МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Н. Г. Сейсебаєва

ВНУТРІШНІЙ КОНТРОЛЬ НА ПІДПРИЄМСТВІ ТА БЕЗПЕКА БІЗНЕСУ



Курс лекцій
для здобувачів ступеня вищої освіти магістра
спеціальності 071 «Облік і оподаткування»
освітньо-професійної програми «Облік і аудит»

Затверджено
вченою радою ЗНУ
Протокол № 5 від 26.11.2024

Запоріжжя

2024

УДК 657.633+334.722:338.246](075.8)
С288

Сейсебаєва Н. Г. Внутрішній контроль на підприємстві та безпека бізнесу : курс лекцій для здобувачів ступеня вищої освіти магістра спеціальності 071 «Облік і оподаткування» освітньо-професійної програми «Облік і аудит». Запоріжжя : Запорізький національний університет, 2024. 65 с.

У виданні подано повний виклад лекцій навчальної дисципліни «Внутрішній контроль на підприємстві та безпека бізнесу». Програмний матеріал розкрито всебічно й системно, унаочнено його рисунками, схемами, таблицями.

Увагу акцентовано на актуальних питаннях внутрішнього контролю та безпеки бізнесу з урахуванням нормативно-правового забезпечення та відповідності міжнародним нормам та стандартам, ведення бізнесу в умовах цифровізації обліково-аналітичних процесів на підприємствах та впровадження інноваційних інформаційних технологій.

Для здобувачів ступеня вищої освіти магістра спеціальності 071 «Облік і оподаткування», які навчаються за освітньо-професійною програмою «Облік і аудит».

Рецензент

Т. І. Батракова, кандидат економ. наук, доцент кафедри фінансів, банківської справи, страхування та фондового ринку

Відповідальний за випуск

Н. М. Проскуріна, доктор економ. наук, професор, завідувач кафедрою обліку та оподатковування

ЗМІСТ

ВСТУП..... 4

Змістовий модуль 1 Теоретичні засади внутрішнього контролю та безпеки бізнесу..... 6
Тема 1. Сутність, функції та принципи внутрішнього контролю та безпеки бізнесу..... 6
Тема 2. Предмет та методи внутрішнього контролю та безпеки бізнесу..... 14

Змістовий модуль 2 Організаційне забезпечення внутрішнього контролю на підприємстві та безпеки бізнесу..... 19
Тема 3. Суб'єкти внутрішнього контролю та безпеки бізнесу й їх функції..... 19
Тема 4. Загальні аспекти організації контрольної роботи на підприємстві..... 30

Змістовий модуль 3 Методичне забезпечення внутрішнього контролю та безпеки бізнесу..... 40
Тема 5. Види методичного забезпечення внутрішнього контролю та безпеки бізнесу..... 40

Змістовий модуль 4 Організаційне та методичне забезпечення внутрішнього контролю на підприємстві та безпеки бізнесу на міжнародному рівні..... 46
Тема 6. Міжнародні стандарти внутрішнього контролю та безпеки бізнесу як організаційне та методичне забезпечення контролю та безпеки на міжнародному рівні..... 46
Тема 7. Аналіз міжнародних стандартів внутрішнього контролю та безпеки бізнесу..... 51
Рекомендована література..... 63
Використана література..... 64

ВСТУП

Курс «Внутрішній контроль на підприємстві та безпека бізнесу» належить до циклу дисциплін вільного вибору студента в межах спеціальності. *Предметом його вивчення* є внутрішній контроль та безпека бізнесу, а також взаємозв'язок між ними, а *об'єктом* – є система внутрішнього контролю та безпеки бізнесу на підприємстві.

Метою вивчення навчальної дисципліни «Внутрішній контроль на підприємстві та безпека бізнесу» є формування системи знань з організації та методики внутрішнього контролю та безпеки бізнесу на підприємстві.

Основними завданнями вивчення дисципліни «Внутрішній контроль на підприємстві та безпека бізнесу» є:

– засвоєння теоретичних основ внутрішнього контролю та безпеки бізнесу як невід'ємної функції управління;

– засвоєння теоретичних основ функціювання служби внутрішнього контролю та безпеки бізнесу;

– вивчення та засвоєння законодавчих та нормативних актів України, міжнародного досвіду та спеціальної літератури щодо організації та функціювання системи внутрішнього контролю та безпеки бізнесу;

– ознайомлення з методикою та технікою проведення контрольних процедур на підприємствах, установах та організаціях;

– набуття практичних навичок з організації та виконання комплексу внутрішньо контрольних процедур та реалізації їх наслідків.

У результаті вивчення навчальної дисципліни студент повинен набути таких результатів навчання (знання, уміння тощо) та компетентностей:

загальні компетентності:

– здатність вчитися та бути готовим до засвоєння та застосування набутих знань;

– здатність до абстрактного мислення, аналізу та синтезу як інструментарію виявлення проблем та прийняття рішень для їх розв'язання на основі логічних аргументів та перевірених фактів;

– здатність працювати самостійно та в команді з урахуванням вимог професійної дисципліни, планування та управління часом;

– здатність працювати автономно;

– знання та розуміння предметної області та розуміння професійної діяльності;

– здатність спілкуватися державною мовою як усно, так і письмово;

спеціальні компетентності:

– здатність досліджувати тенденції розвитку економіки за допомогою інструментарію макро- та мікроекономічного аналізу, робити узагальнення стосовно оцінки прояву окремих явищ, які властиві сучасним процесам в економіці.

– здатність використовувати математичний інструментарій для дослідження економічних процесів, розв'язання прикладних економічних та

оптимізаційних завдань у сфері обліку, аналізу, контролю, аудиту та оподаткування;

– здатність обґрунтовувати методологію та методику облікової політики підприємства та процедури її вибору, складати розпорядчі документи щодо організації обліку на підприємствах;

– здатність проводити аналіз господарської діяльності підприємства з метою прийняття управлінських рішень;

– здатність здійснення облікових процедур із застосуванням спеціалізованих інформаційних систем і комп'ютерних технологій;

програмні результати навчання:

– демонструвати базові знання та розуміння економічних категорій, законів, причинно-наслідкових та функціональних зв'язків, які існують між процесами та явищами на різних рівнях економічних систем.

– розуміти місце і значення облікової, аналітичної, контрольної, податкової та статистичної систем в інформаційному забезпеченні користувачів обліково-аналітичної інформації у розв'язанні проблем у сфері соціальної, економічної та екологічної відповідальності підприємств, установ, організацій.

– усвідомлювати сутність об'єктів обліку, аналізу, контролю, аудиту, оподаткування та розуміти їх роль і місце в господарській діяльності.

– формувати й аналізувати фінансову, управлінську, податкову і статистичну звітність підприємств та правильно інтерпретувати отриману інформацію для прийняття управлінських рішень.

Відповідно до структурно-логічної схеми освітньо-професійної програми «Облік і аудит» курс «Внутрішній контроль на підприємстві та безпека бізнесу» тематично пов'язаний з дисциплінами «Бухгалтерський облік в управлінні підприємством», «Організація облікового процесу на підприємстві», «Організація і методика аудиту», «Контролінг».

Важливе місце у структурі курсу «Внутрішній контроль на підприємстві та безпека бізнесу» відведено лекційним заняттям. Лекція є основним засобом передачі, сприймання та засвоєння навчальної інформації та ключових положень дисципліни. Навчальний матеріал курсу, передбачений програмою для засвоєння в процесі лекційних занять, виноситься на підсумковий контроль.

Лекційний курс передбачає послідовне засвоєння: сутності, функцій та принципів внутрішнього контролю та безпеки бізнесу, предмету та методів внутрішнього контролю та безпеки бізнесу, поняття суб'єктів внутрішнього контролю та їх функцій, міжнародних стандартів внутрішнього контролю та безпеки бізнесу, як організаційного та методичного забезпечення контролю на міжнародному рівні.

Наведений у навчально-методичному виданні матеріал може бути корисний здобувачам ступеня вищої освіти магістра освітньо-професійних програм «Фінанси та кредит», «Економічна кібернетика» у подальшій професійній діяльності та викладачам економічних дисциплін.

ЗМІСТОВИЙ МОДУЛЬ 1
ТЕОРЕТИЧНІ ЗАСАДИ ВНУТРІШНЬОГО КОНТРОЛЮ ТА БЕЗПЕКИ БІЗНЕСУ

Тема 1. Сутність, функції та принципи внутрішнього контролю та безпеки бізнесу

Мета вивчення теми: сформувати чітке розуміння сутності внутрішнього контролю, визначити функції внутрішнього контролю ознайомитися з основними принципами внутрішнього контролю, зрозуміти взаємозв'язок між внутрішнім контролем та безпекою бізнесу, розвинути навички аналізу та оцінки ризиків, сформувати вміння розробляти ефективні системи внутрішнього контролю.

План

1.1 Внутрішній контроль в системі економічного контролю. Виклики сучасних систем внутрішнього контролю та шляхи їх подолання.

1.2 Суть, завдання, функції та принципи внутрішнього контролю та безпеки бізнесу.

1.3 Види та форми внутрішнього контролю та безпеки бізнесу.

Основні терміни та поняття: *внутрішній контроль, економічний контроль, безпека бізнесу, ризики, фінансова звітність, ефективність, дотримання законодавства, інформаційні технології, штучний інтелект, блокчейн, людський фактор, фінансова звітність, ефективність, дотримання законодавства*



1.1 Внутрішній контроль в системі економічного контролю. Виклики сучасних систем внутрішнього контролю та шляхи їх подолання.

Внутрішній контроль – це неодмінна складова сучасного бізнесу, яка забезпечує його ефективність, стабільність та безпеку. Це система заходів, процедур і методів, спрямованих на досягнення цілей організації шляхом виявлення і запобігання ризикам, забезпечення правдивості фінансової звітності, захисту активів та дотримання законодавства.

В системі економічного контролю внутрішній контроль відіграє одну з ключових ролей. Він дозволяє:

– ідентифікувати та оцінювати ризики: виявити потенційні загрози, які можуть негативно вплинути на діяльність підприємства, такі як шахрайство, помилки, неефективність процесів тощо.

– забезпечити правдивість фінансової звітності: гарантувати, що фінансова інформація зображає реальний стан справ на підприємстві.

– захистити активи: зменшити ризики втрати або неправомірного використання активів підприємства.

– дотримання законодавства: забезпечити дотримання всіх вимог чинного законодавства.

– поліпшити ефективність бізнес-процесів: виявити неефективні процеси та запровадити заходи для їх оптимізації.

Елементами системи внутрішнього контролю є:

– контрольне середовище: культура організації, етичні стандарти, рівень компетентності персоналу,

– оцінка ризиків: ідентифікація, аналіз та оцінка ризиків,

– контрольні заходи: процедури та дії, спрямовані на зменшення ризиків,

– інформація та комунікація: збір, аналіз та поширення інформації, необхідної для ефективного функціювання системи внутрішнього контролю,

– моніторинг: регулярна оцінка ефективності системи внутрішнього контролю та внесення необхідних змін.

Ефективна система внутрішнього контролю є одним з найважливіших елементів забезпечення безпеки бізнесу. Вона дозволяє:

– зменшити ризики фінансових втрат: запобігання шахрайству, розкраданню, помилкам у бухгалтерському обліку,

– захистити репутацію компанії: уникнення скандалів, пов’язаних з фінансовими махінаціями або порушеннями законодавства,

– забезпечити довіру інвесторів та кредиторів: надання правдивої фінансової інформації,

– поліпшити конкурентоспроможність: завдяки ефективному управлінню ризиками та оптимізації процесів.

Внутрішній контроль відіграє важливу роль у забезпеченні економічної безпеки бізнесу. Це не просто набір формальних процедур, а комплекс заходів, спрямованих на досягнення стратегічних цілей організації. Ефективна система внутрішнього контролю дозволяє підприємствам працювати більш стабільно, ефективно та безпечно.

Сучасні системи внутрішнього контролю стикаються з низкою викликів, які викликані швидкими змінами технологічного середовища, глобалізацією бізнесу та зростанням кіберзагроз. Розглянемо детальніше ці виклики та шляхи їх подолання.

Основні виклики систем внутрішнього контролю:

– швидкі зміни технологічного середовища: поява нових технологій, таких як штучний інтелект, блокчейн та хмарні обчислення, створює як нові можливості, так і нові ризики для систем внутрішнього контролю,

– глобалізація бізнесу: робота в різних юрисдикціях з різними нормативними вимогами ускладнює управління ризиками та забезпечення єдиного підходу до внутрішнього контролю,

– зростання кіберзагроз: кібератаки становлять серйозну загрозу для конфіденційності, цілісності та доступності інформації, що ускладнює забезпечення безпеки даних,

– регуляторні зміни: постійні зміни законодавства та нормативних вимог потребують оперативного адаптування систем внутрішнього контролю,

– складність бізнес-процесів: зростання масштабів бізнесу та ускладнення його структури ускладнюють контроль за всіма процесами,

– дефіцит кваліфікованих кадрів: нестача спеціалістів у сфері внутрішнього контролю може негативно вплинути на ефективність системи.

Інформаційні технології надають нові можливості для розвитку систем внутрішнього контролю, при цьому відбувається:

– автоматизація рутинних операцій, що зменшує ризик людської помилки та підвищує ефективність контролю,

– аналіз великих даних, який дозволяє виявляти тенденції та аномалії, які важко помітити при ручному аналізі,

– забезпечення доступу до інформації в режимі реального часу, що покращує оперативність прийняття рішень,

– посилення кібербезпеки забезпечує захист інформаційних систем від зовнішніх загроз.

Однак, *інформаційні технології* також створюють нові ризики, такі як кібератаки та залежність від IT-інфраструктури.

Штучний інтелект (ШІ) революціонізує багато галузей, і внутрішній контроль не є винятком. Його впровадження відкриває нові можливості для підвищення ефективності та точності систем контролю: ШІ може автоматизувати велику частину рутинних завдань, таких як звірка даних, аналіз транзакцій та виявлення аномалій. Це звільняє час співробітників для більш стратегічних завдань. За допомогою алгоритмів машинного навчання ШІ може аналізувати великі обсяги даних і прогнозувати потенційні ризики, що дозволяє приймати проактивні заходи. ШІ може автоматизувати багато процедур аудиту, підвищуючи його ефективність та точність та дозволяє адаптувати систему контролю до конкретних потреб кожного підрозділу або процесу.

Блокчейн – це розподілена база даних, яка забезпечує високий рівень безпеки та прозорості. Його застосування в системах внутрішнього контролю має такі переваги: інформація, записана в блокчейн, є практично незмінною, що ускладнює її підробку, всі транзакції в блокчейні є публічними, що забезпечує високий рівень прозорості, відсутність єдиного центру контролю робить блокчейн стійким до хакерських атак.

Застосування блокчейну дозволяє:

– забезпечити цілісність фінансових даних, бо кожна транзакція реєструється в блокчейні, що унеможливлює маніпуляції з даними,

– спростити процес аудиту, тому, що завдяки прозорості даних аудит стає більш ефективним,

– блокчейн дозволяє захистити авторські права на інтелектуальну власність.

Кібербезпека є одним з найважливіших аспектів внутрішнього контролю. Зростання кібератак вимагає від організацій вживати заходів для захисту своїх інформаційних систем шляхом впровадження заходів для захисту конфіденційності, цілісності та доступності інформації. створення систем для виявлення кібератак та швидкого реагування на них.проведення регулярних тренінгів для підвищення обізнаності співробітників про кіберзагрози.

Для досягнення максимальної ефективності необхідно інтегрувати ШІ, блокчейн і кібербезпеку в єдину систему внутрішнього контролю. Це дозволить:

– автоматизувати процеси контролю: ШІ може автоматизувати багато рутинних завдань, а блокчейн забезпечить безпеку даних,

– покращити виявлення аномалій: комбінація ШІ та аналізу блокчейну дозволить виявляти навіть найскладніші шахрайські схеми,

– забезпечити високий рівень довіри до даних: блокчейн забезпечить прозорість і незмінність даних, а ШІ допоможе виявити помилки та аномалії.

Штучний інтелект, блокчейн і кібербезпека є ключовими технологіями, які трансформують системи внутрішнього контролю. Їх інтеграція дозволяє підвищити ефективність, точність і безпеку контрольних процесів. Однак, для успішного впровадження цих технологій необхідно враховувати специфіку кожної організації та розробляти індивідуальні рішення.

Попри розвиток технологій, людський фактор залишається одним з найважливіших елементів системи внутрішнього контролю. Від компетентності та відповідальності співробітників залежить ефективність роботи всієї системи. Важливо забезпечити:

– високий рівень професіоналізму шляхом регулярного навчання та підвищення кваліфікації співробітників,

– свідоме ставлення до своїх обов’язків шляхом формування культури відповідальності та чесності,

– ефективну комунікацію задля забезпечення прозорого обміну інформацією між усіма учасниками процесу внутрішнього контролю.

Забезпечення ефективного внутрішнього контролю вимагає певних витрат. При цьому важливо досягти оптимального співвідношення між ефективністю системи та її вартістю. Для цього необхідно:

– оцінити ризики та приділяти більше уваги тим ризикам, які можуть завдати найбільшої шкоди бізнесу,

– використовувати ризикорієнтований підхід, сконцентрувати зусилля на контролі, який вже існує, та найбільш значущих ризиків,

– регулярно переглядати систему, оцінювати ефективність контрольних заходів та вносити необхідні зміни,

– використовувати технології, за допомогою яких проводити автоматизацію рутинних операцій, що дозволить зменшити витрати на персонал.

Системи внутрішнього контролю в сучасних умовах стикаються з рядом викликів, які вимагають постійного розвитку та адаптації. Для забезпечення ефективного функціювання систем внутрішнього контролю необхідно поєднувати людський фактор, інформаційні технології та ризикорієнтований підхід.

1.2 Суть, завдання, функції та принципи внутрішнього контролю та безпеки бізнесу.

Внутрішній контроль – це система заходів, процедур і методів, спрямованих на забезпечення досягнення цілей організації шляхом виявлення і запобігання ризикам, забезпечення правдивості фінансової звітності, захисту активів та дотримання законодавства.

Завданнями внутрішнього контролю є:

– забезпечення правдивості фінансової звітності шляхом гарантування того, що фінансова інформація зображає реальний стан справ на підприємстві,

– захист активів, шляхом зменшення ризиків втрати або неправомірного використання активів підприємства,

– дотримання законодавства шляхом забезпечення дотримання всіх вимог чинного законодавства,

– поліпшення ефективності бізнес-процесів шляхом виявлення неефективних процесів та запровадження заходів для їх оптимізації,

– запобігання шахрайству шляхом створення умов, які ускладнюють вчинення шахрайських дій.

Функції внутрішнього контролю:

– профілактична: запобігання виникненню негативних подій,
– контрольна: перевірка виконання встановлених правил і процедур,
– оцінна: оцінка ефективності системи управління ризиками,
– коригувальна: внесення змін до системи контролю з метою підвищення її ефективності.

Принципи внутрішнього контролю складаються з культури організації, етичних стандартів, рівня компетентності персоналу, ідентифікації, аналізу та оцінці ризиків, процедур та дій, спрямованих на зменшення ризиків, збору, аналізу та поширення інформації, необхідної для ефективного функціювання системи внутрішнього контролю та захисту бізнесу, регулярної оцінки ефективності системи внутрішнього контролю та захисту бізнесу й внесення необхідних змін.

Безпека бізнесу – це комплекс заходів, спрямованих на захист підприємства від різноманітних загроз, таких як: конкуренція, інфляція, кризи. кібератаки, збої в роботі обладнання. протести, страйки, тероризм, зміни законодавства, міжнародні конфлікти.

Внутрішній контроль є одним з основних інструментів забезпечення безпеки бізнесу. Він дозволяє:

– виявити слабкі місця в системі безпеки,
– створити систему захисту від можливих загроз,
– швидко реагувати на виникнення загроз і мінімізувати їхні наслідки.

Ефективна система внутрішнього контролю є основою для забезпечення безпеки бізнесу. Вона дозволяє виявити і усунути потенційні загрози, захистити активи підприємства та забезпечити його стабільну роботу.

Внутрішній контроль – це неодмінна частина сучасного бізнесу. Він дозволяє забезпечити досягнення цілей організації, захистити активи, підвищити ефективність роботи та забезпечити безпеку бізнесу.

1.4 Види та форми внутрішнього контролю та безпеки бізнесу

Тема внутрішнього контролю та безпеки бізнесу досить широка і містить в собі багато нюансів. Таблиця, яка пропонує інформацію, систематизує різні аспекти цієї теми.

Таблиця 1.1 – Види та форми внутрішнього контролю та безпеки бізнесу

Вид контролю/безпеки	Опис	Приклади
1	2	3
Внутрішній контроль	Систематичний процес, спрямований на забезпечення досягнення цілей організації шляхом виявлення і запобігання ризикам.	Фінансовий контроль, виробничий контроль, кадровий контроль, інформаційний контроль
Безпека бізнесу	Комплекс заходів, спрямованих на захист підприємства від різноманітних загроз.	Фізична безпека, інформаційна безпека, технологічна безпека, фінансова безпека
За об’єктом контролю	Виділяють контроль над різними сферами діяльності підприємства.	Фінансовий, виробничий, кадровий, інформаційний
За періодичністю	Визначається частота проведення контролю.	Постійний, періодичний, одноразовий
За способом проведення	Способи здійснення контролю.	Документальний, фактичний, комплексний
За суб’єктом контролю	Хто здійснює контроль.	Самоконтроль, взаємний контроль, спеціальний контроль
За методами контролю	Інструменти, які використовуються при контролі.	Аналітичний, експертний, статистичний
Форми внутрішнього контролю	Конкретні способи організації контролю.	Внутрішній аудит, ревізія, моніторинг, самооцінка
Аспекти безпеки бізнесу	Основні напрямки забезпечення безпеки.	Фізична безпека, інформаційна безпека, технологічна безпека, фінансова безпека

Детальніше про кожен вид та форму.

Таблиця 1.2 – Види та форми внутрішнього контролю та безпеки бізнесу

Вид/Форма	Опис	Приклади
1	2	3
Фінансовий контроль	Спрямований на забезпечення достовірності фінансової звітності, захист активів та дотримання фінансової дисципліни.	Перевірка касових операцій, банківських виписок, інвентаризація матеріальних цінностей, контроль за рухом грошових коштів, аналіз фінансових показників.
Виробничий контроль	Контролює якість продукції, ефективність виробничих процесів, використання ресурсів.	Контроль за дотриманням технологічних процесів, перевірка якості сировини та готової продукції, облік витрат матеріалів, енергії, праці.
Кадровий контроль	Спрямований на оцінку ефективності роботи персоналу, дотримання трудової дисципліни та виконання посадових обов’язків.	Оцінка результатів праці, проведення атестації, контроль за відвідуванням роботи, перевірка дотримання правил внутрішнього трудового розпорядку.
Інформаційний контроль	Забезпечує захист інформації, контроль за доступом до інформаційних ресурсів.	Захист від кібератак, контроль доступу до корпоративної мережі, резервне копіювання даних, захист від втрати інформації.
Постійний контроль	Регулярні перевірки, що проводяться протягом усього періоду діяльності.	Щоденний контроль за касовими операціями, щомісячний контроль за витратами на виробництво.
Періодичний контроль	Проводиться з певною періодичністю.	Квартальна звірка розрахунків з постачальниками, річна інвентаризація.
Одноразовий контроль	Здійснюється у зв’язку з конкретною подією або ситуацією.	Перевірка фінансової звітності перед поданням до податкової, аудит після злиття компаній.
Документальний контроль	Перевірка первинних документів, регістрів обліку.	Перевірка накладних, рахунків, договорів, актів виконаних робіт.
Фактичний контроль	Перевірка наявності матеріальних цінностей, виконання робіт.	Інвентаризація товарів на складі, перевірка якості готової продукції.
Комплексний контроль	Поєднання документального та фактичного контролю.	Перевірка виконання будівельних робіт за проектом, включаючи контроль за документацією та виконанням робіт на об’єкті.
Самоконтроль	Співробітники самі перевіряють свою роботу.	Самоперевірка якості виконаної роботи, контроль за дотриманням технологічних процесів.
Взаємний контроль	Співробітники контролюють роботу один одного.	Взаємна перевірка виконання завдань, контроль за дотриманням правил безпеки.

Продовження таблиці 1.2

1	2	3
Спеціальний контроль	Проводиться спеціально уповноваженими особами або службами.	Внутрішній аудит, ревізія, контроль якості.
Аналітичний контроль	Порівняння планових і фактичних показників, виявлення відхилень.	Аналіз фінансових звітів, аналіз ефективності використання ресурсів.
Експертний контроль	Оцінка експертами відповідності діяльності підприємства встановленим вимогам.	Експертна оцінка якості продукції, оцінка ефективності системи управління.
Статистичний контроль	Використання статистичних методів для оцінки якості, ефективності.	Статистичний контроль якості продукції, контроль стабільності процесів.
Внутрішній аудит	Незалежна оцінка діяльності підприємства.	Оцінка системи внутрішнього контролю, ефективності використання ресурсів, дотримання законодавства.
Ревізія	Перевірка фінансово-господарської діяльності підприємства.	Перевірка фінансової звітності, інвентаризація активів, контроль за дотриманням податкового законодавства.
Моніторинг	Постійний контроль за виконанням планів і дотриманням встановлених норм.	Моніторинг виконання бюджету, моніторинг якості продукції.
Самооцінка	Оцінка діяльності підприємства самими працівниками.	Оцінка ефективності роботи підрозділу, оцінка власних досягнень.
Фізична безпека	Захист приміщень, обладнання, персоналу.	Системи охорони, відеоспостереження, контроль доступу.
Інформаційна безпека	Захист інформації від несанкційованого доступу.	Антивірусний захист, брандмауери, шифрування даних.
Технологічна безпека	Забезпечення безперебійної роботи обладнання.	Резервне копіювання даних, технічне обслуговування обладнання.
Фінансова безпека	Захист від шахрайства, відмивання коштів.	Контроль фінансових потоків, перевірка контрагентів.

Важливо розуміти, що внутрішній контроль та безпека бізнесу тісно пов’язані і взаємодоповнюючи один одного. Ефективна система внутрішнього контролю є основою для забезпечення безпеки бізнесу.



Питання для самоконтролю

1. Які переваги надає підприємству ефективна система внутрішнього контролю?

2. Які ризики виникають при відсутності адекватного внутрішнього контролю?
3. Як ви розумієте поняття "контрольне середовище"?
4. Яке основне завдання внутрішнього контролю?
5. Чим відрізняється внутрішній контроль від зовнішнього аудиту?
6. Які основні компоненти системи внутрішнього контролю?
7. Які основні загрози для безпеки бізнесу Ви можете назвати?
8. Який зв'язок між внутрішнім контролем і безпекою бізнесу?

Тема 2. Предмет та методи внутрішнього контролю та безпеки бізнесу

Мета вивчення теми полягає в ознайомленні студентів з теоретичними основами внутрішнього контролю та безпеки бізнесу, навчанні ідентифікувати та оцінювати ризики, пов'язані з діяльністю підприємства, розробленні ефективної системи внутрішнього контролю для різних видів діяльності, опануванні методами та інструментами внутрішнього аудиту, застосуванні отриманих знань для вирішення практичних завдань у сфері управління підприємствами.

План

2.1 Предмет і об'єкти внутрішнього контролю та безпеки бізнесу.
2.2 Метод внутрішнього контролю. Способи дослідження документів та господарських операцій.
2.3 Контрольно-ревізійні процедури. Способи дослідження документів.

Основні терміни та поняття: *предмет, об'єкт, метод, контроль, ревізія, процедури*



2.1 Предмет і об'єкти внутрішнього контролю та безпеки бізнесу.

Предмет внутрішнього контролю та безпеки бізнесу – це сукупність економічних відносин, пов'язаних з управлінням підприємством, забезпеченням його ефективності та безпеки. Це комплексний процес, який охоплює всі аспекти діяльності підприємства від стратегічного планування до операційного виконання.

Об’єкти внутрішнього контролю та безпеки бізнесу – це конкретні сфери діяльності підприємства, які підлягають контролю та захисту. Вони можуть бути різноманітними та залежать від специфіки бізнесу.

Таблиця 2.1 – Основні об’єкти внутрішнього контролю

Категорія об’єктів	Приклади об’єктів
1	2
Фінансова діяльність	Доходи, витрати, бюджет, касові операції, банківські рахунки, інвестиції, дебіторська та кредиторська заборгованість.
Виробнича діяльність	Технологічні процеси, якість продукції, використання сировини, енергії, праці, ефективність виробництва.
Інвестиційна діяльність	Інвестиційні проєкти, ефективність використання інвестицій, управління портфелем інвестицій.
Кадрова діяльність	Підбір персоналу, оцінка ефективності праці, дотримання трудової дисципліни, навчання і розвиток персоналу.
Матеріально-технічне забезпечення	Закупівля матеріалів, зберігання запасів, використання основних фондів, логістика.
Інформаційні системи	Комп’ютерні мережі, бази даних, програмне забезпечення, захист інформації.
Дотримання законодавства	Податкове законодавство, трудове законодавство, екологічне законодавство, антимонопольне законодавство.
Репутація компанії	Імідж компанії, взаємовідносини з клієнтами, соціальна відповідальність.

Предмет внутрішнього контролю визначає загальну мету контролю, а об’єкти – конкретні сфери, на які цей контроль спрямований. Наприклад, предмет внутрішнього контролю фінансової діяльності – забезпечення правдивості фінансової звітності. Об’єктами такого контролю можуть бути касові операції, банківські виписки, інвентаризація матеріальних цінностей.

Важливо розуміти, що предмет і об’єкти внутрішнього контролю та безпеки бізнесу можуть змінюватися залежно від розміру підприємства, сфери його діяльності, рівня ризику та інших факторів.

Чому важливо визначати предмет і об’єкти контролю?

- Ефективність контролю: дозволяє сфокусуватися на найбільш важливих аспектах діяльності.
- Попередження ризиків: допомагає виявити потенційні загрози та розробити заходи щодо їх усунення.
- Забезпечення дотримання законодавства: гарантує, що підприємство діє в рамках правового поля.
- Підвищення ефективності бізнесу: дозволяє оптимізувати процеси та знизити витрати.

Визначення предмета і об’єктів внутрішнього контролю є першим кроком до побудови ефективної системи управління ризиками.

2.2 Метод внутрішнього контролю. Способи дослідження документів та господарських операцій.

Метод внутрішнього контролю – це сукупність способів та засобів, які використовуються для перевірки діяльності підприємства на відповідність встановленим нормам, правилам і планам. Він спрямований на забезпечення ефективності та правдивості фінансової звітності, захист активів підприємства та дотримання законодавства.

Спосіб дослідження документів та господарських операцій є одними з найважливіших методів внутрішнього контролю. Вони дозволяють перевірити правильність оформлення документів, законність проведених операцій та відповідність їх до встановлених процедур.

Таблиця 2.2 – Основні способи дослідження документів та господарських операцій

Спосіб	Характеристика	Мета
1	2	3
Порівняння	Зіставлення даних різних документів між собою, а також з плановими показниками, нормативними актами, раніше складеними документами.	Виявлення розбіжностей, помилок, невідповідностей.
Арифметична перевірка	Перевірка правильності математичних розрахунків у документах (суми, відсотки, загальні підсумки).	Виявлення арифметичних помилок.
Логічна перевірка	Оцінка послідовності оформлення документів, відповідності їх змісту характеру проведених операцій.	Виявлення нелогічних дій, порушень процедур.
Хронологічна перевірка	Перевірка дотримання послідовності за часом оформлення документів та проведення операцій.	Виявлення порушень хронології, неточностей у датах.
Формальна перевірка	Перевірка відповідності документів встановленим формам, вимогам до їх оформлення, наявності всіх обов’язкових реквізитів.	Виявлення недоліків у оформленні документів, відсутніх реквізитів.
Субстантивна перевірка	Глибокий аналіз змісту документів, суті проведених операцій, їх відповідності законодавству, нормативним актам підприємства, договорам.	Оцінка обґрунтованості операцій, виявлення порушень законодавства.
Вибірковий контроль	Перевірка не всіх документів, а лише їх вибірки, обраної за певними критеріями.	Зменшення обсягу роботи при збереженні достатньої правдівості результатів.
Аналіз	Глибоке вивчення інформації, виявлення закономірностей і тенденцій.	Оцінка загальної картини, виявлення проблемних зон.
Синтез	Об’єднання окремих елементів інформації в єдине ціле.	Формування загального уявлення про процес.

Продовження таблиці 2.2

1	2	3
Індукція	Перехід від часткових випадків до загальних висновків.	Формулювання узагальнень на основі конкретних фактів.
Дедукція	Перехід від загальних положень до часткових випадків.	Перевірка конкретних фактів на відповідність загальним правилам.

Додаткові способи та методи, які можуть бути використані:

– Аналіз: глибоке вивчення інформації, виявлення закономірностей і тенденцій.

– Синтез: об'єднання окремих елементів інформації в єдине ціле.

– Індукція: перехід від часткових випадків до загальних висновків.

– Дедукція: перехід від загальних положень до часткових випадків.

– Економіко-математичні методи: використання математичних моделей і методів для аналізу економічних процесів.

Застосування цих способів дозволяє:

– виявити помилки та неточності в документах і облікових даних,

– оцінити ефективність роботи підприємства,

– забезпечити правдивість фінансової звітності,

– виявити потенційні ризики,

– забезпечити дотримання законодавства.

Важливо зазначити, що ефективність внутрішнього контролю залежить не тільки від вибору методів, але й від кваліфікації персоналу, який проводить перевірки, а також від наявності сучасних інформаційних технологій.

2.3 Контрольно-ревізійні процедури. Способи дослідження документів.

Контрольно-ревізійні процедури – це систематичний підхід до перевірки фінансової звітності, облікових записів та операцій організації з метою оцінки їх правдивості, відповідності встановленим нормам та виявлення можливих помилок або шахрайств. Одним із ключових елементів цих процедур є дослідження документів.

Розширимо тему способів дослідження документів при проведенні контрольно-ревізійних процедур та розглянемо кілька додаткових аспектів.

Таблиця 2.3 – Способи дослідження документів при проведенні контрольно-ревізійних процедур.

Спосіб дослідження	Характеристика	Мета	Область застосування
1	2	3	4
Аналітичні процедури	Виявлення відхилень від очікуваних результатів, порівняння з попередніми періодами, галузевими стандартами.	Виявлення аномалій та ризиків.	Усі види документів.

Продовження таблиці 2.3

1	2	3	4
Детальна перевірка	Детальне вивчення окремих операцій або груп операцій.	Оцінка обґрунтованості та законності операцій.	Рахунки-фактури, платіжні документи.
Інвентаризація	Фізична перевірка наявності активів.	Виявлення недостач, надлишків, невідповідностей.	Оборотний інвентар, основні засоби.
Перевірка арифметичних розрахунків	Перевірка правильності математичних розрахунків у документах.	Виявлення арифметичних помилок.	Усі види документів.
Порівняння підписів	Порівняння підписів на документах зі зразками.	Виявлення підробок.	Усі документи, що потребують підпису.
Аналіз даних за допомогою IT	Використання програмного забезпечення для аналізу великих обсягів даних.	Виявлення прихованих зв’язків, аномалій.	Усі види документів.

1. Типи документів, що підлягають дослідженню:

– первинні документи: рахунки-фактури, накладні, касові ордери, платіжні доручення тощо,

– вторинні документи: регістри бухгалтерського обліку (журнал-ордер, головна книга), фінансова звітність,

– допоміжні документи: договори, акти виконаних робіт, інвентаризаційні описи.

2. Фактори, що впливають на вибір методів дослідження:

– мета перевірки для виявлення помилок, виявлення шахрайства, оцінка ефективності системи внутрішнього контролю,

– характер діяльності підприємства: виробництво, торгівля, послуги,

– обсяг та складність операцій: кількість документів, різноманітність господарських операцій,

– ризики, пов’язані з діяльністю: фінансові, операційні, пов’язані з дотриманням законодавства,

– використання інформаційних технологій,

– автоматизовані системи контролю: програми для аналізу даних, виявлення аномалій, порівняння з базами даних,

– сканування та розпізнавання документів: переведення паперових документів в електронний вигляд для зручності зберігання та аналізу,

– аналітичні інструменти: графіки, діаграми, таблиці для візуалізації даних та виявлення трендів.

3. Специфічні способи для виявлення різних видів порушень:

– завищення витрат: аналіз рахунків-фактур, перевірка обґрунтованості цін, порівняння з ринковими цінами,

– незаконне привласнення активів: інвентаризація, перевірка касових операцій, аналіз банківських виписок,

– ухилення від сплати податків: аналіз податкових декларацій, розрахунок податкових зобов'язань,

– фальсифікація документів: порівняння підписів, перевірка штампів, аналіз почерку.

4. Роль інформаційних технологій у сучасному аудиті:

– аналітичні процедури: використання програмного забезпечення для аналізу великих обсягів даних, виявлення аномалій та трендів.

– роботизована автоматизація процесів (RPA): автоматизація рутинних завдань, таких як збір даних, перевірка точності, класифікація документів.

– блокчейн: застосування технології блокчейн для забезпечення прозорості та безпеки обміну даними.



Питання для самоконтролю

1. Що таке контрольно-ревізійні процедури і яка їхня мета?
2. Які типи документів підлягають дослідженню під час ревізії?
3. Які фактори впливають на вибір методів дослідження документів?
4. Які основні способи дослідження документів Ви знаєте? Схарактеризуйте кожен з них.
5. Яка роль інформаційних технологій у сучасному аудиті?
6. Які виклики стоять перед аудиторами в умовах цифрової трансформації бізнесу?
7. Що таке ризикорієнтований аудит і як він відрізняється від традиційного аудиту?

ЗМІСТОВИЙ МОДУЛЬ 2
ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ НА ПІДПРИЄМСТВІ ТА БЕЗПЕКИ БІЗНЕСУ

Тема 3. Суб'єкти внутрішнього контролю та безпеки бізнесу й їх функції

Мета вивчення теми полягає в отриманні студентами розуміння: хто саме відповідає за забезпечення внутрішнього контролю та безпеки бізнесу на підприємстві, які конкретні ролі та обов'язки покладаються на кожного суб'єкта внутрішнього контролю, як взаємодіють між собою різні суб'єкти для досягнення загальної мети – забезпечення безпеки бізнесу, які механізми координації та контролю існують для ефективної роботи системи внутрішнього контролю.

План

3.1 Спостережна рада, як суб'єкт внутрішнього контролю та безпеки бізнесу.

3.2 Правління, як суб'єкт внутрішнього контролю та безпеки бізнесу.

3.3 Ревізійна комісія підприємства, як суб'єкт внутрішнього контролю та безпеки бізнесу.

3.4 Керівник підприємства, як суб'єкт внутрішнього контролю та безпеки бізнесу.

3.5 Фінансовий директор, як суб'єкт внутрішнього контролю та безпеки бізнесу та його контрольні функції.

3.6 Головний бухгалтер підприємства як суб'єкт внутрішнього контролю й безпеки бізнесу та його контрольні функції.

3.7 Служба внутрішнього аудиту, як суб'єкт внутрішнього контролю та безпеки бізнесу.

Основні терміни та поняття: *суб'єкт внутрішнього контролю, спостережна рада, правління, керівник, фінансовий директор, головний бухгалтер, ризик, корпоративна культура, фінансова звітність, аудит*



3.1 Спостережна рада, як суб'єкт внутрішнього контролю та безпеки бізнесу.

Спостережна рада – це колегіальний орган управління акціонерним товариством, який здійснює загальне керівництво діяльністю товариства. Однією з важливих функцій спостережної ради є забезпечення ефективного внутрішнього контролю та безпеки бізнесу.

Таблиця 3.1 – Роль спостережної ради у забезпеченні внутрішнього контролю та безпеки бізнесу

Функція спостережної ради	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Затвердження стратегії розвитку	Визначення довгострокових цілей компанії, пріоритетів та напрямків розвитку.	Створення чіткого бачення майбутнього, яке допомагає у формуванні системи внутрішнього контролю.

Продовження таблиці 3.1

1	2	3
Призначення та звільнення членів правління	Формування ефективного складу виконавчого органу, який здатний забезпечити реалізацію стратегії компанії.	Забезпечення професійного менеджменту.
Затвердження внутрішніх документів	Затвердження положень про внутрішній контроль, кодексів корпоративного управління, політик у сфері безпеки інформації тощо.	Створення нормативно-правової бази для ефективного функціювання системи внутрішнього контролю.
Оцінка ризиків	Ідентифікація та оцінка основних ризиків, з якими стикається компанія.	Забезпечення проактивного підходу до управління ризиками.
Контроль за фінансовою звітністю	Перевірка правдивості фінансової звітності, забезпечення її відповідності міжнародним стандартам.	Забезпечення прозорості фінансової інформації.
Забезпечення захисту інтересів акціонерів	Захист прав та інтересів акціонерів, забезпечення рівних можливостей для всіх акціонерів.	Підвищення довіри інвесторів до компанії.
Співпраця з аудиторами	Взаємодія зі зовнішніми аудиторами для забезпечення незалежної оцінки фінансової звітності та системи внутрішнього контролю.	Підвищення правдивості фінансової інформації.
Сприяння розвитку корпоративної культури	Формування культури відповідальності, прозорості та етики в компанії.	Створення атмосфери, яка сприяє дотриманню високих стандартів поведінки.

Важливо розуміти, що ефективність роботи спостережної ради залежить від багатьох факторів, таких як:

– кваліфікація членів спостережної ради: члени ради повинні мати необхідні знання та досвід для оцінки діяльності компанії,

– незалежність членів спостережної ради: члени ради повинні бути незалежними від виконавчого органу та інших зацікавлених сторін,

– час, присвячений роботі в раді: члени ради повинні приділяти достатньо часу для виконання своїх обов’язків,

– ефективність комунікації: між членами ради, між радою та виконавчим органом, між радою та акціонерами повинна бути встановлена ефективна комунікація.

Спостережна рада відіграє ключову роль у забезпеченні внутрішнього контролю та безпеки бізнесу. Завдяки своїм функціям вона сприяє підвищенню ефективності діяльності компанії, зниженню ризиків та підвищенню довіри інвесторів.

3.2 Правління, як суб'єкт внутрішнього контролю та безпеки бізнесу

Правління (виконавчий орган) компанії відіграє ключову роль у забезпеченні ефективного внутрішнього контролю та безпеки бізнесу. Саме правління несе пряму відповідальність за повсякденну діяльність компанії та реалізацію стратегічних цілей.

Таблиця 3.2 – Роль правління у забезпеченні внутрішнього контролю та безпеки бізнесу

Функція правління	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Реалізація стратегії	Розробка та впровадження стратегічних планів компанії.	Забезпечення узгодженості всіх видів діяльності компанії з її стратегічними цілями.
Операційне управління	Безпосереднє керівництво повсякденною діяльністю компанії.	Забезпечення ефективності та ефективності бізнес-процесів.
Управління ризиками	Ідентифікація, оцінка та управління ризиками, з якими стикається компанія.	Запобігання виникненню кризових ситуацій.
Забезпечення дотримання законодавства	Контроль за дотриманням компанією всіх чинних законів та нормативних актів.	Уникнення юридичної відповідальності.
Захист активів компанії	Розробка та впровадження заходів щодо захисту активів компанії від втрат, крадіжок та інших видів загроз.	Збереження майна компанії.
Співпраця зі спостережною радою	Регулярна звітність перед спостережною радою про результати діяльності компанії.	Забезпечення прозорості та підзвітності.
Створення системи внутрішнього контролю	Розробка та впровадження системи внутрішнього контролю, яка відповідає масштабам і специфіці діяльності компанії.	Забезпечення правдивості фінансової звітності та ефективності операцій.

Ключові ролі правління у внутрішньому контролі:

– розробка політик і процедур: правління розробляє детальні політики та процедури, які визначають, як повинні виконуватися різні види діяльності в компанії,

– призначення відповідальних осіб: правління призначає відповідальних осіб за виконання різних функцій і делегує їм повноваження,

– моніторинг та оцінка: правління регулярно моніторить ефективність системи внутрішнього контролю та безпеки бізнесу й оцінює результати її роботи,

– внесення змін: правління вносить необхідні зміни до системи внутрішнього контролю з урахуванням змін у бізнес-середовищі та виявлених недоліків.

Важливість ролі правління складається з безпосередньої відповідальності, бо саме правління несе пряму відповідальність за результати діяльності компанії, з глибокого розуміння бізнесу, бо члени правління мають глибоке розуміння бізнесу компанії та можуть приймати обґрунтовані рішення, з гнучкості, бо правління може швидко реагувати на зміни в бізнес-середовищі.

Правління відіграє центральну роль у забезпеченні ефективного внутрішнього контролю та безпеки бізнесу. Саме від рішень і дій правління залежить успіх компанії.

3.3 Ревізійна комісія підприємства, як суб'єкт внутрішнього контролю та безпеки бізнесу

Ревізійна комісія – це незалежний орган внутрішнього контролю на підприємстві, який створений для перевірки фінансово-господарської діяльності підприємства та дотримання ним законодавства.

Таблиця 3.3 – Роль ревізійної комісії у забезпеченні внутрішнього контролю та безпеки бізнесу

Функція ревізійної комісії	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Перевірка фінансової звітності	Систематична перевірка правильності складання та правдивості фінансової звітності.	Забезпечення надійності фінансової інформації для прийняття управлінських рішень.
Оцінка ефективності системи внутрішнього контролю	Аналіз системи внутрішнього контролю на предмет її відповідності встановленим вимогам та ефективності функціювання.	Виявлення слабких місць у системі внутрішнього контролю та розроблення пропозицій щодо їх усунення.
Виявлення порушень	Виявлення порушень законодавства, внутрішніх документів компанії та недоліків у роботі.	Запобігання втратам та збитків компанії.
Забезпечення дотримання фінансової дисципліни	Контроль за дотриманням фінансової дисципліни на підприємстві.	Зменшення ризику фінансових втрат.

Продовження таблиці 3.3

1	2	3
Підготовка висновків та рекомендацій	Підготовка звітів про результати проведених перевірок з висновками та рекомендаціями щодо усунення виявлених недоліків.	Забезпечення своєчасного вжиття заходів для усунення проблем.
Співпраця з іншими підрозділами	Взаємодія з іншими підрозділами підприємства для отримання необхідної інформації та координації дій.	Забезпечення комплексного підходу до розв'язання проблем.

Ключові ролі ревізійної комісії:

– незалежність: ревізійна комісія повинна бути незалежна від інших підрозділів підприємства для забезпечення об'єктивності оцінки,

– компетентність: члени ревізійної комісії повинні мати необхідні знання та досвід для проведення ревізій,

– систематичність: ревізії повинні проводитися регулярно і за затвердженим планом.

Важливість ролі ревізійної комісії визначається:

– попередженням шахрайства: ревізійна комісія допомагає виявити та запобігти шахрайським діям,

– підвищенням довіри інвесторів: наявність незалежної ревізійної комісії свідчить про прозорість діяльності компанії та підвищує довіру інвесторів.

– удосконаленням управління: результати роботи ревізійної комісії допомагають керівництву компанії вдосконалити системи управління.

Ревізійна комісія є важливим елементом системи внутрішнього контролю підприємства та безпеки бізнесу. Вона забезпечує незалежну оцінку фінансово-господарської діяльності, виявляє ризики та недоліки, сприяє підвищенню ефективності роботи підприємства.

3.4 Керівник підприємства, як суб'єкт внутрішнього контролю та безпеки бізнесу

Керівник підприємства несе найвищу відповідальність за ефективність системи внутрішнього контролю та безпеку бізнесу. Саме він формує корпоративну культуру, встановлює стратегічні цілі та забезпечує дотримання всіх необхідних процедур.

Керівник підприємства є ключовою фігурою в системі внутрішнього контролю та безпеки бізнесу. Його роль полягає не тільки в установленні правил і процедур, але й у створенні такої корпоративної культури, яка сприяє дотриманню високих стандартів етики та відповідальності.

Ключові ролі керівника підприємства:

– лідерство: керівник є лідером, який встановлює високі стандарти і мотивує співробітників до їх дотримання,

– відповідальність: керівник несе персональну відповідальність за результати діяльності підприємства.

Таблиця 3.4 – Роль керівника підприємства у забезпеченні внутрішнього контролю та безпеки бізнесу

Функція керівника підприємства	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Створення корпоративної культури	Формування культури відповідальності, прозорості та дотримання етичних норм.	Створення атмосфери, яка сприяє дотриманню високих стандартів поведінки.
Визначення стратегічних цілей	Визначення довгострокових цілей компанії та розробка стратегії їх досягнення.	Забезпечення узгодженості всіх видів діяльності компанії з її стратегічними цілями.
Призначення відповідальних осіб	Призначення відповідальних осіб за різні напрямки діяльності та делегування повноважень.	Забезпечення чіткого розподілу обов’язків.
Моніторинг діяльності підприємства	Регулярний контроль за діяльністю всіх підрозділів підприємства.	Виявлення проблемних ситуацій на ранніх стадіях.
Забезпечення ресурсами	Надання необхідних ресурсів для ефективного функціювання системи внутрішнього контролю.	Гарантування наявності всіх необхідних інструментів для виконання поставлених завдань.
Співпраця з іншими суб’єктами внутрішнього контролю	Взаємодія зі спостережною радою, ревізійною комісією та іншими підрозділами.	Забезпечення комплексного підходу до управління ризиками.

Важливість ролі керівника підприємства складається із визначення напряму розвитку, тому що від рішень керівника залежить напрямок розвитку компанії, формування команди, тому що керівник формує команду професіоналів, здатних досягати поставлених цілей та створення позитивного іміджу, тому що керівник створює позитивний імідж компанії на ринку.

3.5 Фінансовий директор, як суб’єкт внутрішнього контролю та безпеки бізнесу та його контрольні функції

Фінансовий директор є одним з ключових суб’єктів внутрішнього контролю на підприємстві. Він несе відповідальність за фінансову стабільність

компанії, ефективність використання ресурсів та дотримання фінансової дисципліни.

Таблиця 3.5 – Контрольні функції фінансового директора

Функція фінансового директора	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Розробка та впровадження фінансової політики	Створення чітких правил і процедур у фінансовій сфері.	Забезпечення єдиного підходу до фінансових питань.
Управління фінансовими ресурсами	Оптимізація використання фінансових ресурсів компанії.	Збільшення прибутковості та ефективності бізнесу.
Підготовка фінансової звітності	Складання правдивої та своєчасної фінансової звітності.	Забезпечення прозорості фінансової інформації для інвесторів, кредиторів та інших зацікавлених сторін.
Контроль за виконанням бюджету	Моніторинг виконання бюджету та виявлення відхилень.	Забезпечення ефективного використання коштів.
Управління скарбницею	Організація ефективної роботи скарбниці, управління грошовими потоками компанії.	Зменшення ризиків пов’язаних з грошовими коштами.
Оцінка інвестиційних проєктів	Аналіз ефективності інвестиційних проектів.	Прийняття обґрунтованих рішень щодо інвестицій.
Управління податками	Забезпечення своєчасної та повної сплати податків.	Уникнення податкових ризиків.
Взаємодія з аудиторами	Співпраця з зовнішніми аудиторами для забезпечення незалежної оцінки фінансової звітності.	Підвищення довіри до фінансової інформації.

Ключові ролі фінансового директора у внутрішньому контролі та безпеці бізнесу:

– фінансовий аналіз: проведення фінансового аналізу для виявлення трендів, ризиків та можливостей,

– контроль за витратами: забезпечення ефективного контролю за витратами компанії,

– управління дебіторською та кредиторською заборгованістю: оптимізація дебіторської та кредиторської заборгованості,

– управління ризиками: ідентифікація та управління фінансовими ризиками.

Важливість ролі фінансового директора складається із забезпечення фінансової стабільності, тому що фінансовий директор відповідає за фінансову

стабільність компанії; прийняття обґрунтованих рішень, тому що фінансовий директор надає керівництву компанії обґрунтовані рекомендації щодо фінансових питань; підвищення ефективності бізнесу – фінансовий директор сприяє підвищенню ефективності використання ресурсів компанії.

Фінансовий директор відіграє ключову роль у системі внутрішнього контролю та безпеки бізнесу. Він несе відповідальність за фінансову дисципліну, ефективність використання ресурсів та правдивість фінансової звітності.

3.6 Головний бухгалтер підприємства як суб'єкт внутрішнього контролю й безпеки бізнесу та його контрольні функції

Головний бухгалтер є одним з ключових суб'єктів внутрішнього контролю на підприємстві. Він несе безпосередню відповідальність за організацію бухгалтерського обліку, складання фінансової звітності та забезпечення дотримання фінансової дисципліни.

Таблиця 3.6 – Контрольні функції головного бухгалтера

Функція головного бухгалтера	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Організація бухгалтерського обліку	Створення системи бухгалтерського обліку відповідно до законодавчих та нормативних вимог.	Забезпечення повноти та правдивості облікової інформації.
Складання фінансової звітності	Підготовка фінансової звітності за встановленими формами та стандартами.	Забезпечення прозорості фінансового стану підприємства.
Контроль за виконанням бюджету	Моніторинг виконання кошторису доходів і витрат.	Забезпечення ефективного використання фінансових ресурсів.
Управління дебіторською та кредиторською заборгованістю	Контроль за своєчасним погашенням дебіторської та кредиторської заборгованості.	Зменшення ризику втрати коштів.
Контроль за касовими операціями	Організація ефективного контролю за рухом готівкових коштів.	Запобігання втратам готівки.
Співпраця з податковими органами	Забезпечення своєчасної сплати податків та зборів.	Уникнення податкових ризиків.
Взаємодія з іншими підрозділами	Співпраця з іншими підрозділами підприємства для отримання необхідної інформації.	Забезпечення комплексного підходу до ведення бухгалтерського обліку.

Ключові ролі головного бухгалтера у внутрішньому контролі та безпеці бізнесу:

– контроль за документами: перевірка первинних документів на правильність оформлення та правдивість даних,

– звірка розрахунків: регулярна звірка розрахунків з контрагентами,

– інвентаризація: проведення інвентаризації матеріальних цінностей та грошових коштів,

– аналіз фінансової інформації: аналіз фінансової звітності для виявлення відхилень та трендів.

Важливість ролі головного бухгалтера складається з гарантування правдивості фінансової інформації, бо головний бухгалтер несе відповідальність за правдивість фінансової звітності; забезпечення фінансової дисципліни, тому що головний бухгалтер контролює дотримання фінансової дисципліни на підприємстві та підтримка прийняття управлінських рішень. Головний бухгалтер надає керівництву необхідну фінансову інформацію для прийняття обґрунтованих рішень.

Головний бухгалтер є одним з найважливіших суб'єктів внутрішнього контролю. Його функції спрямовані на забезпечення правдивості фінансової інформації, ефективного використання ресурсів та дотримання фінансової дисципліни.

3.7 Служба внутрішнього аудиту, як суб'єкт внутрішнього контролю та безпеки бізнесу

Служба внутрішнього аудиту – це незалежний підрозділ підприємства, який здійснює систематичну оцінку та аналіз діяльності компанії з метою забезпечення її ефективності, дотримання законодавства та внутрішніх нормативних актів.

Таблиця 3.7 – Контрольні функції служби внутрішнього аудиту

Функція служби внутрішнього аудиту	Опис	Важливість для внутрішнього контролю та безпеки
1	2	3
Оцінка системи внутрішнього контролю	Аналіз ефективності системи внутрішнього контролю та виявлення слабких місць.	Забезпечення надійності системи внутрішнього контролю.
Проведення аудиторських перевірок	Систематична перевірка фінансово-господарської діяльності підприємства.	Виявлення порушень, недоліків та ризиків.
Консультування керівництва	Надання рекомендацій щодо вдосконалення системи управління та підвищення ефективності діяльності.	Сприяння прийняттю обґрунтованих управлінських рішень.

Продовження таблиці 3.7

1	2	3
Моніторинг виконання рекомендацій	Контроль за виконанням рекомендацій, наданих за результатами аудиторських перевірок.	Забезпечення ефективності внутрішнього аудиту.
Оцінка ризиків	Ідентифікація та оцінка ризиків, з якими стикається підприємство.	Розробка заходів щодо управління ризиками.
Забезпечення дотримання нормативно-правових актів	Перевірка дотримання підприємством законодавства та внутрішніх нормативних актів.	Уникнення юридичної відповідальності.

Ключові ролі служби внутрішнього аудиту у внутрішньому контролі та безпеці бізнесу:

– незалежність: служба внутрішнього аудиту повинна бути незалежна від інших підрозділів підприємства,

– об’єктивність: оцінка діяльності підприємства повинна бути об’єктивною та неупередженою,

– професіоналізм: співробітники служби внутрішнього аудиту повинні мати відповідну кваліфікацію та досвід.

Важливість ролі служби внутрішнього аудиту полягає в підвищення довіри інвесторів – наявність служби внутрішнього аудиту свідчить про прозорість діяльності підприємства; попередження шахрайства – служба внутрішнього аудиту допомагає виявити та запобігти шахрайським діям; удосконалення управління – результати роботи служби внутрішнього аудиту допомагають керівництву підприємства вдосконалити системи управління.

Служба внутрішнього аудиту відіграє важливу роль у системі внутрішнього контролю підприємства. Вона забезпечує незалежну оцінку діяльності компанії, виявляє ризики та недоліки, сприяє підвищенню ефективності роботи підприємства.



Питання для самоконтролю

1. Як правління забезпечує дотримання стратегічних цілей компанії?
2. Які основні завдання ревізійної комісії?
3. Які фінансові функції виконує фінансовий директор в системі внутрішнього контролю?
4. Як фінансовий директор забезпечує правдивість фінансової звітності?
5. Які основні завдання головного бухгалтера в системі внутрішнього контролю?
6. Як служба внутрішнього аудиту оцінює ефективність системи внутрішнього контролю?

Тема 4. Загальні аспекти організації контрольної роботи на підприємстві

Мета вивчення теми: сформувати у студентів розуміння, що внутрішній контроль – це не просто перевірка, а систематичний процес, спрямований на забезпечення досягнення цілей підприємства, захист його активів, забезпечення правдивості фінансової звітності та дотримання законодавства; вивчили основні принципи організації контрольної роботи, ознайомилися з різними видами контролю, опанувати навичками оцінки ефективності системи внутрішнього контролю.

План

4.1 Основні етапи створення системи внутрішнього контролю та безпеки бізнесу на підприємстві.

4.2 Розподіл відповідальності. Організація і діяльність ревізійних комісій на підприємствах. Матеріальна та дисциплінарна відповідальність працівників.

4.3 Документальне забезпечення контролю та захисту бізнесу.

4.4 Використання інформаційних технологій для забезпечення внутрішнього контролю та безпеки бізнесу.

Основні терміни та поняття: *контрольне середовище, оцінка ризиків, комунікація, моніторинг, ревізійна комісія, відповідальність, інформаційні технології*



4.1 Основні етапи створення системи внутрішнього контролю та безпеки бізнесу на підприємстві.

Створення ефективної системи внутрішнього контролю є стратегічним завданням для будь-якого підприємства. Це комплексний процес, який вимагає системного підходу та залучення різних функціональних підрозділів.

Важливо розуміти, що створення системи внутрішнього контролю – це не одноразовий процес, а безперервна діяльність. Система повинна постійно розвиватися та адаптуватися до змін у бізнес-середовищі.

Чинниками успішного впровадження системи внутрішнього контролю та безпеки бізнесу є – активна участь керівництва в процесі створення і розвитку системи, залучення співробітників до участі в розробці та впровадженні системи, використання сучасних технологій та регулярна оцінка ефективності системи.

Таблиця 4.1 – Основні етапи процесу створення системи внутрішнього контролю та безпеки бізнесу на підприємстві

Етап	Опис	Мета
1	2	3
1. Аналіз наявного стану	Оцінка поточної системи контролю, виявлення сильних і слабких сторін, ризиків. Збір інформації про процеси, документи, інтерв'ю з персоналом.	Отримати чітке уявлення про те, що вже працює, а що потребує покращення.
2. Формулювання цілей	Визначення стратегічних цілей підприємства та їх зображення в цілях системи контролю. Ідентифікація ключових ризиків, які можуть завадити досягненню цих цілей.	Створити чітку і зрозумілу картину бажаного стану системи контролю.
3. Розробка концепції	Вибір моделі системи контролю, визначення її компонентів (контрольне середовище, оцінка ризиків, контрольні заходи, інформація та комунікація, моніторинг). Розробка політик і процедур.	Створити детальний план побудови системи.
4. Впровадження	Підготовка персоналу, розповсюдження інформації про нову систему, тестування системи в тестовому режимі.	Забезпечити плавний перехід до нової системи.
5. Моніторинг і оцінка	Регулярний збір інформації про роботу системи, порівняння результатів з плановими показниками, виявлення відхилень.	Переконатися, що система працює ефективно і досягає поставлених цілей.

Ключові елементи ефективної системи внутрішнього контролю:

– контрольне середовище: культура організації, етика, структура управління, делегування повноважень,

– оцінка ризиків: ідентифікація, аналіз і управління ризиками.

– контрольні заходи: процедури, які забезпечують досягнення поставлених цілей,

– інформація і комунікація: збір, обробка та розповсюдження інформації для підтримки системи контролю,

– моніторинг: регулярна перевірка ефективності системи контролю.

4.2 Розподіл відповідальності. Організація і діяльність ревізійних комісій на підприємствах. Матеріальна та дисциплінарна відповідальність працівників

Ревізійна комісія – це незалежний орган внутрішнього контролю на підприємстві, який створений для перевірки фінансово-господарської

діяльності. Її основна мета – забезпечити правдивість фінансової звітності, ефективність використання ресурсів та дотримання законодавства.

Таблиця 4.2 – Організація і діяльність ревізійних комісій на підприємствах: детальний аналіз

Аспект	Опис	Мета
1	2	3
Склад комісії	Представники власників/акціонерів, працівники різних підрозділів, незалежні експерти.	Забезпечення об’єктивності та різнобічності оцінки.
Функції	Планові та позапланові ревізії, контроль виконання бюджету, оцінка ефективності використання активів, перевірка дотримання законодавства, підготовка висновків і рекомендацій.	Забезпечення фінансової дисципліни, ефективного використання ресурсів та дотримання законів.
Організація роботи	Планування, проведення ревізій, оформлення результатів, розгляд на засіданнях, взаємодія з іншими органами.	Створення ефективної системи внутрішнього контролю.
Права	Доступ до інформації, вимога пояснень, внесення пропозицій.	Забезпечення повноти та об’єктивності перевірок.
Відповідальність	Об’єктивність, повнота, якість актів, дотримання процедур.	Гарантування правдивості результатів ревізій.
Значення	Забезпечення правдивості фінансової звітності, запобігання зловживання, підвищення ефективності, зміцнення довіри.	Загальна стабільність та прозорість діяльності підприємства.

Детальніше про окремі аспекти:

✓ Планові та позапланові ревізії:

– планові: проводяться згідно з річним планом, охоплюють всі основні напрямки діяльності,

– позапланові: проводяться за необхідності (наприклад, при виявленні ознак шахрайства, зміні керівництва).

✓ Методи ревізії:

– документальна ревізія: перевірка первинних документів,

– фактична ревізія: перевірка наявності матеріальних цінностей,

– аналітична ревізія: аналіз фінансової звітності та інших даних.

✓ Результати ревізії:

– акт ревізії: детальний опис виявлених порушень, їх причин та наслідків,

– рекомендації: пропозиції щодо усунення недоліків та покращення роботи.

Ревізійна комісія важлива для:

– захисту інтересів власників, бо гарантує, що активи компанії використовуються ефективно,

– запобігання фінансовим зловживанням, бо виявляє шахрайство та інші неправомірні дії.

– підвищення довіри інвесторів, що свідчить про прозорість діяльності компанії,

– покращення управління допомагає виявити слабкі місця в системах управління.

Важливо розуміти, що ревізійна комісія є одним з елементів системи внутрішнього контролю. Для досягнення максимальної ефективності її робота повинна бути тісно пов’язана з іншими елементами цієї системи.

Матеріальна та дисциплінарна відповідальність працівників є важливими аспектами трудових відносин. Вони встановлюють межі дозволеної поведінки працівника та визначають наслідки за їх порушення. Розуміння цих видів відповідальності є необхідним як для роботодавців, так і для працівників для забезпечення ефективної та справедливої роботи підприємства.

Таблиця 4.3 – Порівняльна таблиця відповідальності працівників

Характеристика	Матеріальна відповідальність	Дисциплінарна відповідальність
1	2	3
Суть	Обов’язок працівника відшкодувати роботодавцю матеріальну шкоду, заподіяну підприємству внаслідок порушення трудових обов’язків.	Обов’язок працівника понести дисциплінарне стягнення за порушення трудової дисципліни.
Підстави виникнення	Безпосередній причинний зв’язок між діями працівника та заподіяною шкодою; вина працівника.	Невиконання або неналежне виконання трудових обов’язків, порушення трудової дисципліни.
Види відповідальності	Повна, обмежена.	Зауваження, догана, звільнення.
Законодавча основа	Кодекс законів про працю України, цивільне законодавство.	Кодекс законів про працю України, колективний договір, правила внутрішнього трудового розпорядку.
Порядок застосування	Виявлення шкоди, встановлення причинно-наслідкового зв’язку, розрахунок розміру шкоди, складання акту.	Виявлення порушення, складання акту, накладення стягнення наказом.
Наслідки	Матеріальні втрати для працівника.	Обмеження трудових прав, можливе звільнення.
Термін давності	Один рік з моменту виявлення шкоди.	Один місяць з дня виявлення проступку, за результатами ревізії – два місяці.
Особливості	Може застосовуватися спільно з дисциплінарною відповідальністю. Може бути встановлена додаткова матеріальна відповідальність за договором.	Застосовується тільки до працівників, які перебувають у трудових відносинах.

Існує взаємозв’язок між матеріальною та дисциплінарною відповідальністю.

Часто порушення трудових обов’язків може призвести як до матеріальної, так і до дисциплінарної відповідальності. Наприклад, розкрадання майна підприємства тягне за собою як матеріальну відповідальність (відшкодування вартості викраденого майна), так і дисциплінарну (звільнення).

Важливі моменти:

- ✓ Договір про повну матеріальну відповідальність: може бути укладений з певними категоріями працівників (касири, матеріально відповідальні особи).
- ✓ Строк давності для притягнення до матеріальної відповідальності: один рік з моменту виявлення шкоди.
- ✓ Право на оскарження: працівник має право оскаржити накладене дисциплінарне стягнення або вимогу про відшкодування матеріальної шкоди в судовому порядку.

Важливі нюанси

- ✓ Доведення вини: роботодавець повинен довести, що працівник діяв умисно або з грубою необережністю, а також наявність прямого причинно-наслідкового зв’язку між діями працівника та заподіяною шкодою.
- ✓ Право на захист: працівник має право оскаржити накладене дисциплінарне стягнення або вимогу про відшкодування матеріальної шкоди в судовому порядку.
- ✓ Індивідуальний підхід: при застосуванні заходів відповідальності необхідно враховувати конкретні обставини справи, характер порушення та попередню трудову діяльність працівника.

Матеріальна та дисциплінарна відповідальність є важливими інструментами для забезпечення трудової дисципліни та збереження майна підприємства. Розуміння їхньої сутності та особливостей дозволяє як роботодавцям, так і працівникам уникнути непорозумінь та конфліктних ситуацій.

4.3 Документальне забезпечення контролю та захисту бізнесу

Документальне забезпечення контролю – це сукупність документів, які фіксують, оформляють і підтверджують проведення контрольних заходів, результати перевірок, виявлені порушення та вжиті заходи. Воно є невіддільною частиною будь-якої системи контролю, незалежно від її масштабів та сфери застосування.

Цей список не є вичерпним і може бути доповнений іншими документами залежно від особливостей системи контролю та вимог організації.

Кожен з цих документів має свої особливості оформлення і зберігання. Рекомендується розробити шаблони для всіх видів документів, що використовуються в системі контролю, щоб забезпечити їх однорідність і повноту.

Таблиця 4.4 – Основні види документів, що використовуються в системі контролю

Вид документа	Призначення	Основний зміст
1	2	3
План контрольних заходів	Визначення об’єктів, термінів, відповідальних осіб, мети та завдань контролю.	Перелік об’єктів контролю, графік проведення, відповідальні особи, критерії оцінки.
Програма контрольного заходу	Деталізація процедури проведення перевірки.	Перелік документів, які підлягають перевірці, методи контролю, порядок оформлення результатів.
Акт контролю	Оформлення результатів перевірки.	Виявлені порушення, невідповідності, недоліки, пропозиції щодо їх усунення.
Висновок контролю	Загальна оцінка стану контрольованого об’єкта.	Оцінка ефективності системи контролю, висновки та рекомендації.
Претензія	Вимога усунути виявлені порушення.	Опис порушення, вимоги до його усунення, терміни виконання.
Припис	Обов’язкове до виконання розпорядження.	Визначення конкретних заходів, які необхідно вжити для усунення порушення.
Протокол засідання контрольного органу	Фіксація обговорення результатів контролю.	Хід обговорення, прийняті рішення, розподіл відповідальності.

Таблиця 4.5 – Основні види документів, що використовуються в системі контролю з акцентом на інформаційні системи

Тип документа	Інформаційна система	Переваги використання
1	2	3
План контрольних заходів	Система електронного документообігу	Автоматичне нагадування про терміни, централізований доступ, версіювання.
Програма контрольного заходу	Система електронного документообігу	Інтеграція з іншими системами (ERP, CRM), автоматичне формування звітів.
Акт контролю	Система електронного архіву	Швидкий пошук, збереження історії змін, інтеграція з іншими системами.
Висновок контролю	Система електронного архіву	Можливість автоматичного формування на основі даних акту контролю.
Претензія, припис	Система електронного документообігу	Автоматичне направлення, відстеження статусу, електронний підпис.
Протокол засідання контрольного органу	Система електронного протоколювання	Трансляція засідань онлайн, автоматичне формування протоколу, електронне голосування.

Додаткові види документів, які можуть використовуватися залежно від специфіки контролю:

– пояснювальна записка, яка надається відповідальними особами для пояснення причин виявлених порушень,

– довідка, яка підтверджує певні факти, необхідні для проведення контролю,

– розпорядження, що видається керівником для виконання рекомендацій контролю,

– звіт про виконання припису, що підтверджує виконання вимог припису.

4.4 Використання інформаційних технологій для забезпечення внутрішнього контролю та безпеки бізнесу

Сучасний бізнес неможливо уявити без використання інформаційних технологій. Вони проникають у всі сфери діяльності підприємств, від виробництва до управління персоналом. З одного боку, це дозволяє підвищити ефективність роботи, автоматизувати рутинні процеси та приймати більш обґрунтовані рішення. З іншого боку, це створює нові ризики для безпеки бізнесу, пов’язані з кіберзагрозами, несанкційованим доступом до інформації та іншими видами шахрайства.

Таблиця 4.6 – Основні інформаційні технології та застосування їх у внутрішньому контролі та безпеці

Інформаційна технологія	Застосування у внутрішньому контролі та безпеці
1	2
Системи електронного документообігу	Автоматизація обробки документів, контроль доступу, електронний архів
Системи управління базами даних (СУБД)	Зберігання та аналіз даних, створення звітів
Системи аналітики даних	Виявлення аномалій, прогнозування, прийняття рішень на основі даних
Системи контролю доступу	Обмеження доступу до інформаційних ресурсів
Системи захисту інформації	Захист від кібератак, вірусів, несанкціонованого доступу
Системи відеоспостереження	Контроль фізичної безпеки
Хмарні технології	Зберігання даних, забезпечення доступності, масштабованість
Блокчейн	Забезпечення прозорості та безпеки транзакцій, контроль ланцюжків постачання
Штучний інтелект	Автоматизація рутинних задач, виявлення шахрайства, прогнозування ризиків

Таблиця 4.7 – Переваги використання інформаційних технологій у внутрішньому контролі та захисті бізнесу

Перевага	Опис
1	2
Автоматизація	Зменшення ручної роботи, підвищення ефективності
Точність	Зменшення кількості помилок, підвищення правдивості даних
Швидкість	Прискорення процесів обробки інформації
Доступність	Можливість доступу до інформації з будь-якого місця з доступом до інтернету
Безпека	Захист інформації від несанкціонованого доступу
Прозорість	Відстеження всіх дій з інформацією
Масштабованість	Можливість адаптації до зростання бізнесу

Таблиця 4.8 – Ризики, пов’язані з використанням інформаційних технологій у внутрішньому контролі та захисті бізнесу

Ризик	Опис
1	2
Кібератаки	Несанкціонований доступ до інформаційних систем
Помилки програмного забезпечення	Збої в роботі систем, втрата даних
Вихід з ладу обладнання	Перебої в роботі, втрата даних
Несанкціонований доступ співробітників	Використання інформації не за призначенням
Залежність від технологій	Ризик зупинки бізнес-процесів при виході з ладу систем

Використання інформаційних технологій для забезпечення внутрішнього контролю та безпеки бізнесу є необхідним кроком для сучасних підприємств. Це дозволяє не тільки підвищити ефективність роботи, але й знизити ризики, пов’язані з шахрайством, кіберзагрозами та іншими видами злочинної діяльності.

Сучасні програмні продукти для автоматизації внутрішнього контролю часто включають такі функції:

– аналітика даних: виявлення аномалій, прогнозування, візуалізація даних,

– мобільний доступ: можливість доступу до системи з мобільних пристроїв,

– інтеграція з системами електронного документообігу,

– підтримка різних мов та валют,

– модульність: можливість налаштування системи під конкретні потреби.

Важливо розуміти, що вибір програмного продукту – це стратегічне рішення, яке вплине на ефективність системи внутрішнього контролю на довгі роки.

Таблиця 4.9 – Етапи впровадження інформаційних технологій у систему внутрішнього контролю та безпеки бізнесу

Етап	Опис
1	2
1. Аналіз поточних процесів	Оцінка існуючої системи внутрішнього контролю, виявлення слабких місць, визначення потреб в автоматизації.
2. Вибір програмного забезпечення	Вибір відповідного програмного забезпечення з урахуванням потреб та бюджету організації.
3. Розробка концепції впровадження	Створення детального плану впровадження, визначення відповідальних осіб, встановлення термінів.
4. Налаштування системи	Інсталяція та налаштування програмного забезпечення, інтеграція з наявними системами.
5. Навчання персоналу	Проведення тренінгів для співробітників, які будуть працювати з новою системою.
6. Пілотне впровадження	Тестування системи на невеликій частині процесів.
7. Повне впровадження	Перехід на повну роботу в новій системі.
8. Супровід та розвиток	Регулярне оновлення системи, надання технічної підтримки, розвиток системи відповідно до потреб бізнесу.

Таблиця 4.10 – Порівняння традиційної системи внутрішнього контролю та безпеки бізнесу та системи з використанням інформаційних технологій

Критерій	Традиційна система	Система з використанням ІТ
1	2	3
Швидкість обробки даних	Низька	Висока
Точність даних	Можливі помилки при ручній обробці	Висока точність завдяки автоматизації
Доступність інформації	Обмежений доступ, необхідність великої кількості паперових документів	Швидкий доступ до інформації з будь-якого місця
Безпека даних	Ризик втрати даних, несанкційованого доступу	Високий рівень безпеки завдяки технологіям захисту інформації
Вартість	Високі витрати на ручну роботу, зберігання документів	Високі початкові інвестиції, але низькі поточні витрати
Гнучкість	Труднощі зі швидкими змінами	Легкість адаптації до змін в бізнесі

Таблиця 4.11 – Загальне уявлення про функціональність різних типів програмних продуктів.

Характеристика	ERP-системи (SAP, Oracle)	Спеціалізовані системи внутрішнього контролю	Платформи автоматизації робочих процесів (BPA)
1	2	3	4
Основні функції	Облік, управління фінансами, виробництвом, логістикою. Вбудовані модулі контролю.	Спеціалізовані інструменти для планування, проведення та аналізу контрольних заходів.	Автоматизація рутинних задач, інтеграція з іншими системами.
Можливості	Глибока інтеграція різних бізнес-процесів, широкий функціонал.	Детальний аналіз ризиків, планування контрольних заходів, автоматизація збору доказів.	Гнучка конфігурація під конкретні потреби, швидка розробка нових процесів.
Вартість	Висока вартість ліцензії та впровадження.	Середня вартість, залежить від функціоналу.	Відносно невисока вартість, можливі варіанти хмарного розміщення.
Складність впровадження	Вимагає значних ресурсів та часу.	Менш складна, але потребує досвіду в області внутрішнього контролю.	Відносно проста, але може вимагати залучення фахівців.
Інтеграція з іншими системами	Хороша інтеграція з іншими модулями ERP-системи.	Може вимагати додаткової розробки для інтеграції.	Гнучка інтеграція з різними системами за допомогою API.
Типові користувачі	Фінансові директори, керівники підрозділів, аудитори.	Фахівці з внутрішнього контролю, аудитори.	Бізнес-аналітики, розробники.
Приклади використання	Контроль виконання бюджету, контроль якості продукції, оцінка ефективності інвестицій.	Планування і проведення аудиторських перевірок, моніторинг ризиків, оцінка ефективності контрольних заходів.	Автоматизація рутинних задач, таких як збір доказів, підготовка звітів.

Сучасні програмні продукти для автоматизації внутрішнього контролю часто включають такі функції:

– аналітика даних: виявлення аномалій, прогнозування, візуалізація даних,

– мобільний доступ: можливість доступу до системи з мобільних пристроїв,

– інтеграція з системами електронного документообігу,

– підтримка різних мов та валют,

– модульність: можливість налаштування системи під конкретні потреби.

Важливо розуміти, що вибір програмного продукту – це стратегічне рішення, яке вплине на ефективність системи внутрішнього контролю на довгі роки.



Питання для самоконтролю

1. Хто несе відповідальність за організацію та функціювання системи внутрішнього контролю на підприємстві?
2. Які основні завдання ревізійних комісій?
3. Які види відповідальності можуть бути застосовані до працівників за порушення внутрішніх правил?
4. Які основні види документів використовуються в системі внутрішнього контролю?
5. Які вимоги до оформлення контрольних документів?
6. Який термін зберігання контрольних документів?
7. Які основні інформаційні технології використовуються для забезпечення внутрішнього контролю?
8. Які переваги використання інформаційних технологій у системі внутрішнього контролю?

ЗМІСТОВИЙ МОДУЛЬ 3
МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ НА ПІДПРИЄМСТВІ ТА БЕЗПЕКИ БІЗНЕСУ

Тема 5. Види методичного забезпечення внутрішнього контролю на підприємстві та безпеки бізнесу

Мета вивчення теми полягає у розумінні студентами інструментів та підходів, які підприємства використовують для забезпечення ефективного внутрішнього контролю та захисту свого бізнесу.

План

5.1 Організаційне забезпечення внутрішнього контролю та безпеки бізнесу.
5.2 Законодавче забезпечення внутрішнього контролю та безпеки бізнесу.
5.3 Методичне забезпечення внутрішнього контролю та безпеки бізнесу.
5.4 Інформаційне забезпечення внутрішнього контролю та безпеки бізнесу.

Основні терміни та поняття: *обов'язки, дозволи, політика, корпоративна культура, комунікація, законодавство, методичне забезпечення, бази даних, мережі, програмні засоби*



5.1 Організаційне забезпечення внутрішнього контролю та безпеки бізнесу

Організаційне забезпечення є фундаментом для ефективної системи внутрішнього контролю. Воно передбачає створення структури, процесів та культури організації, що сприяють досягненню цілей бізнесу та мінімізації ризиків.

Таблиця 5.1 – Організаційне забезпечення внутрішнього контролю

Елемент організаційного забезпечення	Опис	Приклади
1	2	3
Розподіл обов'язків	Чітке розмежування функцій та відповідальностей між працівниками для запобігання конфлікту інтересів та можливості шахрайства.	Розподіл функцій між відділами закупівель, бухгалтерії та складу.
Сегрегація обов'язків	Розділення функцій авторизації, обробки та контролю операцій.	Один працівник готує платіжний документ, інший його підписує, третій проводить платіж.
Системи дозволів	Встановлення чітких правил доступу до інформації та ресурсів підприємства.	Системи паролів, ролевий доступ до інформаційних систем.
Політики компанії	Розробка та впровадження політик з питань безпеки, етики, конфлікту інтересів тощо.	Політика конфіденційності, політика щодо прийняття на роботу, кодекс етики.
Комісії з внутрішнього контролю	Створення спеціальних комісій для проведення регулярних перевірок та оцінки ефективності системи контролю.	Ревізійна комісія, комісія з етики.
Організаційна структура	Структура організації, що забезпечує ефективний контроль та координацію діяльності.	Лінійно-функціональна структура, матрична структура.
Корпоративна культура	Система цінностей, норм і правил поведінки, що сприяють дотриманню етичних стандартів і відповідального ставлення до роботи.	Проведення тренінгів з етики, заохочення співробітників за дотримання правил.
Комунікація	Ефективна комунікація між усіма рівнями організації щодо питань внутрішнього контролю.	Регулярні збори, інформаційні бюлетені, гаряча лінія.

Приклади організаційних заходів:

– розробка посадових інструкцій для кожного співробітника з чітким визначенням обов'язків та відповідальності,

– впровадження системи електронного документообігу для підвищення прозорості та контролю за рухом документів,

– проведення регулярних тренінгів для співробітників з питань внутрішнього контролю та безпеки,

– створення системи збору та аналізу зворотного зв'язку від співробітників щодо виявлених проблем та пропозицій щодо покращення.

Важливо розуміти, що організаційне забезпечення є динамічним процесом. Воно потребує постійного оновлення та адаптації до зміни внутрішнього та зовнішнього середовища організації.

Ефективне організаційне забезпечення є ключовим фактором успіху системи внутрішнього контролю. Воно забезпечує зменшення ризиків завдяки чіткому розподілу обов'язків та контролю за діяльністю, підвищення ефективності шляхом оптимізації процесів та усунення дублювання функцій, збільшення довіри: як з боку внутрішніх, так і зовнішніх стейкхолдерів, стійкість бізнесу завдяки здатності організації швидко адаптуватися до змін

5.2 Законодавче забезпечення внутрішнього контролю та безпеки бізнесу

Законодавче забезпечення є невіддільною частиною системи внутрішнього контролю. Воно встановлює мінімально допустимі стандарти та вимоги до організації та функціювання підприємств, зокрема до їх систем внутрішнього контролю.

Таблиця 5.2 – Законодавче забезпечення внутрішнього контролю

Вид законодавства	Опис	Приклади
1	2	3
Цивільне законодавство	Регулює загальні правовідносини між суб'єктами господарювання, включаючи відповідальність за заподіяння шкоди.	Цивільний кодекс України
Господарське законодавство	Регулює підприємницьку діяльність, включаючи ліцензування, банкрутство, захист конкуренції.	Господарський кодекс України, Закон України «Про підприємництво»
Трудове законодавство	Регулює трудові відносини, включаючи наймання, звільнення, оплату праці, охорону праці.	Кодекс законів про працю України
Податкове законодавство	Регулює порядок обчислення, сплати та контролю за сплатою податків і зборів.	Податковий кодекс України
Бухгалтерське законодавство	Регулює порядок ведення бухгалтерського обліку, складання фінансової звітності.	Закон України «Про бухгалтерський облік та фінансову звітність в Україні»

Банківське законодавство	Регулює діяльність банків та інших фінансових установ.	Закон України «Про банки і банківську діяльність»
Закони про захист персональних даних	Регулюють збір, обробку та захист персональних даних.	Закон України «Про захист персональних даних»

Значення законодавчого забезпечення для внутрішнього контролю та безпеки бізнесу:

– встановлення мінімальних стандартів: закони визначають обов'язкові вимоги до організації обліку, звітності, внутрішнього контролю тощо,

– захист прав та інтересів учасників господарських відносин: законодавство забезпечує рівні умови для всіх учасників ринку,

– створення стабільного бізнес-середовища: чіткі та зрозумілі правила гри сприяють розвитку підприємництва,

– забезпечення прозорості діяльності підприємств: публічність фінансової звітності та інших видів інформації підвищує довіру інвесторів.

Виклики дотримання законодавства: постійна зміна законодавства: створює необхідність постійного моніторингу змін у законодавстві та адаптації до них внутрішніх процедур, складність законодавства – велика кількість нормативно-правових актів, що регулюють різні аспекти діяльності підприємства, необхідність дотримання міжнародних стандартів бухгалтерського обліку та аудиту.

Забезпечити дотримання законодавства можна шляхом створення системи моніторингу змін у законодавстві, розробки внутрішніх документів, що відповідають законодавчим вимогам, проведення регулярних тренінгів для співробітників, залучення зовнішніх консультантів для оцінки відповідності діяльності підприємства законодавству, впровадження систем автоматизації обліку та звітності.

Законодавче забезпечення є важливим елементом системи внутрішнього контролю, але воно не є самодостатнім. Для забезпечення ефективного функціювання підприємства необхідно поєднувати дотримання законодавчих вимог з іншими видами забезпечення внутрішнього контролю (організаційним, технічним, фінансовим тощо) та безпеки бізнесу.

5.3 Методичне забезпечення внутрішнього контролю та безпеки бізнесу

Методичне забезпечення – це сукупність документів, інструкцій, процедур та алгоритмів, які детально описують, як здійснювати конкретні дії в межах системи внутрішнього контролю. Воно є своєрідним «посібником» для співробітників, який допомагає їм виконувати свої обов'язки відповідно до встановлених стандартів.

Вимоги до методичного забезпечення: методичні матеріали повинні постійно оновлюватися з урахуванням змін у законодавстві, внутрішніх процедурах та технологіях, повинні бути доступні для всіх співробітників, які

їх потребують, інструкції повинні бути написані простою і зрозумілою мовою, без використання спеціальних термінів. Методичні матеріали повинні охоплювати всі аспекти діяльності організації, пов'язані з внутрішнім контролем.

Таблиця 5.3 – Методичне забезпечення внутрішнього контролю та захисту бізнесу

Елемент методичного забезпечення	Опис	Приклади
1	2	3
Посадові інструкції	Детальний опис функціональних обов'язків, прав та відповідальності кожного співробітника.	Інструкція бухгалтера, інструкція менеджера з безпеки.
Процедури	Покрокові інструкції виконання певних дій.	Процедура затвердження договорів, процедура проведення інвентаризації.
Інструкції	Детальні вказівки щодо виконання окремих операцій або дотримання певних правил.	Інструкція з користування системою обліку, інструкція з охорони праці.
Форми документів	Зразки документів, які використовуються в роботі.	Форма акту приймання-передачі матеріальних цінностей, форма звіту про проведену перевірку.
Посібники	Довідкові матеріали з різних питань, пов'язаних з внутрішнім контролем.	Посібник з оцінки ризиків, посібник з проведення внутрішніх аудитів.
Регламенти	Документи, що встановлюють порядок виконання певних робіт або функцій.	Регламент проведення нарад, регламент затвердження інвестиційних проєктів.

Значення методичного забезпечення для внутрішнього контролю та безпеки бізнесу полягає в:

– єдиному підході до виконання всіх робіт, що сприяє підвищенню ефективності та якості,

– зменшенні помилок, бо детальні інструкції мінімізують ймовірність виникнення помилок,

– наявність чітких методичних матеріалів дозволяє швидко адаптувати нових співробітників до роботи,

– детальний опис процедур сприяє підвищенню прозорості діяльності організації.

Приклади використання методичного забезпечення:

1. Розробка стандартних операційних процедур (СОП) для виконання різних видів робіт.

2. Створення чек-листів для контролю якості виконання робіт.

3. Розробка алгоритмів для прийняття рішень в нестандартних ситуаціях.

4. Створення бази знань з питань внутрішнього контролю.

Методичне забезпечення є невіддільною частиною ефективної системи внутрішнього контролю. Воно дозволяє стандартизувати процеси, знизити ризики та підвищити ефективність роботи організації.

5.4 Інформаційне забезпечення внутрішнього контролю та безпеки бізнесу.

Інформаційне забезпечення є невіддільною частиною сучасних систем внутрішнього контролю. Воно передбачає використання інформаційних технологій для збору, обробки, зберігання та аналізу даних, необхідних для прийняття обґрунтованих управлінських рішень та забезпечення ефективної роботи організації.

Таблиця 5.4 – Інформаційне забезпечення внутрішнього контролю

Елемент інформаційного забезпечення	Опис	Приклади
1	2	3
Інформаційні системи	Програмні комплекси, що автоматизують різні бізнес-процеси.	ERP-системи, CRM-системи, системи електронного документообігу.
Бази даних	Структуровані набори даних, що використовуються для зберігання інформації.	База даних клієнтів, база даних матеріальних цінностей.
Мережі	Системи взаємозв'язку комп'ютерів та інших пристроїв.	Локальні мережі, глобальні мережі (Інтернет).
Засоби захисту інформації	Технічні та програмні засоби, що забезпечують безпеку інформації.	Антивіруси, системи контролю доступу.
Системи збору даних	Засоби для збору даних з різних джерел.	Сканери, датчики, системи відеоспостереження.
Системи аналізу даних	Програмні засоби для аналізу великих обсягів даних.	Системи бізнес-аналітики, системи прогнозування.

Роль інформаційного забезпечення у внутрішньому контролі полягає в:

– автоматизації процесів, зменшення кількості ручних операцій, що знижує ризик помилок,

– підвищенні ефективності, шляхом швидкого отримання необхідної інформації для прийняття рішень,

– поліпшенні якості даних, шляхом забезпечення точності та повноти даних,

– підвищенні рівня безпеки, шляхом захисту інформації від несанкційованого доступу.

– підтримці прийняття обґрунтованих рішень, шляхом надання аналітичної інформації для прийняття управлінських рішень.

Приклади використання інформаційного забезпечення:

1. Системи контролю доступу: обмеження доступу до інформаційних ресурсів лише авторизованим користувачам.
2. Системи електронного документообігу: автоматизація процесу обробки документів, забезпечення їхньої цілісності та доступності.
3. Системи відеоспостереження: контроль за доступом на територію підприємства, моніторинг виробничих процесів.
4. Системи аналізу фінансової звітності: виявлення відхилень від планових показників, виявлення ознак шахрайства.
5. Системи управління проєктами: контроль за виконанням проєктів, оцінка ефективності використання ресурсів.

Інформаційне забезпечення є потужним інструментом для підвищення ефективності систем внутрішнього контролю. Однак, необхідно пам'ятати, що інформаційні системи самі по собі не гарантують безпеку. Важливо поєднувати технічні засоби захисту з організаційними заходами та підвищенням обізнаності співробітників про інформаційну безпеку.



Питання для самоконтролю

1. Які основні елементи організаційної структури впливають на ефективність системи внутрішнього контролю?
2. Як розподіл обов'язків може запобігти шахрайству?
3. Яку роль відіграє корпоративна культура у забезпеченні внутрішнього контролю?
4. Які міжнародні стандарти впливають на українське законодавство у сфері внутрішнього контролю?
5. Які основні види методичних матеріалів використовуються в системах внутрішнього контролю? Які критерії оцінки якості методичних матеріалів?
6. Які інформаційні технології використовуються для забезпечення внутрішнього контролю?
7. Як забезпечити захист інформації в умовах цифрової трансформації?

ЗМІСТОВИЙ МОДУЛЬ 4

ОРГАНІЗАЦІЙНЕ ТА МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ВНУТРІШНЬОГО КОНТРОЛЮ НА ПІДПРИЄМСТВІ ТА БЕЗПЕКИ БІЗНЕСУ НА МІЖНАРОДНОМУ РІВНІ

Тема 6. Міжнародні стандарти внутрішнього контролю та безпеки бізнесу як організаційне та методичне забезпечення контролю та безпеки на міжнародному рівні

Мета вивчення теми: надати студентам розуміння важливості та ролі міжнародних стандартів у забезпеченні ефективного внутрішнього контролю та безпеки бізнесу на глобальному рівні.

План

6.1 Опис та порівняльний аналіз основних міжнародних стандартів внутрішнього контролю та безпеки бізнесу.

6.2 Впровадження міжнародних стандартів внутрішнього контролю та безпеки бізнесу: виклики та шляхи їх подолання.

Основні терміни та поняття: *внутрішній контроль, міжнародні стандарти, COSO, COBIT, ISO 27001, IIA, оцінка ризиків, інформаційна безпека.*



6.1 Опис та порівняльний аналіз основних міжнародних стандартів внутрішнього контролю та безпеки бізнесу.

У сучасному динамічному бізнес-середовищі, де ризики та виклики постійно зростають, ефективна система внутрішнього контролю є частиною успішного функціювання будь-якої організації. Для забезпечення єдиного розуміння принципів внутрішнього контролю та підвищення його ефективності були розроблені різноманітні міжнародні стандарти.

Серед найбільш відомих і широко використовуваних міжнародних стандартів внутрішнього контролю можна виділити наступні:

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission):** Цей стандарт пропонує комплексну модель внутрішнього контролю, яка складається з п’яти взаємопов’язаних компонентів: контрольне середовище, оцінка ризиків, контрольні заходи, інформація та комунікація, моніторинг. COSO є одним з найбільш визнаних і широко використовуваних стандартів у світі.
- **COBIT (Control Objectives for Information and related Technology):** Цей стандарт фокусується на управлінні інформаційними технологіями та забезпечує набір цілей контролю, що дозволяють організаціям ефективно використовувати та управляти IT-активами. COBIT часто використовується в поєднанні з COSO для забезпечення комплексного підходу до внутрішнього контролю.

- **ISO 27001:** Цей стандарт міжнародної організації зі стандартизації (ISO) встановлює вимоги до системи управління інформаційною безпекою. Він допомагає організаціям захистити конфіденційність, цілісність та доступність інформації.
- **IIA (Institute of Internal Auditors):** Міжнародний інститут внутрішніх аудиторів розробив Стандарти професійної практики внутрішнього аудиту, які визначають вимоги до проведення внутрішніх аудитів та оцінки ефективності системи внутрішнього контролю.

Таблиця 6.1 – Порівняльна таблиця міжнародних стандартів внутрішнього контролю

Стандарт	Фокус	Основні компоненти	Застосування
1	2	3	4
COSO	Комплексний підхід до внутрішнього контролю	5 компонентів: контрольне середовище, оцінка ризиків, контрольні заходи, інформація та комунікація, моніторинг	Широкий спектр організацій
COBIT	Управління інформаційними технологіями	Цілі контролю, процеси управління IT	Організації, що активно використовують IT
ISO 27001	Інформаційна безпека	14 розділів, що охоплюють різні аспекти інформаційної безпеки	Організації, які хочуть захистити свою інформацію
IIA	Внутрішній аудит	Стандарти професійної практики внутрішнього аудиту	Внутрішні аудитори

Кожен з розглянутих стандартів має свої особливості та фокусується на різних аспектах внутрішнього контролю. Вибір того чи іншого стандарту залежить від конкретних потреб організації, її розміру, сфери діяльності та рівня складності бізнес-процесів. Однак, всі ці стандарти мають одну спільну мету – допомогти організаціям досягти своїх цілей, знизити ризики та підвищити ефективність.

Переваги використання міжнародних стандартів внутрішнього контролю:

- Підвищення довіри інвесторів та партнерів: дотримання міжнародних стандартів свідчить про високий рівень корпоративного управління.
- Зменшення ризиків: ефективна система внутрішнього контролю допомагає виявляти та знижувати різноманітні ризики.
- Поліпшення ефективності бізнес-процесів: стандарти допомагають оптимізувати процеси та уникнути дублювання зусиль.
- Спрощення виходу на міжнародні ринки: дотримання міжнародних стандартів є важливою умовою для успішної діяльності на глобальному ринку.

Міжнародні стандарти внутрішнього контролю відіграють важливу роль у забезпеченні ефективного функціювання організацій. Вибір та впровадження

відповідного стандарту є стратегічним рішенням, яке потребує ретельного аналізу та врахування специфіки кожної організації.

6.2 Впровадження міжнародних стандартів внутрішнього контролю та безпеки бізнесу: виклики та шляхи їх подолання

Впровадження міжнародних стандартів внутрішнього контролю є складним і багатогранним процесом, який вимагає значних зусиль з боку організації. Попри численні переваги, пов'язані з підвищенням ефективності, прозорості та довіри, цей процес супроводжується рядом викликів.

Виклики впровадження:

– впровадження міжнародних стандартів вимагає значних фінансових і людських ресурсів. Необхідно виділити кошти на навчання персоналу, розробку нових процедур та систем, а також на залучення зовнішніх консультантів,

– впровадження нових стандартів часто вимагає зміни культури організації, Співробітники можуть опиратися змінам, особливо якщо вони пов'язані зі збільшенням їхньої відповідальності або зміною звичних способів роботи.

– не всі співробітники мають необхідні знання та навички для роботи в новій системі внутрішнього контролю. Це може вимагати додаткового навчання або залучення нових фахівців.

Таблиця 6.2 – Етапи впровадження міжнародних стандартів внутрішнього контролю

Етап	Опис	Дії
1	2	3
1. Аналіз початкового стану	Оцінка чинної системи внутрішнього контролю.	Проведення аудиту чинних процесів та процедур. Виявлення сильних і слабких сторін. Порівняння з вимогами обраного стандарту.
2. Розробка плану впровадження	Створення детального плану дій.	Визначення цілей впровадження. Розподіл відповідальності між підрозділами. Складання детального графіка робіт. Визначення необхідних ресурсів (людських, фінансових).
3. Навчання персоналу	Підвищення обізнаності співробітників про нові стандарти.	Розробка навчальних програм. Проведення тренінгів та семінарів. Оцінка засвоєння матеріалу.

4. Впровадження нових процедур і систем	Розробка та впровадження нових політик, процедур і систем.	Розробка нових документів (політики, інструкції). Модифікація чинних систем (ІТ-систем, бухгалтерського обліку). Тестування нових процедур.
5. Моніторинг та оцінка	Регулярна перевірка ефективності нової системи.	Встановлення системи моніторингу. Збір даних про ефективність. Аналіз отриманих даних. Внесення коригувань за необхідності.

Існує кілька підходів до впровадження міжнародних стандартів.

Таблиця 6.3 – Переваги та недоліки різних підходів

Підхід до впровадження	Переваги	Недоліки
1	2	3
«Великий вибух»	Швидке досягнення відповідності стандарту; чіткі терміни; мобілізація ресурсів.	Ризик перевантаження персоналу; висока ймовірність помилок; можливість спротиву змін.
Поетапне впровадження	Менший стрес для персоналу; можливість адаптації до змін; зниження ризиків.	Довші терміни впровадження; можливість відкладання важливих завдань.
Комбінований підхід	Об’єднання переваг обох підходів; гнучкість.	Вимагає ретельного планування та координації.

Вибір оптимального підходу залежить від таких факторів:

– розмір компанії: для великих компаній більш доцільним є поетапне впровадження,

– складність бізнес-процесів: чим складніші процеси, тим більше часу і ресурсів потрібно для їх зміни,

– готовність персоналу до змін: якщо співробітники готові до змін, можна застосувати швидкий підхід.

– внутрішні ресурси: наявність необхідних ресурсів (людських, фінансових, технологічних) впливає на вибір підходу.

Важливо розуміти, що жоден з цих підходів не є універсальним. Оптимальний вибір залежить від конкретних умов організації.

Роль топ-менеджменту в процесі впровадження міжнародних стандартів є вирішальною. Керівництво повинно:

– чітко сформулювати, чому організація вирішила впроваджувати стандарт і які результати очікує отримати,

– виділити необхідні фінансові та людські ресурси для успішного впровадження,

– створити культуру, яка підтримує зміни та заохочує співробітників до активної участі в процесі,

– регулярно інформувати співробітників про хід впровадження і відповідати на їхні запитання.

Впровадження міжнародних стандартів внутрішнього контролю є складним, але необхідним процесом для сучасних організацій. Для успішного впровадження необхідно враховувати особливості організації, залучати всіх співробітників, забезпечити необхідні ресурси та створити сприятливе середовище для змін. Результатом цього процесу стане підвищення ефективності, прозорості та конкурентоспроможності організації.



Питання для самоконтролю

1. Що таке міжнародні стандарти внутрішнього контролю і яка їхня основна мета?
2. Яку роль відіграють міжнародні стандарти у забезпеченні безпеки бізнесу?
3. Які переваги дає використання міжнародних стандартів для підприємств?
4. Які основні виклики виникають при впровадженні міжнародних стандартів?
5. Які найбільш відомі міжнародні стандарти внутрішнього контролю та в чому їхні відмінності?
6. Як міжнародні стандарти впливають на організаційну структуру підприємства?
7. Яку роль відіграє вище керівництво в процесі впровадження міжнародних стандартів?
8. Як розподіляється відповідальність за дотримання міжнародних стандартів між різними підрозділами підприємства?

Тема 7. Аналіз міжнародних стандартів внутрішнього контролю та безпеки бізнесу

Мета вивчення теми полягає в наданні студентам розуміння сучасних міжнародних стандартів, які регулюють системи внутрішнього контролю та безпеки бізнесу.

План

7.1 COSO: Комплексний підхід до внутрішнього контролю та безпеки бізнесу.

7.2 COBIT: Фокус на інформаційних технологіях та інтеграція з COSO.

7.3 COBIT: Основні принципи та аспекти інформаційної безпеки.

7.4 Стандарти IIA: Надійний орієнтир для внутрішнього аудиту.

Основні терміни та поняття: *COSO, COBIT, COBIT, стандарти IIA, управління ризиками, корпоративна governance, контрольне середовище, структура управління, комітет з аудиту*



7.1 COSO: Комплексний підхід до внутрішнього контролю та безпеки бізнесу.

Концепція COSO (Committee of Sponsoring Organizations of the Treadway Commission) виникла як відповідь на численні фінансові скандали, які потрясли бізнес-світ у 80-х роках минулого століття. Ці події підкреслили необхідність вдосконалення систем внутрішнього контролю в організаціях для забезпечення надійності фінансової звітності та запобігання шахрайству.

Створення Комісії Тредвея та розробка першого звіту COSO в 1992 році стало знаковим моментом у розвитку теорії та практики внутрішнього контролю. Цей звіт запропонував інтегрований підхід до внутрішнього контролю, визначивши п’ять взаємопов’язаних компонентів, які повинні бути присутні в будь-якій ефективній системі контролю.

Основні етапи розвитку COSO:

- 1992 рік: Публікація першого звіту COSO «Internal Control – Integrated Framework», який став основою для розробки стандартів внутрішнього контролю у багатьох країнах світу.
- 2013 рік: Оновлення звіту COSO з метою врахування змін у бізнес-середовищі та нових викликів, таких як глобалізація, технологічні зміни та зростання кіберзагроз.
- 2017 рік: Публікація звіту COSO ERM (Enterprise Risk Management – Integrated Framework), який розширив концепцію COSO, включивши в неї управління ризиками на рівні всієї організації.

Концепція COSO стала такою популярною через:

– комплексний підхід: COSO пропонує інтегровану модель, яка охоплює всі аспекти внутрішнього контролю,

– гнучкість: концепція COSO може бути адаптована до різних розмірів і типів організацій,

– міжнародне визнання: COSO стала міжнародним стандартом, який визнається регуляторами та інвесторами у всьому світі,

– постійна еволюція: COSO постійно розвивається, щоб відповідати новим викликам і потребам бізнесу.

Концепція COSO:

✓ забезпечила спільну мову для обговорення та оцінки систем внутрішнього контролю,

✓ сприяла підвищенню обізнаності керівництва та співробітників про важливість внутрішнього контролю,

- ✓ допомогла підвищити довіру до фінансової звітності компаній,
- ✓ завдяки COSO організації можуть ефективніше ідентифікувати, оцінювати та управляти ризиками.

Концепція COSO стала фундаментом сучасних систем внутрішнього контролю та безпеки бізнесу. Вона забезпечила організаціям інструменти для побудови ефективних і стійких систем контролю, які допомагають запобігати шахрайству, забезпечувати дотримання нормативних вимог і підвищувати довіру інвесторів. Попри свою популярність, COSO продовжує розвиватися, щоб відповідати новим викликам, які постають перед бізнесом у 21 столітті.

П’ять компонентів COSO

1 Компонент

Контрольне середовище: фундамент системи внутрішнього контролю за версією COSO.

Контрольне середовище – це перший і, мабуть, найважливіший компонент моделі COSO для оцінки та вдосконалення систем внутрішнього контролю. Воно встановлює тон для всієї організації, формуючи основу, на якій будуються інші компоненти системи. Контрольне середовище визначає культуру, цінності та загальний підхід до управління ризиками та забезпечення дотримання стандартів.

1. Культура організації, етика, цінності.

Культура організації – це сукупність цінностей, норм поведінки, переконань та припущень, які поділяють співробітники компанії. Саме культура визначає, як співробітники сприймають важливість контролю, чи готові вони дотримуватися встановлених правил та процедур. Сильна етична культура, яка підкреслює важливість чесності, прозорості та відповідальності, є ключовим фактором для ефективного функціювання системи внутрішнього контролю. Коли співробітники поділяють цінності компанії, вони більш схильні дотримуватися встановлених правил і процедур.

2. Структура управління та повноваження.

Структура управління та розподіл повноважень безпосередньо впливають на ефективність системи внутрішнього контролю. Чітко визначені ролі та відповідальність кожного співробітника сприяють прозорості прийняття рішень та уникненню конфліктів. Ефективна система делегування повноважень дозволяє розвантажити керівництво і залучити до процесу прийняття рішень більшу кількість співробітників.

3. Комітет з аудиту

Комітет з аудиту – це незалежний орган, який наглядає за фінансовою звітністю, системою внутрішнього контролю та аудиторською діяльністю. Він відіграє важливу роль у забезпеченні цілісності фінансової інформації та довіри до компанії. Комітет з аудиту оцінює ефективність системи внутрішнього контролю, забезпечує дотримання вимог законодавства та регуляторних органів, а також надає рекомендації щодо вдосконалення системи.

Чому контрольне середовище так важливо? Бо це:

– фундамент для інших компонентів: контрольне середовище створює основу для інших компонентів системи внутрішнього контролю, без сильної культури та чітко визначених ролей та відповідальності інші компоненти не будуть ефективно працювати,

– підвищення обізнаності: сильне контрольне середовище сприяє підвищенню обізнаності співробітників про важливість внутрішнього контролю та їхньої ролі в забезпеченні його ефективності,

– зменшення ризиків: добре розроблене контрольне середовище допомагає знизити ризик виникнення помилок, шахрайства та інших небажаних подій,

– поліпшення репутації: сильна культура організації та ефективна система внутрішнього контролю підвищують довіру інвесторів, клієнтів та інших зацікавлених сторін.

Контрольне середовище є фундаментом для побудови ефективної системи внутрішнього контролю. Воно визначає культуру організації, структуру управління та роль комітету з аудиту. Інвестуючи в створення сильного контрольного середовища, компанії можуть значно знизити ризики, підвищити свою ефективність та довіру до своєї діяльності.

2 Компонент

Оцінка ризиків: серцевина системи внутрішнього контролю за версією COSO.

Оцінка ризиків – це другий за важливістю компонент моделі COSO після контрольного середовища. Він передбачає систематичне виявлення, аналіз та управління різноманітними загрозами, які можуть перешкоджати досягненню цілей організації.

1. *Ідентифікація ризиків* – це перший крок у процесі оцінки ризиків. Він передбачає виявлення всіх потенційних подій, які можуть вплинути на досягнення цілей організації. Це можуть бути як внутрішні ризики (наприклад, помилки персоналу, неефективні процеси), так і зовнішні (наприклад, зміни законодавства, економічні кризи, природні катаклізми). Для ефективної ідентифікації ризиків можуть використовуватися різноманітні методи, такі як мозковий штурм, аналіз сценаріїв, опитування співробітників тощо.

2. *Аналіз ризиків* – це детальне дослідження ідентифікованих ризиків. Він передбачає оцінку ймовірності виникнення кожного ризику та потенційних наслідків. Для цього можуть використовуватися кількісні та якісні методи. Кількісні методи дозволяють оцінити ризики в грошовому вираженні, що дозволяє порівняти різні ризики між собою. Якісні методи дозволяють оцінити ризики за допомогою таких категорій, як високий, середній та низький.

3. *Відповідні заходи реагування* – це розробка та впровадження заходів для управління виявленими ризиками. Ці заходи можуть бути спрямовані на зниження ймовірності виникнення ризику, зменшення його наслідків або повне уникнення ризику. Вибір конкретних заходів залежить від характеру ризику та ресурсів організації.

Чому оцінка ризиків так важлива? Оцінка ризиків дозволяє організації перейти від реактивного до проактивного управління. Замість того, щоб чекати, поки проблема виникне, організація може вжити заходів для її запобігання. Оцінка ризиків допомагає зосередити ресурси на найбільш важливих ризиках, що дозволяє підвищити ефективність використання ресурсів. Розуміння ризиків, з якими стикається організація, допомагає приймати більш обґрунтовані рішення. Ефективна система управління ризиками допомагає організації стати більш стійкою до зовнішніх потрясінь.

Оцінка ризиків є невід'ємною частиною системи внутрішнього контролю. Вона дозволяє організації виявити потенційні загрози, оцінити їхній вплив і розробити ефективні заходи для їх управління. Регулярна оцінка ризиків є ключем до успішного досягнення цілей організації.

3 Компонент

Контрольні заходи: щит, який захищає бізнес.

Контрольні заходи є невіддільною частиною системи внутрішнього контролю будь-якої організації. Вони слугують своєрідним щитом, який захищає бізнес від різних загроз та забезпечує досягнення поставлених цілей. Згідно з моделлю COSO, контрольні заходи поділяються на три основні категорії: попереджувальні, виправні та ті, що виявлять.

Попереджувальні контролі – це перша лінія оборони, яка спрямована на запобігання виникненню небажаних подій. Вони діють за принципом профілактики, тобто передбачають вжиття заходів до того, як проблема виникне. Прикладами попереджувальних контролів можуть бути:

– розподілення обов'язків, з метою уникнення концентрації повноважень в одних руках,

– встановлення процедур затвердження документів кількома особами для підвищення точності та повноти інформації,

– встановлення обмежень доступу до інформаційних систем та фізичних активів для запобігання несанкційованого доступу,

– перевірка репутації та фінансової стабільності потенційних постачальників перед укладенням договорів.

Виправні контролі – це заходи, які вживаються після того, як небажана подія вже сталася. Їхньою метою є мінімізація негативних наслідків та відновлення нормального функціювання системи. Прикладами виправних контролів можуть бути:

– розробка процедур відновлення даних у разі їх втрати або пошкодження,

– страхування від різних ризиків, таких як пожежа, крадіжка, відповідальність перед третіми особами,

– створення резервних копій важливої інформації для відновлення у разі потреби,

– розробка планів реагування на різні надзвичайні ситуації, такі як природні катаклізми, кібератаки тощо.

Контролі, що виявляють – це заходи, спрямовані на своєчасне виявлення небажаних подій. Вони дозволяють вжити необхідні заходів для усунення проблеми та запобігання її повторенню. Прикладами контролів, що виявляють можуть бути:

– порівняння даних з різних джерел для виявлення розбіжностей,

– проведення регулярних внутрішніх аудитів для оцінки ефективності системи контролю,

– аналіз відхилень фактичних показників від планових для виявлення потенційних проблем,

– аналіз скарг клієнтів для виявлення проблем у процесах обслуговування.

Ефективні контрольні заходи є необхідною умовою для забезпечення надійності фінансової звітності, дотримання нормативних вимог та захисту активів організації. Вони допомагають: ідентифікувати та знизити ризики, які можуть негативно вплинути на діяльність організації, дотримуватися вимог законодавства та регуляторних органів, оптимізувати бізнес–процеси та підвищити ефективність використання ресурсів, запобігти виникненню негативних ситуацій, які можуть пошкодити репутацію організації.

Контрольні заходи є невіддільною частиною системи внутрішнього контролю. Вони забезпечують захист організації від різних загроз та сприяють досягненню її цілей. Для забезпечення ефективності системи контролю необхідно постійно оцінювати та вдосконалювати контрольні заходи, адаптуючи їх до зміни зовнішнього середовища та внутрішніх потреб організації.

4 Компонент

Четвертий компонент моделі COSO – інформація та комунікація – є жилою системою внутрішнього контролю. Він забезпечує ефективний збір, обробку, зберігання та передачу інформації, необхідної для прийняття обґрунтованих рішень та забезпечення дотримання встановлених стандартів.

1. Системи збору, обробки та зберігання інформації.

Цей під компонент стосується всіх аспектів обробки даних в організації. Ефективна система обліку та звітності забезпечує правдивість, повноту та своєчасність даних. Інформація, що використовується для прийняття рішень, повинна бути точною та вільною від помилок, повинна бути зібрана та оброблена, доступна вчасно для прийняття рішень. Доступ до інформації повинний бути наданий тим співробітникам, яким це необхідно для виконання своїх обов’язків.

Сучасні інформаційні технології надають широкий спектр інструментів для збору, обробки та зберігання інформації. Однак, важливо не лише мати технічні засоби, але й забезпечити їх правильне використання та підтримку.

2. Внутрішня та зовнішня комунікація.

Ефективна комунікація є ключовим фактором для успішного функціювання будь-якої організації. В контексті системи внутрішнього контролю, комунікація забезпечує: розуміння цілей, обмін інформацією,

зворотний зв’язок, комунікацію з зовнішніми сторонами. Співробітники повинні чітко розуміти цілі та завдання системи внутрішнього контролю. інформація повинна вільно циркулювати між усіма рівнями організації, співробітники повинні мати можливість висловлювати свої думки та пропозиції щодо вдосконалення системи внутрішнього контролю. Організація повинна ефективно комунікувати з регуляторними органами, аудиторами та іншими зацікавленими сторонами.

Чому інформація та комунікація так важливі?

По-перше, це: основа для прийняття рішень, тому що інформація є основою для прийняття обґрунтованих рішень на всіх рівнях організації.

По-друге, це: забезпечення дотримання встановлених стандартів та процедур.

По-третє, це: виявлення проблем для своєчасного прийняття заходів для їх усунення.

Вчетверте, це: підвищення ефективності роботи організації.

Інформація та комунікація є невіддільною частиною системи внутрішнього контролю. Вони забезпечують ефективний збір, обробку, зберігання та передачу інформації, необхідної для прийняття обґрунтованих рішень та забезпечення дотримання встановлених стандартів. Інвестуючи в розвиток системи інформації та комунікації, організації можуть значно підвищити свою ефективність та знизити ризики.

5 Компонент

1. Моніторинг: Серцебиття системи внутрішнього контролю

П’ятий компонент моделі COSO – моніторинг – є своєрідним пульсом системи внутрішнього контролю. Він забезпечує постійний контроль за ефективністю всіх попередніх компонентів та дозволяє своєчасно виявляти та усувати недоліки.

Безперервний моніторинг

Безперервний моніторинг передбачає постійний контроль за функціюванням системи внутрішнього контролю.

Це охоплює:

– регулярні перевірки: проведення регулярних перевірок дотримання встановлених процедур та стандартів,

– аналіз звітів: аналіз фінансової та операційної звітності для виявлення відхилень від планових показників,

– моніторинг показників ефективності: відстеження ключових показників ефективності (KPI) для оцінки ефективності роботи різних підрозділів,

– аналіз інцидентів: аналіз інцидентів, які відбулися, для виявлення причин та розробки заходів для запобігання їх повторення.

2. Оцінка ефективності

Оцінка ефективності системи внутрішнього контролю проводиться з метою визначення того, наскільки система досягає поставлених цілей. Вона

дозволяє виявити слабкі місця та розробити заходи для їх усунення. Оцінка ефективності може проводитися за допомогою різних методів, таких як:

– самооцінка і це означає, що співробітники самостійно оцінюють ефективність системи внутрішнього контролю у своїх підрозділах,

– внутрішні аудити потребують проведення регулярних внутрішніх аудитів для оцінки ефективності системи в цілому,

– зовнішні аудити, які полягають у залученні зовнішніх аудиторів для проведення незалежної оцінки системи.

Моніторинг так важливий, тому що:

– дозволяє виявляти проблеми на ранніх стадіях, коли їх ще легко усунути,

– результати моніторингу використовуються для постійного вдосконалення системи внутрішнього контролю,

– ефективна система моніторингу підвищує довіру інвесторів, клієнтів та інших зацікавлених сторін.

Моніторинг є завершальним етапом циклу управління ризиками. Він забезпечує постійний контроль за ефективністю системи внутрішнього контролю та дозволяє своєчасно виявляти та усувати недоліки. Ефективна система моніторингу є гарантією того, що система внутрішнього контролю відповідає поточним потребам організації та забезпечує досягнення її цілей.

Всі п’ять компонентів COSO тісно пов’язані між собою і утворюють єдину систему. Наприклад, ефективне контрольне середовище створює основу для проведення оцінки ризиків, а інформація та комунікація необхідні для моніторингу контрольних заходів.

Модель COSO є універсальним інструментом для оцінки та вдосконалення систем внутрішнього контролю. Вона допомагає організаціям зменшити ризики, поліпшити якість фінансової звітності, забезпечити дотримання нормативних вимог, підвищити довіру інвесторів та інших зацікавлених сторін.

7.2 COBIT: Фокус на інформаційних технологіях та інтеграція з COSO

COBIT (Control Objectives for Information and related Technology) – це всеосяжна рамка, розроблена для забезпечення ефективного управління та контролю інформаційними та пов’язаними з ними технологіями (IT). На відміну від більш загальних рамок, таких як COSO, COBIT зосереджується на конкретних аспектах IT, надаючи детальні керівництва та цілі контролю для різних IT-процесів.

Основні цілі COBIT:

– забезпечення адекватності, ефективності та ефективності IT: COBIT допомагає організаціям гарантувати, що їхні IT-системи підтримують бізнес-цілі та функціюють ефективно,

– управління ризиками, пов’язаними з IT: рамка допомагає ідентифікувати, оцінювати та управляти ризиками, пов’язаними з IT, такими як кібербезпека, доступність даних та відповідність нормативним вимогам.

– оптимізація використання ресурсів: COBIT надає рекомендації щодо оптимізації використання IT-ресурсів, таких як персонал, бюджет та технології.

– підвищення довіри до IT: завдяки прозорості та відповідальності, яку забезпечує COBIT, організації можуть підвищити довіру до своїх IT-систем у зацікавлених сторін.

COBIT структурований навколо набору процесів, які охоплюють весь життєвий цикл IT-сервісів. Ці процеси поділяються на чотири основні домени:

- Планування та організація: визначення стратегічних цілей IT, розробка портфеля проєктів, управління програмами та проєктами.
- Оцінка та обґрунтування: оцінка вимог до IT-сервісів, управління ризиками, управління послугами.
- Отримання, розробка та доставлення: розробка та впровадження нових IT-систем, управління змінами, забезпечення якості.
- Моніторинг та оцінка: моніторинг ефективності IT-сервісів, оцінка досягнення цілей, управління інцидентами.

Кожен з цих доменів складається з більш детальних процесів, які надають практичні рекомендації щодо їх виконання.

COSO та COBIT – це доповнювальні рамки, які можуть бути ефективно інтегровані для забезпечення комплексного управління ризиками та контролю в організації.

✓ COSO надає загальну модель внутрішнього контролю, яка охоплює всі аспекти діяльності організації, включаючи фінанси, операції та дотримання нормативних вимог.

✓ COBIT зосереджується на конкретних аспектах IT, надаючи детальні рекомендації щодо управління IT-ризиками та забезпечення ефективності IT-процесів.

Інтеграція COBIT з COSO дозволяє:

– забезпечити комплексне управління ризиками, організації можуть ідентифікувати та управляти ризиками, пов’язаними з IT, в контексті загальної системи внутрішнього контролю,

– поліпшити ефективність IT, COBIT допомагає оптимізувати використання IT-ресурсів та забезпечувати відповідність IT-процесів бізнес-цілям,

– ефективний контроль IT сприяє забезпеченню правдивості фінансової інформації.

Шляхи інтеграції:

– COBIT може бути використаний для більш детального опису того, як контрольні заходи реалізуються в IT-сфері,

– цілі COBIT можуть бути включені до загальної системи цілей організації, що визначається в рамках COSO,

– обидві рамки використовують схожу методологію, що полегшує їх інтеграцію.

Таблиця 7.1 – Інтеграція COBIT з COSO: Табличне порівняння та синергія

Аспект	COSO	COBIT	Інтеграція COSO та COBIT
Фокус	Загальна рамка внутрішнього контролю, охоплює всі аспекти діяльності організації	Зосереджується на управлінні інформаційними технологіями та пов’язаними з ними процесами	Комплексне управління ризиками та контролем, з особливим акцентом на IT
Компоненти	Контрольне середовище, оцінка ризиків, контрольні заходи, інформація та комунікація, моніторинг	Планування та організація, оцінка та обґрунтування, отримання, розробка та доставлення, моніторинг та оцінка	Комбінація компонентів обох рамок для забезпечення всеосяжного контролю
Цілі	Забезпечення досягнення цілей організації, захист активів, забезпечення правдивості фінансової звітності	Забезпечення ефективності та ефективності IT, управління ризиками, пов’язаними з IT	Досягнення цілей організації за допомогою ефективного використання IT
Застосування	Всі види організацій	Організації, які хочуть оптимізувати свої IT-процеси та управління ризиками, пов’язаними з IT	Організації, які хочуть інтегрувати IT в загальну систему внутрішнього контролю
Синергія			Посилення загальної ефективності системи внутрішнього контролю, зниження ризиків, пов’язаних з IT, підвищення довіри до фінансової звітності

COBIT є потужним інструментом для управління інформаційними технологіями. Інтеграція COBIT з COSO дозволяє організаціям забезпечити комплексне управління ризиками та контролем, підвищити ефективність IT та довіру до фінансової звітності.

7.3 ISO 27001: Основні принципи та аспекти інформаційної безпеки

ISO 27001 – це міжнародний стандарт, який встановлює вимоги до системи управління інформаційною безпекою (СУІБ) організації. Це як інструкція з будівництва надійного замку для ваших даних, який захистить їх від будь-яких загроз.

У наш час інформація – це один з найцінніших активів будь-якої компанії. Її втрата або витік можуть призвести до серйозних фінансових втрат, пошкодження репутації та навіть кримінальної відповідальності. ISO 27001 допомагає мінімізувати такі ризики.

Основні принципи ISO 27001:

– системний підхід, вся система управління інформаційною безпекою розглядається як єдине ціле,

– цикл PDCA: постійне вдосконалення системи через планування, виконання, перевірку та дію,

– ризикорієнтований підхід: ідентифікація, оцінка та управління всіма можливими загрозами для інформаційної безпеки.

Стандарт охоплює широкий спектр аспектів інформаційної безпеки, включаючи:

1. Організаційні заходи: політики, процедури, відповідальність тощо.
2. Персонал: навчання, обізнаність, перевірки.
3. Фізичний захист: захист приміщень, обладнання, носіїв інформації.
4. Мережева безпека: захист комп'ютерних мереж від несанкційованого доступу.
5. Управління доступом: контроль доступу до інформаційних ресурсів.
6. Управління інцидентами: виявлення, реагування та розслідування інцидентів інформаційної безпеки.
7. Безперервність бізнесу: забезпечення безперебійної роботи критично важливих систем.

Переваги сертифікації ISO 27001:

– демонстрація високого рівня захисту інформації,

– відповідність міжнародним стандартам підвищує довіру партнерів,

– систематичний підхід до управління ризиками,

– єдина основа для проведення аудиту інформаційної безпеки.

– демонстрація відповідального ставлення до захисту інформації.

ISO 27001 підходить для будь-якої організації, яка обробляє конфіденційну інформацію. Незалежно від розміру та сфери діяльності, цей стандарт допоможе забезпечити належний рівень захисту даних.

Для отримання сертифікату необхідно:

1. Розробити систему управління інформаційною безпекою: впровадити всі вимоги стандарту.
2. Провести внутрішній аудит: перевірити відповідність системи стандарту.
3. Запросити зовнішній аудит: незалежний орган сертифікації проведе оцінку системи.
4. Отримати сертифікат: при успішному проходженні аудиту організація отримує сертифікат.

Сертифікація ISO 27001 – це не одноразова подія, а постійний процес. Система управління інформаційною безпекою повинна постійно розвиватися та вдосконалюватися.

7.4 Стандарти IIA: Надійний орієнтир для внутрішнього аудиту

IIA (Institute of Internal Auditors) – це міжнародна організація, яка встановлює стандарти професійної практики внутрішнього аудиту. Стандарти IIA є своєрідним «кодексом поведінки» для внутрішніх аудиторів, визначаючи їхню роль, відповідальність та вимоги до якості роботи.

Стандарти IIA важливі та актуальні, тому що:

– стандарти забезпечують єдиний підхід до проведення внутрішнього аудиту в різних організаціях по всьому світу,

– завдяки стандартам підвищується якість роботи внутрішніх аудиторів та правдивість їхніх висновків,

– стандарти підкреслюють важливість професіоналізму та об'єктивності внутрішніх аудиторів,

– стандарти підвищують довіру до функції внутрішнього аудиту з боку керівництва та інших зацікавлених сторін.

Основні компоненти стандартів IIA:

– принципи: визначають фундаментальні поняття та цінності внутрішнього аудиту,

– заяви про базові вимоги: конкретизують принципи та встановлюють мінімально необхідні вимоги до проведення внутрішнього аудиту,

– атрибутивні стандарти: описують характеристики організацій та осіб, що здійснюють внутрішній аудит,

– стандарти ефективності: визначають, як оцінювати ефективність діяльності внутрішнього аудиту.

Основні цілі внутрішнього аудиту відповідно до стандартів IIA:

1. Допомога організації досягати своїх цілей: Внутрішній аудит має бути орієнтований на додану вартість для організації.

2. Оцінка та покращення системи контролю: Внутрішній аудит аналізує систему внутрішнього контролю та пропонує рекомендації щодо її вдосконалення.

3. Забезпечення дотримання законів та нормативних актів: Внутрішній аудит перевіряє, чи дотримується організація вимог законодавства.

4. Об'єктивна оцінка ризиків: Внутрішній аудит оцінює ризики, з якими стикається організація.

У січні 2024 року Інститут внутрішніх аудиторів представив нові Глобальні стандарти внутрішнього аудиту (Global Internal Audit Standards IIA™), які набирають чинності з 9 січня 2025 року. Нові стандарти більш орієнтовані на майбутнє та враховують зміни в бізнес-середовищі.

Дотримання стандартів IIA гарантує, що функція внутрішнього аудиту виконує свою роль ефективно та професійно. Це також сприяє підвищенню довіри до внутрішнього аудиту з боку керівництва, акціонерів та інших зацікавлених сторін.



Питання для самоконтролю

1. Які основні відмінності між новими та попередніми стандартами IIA?
2. Як стандарти IIA пов'язані з іншими стандартами (наприклад, ISO 27001)?
3. Які вимоги до кваліфікації внутрішніх аудиторів встановлюють стандарти IIA?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Внутрішній аудит : навч. посіб. / за ред. Ю. Б. Слободяник. Суми : ТОВ «ВПП «Фабрика друку», 2018. 248 с.
2. Каменська Т. О., Редько О. Ю. Внутрішній контроль і аудит в управлінні : практ. посіб. наук. шк. аудиту, Нац. Центр Обліку та Аудиту. Київ : ДП «Інформ.-аналіт. агентство», 2015. 375 с.
3. Немченко В.В., Хомутенко В.П., Хомутенко А.В. Практичний курс внутрішнього аудиту : підручник / за ред. Немченко В.В. Київ : Центр учбової літератури, 2008. 240 с.
4. Гуцаленко Л. В., Коцупатрий М. М., Марчук У. О. Внутрішньогосподарський контроль : навч. посіб. Київ : Центр уч. літератури, 2014. 496 с.
5. Гуцаленко Л. В., Коцупатрий М. М., Марчук У. О. Внутрішньогосподарський контроль : навч. посіб. Електронні дані. Київ : Центр учбової літератури, 2014. URL: http://10.0.2.150/docs/CUL/Vnutr_gospod_kontrol.pdf.
6. Іванюта П. В., Левченко З. М. Внутрішньогосподарський (управлінський) облік у виробничих підрозділах сільськогосподарських господарюючих суб'єктів : навч. посіб. Київ : Центр навч. літератури, 2006. 368 с.
7. Ковальчук С. П. Внутрішньогосподарський контроль : опорний конспект лекцій. Вінниця : Редакційно-видавничий відділ ВТЕІ КНТЕУ, 2019. 114 с.
8. Ковальчук С. П. Внутрішньогосподарський контроль : опорний конспект лекцій. Електронні дані. Вінниця : Редакційно-видавничий відділ ВТЕІ КНТЕУ, 2019. URL: http://10.0.2.150/docs/2019/125_2019/Vnutrishnohospodarskyi kontrol.pdf.
9. Moeller, Robert R. Brink's modern internal auditing: a common body of knowledge / Robert Moeller. 7th ed. Wiley, 2009. 792 p.

Інформаційні джерела:

1. Аудитор України: фахове видання URL: http://www.auditorukr.com.ua/journal/.

2. Інститут внутрішніх аудиторів України. URL: https://iia-ua.org/?tag=%D1%96%D0%B2%D0%B0%D1%83.
3. Методологічні вказівки з внутрішнього аудиту в державному секторі України. URL : http://surl.li/lklw.
4. Міжнародні стандарти аудиту. URL: http://surl.li/lkme.
5. Міністерство фінансів України. URL: http://surl.li/lklq.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Замула І. В., Танасієва М. М. Внутрішній контроль : навч. посіб. Чернівці : Технодрук, 2021. 336 с.
2. Меліхова Т. О. Економічна безпека підприємства: формування, контроль, ефективність : монографія. Херсон, Видавничий дім «Гельветика», 2018. 632 с.
3. Пашкевич М. С., Шишкова Н. Л. Контроль: незалежний, внутрішній, державний : навч. посіб. : у 2 ч. Ч. 1. Незалежний аудиторський та внутрішньогосподарський контроль. М-во освіти і науки України, Нац. гірн. ун-т. Дніпро : НГУ, 2017. 182 с. URL: http://nmu.org.ua

Навчальне видання
(*українською мовою*)

Сейсебаєва Наталія Григорівна

ВНУТРІШНІЙ КОНТРОЛЬ НА ПІДПРИЄМСТВІ ТА БЕЗПЕКА БІЗНЕСУ

Курс лекцій
для здобувачів ступеня вищої освіти магістра
спеціальності 071 «Облік і оподаткування»
освітньо-професійної програми «Облік і аудит»

Рецензент *Т. І. Батракова*
Відповідальний за випуск *Н. М. Проскуріна*
Коректор *Н. Г. Сейсебаєва*