рисунків, 57 бібліографічних посилань.

Об’єктом дослідження є процеси управління аудитом інформаційної системи. Предметом дослідження є методи і моделі управління аудитом програмного забезпечення інформаційної системи на підприємстві.

У роботі наведено концепцію аудиту інформаційної системи підприємства, засновану на використанні системного підходу до управління інформаційними системами, який дозволяє підвищити ефективність бізнес-процесів.

Методичною базою для розв'язання означеної в концепції проблеми виступають розроблені в магістерській роботі імітаційна модель проведення процесу аудиту підприємства та підхід до її реалізації для підприємства зі сфери IT-галузі.

З метою удосконалення діяльності компанії-аудитора було розроблено імітаційну модель проведення процесу аудиту інформаційної системи підприємства, в основі якої лежить процесна модель, а також система підтримки прийняття рішення про доцільність проведення даного процесу.

АУДИТ, ІНФОРМАЦІЙНА СИСТЕМА, ПРОЦЕСНА МОДЕЛЬ, ДИСКРЕТНО-ПОДІЄВЕ МОДЕЛЮВАННЯ, СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення	Повна назва
ІТ	інформаційні технології
ІС	інформаційна система
СУБД	система управління базами даних
ISACA	Асоціація Аудиту та Контролю Інформаційних Систем
ССТА	Центральне Агентство з Обчислювальної Техніки та Телекомунікацій
СВК	Система внутрішнього контролю
ІСТ	інформаційні та комунікаційні технології
ПЕОМ	персональні електронні обчислювальні машини
ПЗ	програмне забезпечення
АРМ	автоматизовані робочі місця
ППП	пакети прикладних програм
ФСА	функціонально -вартісний аналіз
СППР	система підтримки прийняття рішень
ЛПР	особа, яка приймає рішення
БД	база даних
БЗ	база знань
БМ	база моделей

ВСТУП

Актуальність дослідження. Аудит інформаційних систем у загальному розумінні є одним із тих сучасних видів аудиту організацій, що виник у результаті науково-технічного прогресу та еволюційного розвитку світових суспільно-економічних відносин. Стрімкий розвиток світової економіки та господарської діяльності економічних об'єктів виявили недостатність застосування методів аудиту для ефективного вирішення зростаючої кількості управлінських завдань. Це стимулювало потребу появи і розвитку нових видів аудиту, призначених для дослідження різних аспектів діяльності організацій.

Серед нових видів аудиту суттєве місце посідає аудит інформаційних систем. Його поява була зумовлена впровадженням інформаційних технологій у господарську діяльність організацій, їх широким застосуванням для досягнення стратегічних цілей бізнесу, і як наслідок, впливом на результати цієї діяльності. Серед основних постійних споживачів аудиту інформаційної системи організації, у яких інформаційні технології інтегровані в ключові бізнес-процеси.

Дослідженню проблеми аудиту інформаційних систем підприємства присвячено роботи таких вітчизняних і зарубіжних учених Лисенко Ю.Г. [18], Колберт Дж. [24], Сінглетон Т. [38], а також Арене Е., Лоббек Дж., Мельник М.В., Огнєва А.М., Подольський В.І., Робертсон Дж., Скобара В.В., Сиротенко Е.А.

Вибір оптимального підходу і методики проведення аудиту інформаційних систем для конкретного проєкту аудиту в конкретній компанії є одним із ключових чинників проведення успішного та ефективного проєкту ІТ аудиту. Наразі існує безліч різноманітних підходів і методик проведення ІТ аудиту, однак, у зв'язку з тим, що розвиток аудиту інформаційної системи підприємства в Україні розпочався в 90-ті рр. XX ст., виникає проблема

недостатньої міри їхньої розробленості, що й зумовило мету та завдання дослідження.

Метою дослідження є розробка моделей процесу управління аудитом програмного забезпечення інформаційної системи підприємства на підставі узагальнення існуючих методів і підходів з метою підвищення ефективності здійснення даного виду аудиту.

Для досягнення поставленої в роботі мети було сформульовано такі завдання:

1. Обґрунтувати необхідність моделювання процесу проведення аудиту інформаційної системи підприємства.

2. Дати характеристику наявних методів аудиту інформаційної системи підприємства та провести їх порівняльний аналіз.

3. Розглянути теоретичні засади системи проведення процесу даного виду аудиту.

4. Розробити концептуальну схему процесу управління аудитом програмного забезпечення інформаційної системи підприємства.

5. Провести порівняльний аналіз сучасних стандартів аудиту інформаційної системи підприємства.

6. Побудувати процесну модель проведення процесу аудиту інформаційної системи підприємства.

7. Побудувати на основі розробленої процесної моделі імітаційну модель проведення процесу аудиту інформаційної системи підприємства.

8. Провести апробацію побудованої імітаційної моделі.

9. Розробити систему підтримки прийняття рішення компанією-аудитором про доцільність проведення процесу аудиту інформаційної системи підприємства.

Об’єктом дослідження є процеси управління аудитом інформаційної системи. Предметом дослідження є методи і моделі управління аудитом програмного забезпечення інформаційної системи на підприємстві.

Методи дослідження. У дипломній магістерській роботі було використано такі методи: абстрактно-теоретичний метод наукового пізнання, методи дедукції та індукції, метод логічного узагальнення - під час узагальнення теоретичних положень щодо аудиту інформаційних систем, моделювання, систем підтримки прийняття рішення та управління підприємством; порівняльний аналіз методів та стандартів процесу проведення аудиту інформаційних систем, а також програмних продуктів імітаційного моделювання; процесно-орієнтований підхід.

У дипломній роботі отримано такі результати:

Запропоновано концепцію аудиту інформаційної системи підприємства, яка спрямована на досягнення головної мети дослідження - моделювання процесу аудиту інформаційної системи підприємства.

Запропоновано процесну модель аудиту інформаційної системи підприємства, яка дає змогу зацікавленим фахівцям оцінити послідовність етапів аудиту та супутні їм витрати: матеріальні, часові та людські.

На основі процесної розроблено імітаційну модель проведення аудиту інформаційної системи підприємства, що дає можливість спланувати безпосереднє проведення процесу аудиту інформаційної системи підприємства на основі наявних даних, тим самим підвищивши ймовірність досягнення максимального ефекту функціонування компанії-аудитора.

Побудовано систему підтримки прийняття рішення компанією-аудитором доцільності проведення процесу аудиту інформаційної системи підприємства, впровадження якої значно підвищить ефективність прийняття рішення для управління бізнесом, що на теперішній час стає одним із напрямів удосконалення діяльності підприємства в цілому.

Практичне значення отриманих результатів. Запропоновані в роботі концепція та процесна модель аудиту програмного забезпечення інформаційної системи є універсальними та можуть бути застосовані на підприємствах різних галузей з метою досягнення максимальних результатів

розвитку, а імітаційна модель аудиту інформаційної системи та система підтримки ухвалення рішення щодо доцільності проведення процесу аудиту інформаційної системи підприємства можуть бути застосовані аудиторськими та консалтинговими компаніями, що надають послугу аудиту.

Особистий внесок автора. Дипломна робота є самостійно виконаним дослідженням. Усі результати отримані автором самостійно.

Структура та обсяг дипломної роботи. Робота складається зі вступу, трьох розділів, висновків, списку літератури з 57 найменувань джерел. Робота викладена на 89 сторінках, матеріал ілюструють 8 рисунків, 6 таблиць.

Апробація результатів роботи. 13 грудня 2022 року у ході XXIV науково-практичної студентської конференції у Запорізькому Інституті Економіки та Інформаційних Технологій в рамках секційного засідання було зроблено доповідь, результати роботи були опубліковані у збірнику тез конференції [6, 74-75 с.].

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ АУДИТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

1.1 Необхідність моделювання процесу аудиту інформаційних систем

На сьогоднішній день одним із ключових індикаторів ефективності управління бізнесом є впровадження сучасних інформаційних технологій. Їх використання відкриває нові горизонти для розвитку та оптимізації бізнес-процесів, сприяє розширенню ринкових сегментів, зменшенню витрат, підвищенню продуктивності праці, раціональному використанню ресурсів, а також покращенню якості управлінських рішень та надання послуг. Таким чином, інформаційні технології слід розглядати як стратегічний інструмент для вирішення бізнес-завдань та досягнення поставлених цілей.

Інформаційні технології сучасних економічних об'єктів є складним комплексом, який об'єднує інформаційні, програмні, технічні, людські та інші види ресурсів організації в єдине IT-середовище. Його можна визначити як цілісне середовище функціонування всіх IT-активів організації в багатогранності їхнього взаємозв'язку, взаємозалежності та взаємодії. Від стану та ефективності використання IT-середовища значною мірою залежить результативність господарської діяльності в цілому. Тому, інформація щодо її аспектів, у вигляді незалежного оцінювання, дедалі більше цікавить не тільки IT-директорів, а й вище керівництво організацій. Отримати таку інформацію можна за допомогою регулярного та систематичного використання аудиту інформаційних технологій, зокрема, аудиту інформаційних систем [1, 24].

Виникнення та розвиток консультування в галузі інформаційних технологій були зумовлені впровадженням інформаційних технологій у господарську діяльність організацій, їх широким застосуванням для досягнення стратегічних цілей бізнесу, і, як наслідок, впливом на результати

цієї діяльності. Нині актуальність аудиту інформаційних систем різко зросла. [2].

Сучасний ринок насичений апаратно-програмним забезпеченням, багато компаній через низку причин, наприклад, моральне старіння устаткування, бачать неадекватність раніше вкладених коштів в інформаційні системи і шукають шляхи вирішення цієї проблеми. З одного боку, можна повністю замінити інформаційну систему, що, звісно, спричинить серйозні витрати. З іншого - можна модернізувати інформаційну систему. Цей варіант не потребує дорогих вкладень, проте ставить нові питання: наприклад, що залишити з наявних апаратно-програмних засобів, як забезпечити сумісність старих і нових елементів ІС тощо. Саме результати проведення аудиту інформаційної системи підприємства будуть відповіддю на подібного роду запитання. Існує ще одна, більш суттєва причина проведення аудиту, яка полягає в тому, що під час модернізації та впровадження нових технологій їхній потенціал повною мірою не реалізується. Аудит інформаційної системи дає змогу домогтися максимальної віддачі від коштів, що інвестуються у створення та обслуговування ІС [3].

Отже, для обґрунтування актуальності проведення аудиту інформаційних систем підприємства доцільно розглянути частку сегмента консалтингу у сфері інформаційних технологій. Згідно з даними дослідження, проведеного консалтинговою компанією IDC у 2023 році, ринок IT-консалтингу в Україні продовжує стабільно зростати. Останні роки були відзначені зростанням інтересу до цифрової трансформації бізнесу, що сприяло збільшенню попиту на послуги аудиту інформаційних систем та оптимізацію бізнес-процесів.

Останніми роками ринок надання послуг у сфері інформаційних технологій (IT-послуг) виділився в окрему галузь у секторі інформаційно-комунікаційних технологій. За визначенням IDC, під IT-послугами розуміють роботи, виконані зовнішніми по відношенню до замовника компаніями в

області оцінки, планування, побудови, обслуговування і підтримки інформаційних систем, а також навчання співробітників клієнта. ІТ-послуги структурно складаються з послуг з підтримки продуктів (підтримки апаратного і програмного забезпечення) і з професійних послуг (ІТ-аутсорсингу, ІТ-консалтингу, управління ІТ-проектами, реінженірингу бізнес-процесів, стратегічного і фінансового планування, ІТ-продажів, ІТ-маркетингу, навчання) [14].

Загалом ІТ-консалтинг в Україні зростає високими темпами і, за оцінками експертів, є одним із найперспективніших напрямів. Згідно з даними аналітичного звіту IT Ukraine Association за 2023 рік, попит на ІТ-рішення в Україні продовжує стабільно зростати. У 2022 році обсяг ринку ІТ-послуг зріс на 24% порівняно з попереднім роком і становив 6,8 млрд доларів США. Також зростає популярність ІТ-консалтингу, включаючи аудит інформаційних систем, що дозволяє компаніям оптимізувати внутрішні процеси та підвищити безпеку своїх ІТ-інфраструктур.

Однак, аудит в Україні є порівняно новим видом діяльності і тому, процес його розвитку супроводжується виникненням проблемних питань, що зумовлені впливом цілої низки чинників та обставин. По-перше, це недосконаліть законодавства України, що регулює аудит [15].

По-друге, одна з проблем полягає у недостатній кількості методичних розробок з аудиторського контролю, що веде до браку знань та низької компетенції аудитора під час виконання своїх завдань. Більше того, такі тенденції призводять до зниження конкурентоспроможності українських аудиторів у порівнянні з іноземними, які пропонують більш широкий спектр послуг [8].

Ще одним негативним явищем є нестача кваліфікованих аудиторських кадрів, що негативно позначається на якості аудиторських послуг. Це питання піднімають не лише користувачі аудиторських послуг і державні органи, а й самі аудитори, які зацікавлені у стабільному розвитку ринку аудиторських

послуг та підвищенні престижу своєї професії. Наразі аудитори не завжди здійснюють якісну аудиторську перевірку та складають достовірні аудиторські звіти. [9].

Оскільки в Україні практично немає фахівців у галузі аудиту ІВ, підприємствам доводиться звертатися за цією послугою до західних компаній, чиї послуги є досить дорогими, що є наступною проблемою розвитку аудиту [13].

Процес вибору сучасних методів аудиту, а також вибір аудитора і довіра до нього є важливими аспектами, які потребують вирішення. Вибір аудитора, зокрема, є питанням довіри. Клієнт повинен бути впевнений, що аудитору можна довірити інформацію, адже він має забезпечити її конфіденційність. Це безпосередньо пов'язано з професійними якостями аудитора та правовим захистом його діяльності. Проблему вибору методів аудиту та підтвердження об'єктивності одержуваних результатів можна розв'язати використанням сучасних методів математичного моделювання, що й зумовлює актуальність обраної теми дослідження [10].

Таким чином, виникає низка прикладних проблем у процесі становлення та здійснення аудиту інформаційних систем в Україні.

1.2 Методологічна база проведення аудиту інформаційних систем

Дослідження міжнародних професійних стандартів, настанов, рекомендацій та інших прикладних публікацій з аудиту інформаційних технологій, а також вивчення передового досвіду в галузі управління ІТ, дає змогу систематизувати методи ІТ-аудиту, залежно від призначення та змісту. Розрізняють такі класи методів ІТ-аудиту [23]:

загальні методи;

методи оцінки та аналізу ІТ-ризиків;

еталонні методи.

Загальні методи IT-аудиту - це клас методів отримання аудиторських доказів та іншої інформації щодо IT-середовища, необхідних і достатніх для досягнення цілей аудиту та формування аудиторського висновку; застосовуються в усіх випадках IT-аудиту, незалежно від напрямів функціональної спеціалізації, методики виконання, вимог законодавства тощо. Їхня суть полягає у творчому аспекті аудиторської діяльності. Методи оцінки та аналізу IT-ризиків призначені для отримання аудиторських доказів щодо рівня IT-ризику як узагальненого індикатора стану IT-середовища. Еталонні методи: за їхньою допомогою встановлюється відповідність рівня організаційного розвитку IT-середовища до нормативних значень, регламентованих правил, рекомендацій, моделей і критеріїв зрілості тощо. [34].

Структуруємо всі методи і наведемо відповідну схему, яку представимо на рис. 1.1.

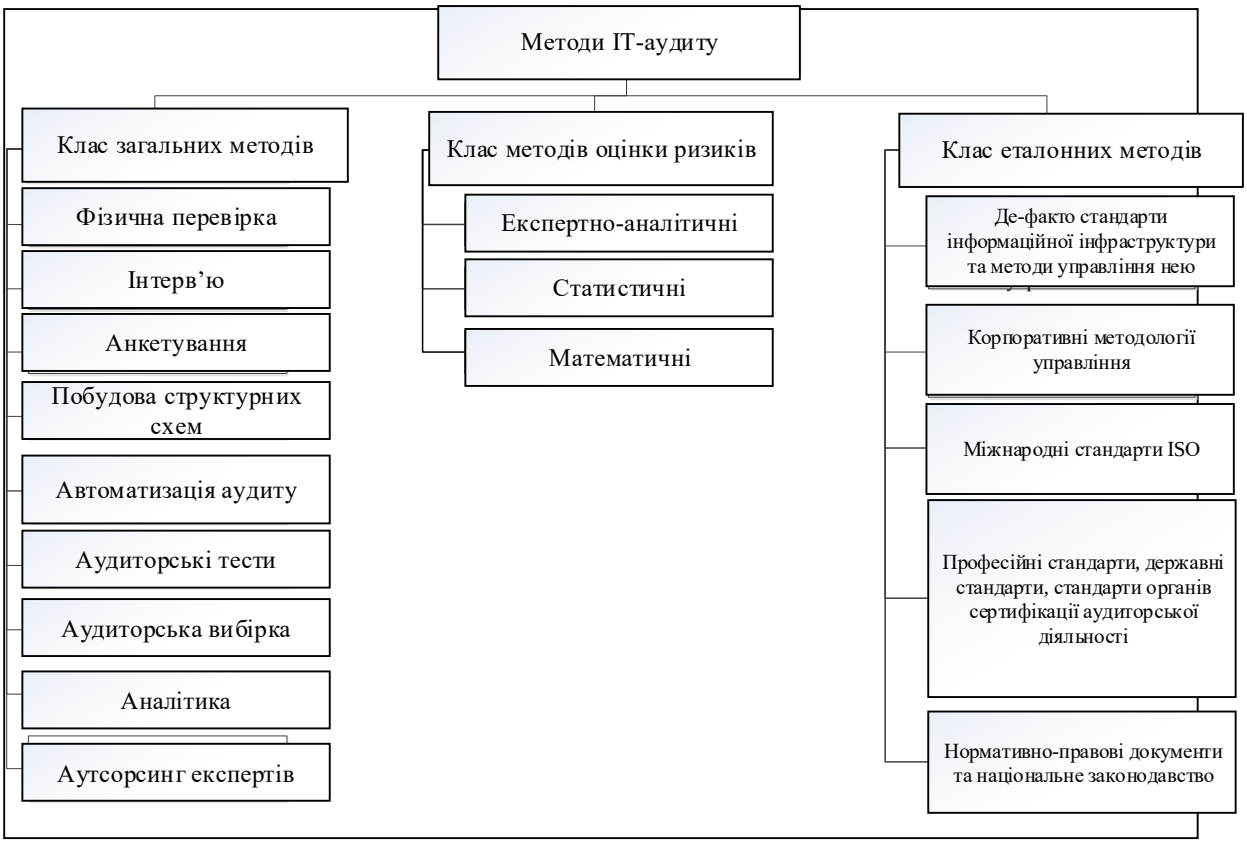

Рисунок 1.1. - Методи аудиту інформаційної системи підприємства

Найтиповішими та найпоширенішими у застосуванні методів класу загальних методів є: фізична перевірка, інтерв'ю, анкетування, побудова структурних схем, комп'ютеризована підтримка проведення аудиту, аудиторські тести, аудиторська вибірка, аналітичні процедури, застосування роботи інших експертів та інші.

Фізична перевірка є методом отримання аудиторських доказів шляхом спостереження фізичної наявності, стану та використання матеріальних ІТ-активів об'єкта аудиту, які можуть бути перевірені фізично. Фізичні докази в ІТ-аудиті є завжди більш значущі, ніж інші, тому завжди бажано забезпечити їхню кількість у достатньому обсязі.

Інтерв'ю є методом отримання аудиторських доказів високого рівня достовірності, що безпосередньо від реальних виконавців бізнес-функцій об'єкта аудиту, вимагає дуже ретельної підготовки. ІТ-аудитори можуть використовувати інтерв'ю для отримання одночасно кількісної та якісної інформації під час виконання процедур збору аудиторських доказів.

Анкетування є методом отримання аудиторських доказів за допомогою особистих листів із запитаннями щодо ІТ-середовища об'єкта аудиту. Фокус-група опитуваних при цьому може бути максимально широкою. За достовірністю отриманих аудиторських доказів цей метод поступається інтерв'ю та фізичній перевірці, проте він є одним із найбільш часто вживаних. З його допомогою можна оцінити ефективність і продуктивність функціонування ІТ-середовища, якість і достатність внутрішнього контролю тощо.

Побудова структурних схем є методом отримання аудиторських доказів шляхом графічного зображення загальної структурної схеми ІТ-середовища організації, з метою відстеження його сильних і слабких сторін, ризиків складових елементів, а також впроваджених внутрішніх контролів.

Комп'ютеризована підтримка проведення аудиту є методом отримання аудиторських доказів шляхом застосування різноманітних спеціалізованих програмних засобів для комп'ютеризованої та автоматизованої підтримки роботи IT-аудитора. До таких засобів відносять: програмні засоби для аудиту загального призначення, спеціалізовані професійні програмні засоби для аудиту, програмні засоби для тестування даних, програмні засоби паралельної симуляції, інтегровані засоби тестування та інші.

Аудиторські тести є методом отримання аудиторських доказів за допомогою тестування двох типів: на відповідність і деталізованих.

Тести на відповідність застосовуються з метою перевірки наявності, а також постійного та ефективного застосування в організації засобів внутрішнього контролю з метою реалізації політик і правил ризиків менеджменту її IT-середовища. Деталізовані тести застосовуються з метою підтвердження або спростування законності та правильності певних IT-процесів. На практиці обсяг необхідних деталізованих тестів визначають тести на відповідність.

Аудиторська вибірка є методом отримання аудиторських доказів на підставі тестування деякої відібраної кількості одиниць із загальної сукупності інформації з елементів IT-середовища з метою оцінки певних характеристик притаманних усій сукупності. Відомими видами вибірки, що застосовуються в IT-аудиті, є вибірка атрибутів, вибірка змінних і статистична вибірка. Вибірка атрибутів зазвичай застосовується в тестах на відповідність, розглядаючи якусь сукупність даних про елементи IT-середовища за наявністю або відсутністю деяких характерних властивостей/атрибутів. Вибірка змінних зазвичай застосовується в деталізованих тестах, розглядаючи певну сукупність даних про елементи IT-середовища зі змінними характеристиками, забезпечуючи водночас висновки щодо відхилень від установлених норм. Вибірка статистична може застосовуватися в різних аудиторських процедурах. Найчастіше її застосовують у вигляді випадкового

відбору, за яким кожен елемент сукупності має однакові шанси потрапити до вибірки.

Аналітичні процедури є методом отримання аудиторських доказів щодо електронної інформації об'єкта аудиту шляхом застосування різноманітних процедур порівняння, встановлення зв'язків і залежностей. Зазвичай такі процедури застосовуються на ранніх стадіях аудиту. За їх допомогою приймаються рішення щодо того, які дані об'єкта аудиту не потребують подальшої верифікації, а також у яких елементах IT-середовища збір аудиторських доказів може бути знижено до мінімуму та в яких він має бути максимально ретельним. У виконанні аналітичних процедур можуть бути дуже корисними засоби комп'ютеризованої підтримки аудиту - CAATs. У сучасній практиці IT-аудиту часто тільки з їх застосуванням можна отримати певну важливу аналітику, яку неможливо забезпечити в інший спосіб.

Застосування роботи інших експертів є методом отримання аудиторських доказів шляхом залучення в процесі IT-аудиту фахівців інших галузей. Така практика зазвичай застосовується з метою підвищення якості та достовірності результатів аудиту. Залучаючи експертів інших галузей, можна досягти необхідного рівня обґрунтованості аудиторського висновку за всіма важливими аспектами, зокрема для досягнення цілей аудиту та задоволення потреб його замовника. Серед основних причин застосування цього методу можуть бути потреба у спеціальних знаннях, необхідних для адекватної оцінки певних видів аудиту, або необхідність делегування частини роботи IT-аудитора на аутсорсинг, з метою пришвидшення процесу проведення аудиту загалом тощо.

Крім типових процедур і авторських розробок, згаданих вище, загальні методи IT-аудиту досить часто ґрунтуються на таких загальновідомих концепціях, як: BPR (реінжиніринг бізнес-процесів), ILM (управління життєвим циклом інформації), OECD (управління безпекою інформаційних

систем і мереж), PDCA (управління життєвим циклом бізнес-процесів), SDLC (управління життєвим циклом створення систем) та інших [35].

Наступним класом методів, який у сучасній практиці IT-аудиту набуває дедалі більшого застосування, є методи оцінки та аналізу IT-ризиків. Потреба їх залучення, на відміну від загальних методів IT-аудиту, як правило, залежить від обраної виконавцем методики проведення, професійних стандартів, рекомендацій та інших норм, якими аудитор керується під час виконання своєї роботи. Серед причин їх застосування можуть бути специфіка IT-середовища, а також цілі, завдання і питання, поставлені перед аудитом його замовником. Основним поняттям у цьому класі методів є IT-ризик. Такий ризик пов'язаний із застосуванням організацією інформаційних технологій для цілей бізнесу, і визначається, як імовірність виконання дії або настання події, що могла б шкідливо вплинути на організацію, зокрема через вплив на її IT-середовище. Відповідно, уся сукупність ризиків IT-середовища, складає середовище IT-ризику, кожний елемент якого, є вірогідністю реалізації певних загроз для організації через уразливості її IT-ресурсів.

Виходячи з рекомендацій міжнародних професійних стандартів та настанов з IT-аудиту, оцінки середовища IT-ризику слід застосовувати як на етапі планування аудиту, так і на етапі його проведення. На етапі планування методи оцінки та аналізу IT-ризиків, як правило, застосовуються з метою встановлення можливості реалізації цілей аудиту, а також забезпечення оптимального способу їх досягнення. Зокрема, встановлюється загальний рівень ефективності ризик-менеджменту IT-середовища організації, на підставі якого робиться висновок щодо доцільності проведення IT-аудиту загалом, а також визначаються й обґрунтовуються межі аудиту; глибина аналізу, застосування аудиторських процедур, зокрема тестів на відповідність та деталізованих, і способи найбільш раціонального та ефективного використання обмежених ресурсів аудиту (забезпечення трудовими, інформаційними, технічними, правовими, методичними, методологічними,

комп'ютеризованими ресурсами, а також забезпечення оптимального способу досягнення цілей аудиту. На етапі проведення ІТ-аудиту методи оцінки та аналізу ІТ-ризиків застосовують, як правило, з метою більш ретельного дослідження інформаційної безпеки організації. Рівень її ефективності та достатності зазвичай встановлюють порівняно з певними еталонами, стандартами та найкращими практиками в цій сфері. Як правило, ІТ-безпеку організації оцінюють за конфіденційністю, доступністю та цілісністю ресурсів ІТ-середовища - так званий "трикутник інформаційної безпеки". Однак, можуть застосовуватися і більш специфічні критерії, залежно від особливостей об'єкта аудиту, наприклад, несуперечливість, підзвітність, автентичність, надійність та інші. Кінцевим результатом оцінки на цьому етапі є висновок про поточний стан ІТ-безпеки, вплив на нього виявлених ІТ-ризиків, їхню сутність тощо, а також рекомендації щодо впровадження необхідних контрзаходів для зниження рівня ризиків до прийнятного рівня. Керуючись міжнародними професійними стандартами та настановами з ІТ-аудиту, а також передовим досвідом у сфері управління ІТ, пропонується для оцінювання середовища ІТ-ризиків визначити й застосовувати поняття притаманного ризику, залишкового ризику, прийнятного ризику, а також ризику контролю та ризику не виявлення.

Притаманний ІТ-ризик є ризиком ІТ-середовища організації, який може завдати їй істотної шкоди, а також суттєво вплинути на достовірність і якість результатів аудиту (зокрема, на досягнення цілей аудиту), без урахування впроваджених контрзаходів для його зниження.

Залишковий ІТ-ризик є ризиком ІТ-середовища такого рівня, який залишається після вжиття відповідних контрзаходів для його зниження.

Прийнятний ІТ-ризик є ризиком можливих збитків організації в такому обсязі, який її керівництво та відповідальні фахівці з ІТ-аудиту погоджуються не враховувати, оскільки вважають таким, що не зможе суттєво вплинути ані на господарську діяльність, ані на достовірність та якість результатів аудиту.

ІТ-ризик контролю є ризиком того, що впроваджена в організації система контрзаходів (внутрішнього контролю ІТ-ризиків) не зможе запобігти певним загрозам шкідливого впливу на ІТ-середовище організації, що можуть спричинити суттєві збитки, а також суттєво вплинути на достовірність та якість результатів аудиту.

ІТ-ризик невиявлення є ризиком того, що процедури незалежної перевірки, які застосовує ІТ-аудитор, не зможуть виявити певну загрозу (або загрози) шкідливого впливу на ІТ-середовище, що може спричинити суттєві збитки, а також суттєво вплинути на достовірність і якість результатів аудиту (досягнення цілей аудиту).

Перевіряючи середовище ІТ-ризику, аудитори обов'язково враховують впроваджені в організації заходи ризик-менеджменту з ІТ, оцінюючи при цьому їхню ефективність, економічність, достатність тощо [23].

Суть ризик-менеджменту ІТ-середовища організації полягає у виборі її керівництвом обґрунтованого набору контрзаходів для зниження рівня виявлених ризиків. Такі контрзаходи є, по суті, елементами єдиної системи внутрішнього контролю (ІТ-контролями) середовища ІТ-ризиків. Доцільність застосування саме терміна "контроль", на відміну від терміна "управління", для опису цієї системи контрзаходів, зумовлена смисловим відтінком, що більш точно описує характер застосування таких заходів для зазначених цілей. Отже, ІТ-контроль пропонується визначити як заходи, що впроваджуються відповідальним менеджментом організації, з метою протидії ризикам ІТ-середовища та їх зниження до прийнятного рівня. При цьому вартість ІТ-контролів має бути меншою за величину можливого збитку. Аналізуючи різні підходи та рекомендації професійних стандартів і настанов щодо оцінювання контролів ІТ-середовища організації, пропонується визначити та розрізняти в процесі ІТ-аудиту такі рівні ІТ-контролів [23]:

загальний - є найнижчим (базовим) рівнем ІТ-контролів організації. Їх впровадження покликане створити в організації робочого простору

різнобічного контролю ключових ІТ-процесів. Вони, по суті, є "фундаментом", на якому можуть бути розроблені контролі додатків та інші специфічні контролі ризиків ІТ-середовища;

програмний - є рівнем ІТ-контролів, який стосується безпосередньо програмного забезпечення (додатків, систем тощо). Передбачає впровадження ручних та автоматизованих процедур контролю ІТ-ризиків, які покликані гарантувати, що всі транзакції в застосунках і системах є авторизованими та записаними, а також, що вони фіксуються та виконуються повною мірою, згідно з визначеними сценаріями (безпомилково, своєчасно тощо);

спеціалізований - є рівнем ІТ-контролів спеціалізованого призначення для контролю ІТ-ризиків, пов'язаних із певною специфікою та особливостями діяльності організації або її ІТ-середовища.

Також, керуючись джерелами, за характером реагування на інциденти (випадки помилок, упущень або злочинних дій) в ІТ-середовищі, доцільно розрізняти ІТ-контролі:

превентивні - запобігають інцидентам,

виявлення - виявляють інциденти і звітують про них відповідальному керівництву;

коригувальні - коригують наслідки інцидентів одразу після виявлення, зменшуючи їхній вплив, а також ідентифікуючи та усуваючи причини їх виникнення.

Відомі нині методи оцінки та аналізу ІТ-ризику можна класифікувати на експертно-аналітичні, статистичні та математичні. З них на практиці найчастіше застосовують експертно-аналітичні методи. Це зумовлено, з одного боку, їхньою простотою, порівняно зі статистичними та математичними, а з іншого - активним залученням відповідального менеджменту організації як експертів. Таким чином, аудитор має можливість перекласти частину відповідальності за результати своєї праці на організацію. Іноді результати залучення експертно-аналітичних методів можуть виявитися

недостатньо точними і достовірними для тих чи інших цілей аудиту, оскільки в них обов'язково присутній суб'єктивний фактор.

Для вирішення цієї проблеми доцільно застосовувати статистичні та математичні методи. Вони дають змогу проаналізувати об'єктивність і точність експертних оцінок, а також отримати додаткову інформацію щодо факторів, які впливають на визначення рівня ризику. Однак їх застосування є більш складним і вимагає від аудитора додаткових спеціальних знань і навичок. За їх допомогою можна прогнозувати рівень ризику, дослідити взаємозв'язки та їхню щільність між його складовими, а також факторами, що на нього впливають. Також вони дають змогу математично підтвердити або скоригувати судження експертів щодо факторів ризику, їхньої значущості тощо. [36].

На особливу увагу заслуговує клас еталонних методів IT-аудиту. Під еталонами розуміють стандарти, методології, системи вимог, інструкції, керівні принципи тощо в галузі управління IT, що встановлюють вимоги до систем елементів, процесів, процедур, методів і засобів, які використовуються під час здійснення проектів інформатизації. До таких еталонів, зокрема тих, що можуть бути корисними для методичного забезпечення IT-аудиту за кращими світовими досвідами, можна віднести [37].

стандарти "de-facto" з побудови ефективної IT-інфраструктури організації та управління нею, зокрема ITIL і COBIT;

деякі корпоративні методології управління інформаційними технологіями, зокрема, ITSM (Hewlett Packard), MOF & MSF, BSI/IT (German Information Security Agency), SSADM (Model Systems Ltd & LBMS Plc);

міжнародні стандарти організації ISO, зокрема, систему стандартів управління якістю ISO-900x, систему стандартів управління IT-послугами ISO-20000x, систему стандартів управління інформаційною безпекою ISO 2700x, а також окремі стандарти ISO 17799, ISO 19011;

професійні стандарти, настанови та нормативні кодекси міжнародних організацій та вищих державних органів регулювання та сертифікації аудиторської діяльності, зокрема, стандарти, настанови та кодекси професійної етики з IT-аудиту ISACA, настанови з IT-аудиту INTOSAI, SAC-Report інституту внутрішніх аудиторів - IIA, міжнародні стандарти (зокрема ISA 1008, ISA 1009) і настанови IFAC;

нормативно-правові документи та національні стандарти окремих країн і союзів держав, такі як законодавчі акти США (FCPA, HIPAA), директиви Євросоюзу (Директива 95/46/ЄС), законодавчі акти Південної Африки (King II, KING III), IT-стандарти США (розроблені NIST: SP800-12, розроблені COSO: Model of Internal Control, розроблені AICPA: специфікація "SysTrust", розроблені SANS-CIS: SANS/GIAC Site Certification, а також відомі методики CMMI та OCTAVE), IT-стандарти Великої Британії (PRINCE2, CRAMM), IT-стандарти Австралії (AS/NZS 4360, AS 8015-2005).

Більшість із зазначених еталонів не є адаптованими безпосередньо до проведення IT-аудиту, тому, як правило, застосовуються для його цілей опосередковано, зокрема методична підтримка.

1.3 Концепція аудиту інформаційної системи підприємства

Поняття «аудит інформаційної системи» містить у собі дві складові: «аудит» та «інформаційна система». Дамо визначення кожної з них [16,17]:

аудит - процедура незалежного оцінювання діяльності організації, системи, процесу, проєкту або продукту;

інформаційна система - це взаємопов'язана сукупність засобів, методів і персоналу, які використовуються для зберігання, обробки та видачі інформації в інтересах досягнення поставленої мети.

Під аудитом інформаційної системи підприємства розуміють оцінювання поточного стану інформаційної системи (яка, можливо, перебуває ще на стадії проектування) на відповідність деякому стандарту або вимогам, які висуваються до неї, з перевіркою інформаційної системи на максимально повне використання її потенціалу [18]. Або ж, під терміном "аудит інформаційної системи" розуміють системний процес одержання й оцінювання об'єктивних даних про поточний стан інформаційної системи, дії та події, що відбуваються в ній, який встановлює ступінь відповідності створеної ІТ-інфраструктури (комплексу апаратних і програмних засобів, призначених для автоматизованого збирання, зберігання, опрацювання, передавання та отримання інформації) вимогам забезпечення наявних процесів [19]. Аудит інформаційної системи підприємства ще інакше називають ІТ-аудитом.

Загальна мета аудиту полягає у сприянні ефективності роботи підприємства, раціональному використанні інформаційних ресурсів у підприємницькій діяльності для отримання максимальних прибутків [20]. А своєю чергою метою аудиту інформаційної системи підприємства є оцінка ефективності використання ІС, адекватності ІС характеру та обсягу бізнесу, оцінка поточного статусу та перспектив розвитку ІС відповідно до потреб бізнесу [19].

Предметом аудиту інформаційних систем, з одного погляду, є стан інформаційної системи підприємства, яка перебуває у сфері аудиторської оцінки [22]. З іншого ж погляду, у процесі аудиту будь-якої інформаційної системи дуже важливо розмежовувати предметну інформацію і технологічну інформацію. Предметна інформація описує структуру інформації про бізнес-процеси, що відбуваються в системі, дані про всі операції, що виконуються в системі, які відображають змістовну спрямованість предметної області, а технологічна - технічні параметри, що забезпечують функціонування предметної частини. Ця інформація і є предметом аудиту ІС. Саме на основі

аналізу технічних параметрів робиться висновок про стан ІС, про її недоліки, а потім формулюються припущення щодо їх усунення [19].

Предмет аудиту конкретизують його об'єкти.

Набір послуг, пропонованих компаніями в рамках аудиту інформаційної системи, досить різноманітний і визначається тим, які елементи компанія-аудитор включає в поняття "інформаційні системи". Обов'язковою стандартною процедурою аудиту інформаційної системи є уточнення меж дослідження системи (опис того, що буде розглядатися як компонент системи, а що як зовнішній вплив), а також вибір точки зору аудитора на процес аудиту. Класично вважається прийнятим розглядати такі підсистеми та зв'язки між елементами цих підсистем: інформаційне, технічне та програмне забезпечення ІС.

Як елементи інформаційного забезпечення виокремлюють: склад об'єктів предметної області, що відображається (структура даних), набір показників, документів, класифікаторів, файлів, баз даних і баз знань, а також способи подання, накопичення, зберігання, перетворення і передавання інформації.

Технічне забезпечення включає вимоги до архітектури апаратних засобів, телекомунікаційні засоби зв'язку, уніфікацію апаратних рішень і мережеві інтерфейси, локальні мережі.

Програмне забезпечення - сукупність СУБД, прикладних і операційних систем, а також інтерфейси між даними системи [19].

Інший підхід відносить до об'єктів аудиту інформаційної системи робочу станцію, сервер, служби та додатки, телекомунікаційну мережу, корпоративну інформаційну систему, інформаційні та бізнес-потоки, політику інформаційної безпеки, включно з іншими адміністративно-організаційними заходами забезпечення інформаційної безпеки підприємства [22].

Суб'єктами аудиту є замовники аудиту та виконавці.

Замовниками аудиту є власники об'єкта аудиту, тобто юридичні та фізичні особи, які здійснюють підприємницьку діяльність.

Виконавцями аудиту є або аудитор, або контролюючі державні органи.

Аудитор (виконавець) — це суб'єкт підприємницької діяльності, який володіє сертифікатом, що підтверджує його кваліфікацію для здійснення аудиторської діяльності на території України. Аудитор може займатися аудиторською діяльністю не тільки як фізична особа, а й у статусі підприємця, але лише після того, як буде внесений до Реєстру аудиторських фірм та аудиторів [22].

Розрізняють внутрішніх і зовнішніх аудиторів [22]:

зовнішні акцентують свою увагу на незалежному підтвердженні надійності та адекватності системи внутрішнього контролю ІС;

внутрішні зосереджені на забезпеченні ефективності системи внутрішнього контролю ІС.

Контролюючі державні органи (Державна податкова інспекція, Органи контрольно-ревізійного управління) проводять аудит діяльності підприємства відповідно до нормативних і законодавчих актів, які регулюють діяльність вищезазначених установ.

Аудитори зобов'язані здійснювати аудит відповідно до певних принципів. Принцип аудиту - основні положення, на основі яких здійснюється аудиторська діяльність.

Методологічні принципи аудиту включають [20]:

1. Планування. Цей принцип належить до обов'язкових, оскільки від нього залежить ефективність проведення аудиторської перевірки.

2. Доцільність вибору методики і техніки аудиту, визначення критеріїв суттєвості та достовірності. З урахуванням професійної підготовки, досвіду компетентності аудитор самостійно обирає методику і техніку проведення аудиту та визначення ступеня планової і фактичної суттєвості.

3. Обґрунтування оцінки значущості аудиторських заходів. Відповідно до Міжнародного та Національного нормативів аудит передбачає забезпечення обґрунтованої та неабсолютної гарантії, що звітність, яку офіційно оприлюднюють, у цілому не містить у собі суттєвих змін. Обґрунтована гарантія досягається під час збирання необхідних доказів та оцінки їхньої значущості для підготовки висновку щодо реальності та об'єктивності в цілому даних звітності.

4. Дотримання методики оцінки ризиків і вибіркової перевірки даних. Вибір методики оцінки загального аудиторського ризику залежить від об'єкта перевірки і є комерційною таємницею аудитора (аудиторської фірми).

5. Аналіз інформації, формування висновків та відповідальність за складений висновок. Формування висновків базується на результатах аналітичних, оцінці прямих висновків, складених на основі аудиторських доказів, які були отримані під час проведення аудитором. Аудитор у своїх висновках формулює всі суттєві аспекти розглянутих ним питань. У разі негативного висновку або відмови від видачі висновку аудитору необхідно чітко вказати всі причини, що спричинили такі рішення.

6. Обґрунтування використання результатів роботи іншого аудитора або фахівця іншої галузі. Взаємодія аудиторів.

7. Повне інформування клієнтів.

8. Контроль якості роботи аудитора.

Кодекс професійної етики аудиторів України встановлює вимоги щодо надання аудиторських послуг та основні принципи етики, які повинні дотримуватись аудитори. Ці вимоги є обов'язковими для всіх аудиторів під час виконання аудиторських завдань. Отже, до принципів етики аудитора належить:

професіоналізм (роботодавці, клієнти, інші зацікавлені сторони визначають рівень професійної підготовки аудиторів);

якість послуг (аудит та аудиторські послуги мають здійснюватися в суворій відповідності до чинного законодавства, нормативних актів і кодексу етики);

довіра (користувачі послуг аудитора мають бути впевненими в тому, що він ніколи не порушить професійної етики і дотримуватиметься її протягом усієї практики).

До фундаментальних засад професійної етики відносять: незалежність суджень, об'єктивність висновків, конфіденційність, чесність, почуття обов'язку перед суспільством, компетентність і високий професіоналізм, відкритість зі своїм клієнтом, організованість і сумлінність, технічні стандарти.

Що стосується методологічної бази проведення аудиту ІВ, то її детально описано в другому пункті першого розділу.

Таким чином, вищевикладена інформація описує систему аудиту інформаційної системи підприємства. Ця система являє собою взаємопов'язаний набір цілей, завдань, суб'єктів, методів, а також принципів аудиту. Її метою є ефективне проведення аудиту інформаційної системи підприємства. Результати, отримані під час проведення аудиту інформаційної системи підприємства, використовуються керівництвом компанії-замовника для ухвалення ефективних управлінських рішень подальшого функціонування підприємства.

Визначимо концептуальну модель проведення аудиту інформаційної системи підприємства.

Потреба в проведенні аудиту інформаційних систем може виникнути на будь-якому часовому етапі діяльності компанії. Як правило, усвідомлення такої необхідності пов'язане з незадовільною роботою наявних програмних продуктів. Аудит інформаційних систем необхідний [21]:

під час впровадження інформаційної системи (CRM, ERP тощо);

під час проведення модернізації вже наявної інформаційної системи з метою отримання знань про те, які з наявних апаратно-програмних засобів необхідно залишити і як забезпечити сумісність старих і нових елементів ІС.

у разі підозри на неефективне функціонування інформаційної системи.

Виходячи з описаних причин проведення аудиту, сформулюємо наявну проблему: наявна на підприємстві інформаційна система не відповідає вимогам і потребам бізнесу, що висуваються до її функціонування. Виходячи з цього, метою цієї концепції є розв'язання наявної проблеми. Формулювання мети таке: проведення аудиту інформаційної системи підприємства для оцінки відповідності наявної інформаційної системи її вимогам і розробка шляхів її модернізації та подальшого розвитку.

Характеристиками описаної проблеми можуть виступати: неефективні засоби комунікації, що спричиняє втрату часу на обмін інформацією; висока трудомісткість опрацювання, підготовки та збору даних, підготовки звітів; низька інформаційна культура та інше.

Для розв'язання наявної проблеми необхідне вирішення такого комплексу завдань:

визначення потреб інформаційної системи;

визначення вимог, що висуваються до інформаційної системи;

визначення наявного стану інформаційної системи;

визначення відповідності поточного стану вимогам і потребам, що висуваються до інформаційної системи;

вироблення рекомендацій щодо модернізації наявної інформаційної системи;

знаходження оптимального варіанту функціонування інформаційної системи.

Розроблені в магістерській роботі процесна та імітаційна моделі проведення аудиту інформаційної системи підприємства є методичною базою для вирішення окреслених завдань.

Як використовуваний інструментарій для створення авторських моделей виступають:

моделювання за допомогою нотацій IDEF0;

імітаційне моделювання;

дискретно-подієве моделювання.

Таким чином, складено концепцію аудиту інформаційної системи підприємства, що описує основну проблему дослідження, розв'язанням якої є розробка процесної та імітаційної моделей процесу аудиту інформаційної системи підприємства.

1.4 Висновки розділу

1. Стрімкий рівень розвитку комп'ютерних технологій призвів до того, що наявні інформаційні системи на сьогодні вже не є оптимальними з погляду протікання бізнес-процесів і фінансової ефективності. Поява нових апаратно-програмних комплексів і концепцій побудови інформаційного середовища та їхнє своєчасне впровадження дає змогу поліпшити обмін даними та систематизувати документообіг у підрозділах і філіях, налагодити ефективніший оперативний і фінансовий облік, створити прозору структуру, якою можна добре керувати. Крім того, здебільшого помітного позитивного ефекту можна досягти тонким налаштуванням і адаптацією вже розгорнутої в організації інформаційної системи. У результаті на перший план виходить необхідність аудиту інформаційної системи компанії з метою визначення ступеня її відповідності сучасним вимогам, цілям і завданням організації, а також виявлення необхідності її вдосконалення та розвитку.

2. Залежно від призначення та змісту розрізняють такі класи методів IT-аудиту: загальні методи, методи оцінки та аналізу IT-ризиків, еталонні методи. Зазначені методи можуть використовуватися в різних комбінаціях, залежно від цілей і завдань, які стоять перед аудитором. Запропонована класифікація

дає можливість цілісно усвідомити сучасне розмаїття методів ІТ-аудиту, систематизувати їх, а також підібрати необхідні для конкретного випадку методи, уникаючи фрагментарності, дублювання, надмірності тощо.

3. На основі виокремленої мети, об'єкта і предмета дослідження розроблено та представлено концептуальну схему аудиту інформаційної системи підприємства, яка визначила властивості модельованої системи і тим самим стала основою для наступних двох розділів роботи.

РОЗДІЛ 2
МОДЕЛЮВАННЯ ТА ПРИКЛАДНІ АСПЕКТИ ПРОЦЕСУ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА

2.1 Сучасні стандарти аудиту інформаційних систем

На сьогодні розроблено низку стандартів для проведення аудиту інформаційних систем, проте найпоширенішими серед них, за даними "IS Audit and Control Journal", є стандарти "de-facto" [24]:

COBIT: Objectives of Control for Information and related Technology, ISACA;

COSO 1992;

ITIL: IT Infrastructure Library - Бібліотека Інфраструктури Інформаційних Технологій, ССТА;

Концепція внутрішнього контролю CMMI.

Кожен документ зосереджується на внутрішньому контролі та певній цільовій групі (наприклад, внутрішні аудитори, менеджери, зовнішні аудитори), надаючи великого значення створенню та оцінці механізмів внутрішнього контролю. Таким чином, порівняння концепцій внутрішнього контролю, представлених у цих документах, є актуальним для всіх трьох цільових груп.

CobiT - це пакет відкритих документів, що містить близько 40 міжнародних та національних стандартів і рекомендацій у галузі управління IT, аудиту та IT-безпеки. Розробники цього стандарту провели аналіз і оцінку, об'єднавши найкращі елементи з міжнародних технічних стандартів, стандартів управління якістю, а також практичних вимог і досвіду в аудиторській діяльності. [25].

Метою цього методичного керівництва є дослідження, розробка та поширення сучасних і глобально прийнятних правил у сфері управління IT та їхньої перевірки.

Цей стандарт охоплює широкий спектр питань якісної перевірки інформаційних технологій і, зокрема, ІС. Для аудиторів позитивною рисою практичних рекомендацій, зібраних у рамках цього стандарту, є описовий характер і відсутність вузько спеціальних технічних термінів. CobiT розглядає управління IT і перевірку їхньої роботи як процеси, пов'язані із загальною стратегією управління бізнесом, тобто неефективне управління в галузі IT може призвести до низьких результатів у бізнесі, і навпаки. У рамках стандарту реалізується підхід PDCA-циклу (PDCA: plan - do - check - act, тобто плануй - роби - перевіряй - дій). Вимоги бізнесу мають відповідати можливостям інформаційних технологій, а також мають бути чітко задокументовані та кількісно і якісно виміряні (plan, тобто плануй). Обране рішення має бути впроваджене і використане (do, тобто роби). Результати від впровадження мають відповідати критеріям, обраним на першому етапі (check, тобто перевіряй). Відхилення мають бути оцінені та необхідних заходів вжито (act, тобто дій) [26].

Стандарт складається з 4 доменів, розбитих на 34 процеси, які засвідчують конфіденційність, цілісність, доступність важливої та критичної інформації [28]:

Планування й організація:

розробка стратегічного плану;

побудова інформаційної архітектури;

побудова технологічної моделі;

визначення структури та організації IT;

управління інвестиціями в IT;

узгодження цілей бізнесу в IT;

управління людськими ресурсами;

відповідність зовнішнім вимогам;

оцінка ризиків;

управління проектами;

управління якістю.

Придбання та впровадження:

вибір рішення;

придбання/розробка додатків;

придбання системних ресурсів;

підтримка технологічної документації;

встановлення та налаштування додатків;

управління змінами.

Супровід і підтримка:

обслуговування користувачів;

управління послугами третіх осіб;

управління продуктивністю і потужністю;

забезпечення безперервності діяльності;

забезпечення інформаційної безпеки;

класифікація та розподіл витрат;

навчання користувачів;

допомога та консультування користувачів;

управління конфігурацією;

управління проблемами та збоями;

управління інформацією;

управління інфраструктурою;

управління операціями.

Моніторинг та оцінка:

моніторинг процесів;

внутрішній контроль;

відповідність вимогам зовнішніх осіб і органів;

зовнішній аудит.

Використання стандарту CobiT під час аудиту ІС дає змогу пов'язати управління інформаційними технологіями з бізнес-завданнями підприємства (див. рис. 2.1).

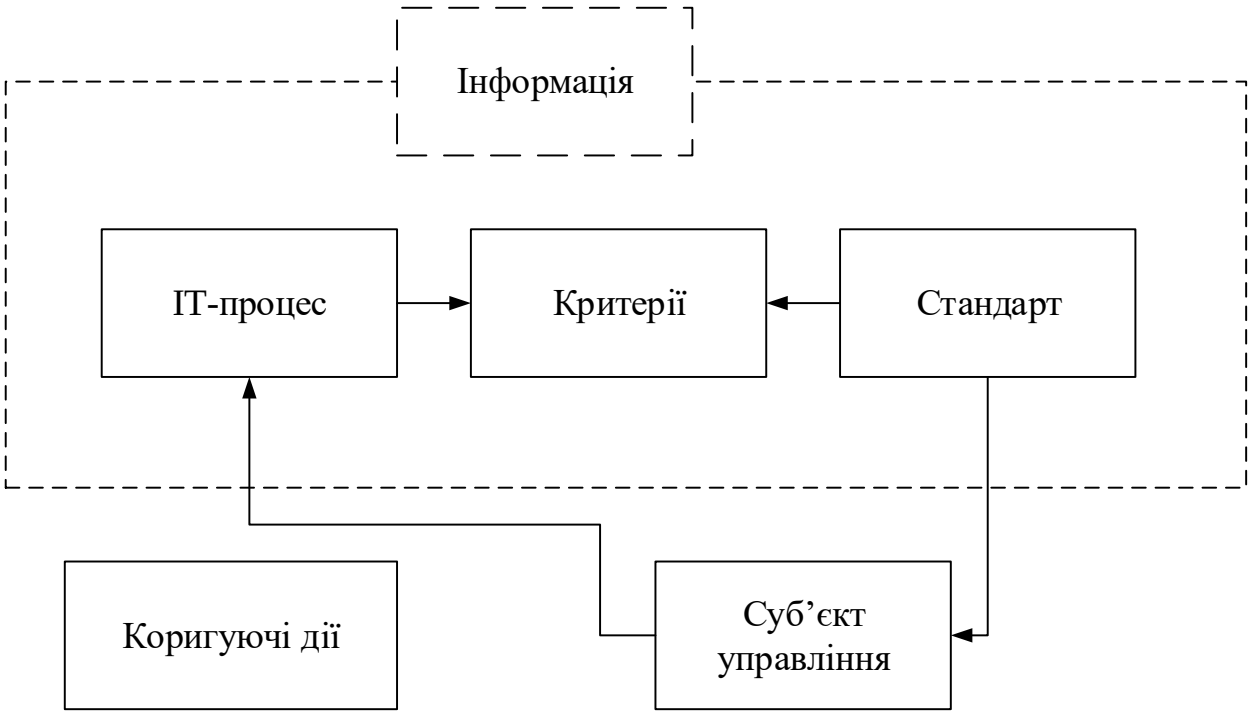

Рисунок 2.1 - Управління IT-процесами

У межах цієї методології проводиться аналіз таких ресурсів [25]:

а) Трудові ресурси - менеджмент, штатними та позаштатними працівниками організації; враховуються їхні навички, розуміння завдань та продуктивність праці;

б) Програми - програмне забезпечення, що використовується в роботі організації;

в) Технології - операційні системи, бази даних, системи управління тощо;

г) Обладнання - апаратне забезпечення ІС організації, з урахуванням їх обслуговування;

д) Інформація - записи, документи, зовнішні та внутрішні, структуровані та неструктуровані, текстові та графічні, відео тощо.

Аналіз проводиться на основі таких критеріїв оцінки:

Ефективність: Цей критерій оцінює відповідність та узгодження інформації з бізнес-цілями.

Технічний рівень: Цей критерій оцінює відповідність встановленим стандартам та рекомендаціям.

Безпека: Це стосується захисту інформації.

Цілісність: Цей критерій вимірює точність та повноту інформації.

Придатність: Це оцінює доступність інформації для поточних та майбутніх бізнес-процесів, а також захист необхідних та пов'язаних ресурсів.

COSO - стандарт, покликаний поліпшити якість фінансової звітності через ефективне управління системою внутрішнього контролю. Цей стандарт було опубліковано в 1992 р. Комітетом спонсорських організацій (Committee of sponsoring organizations). Стандарт складається з чотирьох частин [38]:

- Executive summary являє собою огляд загального підходу до внутрішнього контролю;
- Framework дає визначення СВК, її компонентів і містить критерії оцінки СВК підприємства;
- Reporting to external parties - частина стандарту, що дає загальні рекомендації щодо складання звітів про функціонування СВК як для укладачів і менеджменту фірми, так і для зовнішніх користувачів;
- Evaluation tools містить практичні рекомендації, корисні під час проведення внутрішньої оцінки СВК.

Framework - це основна частина в цьому стандарті, вона містить опис загальних методичних і приватних практичних питань функціонування системи внутрішнього контролю. Внутрішню контрольну процедуру в COSO визначають як процес, що підпадає під вплив ради директорів, керівництва та

іншого персоналу підприємства, розроблений з метою надання розумної впевненості щодо досягнення поставлених цілей у таких галузях [38]:

- ефективність і продуктивність операційної діяльності;
- надійність фінансової звітності;
- дотримання необхідних законів і регламентів.

Таким чином, як випливає з визначення, цей стандарт передбачає поділ усіх завдань підприємства на три групи - операційна діяльність, фінансова звітність, відповідність законодавчим актам. Досягнення поставлених цілей здійснюється за допомогою реалізації керівництвом підприємства послідовних дій у таких галузях:

- контрольне середовище;
- оцінка ризику;
- дії щодо здійснення контролю;
- інформація та комунікації;
- моніторинг.

Стандарт зачіпає такі чинники, як загальні концепції менеджменту і стиль керівництва, правила і прийоми роботи з трудовими ресурсами, чесність і особисті якості співробітників, організаційна структура, а також уважність і керівна роль ради директорів. Стандарт COSO включає керівництво до оцінки кожного з цих факторів [38].

ITIL - стандарт, спочатку розроблений Центральним Агентством з Обчислювальної Техніки та Телекомунікацій, згодом Державною Торговою Палатою Великої Британії [29].

ITIL являє собою серію книжок, у яких викладено теоретичні аспекти та практичний досвід у сфері управління IT і надання високоякісних інформаційних послуг [26].

За останнє десятиліття бібліотека ITIL de-facto стала світовим стандартом організації робіт IT-підрозділів та IT-компаній.

Мета ITIL - розробка підходу до управління якістю інформаційних послуг незалежно від постачальника.

У семи томах ITIL описано набір процесів, необхідних для того, щоб забезпечити постійну високу якість IT-сервісів і підвищити ступінь задоволеності користувачів. Слід зазначити, що всі ці процеси націлені не просто на забезпечення безперебійної роботи компонент IT-інфраструктури. Набагато більшою мірою вони націлені на виконання вимог користувача і замовника. Зрештою, всі процеси ITIL працюють на підвищення конкурентоспроможності, будучи невід'ємною частиною успішної компанії.

Використаний у бібліотеці процесний підхід повністю відповідає стандартам серії ISO 9000. Процесний підхід акцентує увагу підприємства на досягненні поставлених цілей, а також на ресурсах, витрачених на досягнення цих цілей. Процесний підхід не має собі рівних щодо забезпечення вимірності та керованості діяльності підприємства, що, власне, і зробило його таким популярним.

Слід зазначити, що ITIL є окремим випадком більш загальної концепції ITSM (IT Service Management) - Information Technology Service Management [29].

Поточна редакція ITIL містить у собі сім книг [30]:

сервісна підтримка (service support);

доставка сервісів (service delivery);

планування впровадження управління сервісом (planning to implement service management);

управління інфраструктурою ICT (ICT infrastructure management);

управління прикладними програмами (application management);

управління безпекою (security management);

бізнес-перспективи, частина 2 (business perspective, volume II).

Також є "додаткова" книга - управління програмним забезпеченням (software asset management).

У 2007 р. з'явилася нова третя версія бібліотеки найкращого досвіду у сфері управління сервісами ITIL. Нова версія складається з трьох частин [30]:

- ядро (core);
- додаткові книги (complementary);
- інтернет-частина (Web).

До "ядра" входять такі книжки:

- за сервісною стратегією (service strategy);
- за перехідними процесами сервісів (service transition);
- за операційними процесами сервісів (service operation);
- з проєктування сервісів (service design) та їх постійного вдосконалення (continual service improvement).

Серія додаткових книжок (complementary) має стати наочним посібником для дій працівників сфери IT з огляду на окремі сектори ринку (державний, фінансовий тощо) та національні особливості.

Проте, ITIL може бути корисний аудиторам, оскільки надає дві концепції роботи інформаційних технологій: цілісний підхід до управління сервісом і орієнтація на користувача. Цілісний підхід до управління сервісом розглядає процес управління в цілому, а не його окремі частини, і враховує, що:

- усі вимоги до операційної діяльності та підтримки враховуються;
- розробляються плани тестування;
- визначається вплив зміненої або нової ІС на наявну інфраструктуру;
- визначаються майбутні вимоги.

Орієнтація на користувача є основою надійного функціонування в майбутньому [39].

CMMI (Capability Maturity Model Integration) - це зібрання практичних рекомендацій для поліпшення процесів розробки програмних продуктів, ІС.

Стандарт був виданий американським інститутом Software engineering institute у 2002 р.

Цей стандарт покриває чотири предметні області, які в самому стандарті називаються дисциплінами [30]:

- системний інжиніринг (system engineering);
- інжиніринг програмного забезпечення (software engineering);
- розробка вбудованих продуктів і процесів (integrated product and process development, IPPD);
- робота з постачальниками (supplier sourcing).

Системний інжиніринг розглядає процеси розроблення систем, іноді включно з програмним забезпеченням.

Ця дисципліна сфокусована на основних потребах фінальних користувачів, їхніх очікуваннях від інформаційної системи та обмеженнях, що можуть перешкодити її оптимальному функціонуванню.

Програмний інжиніринг розглядає процеси розроблення, у т.ч. застосування систематичного підходу з кількісними аспектами до розроблення, функціонування та його підтримки.

Розроблення вбудованих продуктів і процесів - це підхід, який забезпечує своєчасну взаємодію користувачів із розробниками протягом усього процесу розроблення та функціонування інформаційної системи.

Робота з постачальниками - це дисципліна, яка розглядає придбання додаткових продуктів від постачальника, тобто можливі функції підтримки, оновлення компонентів систем, додавання нових модифікацій.

Найпродуктивнішим вважається розгляд усіх чотирьох дисциплін користувачем одночасно, особливо перших двох.

Під час аналізу системи із застосуванням CMMI виокремлюють рівні можливостей і зрілості. Рівень можливостей (capability level) розглядає загальні та приватні цілі та практичні дії щодо їх реалізації. Існує шість рівнів можливостей [26]:

рівень 0 - незавершений;

рівень 1 - той, що працює / поточний;

рівень 2 - керований;

рівень 3 - визначений і керований;

рівень 4 - якісне управління;

рівень 5 - оптимальний.

Рівні зрілості характеризують підприємство загалом. Виділяють п'ять рівнів, які застосовують до аналізу кожної з областей процесів, розглянутих вище:

- рівень 1 - початковий;
- рівень 2 - керований;
- рівень 3 - визначений;
- рівень 4 - управління якістю;
- рівень 5 - оптимальний.

Компоненти стандарту CMMI подано у вигляді схеми (див. рис. 2.2).

Область процесів включає [26]:

- управління процесом полягає в тому, щоб ефективно визначати, планувати, забезпечувати ресурсну базу, застосовувати, проводити моніторинг, контролювати, вимірювати й оцінювати, покращувати процеси в різних проєктах. Інакше кажучи, ця галузь стандарту ставить собі за мету забезпечення максимальних вигод від навчання, інновацій та структурування поточної діяльності підприємства;

- управління проєктом схоже у своїй практичній реалізації на управління процесом, тільки об'єктом управління, контролю і планування є проєкт і ускладнюється взаємодією з постачальниками, його якісним і кількісним аналізом, а також управлінням ризиками та аналізом сумісності проєкту з поточною ІС;

- інжиніринг - розробка і підтримка в усіх процесах, супутніх створенню ІС (включно із системним і програмним інжинірингом), і включає:

- планування проєкту;
- моніторинг і контроль проєкту;
- роботу з постачальниками;
- аналіз сумісності проєкту та управління ризиками;
- управління персоналом (командна гра);

- підтримка - це дії, які супроводжують процес розроблення, у таких галузях, як управління конфігураціями, менеджмент якості продукту, вимірювання та оцінювання, підготовка організаційної структури до впровадження, аналіз рішень, аналіз випадкових подій і методів розв'язання їхніх результатів.

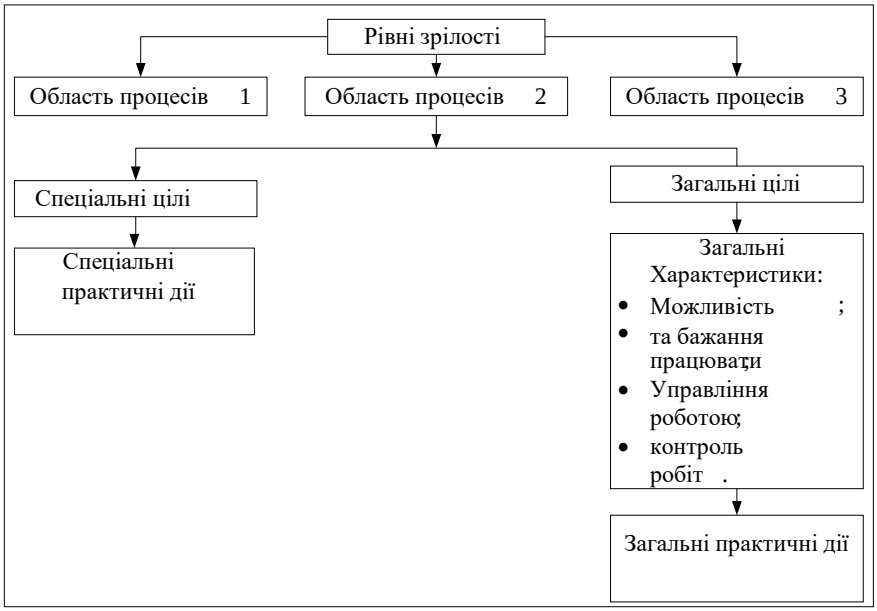

Рисунок 2.2 - Структурні компоненти стандарту CMMI

Завдання цього стандарту полягає в скороченні витрат і витрат на поліпшення поточної ІС за допомогою логічного та послідовного аналізу поточних процесів її управління [26].

Розглянувши основні стандарти, що використовуються в галузі управління та аналізу ІС, доцільно провести їх порівняння з найповнішим і

найдетальнішим стандартом CobiT за процедурами, що в ньому розглянуті, та як категорії оцінювання обрати частоту і глибину розкриття інформації.

2.2 Процесна модель проведення процедури аудиту інформаційних систем

Для розуміння процесів аудиту інформаційних систем необхідно використовувати два підходи: попроцесний і поелементний [31].

Суть попроцесного підходу полягає в перевірці всіх істотно важливих процесів обробки інформації та закінчуючи наданням її керуючій ланці підприємства для аналізу та формування управлінських рішень [32].

При поелементному підході аудитор досягає розумної впевненості щодо елементів функціонування ІС у частині забезпечення достовірності фінансової звітності економічного суб'єкта. Під елементами в цьому випадку розуміються структурні одиниці ІС.

Поелементний підхід до аудиту ІС передбачає поділ структурних компонентів (елементів) господарських операцій (розглянуті в другому пункті першого розділу) в ІС і перевірку їх роботи.

Структурні елементи поділяються на дві групи: функціональні та інформаційні. Функціональні елементи своєю чергою поділяються на модулі технічного, технологічного та ергономічного забезпечення, під час аудиту яких аудитору слід розглянути можливості залучення зовнішніх експертів [31, 33].

Сукупність організаційних, методичних і технічних прийомів, які здійснюються за допомогою певних процедур, складають аудиторський процес [18].

Розглянемо процес проведення процедури аудиту інформаційної системи. Для цього побудуємо процесну модель [побудована самостійно, на основі даних із джерела 18].

Вхідною інформацією є: заявка на проведення аудиту ІС, інформаційна система, супровідна документація щодо ІС, загальна інформація про підприємство-замовника, стандарти.

Механізмами виступають: аудиторська фірма, підприємство-замовник аудиту ІС і робоча група аудиторів.

Управління включають: нормативно-правове забезпечення аудиторської діяльності (Закон України "Про аудиторську діяльність", Стандарти аудиту, Кодекс етики професійних бухгалтерів і Положення Аудиторської палати України), стандарти з аудиту інформаційної системи, база фактів (штатний розклад), база правил (посадові інструкції, технічна документація), критерії ІС і опис процесів та інша нормативно-правова база.

Вихідна інформація: підписаний договір на надання аудиторської послуги, узгоджена "Пропозиція", аудиторський звіт, результати вивчення інформаційних потоків і процесів підприємства, аналіз захищеності та безпеки ІС; результати діагностики апаратного комплексу, програмного забезпечення, мережевої інфраструктури; ступінь відповідності стандартам і бізнес-процесам підприємства; ступінь економічної ефективності ІС.

Проведемо декомпозицію основного процесу "Аудит інформаційної системи" - послідовну деталізацію вихідної моделі процесу до заданого рівня шляхом створення детальних моделей для кожного об'єкта процесу.

Аудит ІС містить у собі три етапи:

планування процедури аудиту інформаційної системи підприємства;

проведення процедури аудиту;

підготовка та підписання звітних документів.

Перший етап "Планування процедури аудиту" включає в себе такі підетапи:

1.1. Узгодження цілей і завдань процедури аудиту інформаційної системи;

1.2. Підготовка та узгодження плану проведення аудиту інформаційної системи;

1.3. Розробка пропозиції замовнику та підписання договору на надання аудиторських послуг.

Далі проведемо декомпозицію цього етапу і представимо процес у нотаціях процедур.

На першому етапі формулюються цілі та завдання аудиту, узгоджуються з призначеними відповідальними за це працівниками підприємства-замовника, після чого проводиться планування аудиту інформаційної системи або, інакше кажучи, розробка загальної стратегії та деталізації підходу до очікуваного характеру, термінів проведення та обсягу аудиторських процедур. Визначаються важливі області та процеси, аудиту яких слід приділити належну увагу для виявлення потенційно слабких місць. Для підвищення ефективності послуг, що надаються, та координації дій, аудиторська отримує загальну інформацію про діяльність організації, обговорює особливості функціонування системи та визначені аудиторські процедури з працівниками. Після цього складається передбачуваний досить детальний план дій проведення процедури аудиту інформаційної системи, в якому викладено; сутність, мету, завдання, тривалість і охоплення аудиту, а також і необхідні ресурси та інше.

Після вивчення підприємством-замовником плану дій проведення процедури аудиту, ним складається "Технічне завдання" - документ, у якому зазначається перелік вимог, умов, цілей і завдань, поставлених Замовником, що мають ураховуватись під час надання послуги, розробки проекту тощо. З боку ж аудиторської фірми складається документ "Пропозиція" - виражене в письмовій формі бажання (обґрунтування) спроможності аудиторської фірми надати аудиторські послуги Замовнику. Ці обидва документи узгоджуються двома сторонами, після чого настає кінцева подія 1-го етапу - а саме, підписання договору на надання аудиторських послуг.

Другий етап "Проведення процедури аудиту" (див. додаток Е) починається з діагностики апаратного комплексу, програмного забезпечення та мережевої інфраструктури, а також виявлення, класифікації та інвентаризації компонентів інформаційних систем.

Інвентаризація та аналіз складових інформаційних систем. У рамках цієї роботи робоча група аудиторів проводить комплексну оцінку інформаційної системи з урахуванням її особливостей. Така оцінка включає аналіз інформаційних потоків апаратного та програмного забезпечення, мережевої інфраструктури та адміністрування компонентів. На даному етапі процедури проведення аудиту необхідно провести повне дослідження і класифікацію елементів інформаційної системи, проте лише тих, заміна яких може призвести до підвищення якісного рівня функціонування інформаційної системи загалом, або її складових.

Цей етап обстеження виявляється досить корисним для більшості керівників підприємств, тому що керівник не завжди володіє узагальненою і структурованою інформацією про наявну інформаційну систему підприємства та представляє її як розрізнену сукупність окремих елементів.

Щодо апаратних засобів доцільно проаналізувати такі важливі аспекти:

типи, технічні характеристики та потужність ЕОМ;

кількість, технічні характеристики та ємність головних накопичувачів і високопродуктивних принтерів;

кількість, "інтелектуальність" та орієнтованість (пристосованість до застосування) дисплеїв і принтерів;

кількість і характеристики інших пристроїв введення-виведення;

внутрішні обчислювальні мережі та їхні компоненти;

зовнішні телекомунікаційні зв'язки;

місця встановлення технічних засобів;

доступність і характерний час відповіді (за нормального і пікового навантаження) центральних і периферійних ЕОМ;

"історія розвитку" (частка приросту, розвиток продуктивності та ємності) технічних засобів;

можливості розширення технічних засобів тощо.

Необхідно охарактеризувати такі компоненти програмних засобів:

операційні системи, їхні розширення, системи теледоступу;

мережеві програмні засоби та засоби теледоступу, системи управління та комунікації ПЕОМ;

СУБД;

допоміжні програми (управління дисковими накопичувачами, налаштування систем, контроль виконання тощо);

інструменти кінцевого використання;

розвиток оточення інформаційної системи (інструменти та мови аналізу, дизайну і програмування, а також транслятори з мов);

системи безпеки (збереження і захисту даних);

використовувані зовнішні програмні засоби;

дані про можливості розширення програмних засобів.

Отримана інформація про елементи інформаційної системи має бути суворо документована і, бажано, подана в графічній формі.

На етапі аналізу програмного забезпечення інформаційної системи необхідно оцінювати різні види програмного забезпечення: системне, мережеве, офісне, прикладне. Оцінка ПЗ має проводитися як загалом за інформаційною системою, так і за окремими автоматизованими робочими місцями. При цьому необхідно класифікувати програмне забезпечення за ступенем його важливості. Такий підхід дасть змогу оцінити відповідність даного АРМ поставленим перед ним функціональним завданням, які були виявлені на попередніх етапах аудиту. За необхідності потрібно розробити рекомендації щодо інсталяції необхідного, заміни застарілого або такого, що не відповідає апаратним можливостям, ПЗ, а можливо, і щодо усунення деяких програм через відсутність необхідності в них.

Під час вибору ПЗ необхідно керуватися певними критеріями. Аналіз технічної документації пакетів прикладних програм, а також літературних джерел дав змогу виявити перелік критеріїв, які характеризують у різних аспектах застосування ППП, що їх можна згрупувати в підмножини та розробити для них систему класифікації (таблиця 2.1).

Таблиця 2.1 - Критерії відбору програмних продуктів

Найменування критерію	Зміст підкритеріїв
1. Призначення і можливості	Предметна сфера використання, забезпечення функцій управління, можливості розширення функцій і оптимізації розрахунку, можливість взаємозамінності технічних засобів, універсальність
2. Оптимальні ознаки та властивості	Вхідна та керівна мова, спосіб зберігання даних, спосіб доступу до даних, генерація звітних документів, мова програмування
3. Вимоги до технічних і програмних засобів	Обчислювальна система, обсяг оперативної пам'яті, обсяг зовнішньої пам'яті, тип операційної системи, допоміжні програмні засоби, сумісність із використовуваною СУБД
4. Документація ПП	Загальний посібник із використання, посібник системного та програмного рівня
5. Фактори фінансового порядку	Витрати на придбання пакета, опрацювання, встановлення; підготовку персоналу, техніки; обслуговування та здійснення технічної підтримки
6. Особливості встановлення і розвитку	Обсяг робіт і тривалість встановлення, час встановлення, необхідні модифікації ОС і СУБД
7. Особливості функціонування	Залежність робочих характеристик від використовуваних технічних і програмних засобів, можливість обслуговування силами фахівців підприємства
8. Участь постачальника ПП у впровадженні та супроводі	Навчання персоналу, перехід від старої системи до нової, коригування системи помилок, модифікація, простота використання
9. Перспективи	Удосконалення концепції та використовуваних методів, підключення нових функціональних можливостей, сумісність зі старою версією

Для кожної комплексної та одиничної характеристики на основі оцінок кількох експертів (наприклад, за бальною шкалою) встановлюють

середньозважені вагові коефіцієнти значущості, які нормують усередині групи:

$$K_{n_j} = \frac{K_j}{\sum_{j=1}^{m} K_j}$$

де Kn - комплексний нормований ваговий коефіцієнт;

Kj- комплексний ваговий коефіцієнт для j-тої комплексної характеристики;

m - кількість комплексних характеристик.

Одиничні характеристики визначаються як:

$$O_i = \delta_i \times \varpi_i$$

де – Oi зважена оцінка i-ої одиничної характеристики.

Комплексні оцінки визначаються як:

$$O_k = \sum_{1}^{n} O_j$$

де – Ok зважена оцінка j-ої комплексної характеристики.

Зважені оцінки характеристик підсумовуються за групами і загалом:

$$Z = \sum_{1}^{n} O_k$$

де Z - інтегральна оцінка програмного продукту.

Під час аналізу мережевої інфраструктури необхідно визначити:

використовувані стандарти;

кабельну інфраструктуру;

кількість, характер і взаємозв'язок сегментів мережі;

топологію мережі.

Після проведення цієї роботи з'являється можливість за необхідності розробити рекомендації щодо оптимізації мережевої інфраструктури.

Наступним кроком є вивчення інформаційних і бізнес-процесів підприємства-замовника та аналіз захищеності й безпеки інформаційної системи.

Етап вивчення інформаційних і бізнес-процесів досить важливий для подальшої роботи. Саме на цьому етапі необхідно виявити:

групи завдань, про які йшлося під час опису загальної характеристики процесу аудиту ІС;

обсяги потоків інформації;

обсяги інформації, які необхідно обробляти і зберігати в рамках конкретних автоматизованих робочих місць;

необхідна швидкість обміну інформацією між АРМ;

форми подання оброблюваної інформації;

повноту автоматизації бізнес-процесів цього підприємства.

Під час проведення цього етапу доцільно побудувати потоки даних, що дають змогу провести аналіз діяльності підприємства.

Що стосується аналізу захищеності та безпеки інформаційної системи, то він включає:

1. Аналіз відповідної організаційної структури забезпечення інформаційної безпеки.

2. Аналіз наявної нормативно-правової бази інформаційної безпеки автоматизованої системи, зокрема оцінка прийнятої політики безпеки, організаційно-розпорядчих документів, положень та інструкцій щодо забезпечення захисту інформації.

3. Аналіз заходів технічного захисту інформації, зокрема аналіз наявних заходів і засобів технічного захисту інформації, а також порядку їхнього застосування, розгляд і аналіз використовуваних замовником засобів розмежування доступу та захисту від несанкціонованого доступу, антивірусних засобів, міжмережевих екранів, захисту за допомогою паролів,

системи виявлення вторгнень, криптографічних засобів захисту інформації, методів контролю цілісності.

4. Виявлення загроз безпеці (як внутрішніх, так і зовнішніх) та наявних вразливих місць у компонентах системи, а також оцінювання ризиків.

5. Вироблення рекомендацій щодо доопрацювання наявної системи захисту інформації підприємства. Рекомендації можуть стосуватися вдосконалення організаційно-штатної структури, доопрацювання і створення нормативних документів, положень та інструкцій із забезпечення інформаційної безпеки. Крім того, робоча група аудиторів може дати рекомендації щодо застосування штатних засобів захисту компонентів, а також щодо використання додаткових систем захисту інформації та методів контролю й аудиту стану інформаційної безпеки.

Після цього перевіряють інформаційну систему на відповідність загальним стандартам, внутрішньокорпоративним стандартам управлінського обліку - MRP II, ERP, CSRP тощо, а також бізнес-процесам підприємства.

В рамках внутрішньокорпоративних стандартів до інформаційної системи висуваються такі вимоги:

Функціональна повнота системи – система повинна забезпечувати всі необхідні функції.

Локалізація інформаційної системи – адаптація системи до специфіки регіону чи мови.

Надійність захисту інформації – забезпечення високого рівня безпеки даних.

Реалізація віддаленого доступу та роботи в розподілених мережах – можливість доступу до системи з різних локацій.

Наявність інструментальних засобів адаптації та супроводу системи – підтримка та модернізація системи.

Забезпечення обміну даними між вже впровадженою інформаційною системою та іншими програмними продуктами, що використовуються на підприємстві – інтеграція з іншими системами.

Можливість консолідації інформації – об'єднання даних з різних джерел.

Наявність спеціальних засобів для аналізу стану системиПід час проведення цього етапу необхідно відповісти на запитання про відповідність наявної системи поточному стану організації виробництва та управління підприємством, з урахуванням цілей виробника, що полягають у встановленні балансу комерційних, виробничих і фінансових цілей.

Варто відзначити, що існує п'ять рівнів організації бізнес-процесів на підприємстві:

1. Хаос – стан, коли комерційні, виробничі та фінансові цілі перебувають у дисбалансі. Хаос характеризується відсутністю системного підходу; підприємство сприймається як набір окремих елементів.

2. Контроль – досягнення балансу між комерційними, виробничими та фінансовими цілями підприємства. На цьому рівні передбачено "налагоджений" облік і контроль основних процесів.

3. Оптимізація – спрощення ключових бізнес-процесів на підприємстві, що призводить до зниження витрат.

4. Адаптація – поліпшення бізнес-процесів у відповідь на зміни в зовнішньому середовищі.

5. Світовий клас.

На кожному етапі переходу підприємства з одного рівня на інший може використовуватися певна система управлінського обліку та система якості. При цьому процес переходу розглядається як безперервне поліпшення бізнес-процесів. Заключним же кроком у рамках етапу проведення процедури аудиту є оцінка економічної ефективності інформаційної системи.

Єдиного підходу до визначення кількісних значень економічного ефекту, що забезпечується функціонуванням інформаційної системи підприємства,

наразі не вироблено. У вітчизняній літературі часто розглядають два підходи, що базуються на розрахунку річного та інтегрального економічного ефекту.

Порівняльний аналіз двох підходів, що базуються на розрахунку річного та інтегрального економічного ефекту, наведено в таблиці 2.2.

Таблиця 2.2 - Порівняльна характеристика методів аналізу економічної ефективності

Найменування критерію	Методика визначення річного економічного ефекту	Методика визначення інтегрального економічного ефекту
Основні показники	Річний економічний ефект; Термін окупності одноразових витрат	Інтегральний (сумарний) ефект; Період повернення одноразових витрат
Розрахунковий період	Перший рік промислового використання	Часовий відрізок від року початку фінансування робіт пов'язаних з ІС, до року закінчення ефективності використання ІС
Основні принципи	Економічний ефект є різницею наведених витрат на базову технологію без ІС та із застосуванням ІС; Величина економічно приведених витрат є оцінкою результату використання ІС; Одноразові витрати враховуються за весь період їх реалізації до розрахункового року. Експлуатаційні витрати враховуються тільки за один рік - розрахунковий. Річні витрати цього року приймаються як незмінні під час розрахунку терміну окупності витрат.	Економічний ефект є різницею між вартісною оцінкою результату використання ІС і витратами на досягнення цього результату; Усі види економії враховуються у складі відповідних витрат, одноразових та експлуатаційних; Дослідження витрат і результатів проводять у динаміці за весь період створення і використання ІС. Для спрощення розрахунків може робитися допущення про незмінність результатів і експлуатаційних витрат за роками розрахункового періоду
Наслідки	Висновок про економічну ефективність ІС робиться на основі дослідження і вартісної оцінки переваг використання ІС порівняно з базовою технологією - у перший рік промислової експлуатації	Висновок про економічну ефективність ІС робиться на основі прогнозування масштабів створення і використання ІС за всім життєвим циклом, обліку всіх витрат і всіх результатів.

Також використовують функціонально-вартісний аналіз - метод комплексного системного дослідження функцій об'єктів, спрямований на забезпечення суспільно необхідних споживчих властивостей об'єктів і мінімальних витрат на їх прояв на всіх етапах життєвого циклу. Метод ФСА базується на твердженні про те, що витрати, пов'язані зі створенням і використанням будь-якого об'єкта, зумовлені необхідністю виконання об'єктом заданих функцій.

ФСА має принципову відмінність від традиційних способів оцінювання та зниження виробничих і експлуатаційних витрат, оскільки передбачає використання функціонального підходу, сутність якого полягає в розгляді інформаційної системи не в її конкретній формі, а як сукупності функцій, які вона має виконувати. Кожна з функцій аналізується з позиції можливих принципів і способів виконання за допомогою сукупності спеціальних прийомів. У ФСА під функцією розуміють зовнішній прояв властивостей будь-якого об'єкта в даній системі відносин. Найчастіше її ототожнюють із призначенням, станом аналізованого об'єкта, його здатністю до дії, впливу, задоволення потреби.

Важливою умовою ефективного застосування цього методу є чітка послідовність етапів його проведення: підготовчого, інформаційного, аналітичного, творчого, дослідницького, рекомендаційного, впровадження результатів.

На заключному етапі відбувається підготовка та підписання звітних документів (див. додаток Ж), а саме аудиторського звіту, який містить таку інформацію:

Інформація про поточний стан ІС:

оцінка поточного стану ІС;

аналіз ІТ-ризиків та ідентифікація ключових ресурсів ІС;

наявна архітектура ІС;

розподіл ролей і відповідальності;

політики та процедури, документація.

Рекомендації щодо поліпшення стану ІС:

створення еталонної архітектури;

рекомендації з організації/оптимізації обслуговування ІС організації;

рекомендації з оцінки ризиків;

вимоги та рекомендації щодо політики інформаційної безпеки;

рекомендації щодо вироблення необхідних політик і процедур, документації.

Вимоги до персоналу та навчання.

Рекомендації щодо методів отримання своєчасної та об'єктивної інформації про поточний стан ІС організації.

Рекомендації щодо впровадження поліпшень.

Результати аудиту ІС організації можна розділити на три основні групи:

1. організаційні - планування, управління, документообіг функціонування ІС;

2. технічні - збої, несправності, оптимізація роботи елементів ІС, безперервне обслуговування, створення інфраструктури тощо;

3. методологічні - підходи до вирішення проблемних ситуацій, управління і контролю, загальна впорядкованість і структуризація.

Таким чином, у процесі проведення аудиту інформаційних систем замовник із незалежного джерела отримує: інформацію про слабкі місця і ділянки в інформаційній системі, технологічному процесі обробки даних; оцінку адекватності та ефективності використовуваних організаційно-технічних заходів; реальне розуміння, на якому рівні зрілості перебуває управління інформаційною системою на підприємстві. Однак, ефективну й оперативну процедуру аудиту інформаційної системи підприємства може бути надано лише в разі усунення "вузьких місць" кожного описаного підетапу в разі їх існування.

2.3 Імітаційна модель проведення аудиту інформаційної системи підприємства

Складність економічних систем, що зростає, вимагає застосування адекватних методів їх дослідження, вдосконалення та проектування. Найефективнішим методом системного аналізу складних об'єктів є метод імітаційного моделювання [52].

Імітаційне моделювання дає змогу відображати процеси, так, наче б вони відбувалися в реальності. Для проведення імітаційного моделювання проводять побудову моделі досліджуваної системи, яка з достатньою точністю описує реальну систему [40]. Імітаційна модель являє собою абстрактний об'єкт, що замінює об'єкт дослідження в процесі його вивчення, перебуває у відносинах схожості з останнім і використовується для оцінки динаміки досліджуваного процесу. Імітаційна модель дає змогу отримувати докладну статистику про різні аспекти функціонування системи залежно від вхідних даних [20].

Використання імітаційного моделювання дає змогу вивчити поведінку системи в часі. Вагомим плюсом є те, що часом у моделі можна керувати: сповільнювати у випадку з процесами, що швидко протікають, і прискорювати для моделювання систем із повільною мінливістю. Можна імітувати поведінку тих об'єктів, реальні експерименти з якими дорогі, неможливі або небезпечні [40].

Виділяють 3 основні підходи (парадигми) в імітаційному моделюванні [41]:

системна динаміка - метод, що дає змогу вивчення динаміки процесів у складних системах. Системно-динамічні моделі зазвичай задають у вигляді потокових діаграм, що складаються з накопичувачів і потоків, петель зворотного зв'язку та допоміжних змінних і констант;

дискретно-подієве (процесне моделювання) - метод опису процесів, що відбуваються в системі, у вигляді послідовності операцій. Описуються дискретно-подієві моделі у вигляді блоків, що обробляють заявки відповідно до заданих параметрів, і з'єднань між ними, що визначають послідовність операцій;

агентне моделювання - метод опису системи як безлічі незалежних об'єктів (агентів), кожен з яких є програмно або апаратно реалізованою системою, що взаємодіють один з одним і з навколишнім середовищем.

В основі імітаційної моделі магістерської роботи лежить розроблена процесна модель проведення аудиту інформаційної системи підприємства, тому буде використано дискретно-подієвий підхід моделювання, тому що саме в основі кожної процесоно-орієнтованої (дискретно-подієвої) моделі лежить діаграма процесу - послідовність з'єднаних між собою блоків, які задають послідовність операцій, які здійснюватимуться над заявками, що проходять по діаграмі процесу.

У зв'язку з ускладненням економічних систем, комп'ютерне моделювання стало одним з ефективних інструментів їхнього вивчення та обов'язковим етапом в ухваленні управлінських рішень. Очевидною проблемою є вибір пакета імітаційного моделювання, що підтримує дискретно-подієве моделювання [42]. Існує понад 100 різних систем імітаційного моделювання [44]. Проаналізуємо підтримку трьох основних підходів деякими пакетами імітаційного моделювання (див. таблицю 2.3) [43].

Отже, дискретно-подієві моделі можна будувати за допомогою деяких програмних продуктів. Очевидною проблемою стає вибір використовуваного програмного пакета імітаційного моделювання. Однозначної відповіді на це питання не існує, оскільки не встановлено єдиного критерію оцінювання переваг різних засобів імітаційного моделювання.

Більшість з програмних систем імітаційного моделювання підтримують лише одну парадигму побудови імітаційних моделей і не дають змоги

використовувати сучасний об'єктно-орієнтований підхід до опису моделей. Крім того, більшість із перерахованих продуктів відрізняє відсутність якісної локалізації та підтримки для українських умов.

Таблиця 2.3 - Порівняльна характеристика методів аналізу економічної ефективності

Метод	Ithink	Powersim	Пілгрім	Process charter	ARENA	Any Logic	Star Logo
Системна динаміка	+	+	-	-	+	+	-
Агентні моделі	-	-	-	-	-	+	+
Дискретно-подієве	+	-	-	-	+	+	-

Єдиною відомою на сьогоднішній день системою імітаційного моделювання, в якій реалізовано всі три сучасні парадигми побудови імітаційних моделей є програмне середовище AnyLogic. Цей продукт також дає можливість використання як однієї парадигми на вибір, так і застосування багатопідходного моделювання, що значно розширює сферу застосування цієї системи порівняно з аналогічними програмами. Крім того, наявність сучасного графічного інтерфейсу дає змогу конструювати моделі з численних готових об'єктів, що містяться в готових проблемно-орієнтованих бібліотеках [52, 46].

Таким чином, ПП Anylogic дають змогу швидко, якісно будувати й аналізувати моделі, зокрема, дискретно-подієву модель процесу проведення аудиту інформаційної системи підприємства.

Модель побудовано за допомогою об'єктів бібліотеки Enterprise Library, розробленої для підтримки дискретно-подієвого моделювання [46].

Припущення, на яких ґрунтується модель проведення процесу аудиту інформаційної системи підприємства:

1) аудит інформаційної системи складається з 4 етапів (детально описані в процесній моделі):

діагностика апаратного комплексу, програмного забезпечення та мережевої інфраструктури, а також виявлення, класифікація та інвентаризація компонентів інформаційних систем;

вивчення інформаційних і бізнес-процесів підприємства-замовника та аналіз захищеності та безпеки інформаційної системи;

перевірка інформаційної системи на відповідність загальним стандартам, внутрішньокорпоративним стандартам управлінського обліку, а також бізнес-процесам підприємства;

оцінка економічної ефективності інформаційної системи;

2) Компанії можуть проводити як усі етапи аудиту ІС, так і кожен окремо, але за умови, що кожен попередній етап уже виконано. Тобто, наприклад, без проведених 1-го і 2-го етапів аудиту не можна одразу приступити до виконання 3-го.

Імітаційна модель складається з набору взаємопов'язаних елементів, які входять у модель як змінні. Використовуються також наступні параметри: (таблиця 2.4):

Крім перерахованого у моделі використовуються елементи управління - бігунки, які дають змогу графічно вибирати число із заданого діапазону значень шляхом перетягування рукоятки. Бігунки в моделі використовуються для зміни значень чисельних змінних ResoursePool, ResoursePool1, ResoursePool2 і ResoursePool3 під час проведення імітаційного експерименту моделі. Для цього необхідно бігунки пов'язати з цими змінними (тобто присвоювати їм поточне значення кожного бігунка), для чого необхідно в основних властивостях бігунків установити прапорець Зв'язати з

ResoursePool.capacity, ResoursePool1.capacity, ResoursePool2.capacity і ResoursePool3.capacity відповідно.

Таблиця 2.4 - Опис параметрів моделі

Ім'я	Тип	Опис
i0	інтегр	Кількість відмовлених заявок
i1	інтегр	Загальна кількість проведених процедур 1 етапу аудиту
i2	інтегр	Загальна кількість проведених процедур 2 етапу аудиту
i3	інтегр	Загальна кількість проведених процедур 3 етапу аудиту
i4	інтегр	Загальна кількість проведених процедур 4 етапу аудиту
Sr1	інтегр	Середня кількість днів проведення 1 етапу аудиту
Sr2	інтегр	Середня кількість днів проведення 2 етапу аудиту
Sr3	інтегр	Середня кількість днів проведення 3 етапу аудиту
Sr4	інтегр	Середня кількість днів проведення 4 етапу аудиту

У моделі параметри мають такий вигляд (див. рис. 2.3):

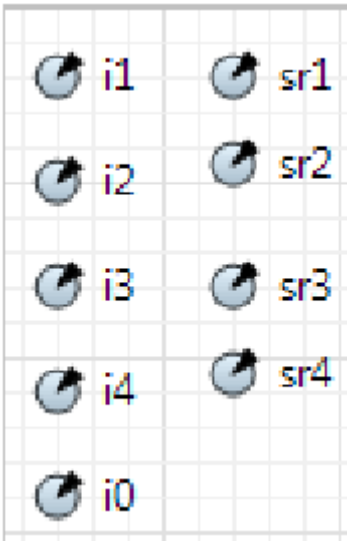

Рисунок 2.3 - Зовнішній вигляд параметрів моделі

Тобто, розроблена модель дає змогу змінювати кількість днів, необхідних для проведення кожного з чотирьох етапів аудиту інформаційної системи підприємства, та щоразу аналізувати новоотримані статистичні дані кількості опрацьованих заявок для ухвалення рішення щодо ефективного використання фонду робочого часу компанії. А для усунення вузьких місць (якщо такі є) шляхом, наприклад, скорочення тривалості різних етапів аудиту, що досягається, як один із варіантів, за рахунок розширення робочої групи аудиторів.

Бігунки мають такий вигляд (див. рис. 2.4):

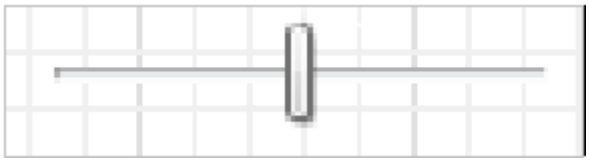

Рисунок 2.4 - Зовнішній вигляд елемента управління - бігунка

Таким чином, з урахуванням опису всіх об'єктів, побудована імітаційна модель представлена на рис. 2.5. Апробацію моделі проведено в другому пункті третього розділу.

Розроблена імітаційна модель проведення процесу аудиту інформаційної системи дає змогу компанії, що надаватиме даний вид послуги, визначити кількість опрацьованих заявок із загальної кількості заявок, що надходять на проведення аудиту ІС, із виведенням статистичної інформації про кількість кожного з чотирьох проведених етапів аудиту для подальшого аналізу наявної ситуації та, за необхідності, її покращення шляхом зміни значень змінних моделі.

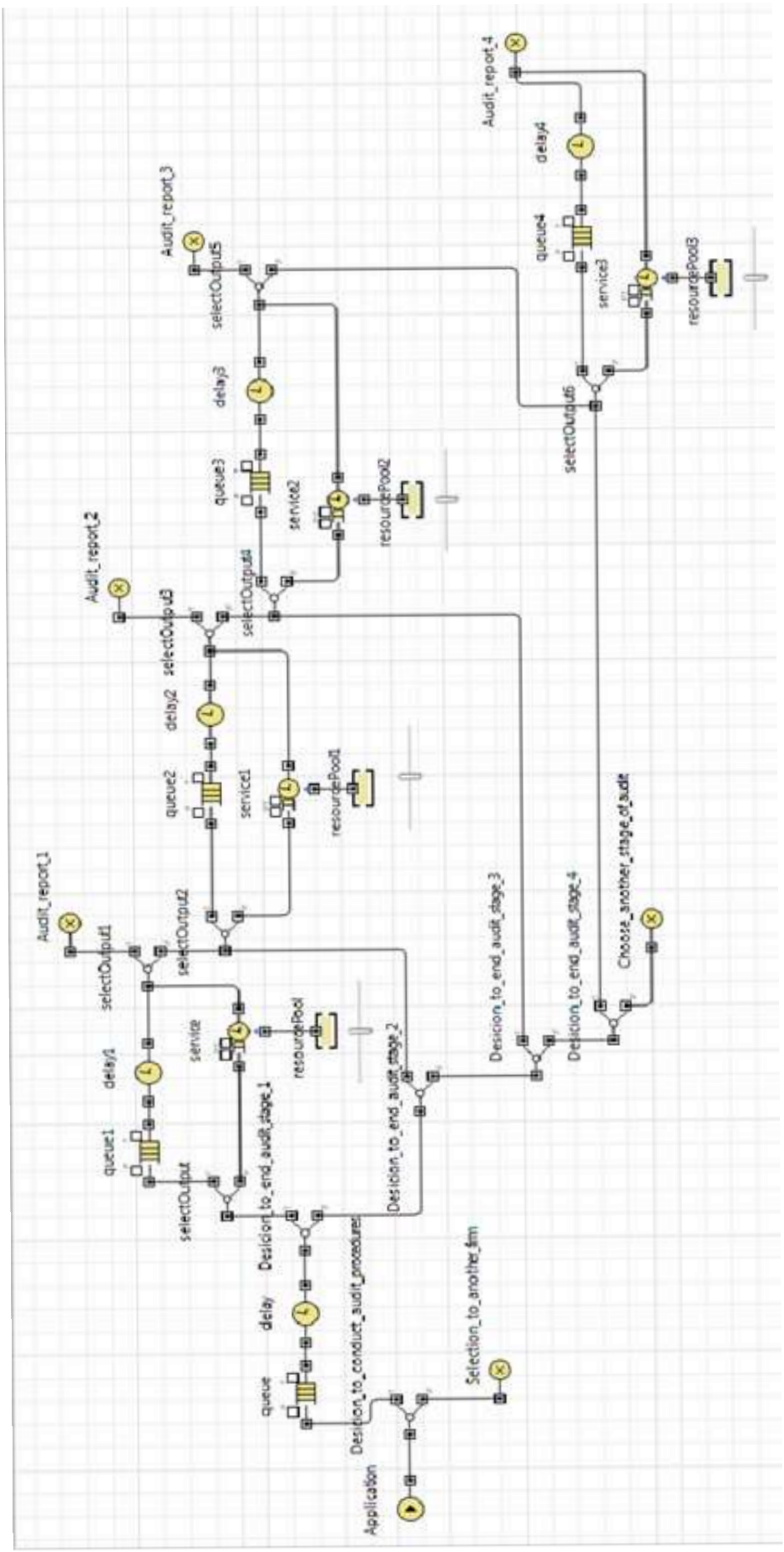

Рисунок 2.5 - Структура імітаційної моделі процедури аудиту інформаційної системи підприємства

Тобто модель дає можливість спланувати безпосереднє проведення процесу аудиту інформаційної системи підприємства на основі наявних даних, тим самим підвищивши ймовірність досягнення максимального ефекту функціонування компанії-аудитора.

2.4 Висновки розділу

У результаті аналізу вітчизняних і зарубіжних джерел автором було наведено порівняльну характеристику деяких стандартів аудиту інформаційних систем, що розроблені відповідно до міжнародних стандартів аудиту і містять основні принципи та найважливіші обов'язкові процедури. Специфічний характер здійснення такого контролю вимагають застосування низки норм, які характерні для цієї галузі. Завданням стандартів аудиту ІВ є інформування аудиторів на мінімально можливому рівні для відповідності професійній відповідальності, встановленій Кодексом етики. Стандарти аудиту ІВ встановлюють норми, які визначають обов'язкові вимоги в галузі аудиту ІВ та складання звітності.

1. У роботі детально описано процес проведення аудиту інформаційних систем за допомогою процесної моделі, побудованої в нотаціях IDEF. Ця модель є основою для побудованої автором імітаційної моделі аудиту інформаційних систем.

2. У результаті аналізу вітчизняних і зарубіжних джерел автором було наведено порівняльну характеристику програмних продуктів імітаційного моделювання з метою вибору відповідного для побудови дискретно-подієвої моделі проведення процесу аудиту інформаційних систем підприємства. аудиту інформаційних систем і необхідні компетенції для

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Апробація імітаційної моделі проведення процесу аудиту інформаційної системи підприємства

Для того, щоб отримати коректні результати під час експериментування, необхідно здійснити завдання реалістичних даних для кожної з відомих змінних моделі.

Апробацію моделі, побудованої в третьому пункті другого розділу, здійснено на основі статистичних даних з актуальних досліджень IT-консалтингових компаній України, таких як SoftServe, Ciklum, EPAM Systems та Luxoft. Також використовувалися експертні оцінки IT-фахівців з компаній Intellias, Infopulse та N-iX, які надають послуги аудиту інформаційних систем і оптимізації процесів для підприємств у різних секторах економіки.

Почнемо зміну властивостей змінних і самої моделі відповідно до наявної статистичної інформації.

У вкладці Модельний час панелі Властивості розділу Simulation: Main позначимо одиницями модельного часу дні. Модельний час становить 1 рік.

Згідно з даними консалтингової компанії IT Ukraine Association, у 2022 році в Україні було зареєстровано понад 70 000 заявок на проведення аудиту, з яких приблизно 15% припадали на аудит інформаційних систем (ІС). Враховуючи ці дані, модельована компанія, яка обслуговує 20% загального ринку цих послуг, обробляє близько 2 100 заявок на рік, що становить близько 175 заявок на місяць або 6-7 заявок на день. Таким чином, у поле «Кількість заявок, що прибувають за 1 раз», вкладки Основні панелі Властивості введемо значення 6 з інтенсивністю прибуття 2 заявки.

Для об'єктів queue, queue1, queue2, queue3 і queue4 у вкладці Основні панелі Властивості визначимо Максимально можливу місткість у моделі.

Для об'єктів delay, delay1, delay2, delay3 і delay4 у вкладці Основні панелі Властивості встановимо максимальну місткість.

Обробка заявки на проведення процесу аудиту інформаційної системи підприємства займає в компанії приблизно 1 день. Тому задамо час обслуговування, розподілений за трикутним законом із середнім значенням, що дорівнює 1, мінімальним - дорівнює 0.5 і максимальним - 1.5 дням, для об'єкта delay: введемо в поле Час затримки вкладки Основні панелі Властивості triangular(0.5, 1, 1.5). Функція triangular() є стандартною функцією генератора випадкових чисел AnyLogic.

Аналогічно заповнимо поля Час затримки для об'єктів delay1, delay2, delay3 і delay4: triangular(0.5, 1, 1.5), triangular(4, 5, 8), triangular(4, 7, 10), triangular(6, 10, 13) і triangular(8, 9, 11) відповідно. Дані отримано на основі експертних думок фахівців у сфері аудиту інформаційних систем таких українських компаній, як SoftServe, Infopulse, N-iX та Intellias, шляхом проведення електронних консультацій у 2023 році.

У полі Дія під час входу вкладки Основні панелі Властивості для об'єктів Audit_report_1, Audit_report_2, Audit_report_3, Audit_report_4 і Selection_to_another_firm встановимо таке: i1++, i2++, i3++, i4++ і i0++ відповідно. Об'єкт Choose_another_stage_of_audit залишимо без зміни, оскільки для результатів цієї моделі смислового навантаження він не несе.

Для наступних об'єктів задамо у вкладці Основні панелі Властивості значення, зазначені в таблиці 3.1. Дані отримано на основі експертних думок фахівців у галузі аудиту інформаційних систем таких українських компаній, як SoftServe, Intellias, Infopulse, N-iX та Ciklum, шляхом проведення електронних консультацій у 2023 році. За даними консалтингової компанії IT Ukraine Association, з усіх заявок на проведення аудиту інформаційних систем, на перший етап припадає близько 10% від загальної кількості заявок, на

другий — 50%, на третій — 15%, а на четвертий — 25%. У 2022 році більшість таких компаній задовольняли близько 85% заявок на проведення аудиту, причинами відмови залишаються: невідповідність бюджету, надмірна завантаженість замовленнями та інші об'єктивні причини. Крім того, замовники можуть відмовитися від послуг компанії, куди була надіслана заявка.

Об'єкт Desicion_to_conduct_audit_procedures. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.9.

Об'єкт Desicion_to_end_audit_stage_1. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.1.

Об'єкт Desicion_to_end_audit_stage_2. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.5.

Об'єкт Desicion_to_end_audit_stage_3. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.15.

Об'єкт Desicion_to_end_audit_stage_4. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.25.

Припустимо, що 30-50% підприємств-замовників після проведення одного з етапів аудиту погоджуються на проведення наступного.

Об'єкт selectOutput1. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.6.

Об'єкт selectOutput3. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.7.

Об'єкт selectOutput5. У вкладці Основні палітри Властивості встановимо прапорець Із заданою ймовірністю і в полі Ймовірність панелі Властивості введемо 0.65.

Імовірності об'єктів selectOutput, selectOutput2, selectOutput4 і selectOutput6 залишимо без зміни (за замовчуванням дорівнюють 0.5)

Задамо значення деяких параметрів моделі, а саме середньої кількості днів проведення кожного з етапів аудиту інформаційної системи підприємства (див. таблицю 3.1).

Налаштуємо в цій моделі, щоб поточне значення цих параметрів можна було змінювати в інтервалі від мінімального до максимального значення. Для цього скористаємося розглянутою раніше методикою створення елементів управління - бігунків. А також помістимо ці бігунки в окрему панель під назвою Панель налаштувань експерименту.

Таблиця 3.1 - Значення параметрів моделі

Ім'я	Поточне	Мін значення	Макс значення
Sr1	5	3	7
Sr2	7	5	9
Sr3	10	7	13
Sr4	8	6	12

Назви типу "Середня кількість днів проведення першого етапу аудиту" додано за допомогою елемента Текст Палітри Презентація. Цифрові значення характеристик є також елементами Текст Палітри Презентація. Однак у вкладці Динамічні палітри Властивості в полі текст потрібно відповідно написати: format(sr1), format(sr2), format(sr3), format(sr4), пов'язуючи їх тим самим із параметрами sr1, sr2, sr3 і sr4. Також для наочності отриманих результатів імітації моделі необхідно створити деякі елементи статистики

текстового формату, аналогічно попереднім елементам. Дані, які вводяться у вкладці Динамічні палітри Властивості, зазначені в таблиці 3.2.

Таблиця 3.2 - Дані для елементів статистики

Назва	Формула
Загальна кількість оброблених заявок:	format(i0+i1+i2+i3+i4)
Кількість відмовлених заявок:	format(i0)
Загальна кількість проведених процедур аудиту:	format(i1+i2+i3+i4)
Загальна кількість проведених процедур першого етапу аудиту:	format(i1)
Загальна кількість проведених процедур другого етапу аудиту:	format(i2)
Загальна кількість проведених процедур третього етапу аудиту:	format(i3)
Загальна кількість проведених процедур четверого етапу аудиту:	format(i4)

Таким чином, за результатами моделювання із 282 заявок, що надійшли на вхід, на проведення аудиту інформаційної системи підприємства на виході отримано:

34 незадоволених заявок, зокрема з ініціативи самих замовників;

88 задоволених заявок, які розподілено так: проведено 12 процедур першого етапу аудиту, 41 - другого, 15 - третього і 20 процедур четвертого етапу аудиту, за заданої середньої тривалості 5, 7, 10 і 8 днів виконання першого, другого, третього і четвертого етапів аудиту ІС відповідно;

138 заявок перебувають у процесі опрацювання.

У цьому випадку встановлено такі значення наявних ресурсів (днів): 9, 11, 15 і 14 відповідно для 1-го, 2-го, 3-го і 4-го етапів аудиту.

Далі скоротимо за допомогою бігунків кількість наявних ресурсів (але не менше за встановлене мінімальне значення) і визначимо для них такі

значення: 8, 7, 11 і 9 днів відповідно для 1-го, 2-го, 3-го і 4-го етапів і проведемо чергову імітацію моделі з урахуванням внесення змін. При цьому слід пам'ятати, що середня кількість днів аудиту також зменшиться.

Таким чином, з 291 заявки, що надійшла на вхід, на проведення аудиту інформаційної системи підприємства на виході отримано:

29 незадоволених заявок, зокрема з ініціативи самих замовників;

110 задоволених заявок, які розподілено так: проведено 18 процедур першого етапу аудиту, 50 - другого, 14 - третього і 28 процедур четвертого етапу аудиту, за заданої середньої тривалості 5, 7, 10 і 8 днів виконання першого, другого, третього і четвертого етапів аудиту ІС відповідно;

152 заявки перебувають у процесі опрацювання.

Далі скоротимо за допомогою бігунків кількість наявних ресурсів (але не менше встановленого мінімального значення) і визначимо для них такі значення: 6, 5, 9 і 7 днів відповідно для 1-го, 2-го, 3-го і 4-го етапів і проведемо чергову імітацію моделі з урахуванням внесення змін. При цьому слід пам'ятати, що середня кількість днів аудиту також зменшиться.

Таким чином, із 318 заявок, що надійшли на вхід, на проведення аудиту інформаційної системи підприємства на виході отримано:

33 незадоволених заявок, зокрема з ініціативи самих замовників;

137 задоволених заявок, які розподілено так: проведено 19 процедур першого етапу аудиту, 66 - другого, 22 - третього і 30 процедур четвертого етапу аудиту, за заданої середньої тривалості 4, 5, 8 і 6 днів виконання першого, другого, третього і четвертого етапів аудиту ІС відповідно;

115 заявок перебувають у процесі опрацювання.

Отже, бачимо, що скорочення максимальної кількості днів проведення кожного з етапів аудиту призвели до того, що збільшилася кількість оброблених заявок за рахунок зменшення показника середньої тривалості виконання кожного з етапів аудиту. Ці дані будуть використовуватися

компанією-аудитором для ефективного ресурсу розподілу, якими вона володіє.

3.3 Система підтримки прийняття рішення компанією-аудитором про доцільність проведення процесу аудиту інформаційної системи підприємства

Системи підтримки прийняття рішень виникли на початку 70-х років XX століття завдяки подальшому розвитку управлінських інформаційних систем. Досі немає єдиного визначення СППР. Наприклад, під СППР розуміють "інтерактивну прикладну систему, що забезпечує кінцевим користувачам, які ухвалюють рішення, легкий і зручний доступ до даних і моделей з метою ухвалення рішень у напівструктурованих і неструктурованих ситуаціях у різноманітних галузях людської діяльності". Відомі й інші визначення, зокрема: "СППР - це такі системи, що ґрунтуються на використанні моделей і процедур з опрацювання даних і думок, які допомагають керівнику ухвалювати рішення", "СППР - інтерактивні автоматизовані системи, що допомагають особам, які ухвалюють рішення, використовувати дані та моделі для розв'язання неструктурованих і слабкоструктурованих проблем", "СППР - комп'ютерна інформаційна система, яка використовується для підтримки різних видів діяльності під час ухвалення рішень у ситуаціях, коли неможливе і Нарешті, існує твердження, згідно з яким СППР являє собою специфічний і добре описуваний тип систем на базі персональних комп'ютерів. Таке розмаїття визначень систем підтримки ухвалення рішень спричинене широким діапазоном різних форм і типів СППР [57].

Розглянемо загальний процес ухвалення рішень, який складається з трьох етапів [53]:

фаза аналізу проблеми та визначення цілей ухвалення рішення;

фаза проектування або визначення альтернативних шляхів розв'язання задачі ухвалення рішення;

фаза вибору найбільш прийнятного рішення.

На етапі аналізу проблеми та визначення цілей ухвалення рішення проводять всебічний аналіз проблеми, щодо якої треба ухвалити рішення, збирають дані та відповідні знання, що стосуються проблеми. Також на цій фазі вирішуються організаційні питання щодо створення СППР.

На фазі проектування або визначення шляхів альтернативних рішень формулюються альтернативні шляхи досягнення мети, проводиться їхній аналіз залежно від прийняття того чи іншого рішення. З'ясовується необхідність отримання додаткових знань і даних про проблему, що може спричинити повернення до першого етапу (аналізу). Особа, яка ухвалює рішення (ОПР), формулює і підраховує кілька альтернативних дій та обмірковує можливий результат від реалізації кожної з них. Оцінюється кінцевий результат.

На фазі вибору рішення обирається найкраща за деяким критерієм альтернатива. Крім цього, на цій фазі формують бази даних і знань, моделюють процес, щодо якого ухвалюють рішення, розробляють зручні форми представлення результатів.

Загалом три фази прийняття рішення можна представити так, як показано на рис. 3.6 [53].

Очевидно, що реалізація фаз у часі може перетинатися, наприклад, аналіз проблеми та збір відомостей може тривати на всіх трьох етапах. Фазу визначення альтернативних шляхів розв'язання задачі (тобто проектування) можна розпочати до завершення першої, оскільки перша може затягнутися. Те саме стосується фази вибору. При цьому на всіх етапах передбачається активне використання комп'ютера [53]:

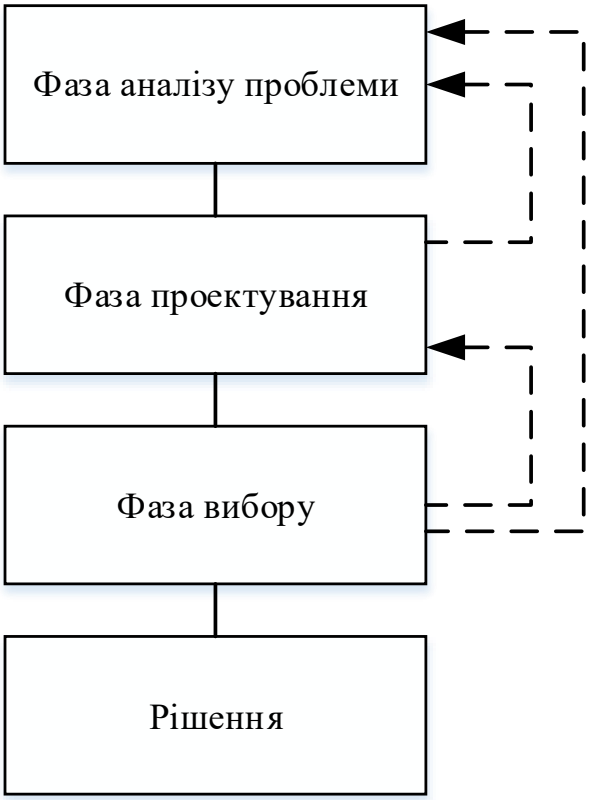

Рисунок 3.6 - Фази прийняття рішень

- формування бази даних і знань;
- моделювання процесу, щодо якого ухвалюють рішення;
- обчислення оптимальних, раціональних та інших вхідних впливів, необхідних для розв'язання задачі;
- аналіз варіантів вирішення завдання.

Інструментом ефективного прийняття рішення щодо доцільності проведення процесу аудиту інформаційної системи підприємства компанією-аудитором є система підтримки прийняття рішення. Отже, перейдемо до створення системи підтримки прийняття рішення компанією-аудитором щодо доцільності задоволення заявки на проведення аудиту інформаційної системи підприємства. Мета створення цієї СППР полягає в розробленні системи, яка давала б змогу компанії-аудиторові ухвалювати ефективні рішення щодо того,

чи вигідним буде задовольнити заявку, що надійшла від клієнта, на проведення аудиту інформаційної системи підприємства в рамках відповідності цілям функціонування компанії-аудитора.

Шаблон схеми структури структури системи підтримки прийняття рішень процесу проведення аудиту інформаційної системи підприємства подано на рис. 3.7.

Розглянемо принцип функціонування цієї системи. Підприємство-замовник послуги аудиту інформаційної системи підприємства, перебуваючи в проблемному полі, генерує інтегруючу мету і надсилає заявку (запит) на проведення аудиту компанії, що буде її (його) обробляти.

На цю заявку реагують фахівці відділу IT-консалтингу компанії-аудитора, до якої надійшов запит, і перенаправляють її ОПР.

Особою, яка приймає рішення, є начальник відділу IT-консалтингу.

Компанія-аудитор володіє певним набором характеристик: цілями і завданнями функціонування, певним набором ресурсів, моделлю функціонування, плануванням, які входять до блоку "Характеристики компанії-аудитора".

Компанії-аудитор націлена насамперед на отримання прибутку у сфері послуг із постійним зростанням рівня його значення, потім на розвиток бізнесу та підвищення рівня керівництва, а також на благопристойну суспільну репутацію. Однак для досягнення сформульованих цілей необхідно реалізувати низку завдань:

– надання швидких і якісних консалтингових послуг (якщо припускати, що компанія-аудитор надає один вид послуги консалтингу - у сфері IT-консалтингу, то завданням функціонування є дієва допомога з аналізу проблем функціонування інформаційних систем клієнта з подальшим знаходженням найефективніших способів, що забезпечують оптимальне використання часових і матеріальних ресурсів);

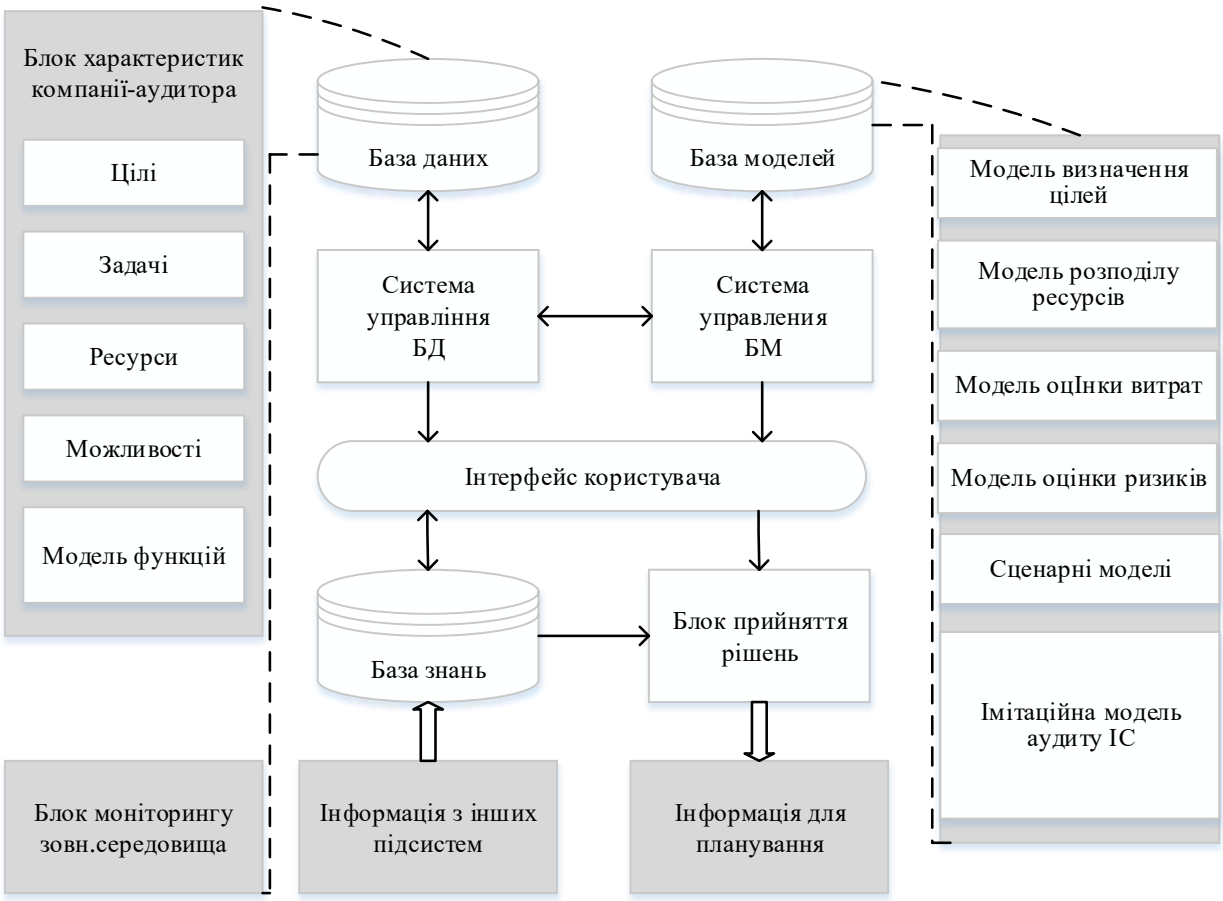

Рисунок 3.7 - Шаблон схеми структури системи підтримки ухвалення рішень компанією-аудитором щодо доцільності проведення процесу аудиту інформаційної системи підприємства

- підвищення якості послуг;
- скорочення витрат;
- підвищення кваліфікації співробітників;
- оцінка вимог клієнта та їх задоволення;
- збереження клієнтської бази та залучення нових клієнтів тощо.

Досягнення основної мети діяльності компанії можливе тільки на основі планування, спрямованого на забезпечення комплексності, збалансованості та взаємозв'язку всіх його елементів. На основі системи планів, створених компанією, надалі здійснюються організація запланованих робіт.

Реалізація завдань і тим самим досягнення поставлених цілей передбачає використання компанією тих чи інших ресурсів. До ресурсів компанії належать категорії ресурсів:

матеріально-речові, які представлені в предметній формі, в доступних для огляду образах (інформація, капітал тощо);

трудові (людські) ресурси, які мають особистісний характер, що виявляється у здатності до дій і не супроводжується втіленням у будь-якому речовому образі;

У розробленій моделі СППР акцентується увага на трудових ресурсах, конкретно - на фахівцях IT-відділу, які проводять аудит інформаційної системи підприємства та фінансових.

Модель функціонування для цієї конкретної СППР має два результати: задовольняти цю заявку, а саме проводити процес аудиту, або відмовляти в задоволенні цієї заявки.

Однією з найважливіших складових для успішного розвитку бізнесу, безумовно, є його здатність своєчасно реагувати на ризики і можливості, що з'являються. Причому частину ризиків і можливостей можна спрогнозувати заздалегідь за ледь помітними сигналами, іншу ж їхню частину можна лише констатувати постфактум і постаратися мінімізувати збитки або обернути собі на користь. Своєчасно - означає, що інформація про потенційні ризики і можливості повинна надійти до керівництва компанії за деякий час до настання тієї чи іншої події. У результаті чого у менеджменту компанії з'являється можливість відповідним чином підготуватися й успішно використати можливість, що з'являється, на благо свого бізнесу або ж звести нанівець можливий збиток у разі появи того чи іншого ризику. Для того, щоб усе вищесказане стало можливим, у компанії має функціонувати система моніторингу зовнішнього середовища, яка входить до блоку моніторингу зовнішнього середовища, спрямована на виявлення як ризиків, так і можливостей.

Підсистема інтерфейсу користувача призначена для здійснення зв'язку між користувачами СППР і внутрішніми елементами системи та забезпечує введення і виведення інформації для ЛПР.

Підсистема зберігання інформації складається з трьох підсистем: підсистеми даних (база даних і система управління базою даних), підсистеми моделей (база моделей і система управління базою моделей) і підсистеми знань (база знань), які призначені для накопичення даних і моделей.

Схему інформаційних потоків у разі застосування СППР на підприємстві подано на рис. 3.7. Стрілками показано напрямки руху інформації.

У базі даних міститься сукупність відомостей про замовників і клієнтів компанії-аудитора, інформацію про раніше проведений аудит. Ядром бази даних є модель даних, яка є структурою даних, угодами про способи їхнього представлення та операцій маніпулювання ними. У сучасній технології баз даних для створення баз даних, їх підтримки та обслуговування використовується спеціалізоване програмне забезпечення - системи управління базами даних. СУБД - це комплекс програмних і мовних засобів, необхідних для створення та експлуатації баз даних. Під час експлуатації баз даних СУБД забезпечує редагування структури бази даних, заповнення її даними, пошук, сортування, відбір даних за заданими критеріями, формування звітів.

База знань містить у собі інформацію накопиченого попереднього досвіду ухвалення рішення про доцільність проведення процесу аудиту інформаційної системи підприємства, а також інформацію, що надає допомогу в ухваленні цього рішення.

База моделей безпосередньо пов'язана з блоком "Характеристики компанії-аудитора" і включає такі моделі:

- модель цілепокладання;
- модель ефективного розподілу ресурсів;
- модель оцінки витрат;

- сценарні моделі розвитку подій;
- імітаційна модель проведення процесу аудиту інформаційної системи підприємства як окремий випадок сценарних моделей;
- моделі оцінки ризиків.

Отже, після отримання заявки компанією-аудитором, за допомогою системи управління базою даних, а також інформації з інших підсистем (підсистема документообігу, підсистема стратегічного управління, фінансово-економічна), на основі наявних методів і моделей, ЛПР ухвалює управлінське рішення щодо задоволення або відмови в задоволенні заявки на проведення процесу аудиту інформаційної системи підприємства-замовника. Тобто, блок ухвалення рішення в інтерпретації цієї моделі є алгоритмом, що обирає одне рішення з двох варіантів.

Результати цього рішення та планові показники входять до системи планування, яка надалі коригує майбутнє функціонування діяльності компанії-аудитора з урахуванням наявних змін.

Таким чином, упровадження системи підтримки ухвалення рішення може значно підвищити ефективність ухвалення рішення для управління бізнесом, що наразі стає одним із напрямів удосконалення діяльності підприємства загалом.

3.3 Висновки розділу

1. На основі конкретних статистичних даних Аудиторської палати України, а також різних компаній, що надають послугу аудиту інформаційних систем, проведено апробацію побудованої в другому розділі імітаційної моделі, результати якої можуть бути використані компанією-аудитором для ефективного розподілу часових і людських ресурсів, які вона має в своєму розпорядженні.

2. Для підвищення ефективності прийнятих рішень в управлінні бізнесом компанією-аудитором, було запропоновано СППР, що дає змогу отримати доступ до необхідної інформації та в оперативному порядку оцінити вплив прийнятих рішень на стан компанії в майбутніх періодах.

ВИСНОВКИ

Підвищення ефективності використання бюджету та зниження витрат на впровадження та експлуатацію сучасних інформаційних систем на підприємстві, а також аналіз перспектив їх модернізації є актуальними питаннями стратегії розвитку сучасного підприємства. Особливе значення процес аудиту інформаційних систем має для великих компаній з розвиненою мережею філій і підрозділів, які організовують і реалізують низку комплексних проєктів і детально планують свій план перспективного розвитку, тому що в цьому разі обсяг фінансових витрат на сучасну інформаційну інфраструктуру є доволі великим, і в разі помилково ухваленого рішення компанія може зазнати значних збитків, як матеріальних, так і тимчасових. Таким чином, компанії не можуть дозволити собі ухвалювати важливі рішення без застосування відповідного інструментарію, орієнтованого на планування змісту, часу, якості, вартості, відхилень, контрактів, персоналу, комунікацій тощо параметрів проєктів інформатизації на базі результатів аудиту інформаційних систем та програмного забезпечення.

Серед інструментів прийняття рішень за комплексністю, охопленням і складністю таким проєктам відповідає апарат моделювання. Побудова комплексу моделей і методів оптимального управління процесом аудиту інформаційних систем має відповідати структурі компанії. Проте навіть розв'язання окремих завдань у плануванні впровадження та оцінки експлуатації інформаційних систем уможливлюють отримання відчутного економічного ефекту, здобуття досвіду для їх використання в перспективі в комплексі математичного забезпечення таких систем та розробки відповідного програмного забезпечення.

Незважаючи на затребуваність моделей процесу проведення аудиту інформаційної системи підприємства в Україні ринок аудиту інформаційних систем перебуває в процесі становлення. Відсутність розвиненого

математичного інструментарію для розв'язання комплексних проблем цієї галузі й визначили напрям цього дослідження.

Для усунення зазначеного методичного провалу в роботі запропоновано комплекс моделей оптимізації діяльності. Комплекс моделей розв'язує проблеми процесного та імітаційного моделювання завдань аудиту інформаційної системи підприємства

У результаті дослідження в даній магістерській роботі було досягнуто поставленої науково-практичної мети моделювання процесу проведення аудиту інформаційної системи підприємства з використанням інструментів процесного та імітаційного моделювання, яка є актуальною для українських компаній. При цьому отримано такі наукові результати:

Запропоновано концепцію аудиту інформаційної системи підприємства.

Запропоновано процесну модель аудиту інформаційної системи підприємства, яка дає змогу зацікавленим фахівцям оцінити послідовність етапів аудиту та супутні їм витрати: матеріальні, часові та витрати людського капіталу.

На основі процесної розроблено імітаційну модель проведення аудиту інформаційної системи підприємства, що дає можливість спланувати безпосереднє проведення процесу аудиту інформаційної системи підприємства на основі наявних даних, тим самим підвищивши ймовірність досягнення максимального ефекту функціонування компанії-аудитора.

Запропоновано структуру системи підтримки ухвалення рішення компанією-аудитором щодо доцільності проведення процесу аудиту програмного забезпечення інформаційної системи підприємства, впровадження якої значно підвищить ефективність ухвалення рішення для управління бізнесом, що на теперішній час стає одним із напрямів удосконалення діяльності підприємства в цілому.

Перспективою подальших розробок досліджуваної теми є оцінка економічної та проєктної ефективностей на базі запропонованих моделей та

впровадження відповідної системи підтримки прийняття рішень на підприємствах IT сектору згідно запропонованого науково-методичного підходу, який було удосконалено на базі результатів імітаційного моделювання.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аглицький, І.А. Інформаційні технології і бізнес / І.А.Аглицький // Експерт автоматизації. - 2009. - №29. - С 75-80.

2. Шкарін М.М. Автоматизація аудиту інформаційної системи підприємства: автреф. дис. на здобуття наук. ступеня канд. ек. наук: спец. 08.03.02 / М.М. Шкарін Н. - Суми, 2011 - 20 с.

3. Дяченко О.М. Актуальність аудиту інформаційних систем зросла / О.М. Дяченко // Національний банківський журнал. - 2011. - №3.

4. Інтернет-портал "Тренінги в Україні" [Електронний ресурс] / Анненко О.А. ЄБРР порахував консультантів / О.А Анненко. - 2011. - Режим доступу: http://www.training.com.ua/live/news/ebrr_poschital_konsultantov

5. Інформаційний Бюлетень "Ділові консультаційні послуги" [Електронний ресурс] / Огляд ринку консалтингових послуг України // EBRD-Business Advisory Services Newsletter - 2011. - №4. - Режим доступу:
http://www.inwent.org.ua/ebrd_sbs/BAS%20Newsletter%20N1.pdf

6. Програма Ділових Консультацій Європейського банку реконструкції та розвитку [Електронний ресурс] / Ринок консультаційних послуг в Україні // Оцінки ІКГ "Астарта-Таніт". - 2011. - №11. - Режим доступу: http://www.astarta.com.ua/assets/files/101115%20consulting.pdf

7. Агєєв М. Чи зросте попит на IT-консалтинг? / М. Агєєв // Комп'ютерний Огляд. - 2008. - №49 (666). - С. 40-41.

8. Шевчук О. О. Аудит в Україні - проблеми та перспективи розвитку / О.О. Шевчук, Н.Г. Здирко // Збірник наукових праць кафедри економічного аналізу Тернопільського національного економічного університету. - 2010. - №6. - С. 530-531.

9. Драч В. І. Наступний крок: забезпечення якості аудиторських послуг / В. І. Драч // Аудитор України. - 2009. - №5/6. - С. 60-61.

10. Шульман М. К. Проблеми практичної реалізації принципу незалежності в діяльності аудитора / М. К. Шульман // Аудитор України. - 2007. - №14. - С. 23-25.

11. Мишко С.П. Обсяг українського ІТ-ринку в 2013 році - $3,6 млрд / С.П. Мишко // Forbes Україна. - 2012. - №12. - С. 12-15.

12. Прес-центр компанії FTL [Електронний ресурс] / Експерти констатують зростання обсягу ІТ-послуг в Україні. - 2012. - Режим доступу: http://ftl.com.ua/ekspertyi-konstatiruyut-rost-obema-it-uslug-v-ukraine.html

13. Ганієва Е.Ш. Проблеми та перспективи проведення аудиту інформаційної безпеки підприємства [Електронний ресурс] / Е.Ш. Ганієва // Вісник Бердянського університету менеджменту та бізнесу. - 2011. - №1 (13). - Режим доступу: http://pk.napks.edu.ua/library/compilations_vak/nvfbi/2009/2/p_41_43.pdf

14. Чайковська М.П. Актуальні аспекти ІТ-ринку України / М.П. Чайковська // Економічні інновації. - 2007. - №27- С. 316 - 325.

15. Несторенко І.І. Насамперед ми хочемо вдосконалити нормативну базу, що регулює аудиторську діяльність / І.І. Нестеренко // Аудитор України. Нестеренко // Аудитор України. - 2010. - № 2. - С. 20-22.

16. Аналітичний портал ринку веб-розробок [Електронний ресурс] / Єжиков А. Аудит сайту: користь чи фікція? / А. Єжиков. - 2013. - №3.

17. Кащена Н.Б. Цифрові інновації як драйвер модернізації системи інформаційного сервісу бізнес-адміністрування // Збірник матеріалів VIII Міжнародної науково-практичної конференції; 08 грудня 2022 року — К.: КНЕУ, 2022. – с.273-274.

18. Інформаційні системи і технології: додатки в економіці та управлінні: Навчальний посібник / [Ю.Г. Лисенко, В.Н. Андрієнко, Т.С. Шаталова та ін.]; за ред. проф. Ю.Г. Лисенко. - Донецьк: ТОВ "Юго-Восток, Лтд", 2004. - Книга 6. - 377 с.

19. Жуков А.А. Технологія аудиту банківських інформаційних систем / А.А. Жуков, Н.В. Третяк // Прикладна інформатика. - 2006. - №1. - С. 18-25.

20. Аудит: Навч. Посібник / Л.М. Полякова, М.В. Корягін, В.І. Воськало, В.М. Чубай. Воськало, В.М. Чубай. - Серія "Дистанційне навчання". - №21. - Львів: Видавництво Національного університету "Львівська політехніка", 2004. - 248 с.

21. Облік, аналіз, аудит, оподаткування та фінансовий моніторинг в умовах глобалізаційних змін [Електронний ресурс]: Збірник матеріалів VIII Міжнародної науково-практичної конференції; 08 грудня 2022 року — К.: КНЕУ, 2022. — 305 с.

ISBN 978-966-926-426-8

22. Огнєва А. М. Аудит інформаційних систем і технологій / А.М. Огнєва // Вісник Хмельницького національного університету. - 2009. - № 6. - С. 229-232.

23. Лазарева С.Ф. Сучасні методи аудиту інформаційних технологій [Електронний ресурс] / С.Ф. Лазарева // Бібліотечний вісник Вернадського. - 2010. - №3. - Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Dtr_ep/2011_4/files/EC411_06.pdf

24. Janet L. Colbert. Порівняння внутрішніх контролів: COBIT, ITIL і COSO [Електронний ресурс] / Колберт Джанет Л., Брауен Пол Л. // IS Audit and Control Journal. - 2007. - № IV

25. Офіційний веб-сайт Асоціації Аудиту та Контролю Інформаційних Систем [Електронний ресурс]. - Режим доступу: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

26. Баранова О.В. Методологічні підходи до аудиту інформаційних систем / О.В. Баранова // Аудит і фінансовий аналіз. - 2009. - №3. - с. 1-9.

27. Закалінська К.О. Оцінка ринку засобів автоматизації аудиторської діяльності [Електронний ресурс] / К.О. Закалінська // Бібліотечний вісник Вернадського. - 2011. - №4. - Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Vdnuet/econ/2009 _4/26.pdf

28. Cobit Mapping: огляд міжнародних IT-настанов, 2nd видання. - США, IT Governance Institute. - 2006.

29. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів : ДСТУ 4163-2003. – (Національний стандарт України).

30. Legezo D. Третій приходить. ITIL v. 3 / D. Legezo // Intelligent enterprise. - 2008. - № 2. - P. 12-15

31. Баранова О.В. Аудит інформаційних систем / О.В. Баранова // "Вісник Фінансової Академії". - 2009. - № 1. - С.25-32.

32. Економіка та управління якістю: облік, аналіз, методи, моделі, інструменти та аудит: (Зб. наук. ст.) За заг. ред. О.В. Баранова // Аудит інформаційних систем в умовах комп'ютерної обробки даних. - Тамбов: ТДТУ, 2008. - №3. - 65 с.

33. Подольський В.І. Комп'ютерний аудит / В.І. Подольський, Н.С. Щербакова, В.Л. Комісаров - М.: ЮНИТИ-ДАНА, 2004. - 176 с.

34. IT Methods Students Note // INTOSAI. - 2007. - 97 p.

35. Рудницький В.С. Методологія та організація аудиту / В.С. Рудницький. - Т.: Економічна думка, 1998. - 196 с.

36. Володіна, О. Аудит інформаційної системи / О. Володіна // Кабельник. - 2007. - № 9. - С.42-59.

37. IT-стандарти, керівні принципи, а також інструменти та методики для професіоналів у сфері аудиту, а також забезпечення та контролю // ISACA, 2010. 330 p.

38. Tommie Singleton. Модель COSO: як IT-аудитори можуть використовувати її для оцінки ефективності внутрішнього контролю

(Частина 1, Частина 2) // Journal of Information Systems Control Journal, ISACA, 2007-2008. - P. 5.

39. Міжнародний стандарт аудиту 401 -Аудит в середовищі комп'ютерних інформаційних систем // IFAC, 2004. - 6 p.

40. Офіційний веб-сайт Аудиторської палати України [Електронний ресурс]. - Режим доступу: http://www.apu.com.ua/content.php?lang=ukr&c=page.php&id=17&lang=ukr

41. Офіційний веб-сайт компанія IT Dopomoga [Електронний ресурс]. - Режим доступу: http://it-dopomoga.com.ua/itconsulting.html

42. Ситник В.Ф. Системи підтримки ухвалення рішень / В.Ф. Ситник - К.: КНЕУ,2004. - 614 с.

43. The Worldwide Market for Self-paced eLearning Products and Services: 2010-2015 Forecast and Analysis [Електронний ресурс] / Sam S. Adkins // Ambient Insight Comprehensive Report. - 2011. - P. 17 - Режим доступу до джерела: www.ambientinsight.com

44. Державна уніфікована система документації. Формуляр-зразок. Вимоги до побудови : ДСТУ 3844-99. – (Національний стандарт України).

45. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення : ДСТУ 3008-95. – (Національний стандарт України).

46. Дроніков А. Закодированная торговля / А. Дроніков // Бізнес. – 1997. – № 14. – С. 60.

47. Інформаційні системи в менеджменті : підручник [для студ. вищ. навч. закл.] / В.П. Бондар, В.О. Новак, В.В. Матвєєв, Ю.Г. Симоненко. – К. : Каравела, 2008. – 616 с.

48. Інформаційні системи і технології в економіці : посібник [для студ. вищ. навч. закл.] / за ред. В.С. Пономаренка. – К. : Академія, 2002. – 544 с.

49. Bachmann, J., Ramanujam, R., & Sengupta, S. (2023). Information Systems Audit: Integrating Best Practices and Emerging Trends. Journal of Information Technology Management [Електронний ресурс]. - Режим доступу: - https://www.researchgate.net/publication/361025642_Emerging_technology_and_auditing_practice_analysis_for_future_directions.

50. ISACA. (2022). COBIT 2019 Framework: Governance and Management of Enterprise IT. Information Systems Audit and Control Association [Електронний ресурс]. - Режим доступу: https://www.isaca.org/resources/cobit/cobit-5.

51. ISO/IEC 27001:2022. Information Security Management. International Organization for Standardization [Електронний ресурс]. – Режим доступу: https://www.iso.org/publication/PUB100484.html.

52. Singleton, T., & Stroud, K. (2021). Auditing Information Systems: A Comprehensive Approach. IT Governance Publishing [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/352006721_IT_Governance_and_Information_Security_Guides_Standards_and_Maturity_Frameworks

53. Micheli, M., & Boffey, R. (2023). Risk Management in IT Audits: Practical Guide for Auditors. Springer [Електронний ресурс]. – Режим доступу: https://audit.scot/uploads/docs/um/risk_management_framework_24-26.pdf

54. National Institute of Standards and Technology (NIST). (2022). Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. NIST [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

55. IT Governance Institute. (2023). Implementing IT Governance: Aligning Business and IT with COBIT. Van Haren Publishing [Електронний ресурс].

– Режим доступу: https://www.researchgate.net/publication/255568541_Designing_a_New_Integrated_IT_Governance_and_IT_Management_Framework_Based_on_Both_Scientific_and_Practitioner_Viewpoint

56. Rezvani, S., & Zadeh, M. (2022). Simulation Models for Efficient IT Auditing. Journal of Simulation and Analysis [Електронний ресурс]. – Режим доступу: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/trust/documents/ey-2022-global-audit-quality-report.pdf

57. Yoo, D., & Song, J. (2023). Digital Transformation and Information Systems Audit: Challenges and Solutions. Journal of Enterprise Information Management [Електронний ресурс]. – Режим доступу: https://ideas.repec.org/s/eee/ijoais.html