МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ФІНАНСІВ ТА ОБЛІКУ
КАФЕДРА ОБЛІКУ І ОПОДАТКУВАННЯ

Макар Андрій Іванович

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА НА НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ РІВНЯХ: ОБЛІКОВО-АНАЛІТИЧНИЙ АСПЕКТ

Спеціальність 071 – Облік і ополаткування

Кваліфікаційна робота за ступенем освіти «магістр»

Студент групи ОМОм-22
Макар А.І.
_____

Науковий керівник
к.е.н., доцент Фаріон В. Я.
_____

Кваліфікаційну роботу допущено до захисту:

«____» _____ 2024 р.

Зав. кафедри обліку і оподаткування
д.е.н., професор
Задорожний З.-М. В. _____

ТЕРНОПІЛЬ – 2024

ЗМІСТ

ВСТУП

Ефективне функціонування суб’єктів підприємництва сьогодні залежить від того, наскільки якісно та оперативно керівництво приймає рішення, опираючись на ретельний аналіз інформації про внутрішнє та зовнішнє середовище. У зв'язку зі зростанням інформаційних технологій та загальною інформатизацією суспільства, значення інформації в економіці і суспільстві взагалі зросло. Інформація стала одним з найважливіших ресурсів управління разом із людськими, фінансовими та матеріальними ресурсами. Зростаюча важливість інформації призвела до створення інформаційного простору, який потрібно захищати від несанкціонованого або ненавмисного втручання на різних рівнях, включаючи національний, регіональний та рівень окремих підприємств. У сфері бізнесу захист інформації може приносити значні прибутки та сприяти укладанню вигідних контрактів з партнерами, що зміцнює конкурентоспроможність суб’єктів господарювання і підвищує ефективність бізнес-процесів.

Дослідженням інформаційної безпеки підприємства на національному та міжнародному рівнях приділяють багато уваги вчені, а саме Адонін С., Акімова Н., Василішин С., Дейнега О., Дудченко Н., Жук Н., Захарова Н., Калашнікова Ю., Карбівничий І, Качан О., Кирильєва Л., Кузьомко В., Наумова Т., Парфентій Л., Ткачук Т., Черевко О., Яцух О. та інші.

Проте, сучасний стан розвитку економічних відносин висуває нові вимоги до інформаційної безпеки підприємства. З’являється значний перелік факторів, що обумовлюють необхідність впровадження більш ефективних систем управління інформаційною безпекою підприємства.

Мета і завдання дослідження. Мета кваліфікаційної роботи полягає в обґрунтуванні теоретико-методичних положень інформаційної безпеки підприємств на національному та міжнародному рівнях.

Відповідно до поставленої мети визначено сукупність завдань, спрямованих на її досягнення:

- розкрити суть та завдання інформаційної безпеки підприємства;

- дослідити реалії управління інформаційною безпекою підприємства;

- дати оцінку фінансового стану підприємства;

- провести аналіз фінансової стійкості та ліквідності підприємства;

- розкрити методику аналітичної діагностики ділової активності як детермінанти інформаційної безпеки підприємства;

- розкрити сучасні практики впровадження аудиту інформаційної безпеки підприємства;

- провести аналіз ризиків у системі досягнення інформаційної безпеки підприємства.

Об'єктом дослідження є інформаційна безпека ТОВ «Шредер».

Предметом дослідження є стан та перспективи розвитку інформаційної безпеки підприємств на національному та міжнародному рівнях.

Методи дослідження. Методологічною основою дослідження є діалектичний метод пізнання. У процесі дослідження теоретичних аспектів обліково-аналітичного забезпечення управління інформаційною безпекою підприємства використовувалися загальнонаукові методи: аналіз та синтез, групування і порівняння, узагальнення.

Інформаційною базою дослідження слугували наукові праці вітчизняних та зарубіжних вчених, матеріали науково практичних конференцій, семінарів, круглих столів з питань інформаційної безпеки підприємства, фактичні дані досліджуваного підприємства, інтернет-ресурси, тощо.

Наукова новизна одержаних результатів полягає в розробленні й обґрунтуванні теоретико-методичних положень та практичних рекомендацій щодо вдосконалення аналізу інформаційної безпеки підприємств.

Практичне значення одержаних результатів. Результати та висновки, які були отримані в ході проведеного дослідження, слугують основою для оцінки та забезпечення інформаційної безпеки у підприємства. Практичне значення полягає у розробці методик аналізу фінансової стійкості, ділової активності та загальної оцінки фінансового стану організації.

Апробація результатів роботи. За результатами дослідження опубліковано тези у збірнику кафедри обліку і оподаткування.

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 68 сторінок. Робота містить 12 таблиць, 10 рисунки, 4 додатки. Список використаних джерел налічує 61 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ОБЛІКОВО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

1.1. Суть та завдання інформаційної безпеки підприємства

Концепція загроз інформаційній безпеці з'явилася практично одночасно з появою інформаційного середовища. Спочатку, як відмічає Качан О.І., «це були прояви крадіжки інформації з комп'ютера, незаконне використання, порча інформації на комп'ютерах, а пізніше з розвитком інформаційних мереж інформаційна небезпека перетворилась в засоби перекачування по мережі неправдивої інформації, вірусів» [21]. На даний час питання забезпечення інформаційної безпеки стосується майже всіх учасників глобального інформаційного простору. Україна, як активний учасник життєвого циклу інформації, не залишається осторонь цих процесів. Це виявляється як на загальному міжнародному рівні, так і всередині кожного окремого суб'єкта підприємництва.

«Важливим аспектом вивчення систем управління інформаційною безпекою є визначення їх важливості для сучасного розуміння інформаційної безпеки та реалізації базових бізнес-процесів» [4].

У сучасних умовах всі суб'єкти господарювання повинні звертати належну увагу щодо захисту інформації, оскільки це важливий аспект забезпечення ефективної діяльності суб'єкта господарювання в умовах жорсткої конкуренції. Захист конфіденційної інформації, що становить конкурентну перевагу суб'єкта господарювання, є критичним, оскільки втрата такої інформації (наприклад, через крадіжку або випадкове знищення) може суттєво зашкодити.

Питання захисту даних, як відмічає Дейнега О., «є пріоритетними в більшості розвинених країн і вирішуються на національному рівні» [11, с. 72].

Окрім цього, як відмічає науковець, «практика показує, що у більшості вітчизняних підприємств ще не склалася культура захисту інформації, й крім того, деякі підприємства не мають достатньо вільних обігових коштів для забезпечення захисту інформації» [11, с. 72].

Зважаючи на це відмітимо, що розробка стратегії інформаційної безпеки підприємства вимагає глибокого знання основних підходів до теоретичних та методичних засад, врахування власної перспективи та уваги до актуальних тенденцій. Початковим кроком є розгляд етимології основних дефініцій, що лежать в основі розробки стратегічних компонентів методології та визначення шляхів досягнення поставленої мети. Особливу увагу слід приділити розумінню термінів «безпека» та «інформаційна безпека»

Так, Адонін С. В. Та Калашнікова Ю. М. зазначають, що «безпека – це стан складної системи, зовнішні й внутрішні чинники якого не спричиняють негативні зміни у функціонуванні» [1].

Дудченко Н. В. Й Карбівничий І. В. відмічають, що безпека – це «ступінь захищеності від негативних впливів та його спроможність протистояти змінам умов функціонування» [14].

Водночас Колісник О. зазначає, що безпека – це «певний стан захищеності будь-якого суб'єкту від загроз, який можливо досягти лише за умов певної діяльності» [25].

Таким чином бачимо, що дефініція «безпека» розглядається з трьох основних позицій, а саме:

- певний стан. Безпеку можна розглядати як конкретний стан, коли немає загроз чи ризиків, які можуть завдати шкоди особі, організації чи державі.
- спроможність до захисту. Це означає, що безпека може визначатися як здатність особи, організації чи держави відстояти себе від потенційних загроз або негативних подій.
- система заходів, дій. Безпеку також можна тлумачити як систему заходів і дій, спрямованих на запобігання, виявлення та мінімізацію ризиків і загроз.

Окрім цього слід зазначити, що термін «безпека» часто асоціюється з конкретними суб'єктами (суспільством, системою, державою, особою) і включає в себе ідеї ризику, загроз та небезпеки.

Слід також відмітити, що при розгляді суті поняття «безпека» важливо відзначити, що кожен аспект безпеки не існує окремо і має розглядатися в контексті, оскільки безпечний стан може бути досягнутий лише через виконання комплексу заходів, що призводять до формування здатності суб'єкта захищати свої інтереси. Отже, суб’єкт підприємництва або будь-який інший суб'єкт перебуває у стані безпеки не лише тоді, коли відсутні загрози, але й коли вони можуть бути виявлені та відвернуті.

Щодо інформаційної безпеки підприємства, то відмітимо, що на думку Чубаєвського В. та Жук Т., вона «охоплює процеси не тільки захисту інформації, але й, наприклад, обміну інформацією» [55, с. 108].

Дудатьєв А. В. зазначає, що «інформаційна безпека – це суспільні правовідносини щодо процесу створення, накопичення, підтримки, збереження та охорони необхідних інформаційних даних на підприємстві» [13, с. 108].

Ткачук Т.Ю. висловлює думку, що інформаційна безпека України є необхідною складовою системи забезпечення національної безпеки в цілому. Під поняттям інформаційна безпека розуміється «стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері від внутрішніх і зовнішніх загроз, що забезпечує стійкий розвиток» [49].

Деякі дослідники вважають, що інформаційна безпека, враховуючи двоєдину сутність інформації, має охоплювати як захист об’єктивних, так і суб’єктивних її аспектів. Перший аспект проявляється у безпеці інформації, другий - у формі інформаційно-психологічної безпеки. Узагальнюючи це, ми вважаємо, що ключовим для ефективного управління суб’єктом господарювання є створення інформаційної системи, яка застосовуватиме інноваційні технології для відображення всіх процесів операційної діяльності компанії. Інформаційна безпека, на нашу думку, полягає в створенні відповідних умов для ефективної системи обміну та захисту інформацією на

фірмі.

В. Кузьомко відмічає, що загрози, що виникають внаслідок цифрової трансформації, можуть бути успішно подолані лише за умови взаємодії економічних, організаційних та технічних методів. «Відповідно одним з пріоритетних напрямів забезпечення інформаційної безпеки бізнесу має стати постійне підвищення рівня інформаційної (цифрової) грамотності працівників, й такі завдання відповідають організаційному напряму забезпечення безпеки бізнесу» [28, с. 28]

Поняття інформаційної безпеки, як зазначає Коваленко Ю. О., можна розглядати з різних точок зору. «По-перше, як охоронний статус соціального інформаційного середовища, що забезпечує формування, використання та розвиток інформаційного середовища на благо громадян, підприємств і держави; по-друге, незалежно від наявності внутрішніх і зовнішніх інформаційних загроз існування і поступовий розвиток інформації гарантується в стані, який захищає інформаційні потреби окремих людей, суспільств і країн» [24, с. 124]. Тим часом, рівень свідомості визначає ступінь адекватності сприйняття навколишньої реальності об'єктом, а також обґрунтованість майбутніх рішень і дій [24, с. 124].

Черевко О.В. трактує дефініцію інформаційна безпека як «стан захищеності потреб в інформації особистості, підприємства і суспільства, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз, тобто відношення рівня інформаційного захисту до рівня інформаційних загроз» [54, с. 26]

Інформаційна безпека, як зазначає Легомінова С. В., «означає захист інформації та її допоміжної інфраструктури від випадкових або зловмисних дій, які можуть завдати шкоди самій інформації, її власнику або допоміжній інфраструктурі» [31, с. 88].

Отже, одна з особливостей інформаційної безпеки досліджуваного підприємства ґрунтується на тому, що необхідно використовувати не лише технологічні рішення чи продукти. Важливим аспектом є те, що на

сьогоднішній день головним джерелом загроз є люди.

Щодо цього Акімова Н. С., Кирильєва Л. О. та Наумова Т. А. зазначають, «основними напрямами у цьому контексті є: створення культури, за якої співробітники підприємств прагнули б до взаємодії і самі зверталися до служби безпеки, замість її уникнення; обмеження збереження, завантаження або копіювання даних на свій пристрій» [2, с. 8].

Узагальнюючи різноманітні погляди та визначення провідних вчених, ми приходимо до висновку, що інформаційна культура представляє собою організаційний процес, спрямований на забезпечення безпеки інформаційного середовища суб'єкта підприємництва. Під час цього процесу ефективно та вчасно виявляються та уникаються негативні інформаційні впливи, а також дотримуються етичні норми, стандарти та правила.

Потрібно розуміти, на що спрямована інформаційна безпека. Існують конкретні критерії, які визначає інформаційна безпека (рис 1.1.).

Рис. 1.1. Основні критерії інформаційної безпеки підприємства

Ми погоджуємося з поглядом багатьох дослідників, що для забезпечення безпеки інформації суб’єкт господарювання може використовувати технічні, організаційні методи та реалізувати правове забезпечення захисту своєї інформації. Зважаючи на дані пропозиції, ми розширили та доповнили основні шляхи захисту інформації (рис. 1.2.).

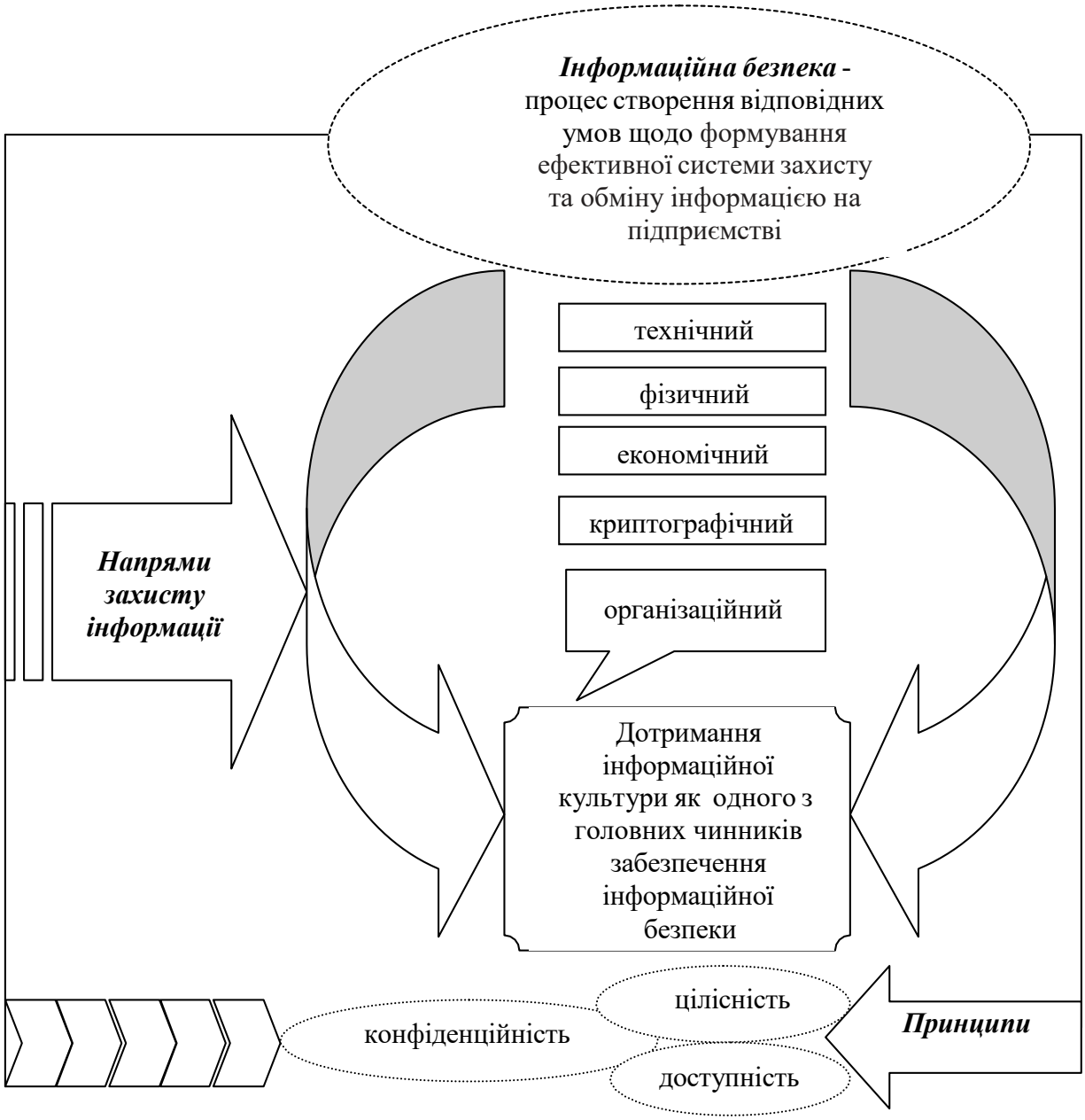

Рис. 1.2. Шляхи захисту власної інформації суб'єкта господарювання

Отже, за результатами дослідження можна стверджувати, що серед основних вимог до проведення комерційних операцій суб'єктами господарювання важливою є конфіденційність, аутентифікація, цілісність та гарантії збереження таємниці. При забезпеченні власної інформаційної безпеки суб'єкти господарювання намагаються забезпечити її цілісність, конфіденційність, доступність та юридичну значимість, що є основними напрямами. Якщо перші чотири вимоги можна забезпечити технічними засобами, то виконання двох останніх залежить не лише від технічних засобів, а

й від організаційних аспектів, зокрема від відповідальності працівників та дотримання інструкцій та законів, що захищають права контрагентів від можливих зловживань.

1.2. Управління інформаційною безпекою підприємства

Можливість зовнішнього та внутрішнього втручання в інформаційну систему має вплив на її цілісність та якість інформації і може призвести до негативних наслідків у діяльності суб’єкта підприємництва. Для забезпечення безпеки інформації необхідно створити ефективну систему управління, що допоможе знизити рівень незахищеності інформації та перешкодити зловмисникам у доступі, розповсюдженні або витоку цієї інформації.

Управління інформаційною безпекою стає невід'ємною складовою стратегічного менеджменту суб’єктом господарювання, оскільки враховує як загальні аспекти (об'єкти, предмети, зв'язки), так і їх особливості. Потреба використання міжнародних стандартів у формуванні системи управління інформаційної безпеки підприємств має ґрунтуватися на ризик-орієнтованому підході до управління інформаційними технологіями.

«Метою управління інформаційною безпекою є довгостроковий захист даних: конфіденційність даних (обмеження доступу, лише авторизованим користувачам; неможливості несанкціонованого отримання будь-яких даних), цілісність (здатність гарантувати точність та повноту даних; неможливості навмисного або випадкового модифікування інформації), доступність(дані та послуги, які на них покладаються, мають бути доступні авторизованим користувачам як у компанії, так і за її межами; оперативне отримання офіційно запитуваної інформації)» [61].

Зважаючи на це відмітимо, що конфіденційність, цілісність і доступність інформації суб’єкта господарювання можуть бути порушені різними шляхами.

Управління інформаційною безпекою передбачає виявлення потенційних загроз для суб’єкта підприємництва, оцінку їхньої ймовірності та можливого впливу, а також розробку та впровадження стратегій для мінімізації ризиків з використанням наявних ресурсів [61]. Для даних з підвищеним рівнем ризику можуть бути застосовані додаткові заходи управління конфіденційністю. Для забезпечення цілісності даних можна використовувати такі заходи, як контроль версій, керування доступом користувачів і перевірка контрольних сум. Щодо доступності, типові дії включають технічне обслуговування та ремонт апаратного забезпечення, встановлення виправлень і оновлень, а також впровадження процедур реагування на інциденти та аварійного відновлення, щоб уникнути втрати даних в разі кібератаки.

Як відмічає Панченко В., «до вказаних завдань інформаційної безпеки відносять також гарантування вірогідності інформації, забезпечення юридичної значущості інформації (електронні документи), організація не відстежуваності дій користувача» [37, с. 106].

Інформаційна безпека суб’єкта господарювання має гарантувати захист від будь-яких порушень функціонування інформаційної системи «через вплив на інформаційні канали та сигналізацію, керування та віддаленого завантаження баз даних, комутаційного обладнання, системного й прикладного програмного забезпечення; неправомірних дій користувачів і персоналу; несанкціонованого доступу до інформаційних даних; витоку даних, впливу на цілісність мережі й інформації, доступності баз даних; руйнування зовнішніх та вбудованих засобів захисту» [37, с. 106].

Основними кроками у створенні політики інформаційної безпеки, як відмічають Костюченко В.В. та Шиковець К.О. є наступні: 1) повне реєстрування всіх ресурсів, які потребують захисту; 2) складання переліку можливих загроз для кожного з цих ресурсів; 3) оцінка ймовірності виникнення кожної загрози; 4) виконання заходів для ефективного захисту кожного ресурсу [26, с. 90].

Слід також відмітити, що для забезпечення ефективної роботи

підприємства необхідно постійно контролювати, виявляти та управляти ризиками інформаційного об’єкту. Для запобігання виникненню збоїв на об’єкті необхідно належним чином організувати процес управління ризиками, що можна досягти через впровадження системи управління безпекою на фірмі та обмеження доступу до цінної інформації. Основні етапи побудови такої системи управління інформаційною безпекою суб’єкта підприємництва можна побачити на рисунку 1.3.

Рис. 1.3. Етапами побудови системи управління інформаційної безпеки суб’єкта господарювання

Окрім цього відмітимо, що для запровадження системи управління інформаційною безпекою суб’єкта господарювання можна використовувати загальний план з визначеними кроками, а саме:

- отримання завдання від керівництва та підтримка його, з важливості узгодження з бізнес-цілями суб’єкта підприємництва, виділення необхідних ресурсів та сприяння організаційній культурі безпеки;

- формування структури управління, яка визначає ролі, обов'язки та лінії звітності щодо інформаційної безпеки суб’єкта господарювання, включаючи призначення відповідального за інформаційну безпеку компанії або формування керівного комітету з інформаційної безпеки
- встановлення сфери застосування та меж діяльності, включаючи реєстр інформаційних активів, процесів та систем, що потребують захисту, з урахуванням бізнес-цілей та пріоритетів суб’єкта господарювання;
- розробка політики високого рівня з інформаційної безпеки суб’єкта господарювання, яка відображає підхід до інформаційної безпеки та бізнес-цілей загалом, затвердження вищим менеджментом компанії та оголошенням всім співробітникам;
- впровадження програми моніторингу та обчислення, включаючи визначення ключових показників ефективності та їх узгодження з бізнес-цілями суб’єкта господарювання;
- визначення методології оцінки ризику, що відповідає схильності та бізнес-цілям суб’єкта господарювання;
- проведення оцінки ризиків, включаючи визначення, аналіз та оцінку потенційних загроз для інформаційних активів суб’єкта господарювання з урахуванням їх впливу на поставлені цілі;
- розробка та впровадження плану обробки ризиків, включаючи вибір відповідних заходів зменшення ризику та навчання працівників компанії;
- розподіл обов'язків з інформаційної безпеки компанії, забезпечення відповідності їх бізнес-цілям та структурі суб’єкта господарювання;
- проведення програм навчання та підвищення обізнаності працівників компанії щодо їх ролі у захисті інформаційних активів суб’єкта господарювання;
- проведення внутрішнього аудиту та перевірки керівництва для оцінки продуктивності та ефективності системи управління інформаційною безпекою суб’єкта підприємництва, при необхідності впровадження коригувальних заходів;

- встановлення процесу управління інцидентами, включаючи розробку процедур реагування на інциденти безпеки;
- постійне вдосконалення для адаптації до змін у бізнес-середовищі суб’єкта підприємництва та зовнішніх та внутрішніх загроз;
- отримання сертифікації (необов'язково) в акредитованому органі сертифікації, такому як ISO/IEC 27001, що може забезпечити зовнішню перевірку зобов'язань суб’єкта підприємництва щодо інформаційної безпеки.

Таким чином, враховуючи наведені кроки, суб’єкти господарювання мають можливість не лише знизити рівень ризиків у сфері інформації, але й підтримувати свої стратегії в галузі бізнесу, сприяючи отриманню конкурентної переваги на ринку. Однак важливо адаптувати виокремленні кроки до особливостей конкретного суб’єкта підприємництва.

Слід також зазначити, що система управління інформаційною безпекою суб’єкта господарювання є складовою загальної системи управління, яка ґрунтується на аналізі та оцінці ризиків і призначена для мінімізації та контролю виявлених загроз. Ця система включає в себе програмні, апаратні, людські та фінансові ресурси. Правильно сконфігурована система управління інформаційною безпекою суб’єкта господарювання забезпечує досягнення поставлених цілей щодо захисту, збереже конфіденційність інформації та запобіжить несанкціонованому доступу.

Модель управління інформаційною безпекою суб’єкта підприємництва відображено на рис. 1.4.

Дотримання суб’єктом господарювання відмічених у моделі етапів управління інформаційною безпекою, дасть можливість одержати такі переваги;

- систематичне виявлення загроз та вразливостей безпеки компанії;
- оцінка ризиків та прийняття рішень на основі бізнес-цілей суб’єкта господарювання;
- ефективне керування інформаційними активами суб’єкта господарювання у критичних ситуаціях.

Рис. 1.4. Модель управління інформаційною безпекою суб'єкта господарювання

Підводячи підсумки відмітимо, що у сучасних умовах конкуренції, коли інформація про стратегію, продукцію, збутову та інші аспекти діяльності суб'єкта господарювання стає ключовою у боротьбі за успіх, й тому важливо пам'ятати про захист цієї інформації. Суб'єкт підприємництва повинен постійно відслідковувати джерела потенційних загроз та бути готовим захищати свою інформацію. Ефективна система управління інформаційною безпекою є ключовим елементом, що дозволяє суб'єкту господарювання працювати ефективно, стійко та залишатися конкурентоспроможним на ринку.

Окрім цього відмітимо, що ефективне управління інформаційною безпекою становить основу для розвитку суб'єкта господарювання та підвищення його конкурентоспроможності на ринку. Без належного захисту

інформації неможлива забезпеченість економічної стійкості суб’єкта господарювання.

Висновки до розділу 1

Узагальнюючи результати дослідження теоретичних аспектів обліково-аналітичного забезпечення управління інформаційною безпекою підприємств, можна зробити наступні висновки:

1. Інформаційна безпека – це набір заходів, спрямованих на захист інформації від неправомірного використання, незаконного доступу, розголошення, пошкодження, маніпулювання або небажаних змін, які можуть вплинути на її конфіденційність, цілісність та доступність.

2. Встановлено, що серед основних вимог до проведення комерційних операцій суб’єктами господарювання важливою є конфіденційність, аутентифікація, цілісність та гарантії збереження таємниці. При забезпеченні власної інформаційної безпеки суб’єкти господарювання намагаються забезпечити її цілісність, конфіденційність, доступність та юридичну значимість, що є основними напрямами. Якщо перші чотири вимоги можна забезпечити технічними засобами, то виконання двох останніх залежить не лише від технічних засобів, а й від організаційних аспектів, зокрема від відповідальності працівників та дотримання інструкцій та законів, що захищають права контрагентів від можливих зловживань.

3. У сучасних умовах конкуренції, коли інформація про стратегію, продукцію, збутову та інші аспекти діяльності суб’єкта господарювання стає ключовою у боротьбі за успіх, й тому важливо пам'ятати про захист цієї інформації. Суб’єкт підприємництва повинен постійно відслідковувати джерела потенційних загроз та бути готовим захищати свою інформацію. Ефективна система управління інформаційною безпекою є ключовим елементом, що дозволяє суб’єкту господарювання працювати ефективно, стійко та залишатися конкурентоспроможним на ринку. Ефективне управління інформаційною

безпекою становить основу для розвитку суб’єкта господарювання та підвищення його конкурентоспроможності на ринку. Без належного захисту інформації неможлива забезпеченість економічної стійкості суб’єкта господарювання.

4. Виокремлені етапи управління інформаційною безпекою, дадуть можливість одержати суб’єкту господарювання такі переваги; систематичне виявлення загроз та вразливостей безпеки компанії; оцінка ризиків та прийняття рішень на основі бізнес-цілей суб’єкта господарювання; ефективне керування інформаційними активами суб’єкта господарювання у критичних ситуаціях.

РОЗДІЛ 2
МЕТОДИКА АНАЛІЗУ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Оцінка фінансового стану підприємства

Початковим етапом у процесі аналізу інформаційної безпеки суб’єкта господарювання є проведення оцінки його фінансового стану. Це оцінювання іноді називають експрес-аналізом фінансового стану, оскільки його мета полягає у швидкому реагуванні та ухваленні управлінських рішень для зміцнення фінансової стабільності суб’єкта підприємництва в майбутньому.

У зв’язку з цим, господарська діяльність суб’єктів господарювання вимагає організованого, ефективного управління, яке включає в себе ряд взаємопов’язаних функцій, що здійснюються послідовно та своєчасно. У зв'язку з цим, важливо провести дослідження щодо сутності, завдань і потреби в системному аналізі фінансового стану суб’єкта підприємництва.

Фінансовий стан суб’єкта підприємництва, як відмічають Поддєрьогін А.М., Білик М.Д., Буряк Л.Д., Булгакова С.О. та Куліш А.П., «це комплексне поняття, яке є результатом взаємодії всіх елементів системи фінансових відносин підприємства, визначається сукупністю виробничо-господарських факторів і характеризується системою показників, що відображають наявність, розміщення і використання фінансових ресурсів» [41].

Фінансовий стан суб’єкта підприємництва є результатом його діяльності у виробничій, комерційній та фінансово-господарській сферах, що взаємопов'язані між собою. Він безпосередньо впливає на всі аспекти функціонування компанії. Наприклад, безперебійне виробництво та реалізація якісної продукції позитивно впливають на фінансовий стан, оскільки вони сприяють збільшенню обсягів виробництва і реалізації, зниженню собівартості

продукції і, відповідно, збільшенню прибутку.

Водночас, нерегулярність виробничих процесів, зниження якості продукції та проблеми з її реалізацією призводять до зменшення прибутку, що негативно впливає на фінансову стійкість суб'єкта підприємництва. Це може призвести до нестачі коштів і, внаслідок цього, до перебоїв у забезпеченні необхідних ресурсів для виробництва.

Фінансова діяльність суб'єкта підприємництва має бути спрямована на систематичне залучення та ефективне використання фінансових ресурсів, дотримання фінансової дисципліни, забезпечення раціонального використання власних та залучених ресурсів і створення фінансової стійкості для ефективного функціонування компанії. Оцінка фінансового стану суб'єкта підприємництва має велике значення для забезпечення його стабільності та успішності.

«Метою оцінки фінансового стану підприємства в системі антикризового управління є розробка і реалізація заходів, направлених на швидке відновлення платоспроможності, відновлення достатнього рівня фінансової стійкості підприємства, встановлення можливості підприємства продовжувати свою господарську діяльність, подальшого розвитку, забезпечення прибутковості і зростання виробничого потенціалу і ухвалення відповідних рішень» [51].

Основні завдання оцінки фінансового стану суб'єкта підприємництва представлені на рисунку 2.1.

Слід також відмітити, що фінансовий стан суб'єкта господарювання визначається такими факторами:

- прибутковість діяльності компанії;
- оптимальне розміщення активів компанії;
- ефективність використання залишкового прибутку після оплати податків та зборів;
- наявність достатніх фінансових ресурсів компанії для забезпечення виробництва та реалізації продукції контрагентам;
- рівень платоспроможності та ліквідності компанії.

Рис. 2.1. «Основні завдання оцінки фінансового стану підприємства» [34, с. 46]

«Метою оцінки фінансового стану підприємства є аналіз фінансової спроможності підприємства, а також розробка і реалізація заходів, направлених на швидке відновлення платоспроможності, відновлення достатнього рівня фінансової стійкості підприємства, встановлення можливості підприємства продовжувати свою господарську діяльність, можливості подальшого розвитку, забезпечення прибутковості і зростання виробничого потенціалу і ухвалення відповідних рішень» [59].

Необхідно відзначити, що важливість аналізу фінансового стану суб’єкта господарювання проявляється у його ролі в формуванні його фінансової стратегії, виявленні слабких місць у функціонуванні компанії та у прийнятті управлінських рішень для підвищення ефективності управління.

За допомогою аналізу, як зазначають Нагорний П.Д. та Базюк Д.С., «можна забезпечити: оцінку рівня ефективності діяльності господарюючих систем та виявлення факторів і причин досягнення існуючого стану; визначення тенденцій розвитку підприємства за показниками його фінансового стану; розроблення сценаріїв розвитку економічної діяльності суб’єктів господарювання: накопичення, трансформацію і ефективне використання

інформаційної бази фінансового характеру; визначення рівня кредитоспроможності підприємства як позичальника фінансових ресурсів для здійснення господарської діяльності; якісне планування, прогнозування, бюджетування. визначення потреби і ефективне розміщення фінансових ресурсів; ефективне формування і використання потоків грошових коштів; створення рейтингових систем оцінки фінансового стану господарюючих систем; своєчасне вживання заходів, спрямованих на підвищення платоспроможності, фінансової стійкості і прибутковості підприємств; визначення резервів поліпшення фінансового стану господарюючих систем; обґрунтування політики розподілу і використання прибутку для потреб господарюючих систем і їх власників; оцінку рівня підприємницького ризику щодо можливості погашення зобов'язань, здатності до нарощування чистих активів, залучення інвестицій і прийняття управлінських рішень» [34, с 45-46].

Слід також відмітити, що на фінансовий стан суб'єкта господарювання значний вплив мають багато факторів.

Класифікаційні ознаки, за якими можна класифікувати фактори, що впливають на фінансовий стан суб'єкта господарювання зображено на рисунку 2.2.

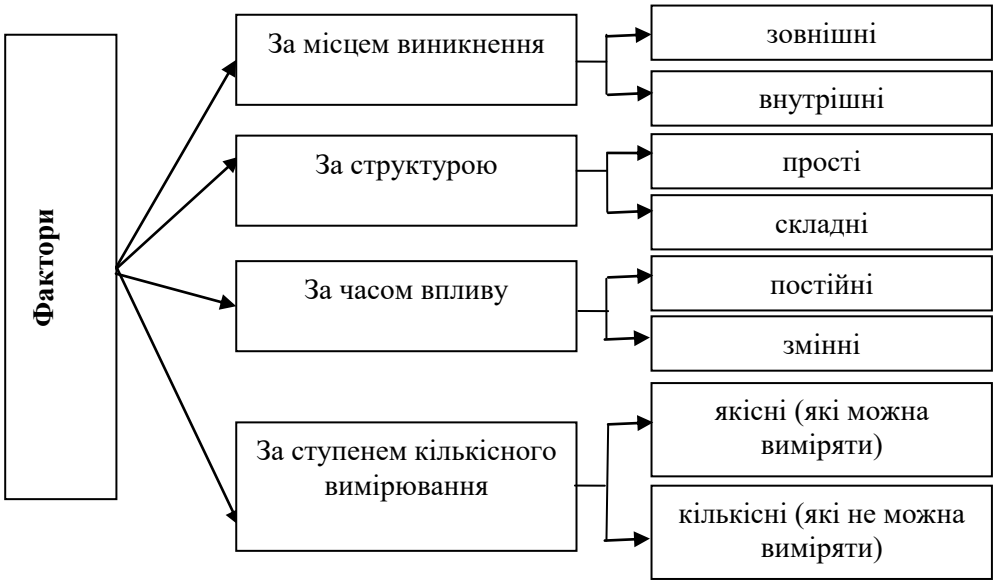

Рис. 2.2. Класифікація факторів, що впливають на фінансовий стан суб'єкта господарювання

Пряме оцінювання фінансового стану визначається рівнем прибутку та доходу суб’єкта господарювання, а також структурою його капіталу і активів. Ці показники визначають рівень ліквідності та платоспроможності,фінансової стійкості, а також ефективність використання капіталу суб’єктом господарювання. Зовнішні фактори впливають на загальну оцінку фінансового стану, хоча цей вплив є непрямим. Оцінка впливу зовнішніх факторів на фінансовий стан суб’єкта підприємництва важко кількісно виразити, але ці фактори впливають на його внутрішнє середовище, що вже має прямий вплив на фінансовий стан компанії. Таким чином, вплив зовнішніх факторів переважно є непрямим.

Недостатнє або несправне управління активами компанії може призвести до проблем, таких як затримка у виплаті боргів контрагентам за отримані товарно-матеріальні цінності, недостатнє або неправильне забезпечення необхідними ресурсами для здійснення діяльності, що може призвести до погіршення виконання зобов'язань перед різними зацікавленими сторонами. Належне забезпечення активами в межах потреб і їх раціональне використання створюють сприятливі умови для подальшого покращення показників управління якістю і кількістю [17].

Для проведення комплексного аналізу фінансового стану суб’єкта господарювання важливо оцінити загальні тенденції, які відображають його фінансове здоров'я з різних сторін. Показники та фактори належного фінансового стану компанії можуть включати в себе: стійку платоспроможність, ефективне використання капіталу, розрахунків та наявність стабільних фінансових ресурсів. Неналежний фінансовий стан фірми може проявлятися через неефективний розподіл коштів, відсутність достатньої кількості оборотних коштів, постійну заборгованість за платежами та негативні тенденції у виробництві. Оцінка дохідності та рентабельності відіграє важливу роль у цьому аналізі, включаючи аналіз структури доходів та їх взаємозв'язок з прибутком. Також важливо проаналізувати вплив факторів, що формують прибуток, та чинники, що впливають на загальну прибутковість суб’єкта

господарювання.

У процесі аналізу фінансового стану ТОВ «Шредер» будемо використовувати методи горизонтального аналізу, що оцінюють абсолютні й відносні зміни в показниках фінансової звітності, а також вертикального аналізу для визначення питомої ваги окремих статей фінансової звітності.

Зважаючи на це відмітимо, що аналіз слід розпочинати з оцінки активів ТОВ «Шредер». Цей етап має велике значення, оскільки розмір та структура активів компанії впливають на обсяги діяльності суб'єкта господарювання, його фінансовий та соціально-економічний розвиток, а також на рівень платоспроможності, ліквідність, фінансову стійкість, ділову активність та загальну конкурентоспроможність, тощо.

Дані щодо структури та динаміки майна ТОВ «Шредер» за 2021-2023 рр представлені в таблиці 2.1.

Таблиця 2.1

Аналіз складу та динаміки майна ТОВ «Шредер» за 2021–2023 рр.

Показник	Значення показників по роках, тис. грн			Відхилення показників по роках			
				2022/2021		2023/2022	
	2021	2022	2023	абс. тис. грн	віднос., %	абс. тис. грн	віднос., %
1. Необоротні активи	**140717**	**152469**	**180137**	**11752**	**8,4**	**27668**	**18,1**
1.1. Нематеріальні активи	303	1238	1963	935	308,6	725	58,6
1.2. Основні засоби	130396	138247	164562	7851	6,0	26315	19,0
1.3. Відстрочені податкові активи	10018	12984	13477	2966	29,6	493	3,8
1.4. Довгострокова дебіторська заборгованість	—	—	135	—	—	135	—
2. Оборотні активи	**574873**	**976368**	**1096458**	**401495**	**69,8**	**120090**	**12,3**
2.1. Запаси	255299	334518	307898	79219	31,0	-26620	-8,0
2.2. Короткострокова дебіторська заборгованість	298868	570419	651905	271551	90,9	81486	14,3
2.3. Гроші та їх еквіваленти	17158	68075	142719	50917	296,8	74644	109,6
2.4. Витрати майбутніх періодів	3548	3356	4821	-192	-5,4	1465	43,7
Разом	**715590**	**1128837**	**1276595**	**413247**	**57,7**	**147758**	**13,1**

За даними таблиці 2.1, бачимо, що на ТОВ «Шредер» відслідковується постійний ріст вартості майна протягом зазначеного періоду. Так, у 2022 році вартість майна зросла на 413247,00 тис. грн. або на 57,7% у порівнянні з 2021 роком, а в 2023 році вона зросла на ще 147758 тис. грн. або 13,1% порівняно з 2022 роком. Ці дані свідчать про зростання майнового потенціалу ТОВ «Шредер».

У структурі майна ТОВ «Шредер» левову частину займають оборотні активи, які у 2021 році становили 80,3% від валюти балансу, у 2022 році - 86,5%, а у 2023 році - 85,9%, що свідчить про позитивну тенденцію. За період з 2021 по 2023 рік вартість оборотних активів зросла на 521585 тис. грн. або на 90,7%, досягнувши рівня 1096458 тис. грн.

Слід також відмітити, що значну частку у складі оборотних активів ТОВ «Шредер» займає короткострокова дебіторська заборгованість. Так, упродовж 2022 року величина короткострокової дебіторської заборгованості зросла на 271551 тис. грн. (90,9%), а у 2023 році зросла на 81486 тис. грн. (14,3%). Сума грошових коштів та їх еквівалентів у 2022 році порівняно з 2021 роком зросла в 4 рази, на 50917 тис. грн., а до кінця 2023 року на 74644 тис. грн. або 109,6%.

Щодо запасів, то відмітимо, що у 2023 році також спостерігається їх зростання у порівняні із 2021 роком. Так, станом на кінець 2023 року вартість запасів збільшилась на 52599 тис грн, або 20,6%. Разом з тим слід відмітити, що у порівняні із 2022 роком простежується зменшення запасів на 26620 тис грн, або 8,0%.

Щодо необоротних активів ТОВ «Шредер» відмітимо, що у порівнянні з 2021 роком, у 2022 році вартість необоротних активів зросла на 11752 тис. грн. або на 8,4%, досягнувши рівня 152469 тис. грн. У 2023 році відбулося подальше зростання на 27688 тис. грн. або на 18,1%. Левову частку у структурі необоротних активів займають основні засоби, а саме 92,7% у 2021 р.; 90,7% у 2022 р.; 91,4% у 2023 р.

Щодо нематеріальних активів, то відмітимо, що їх частка у структурі необоротних активів є незначною, й у порівняні із 2021 роком збільшилась на

0,9 процентних пункти, й на кінець 2023 року становила 1,1%.

Також із даних таблиці бачимо, що у складі необоротних активів на ТОВ «Шредер» є відстрочені податкові активи. У порівнянні з 2021 роком, у 2022 році величина відстрочених податкових активів зросла на 2966 тис. грн. або на 29,6%, досягнувши рівня 12984 тис. грн. У 2023 році відбулося подальше зростання на 493 тис. грн. або на 3,8%. досягнувши рівня 13477 тис. грн.

Потрібно також відмітити, що майно досліджуваного підприємства формується шляхом використання як власних, так і залучених ресурсів. Тож ми дослідимо, які джерела використовувалися для формування активів ТОВ «Шредер» протягом 2021–2023 років. Результати цього аналізу представлені у таблиці 2.2.

Таблиця 2.2

Аналіз складу та динаміки капіталу ТОВ «Шредер» за 2021–2023 рр.

Показник	Значення показників по роках, тис.грн			Відхилення показників по роках			
	2021	2022	2023	2022/2021		2023/2022	
	тис. грн.	тис. грн.	тис. грн.	абс. тис. грн.	віднос., %	абс. тис. грн.	віднос., %
1. Власний капітал	**434569**	**551466**	**755222**	**116897**	**26,9**	**203756**	**36,9**
1.1. Зареєстрований капітал	337129	337129	337129	—	—	—	—
1.2. Резервний капітал	1460	1460	1460	—	—	—	—
1.3. Нерозподілений прибуток	95980	212877	416633	116897	121,8	203756	95,7
2. Позиковий капітал	**281021**	**577371**	**521373**	**296350**	**105,5**	**-55998**	**-9,7**
2.1. Довгострокові зобов’язання і забезпечення	6950	3751	5364	-3199	-46,0	1613	43,0
2.2. Поточні зобов’язання і забезпечення	274071	573620	516009	299549	109,3	-57611	-10,0
- короткострокові кредити банків	9020	160287	—	151267	1677,0	-160287	-100,0
- поточна кредиторська заборгованість за:	—	—	—	—	—	—	—
довгостроковими зобов’язаннями;	4017	5576	344	1559	38,8	-5232	-93,8
товари, роботи, послуги	117594	108209	103989	-9385	-8,0	-4220	-3,9
розрахунками з бюджетом	5966	19405	2064	13439	225,3	-17341	-89,4
розрахунками зі страхування	448	733	1387	285	63,6	654	89,2
розрахунками з оплати праці	2137	2882	5688	745	34,9	2806	97,4

Продовження таблиці 2.2

1	2	3	4	5	6	7	8
- поточна кредиторська заборгованість за одержаними авансами	7857	5767	6223	-2090	-26,6	456	7,9
- поточна кредиторська заборгованість із внутрішніх розрахунків	114053	256179	374996	142126	124,6	118817	46,4
- поточні забезпечення	12298	14447	21122	2149	17,5	6675	46,2
- інші поточні зобов'язання	681	135	196	-546	-80,2	61	45,2
Разом	**715590**	**1128837**	**1276595**	**413247**	**57,7**	**147758**	**13,1**

За результатами аналізу складу джерел формування капіталу ТОВ «Шредер» можна зробити висновок, що величина власного капіталу на підприємстві постійно зростає. Так, протягом досліджуваного періоду спостерігається зростання капіталу з 434569 тис. грн. до 755222 тис. грн., або на 73,8%.

Однак не зважаючи на таке зростання, частка власного капіталу у валюті балансу зменшилася на 1,5 процентних пункти з 60,7% у 2021 році до 59,2 % у 2023 році. Разом з тим, якщо порівнювати із 2022 роком, то простежується зростання частки власного капіталу у валюті балансу на 10,3 процентних пункти.

Слід відмітити, що причиною зростання власного капіталу є одержання ТОВ «Шредер» прибутку. У порівнянні з 2021 роком, у 2022 році величина нерозподіленого прибутку зросла на 116897 тис. грн. або на 121,8%, досягнувши рівня 212877 тис. грн. У 2023 році відбулося подальше зростання на 203756 тис. грн. або на 95,7%. досягнувши рівня 416633 тис. грн.

У структурі позикового капіталу ТОВ «Шредер» найбільшу частку складають поточні зобов'язання і забезпечення (97,5% у 2021 році, 99,0% у 2023 році). Протягом 2023 року спостерігається збільшення суми поточних зобов'язань і забезпечення на 109,3% або 299549 тис. грн., а на кінець 2023 року вона зменшилася на 57611 тис. грн або 10,0%. Величина довгострокових зобов'язань і забезпечень у 2022 році зменшується на 3199 тис. грн або 46,0%, а

у 2023 році збільшується на 1613 тис. грн або 43% у порівняні із 2022 роком.

Отже, за підсумками проведеного дослідження можна зробити висновок, що ТОВ «Шредер» характеризується достатньою кількістю власного капіталу й є незалежним від залучених джерел фінансування.

2.2. Аналіз фінансової стійкості та ліквідності підприємств

У сучасних умовах фінансова стійкість суб’єкта господарювання вважається одним із ключових аспектів його господарського механізму і визначає його економічний потенціал. Загроза банкрутства ставить перед суб’єктом підприємництва завдання забезпечити свою фінансову стійкість та покращувати фінансові показники діяльності. Кожен суб’єкт підприємництва повинен забезпечувати стабільний стан своїх фінансових ресурсів, щоб виконувати зобов'язання перед контрагентами, власниками, державою та співробітниками компанії. У зв’язку з цим, суб’єкт підприємництва має дбати про такий стан ресурсів, що дозволить йому безперебійно працювати.

В економічній літературі, як відмічають Вівчар О. та Кос, Т., «існує багато різних підходів до визначення суті фінансової стійкості» [6, с. 116].

Так, Докієнко Л.М. зазначає, що «фінансова стійкість підприємства являє собою об'єкт фінансового управління господарською діяльністю та характеризує такий стан фінансових ресурсів, їх формування, розподіл і використання, що забезпечує пропорційний, збалансований розвиток підприємства за збереження платоспроможності та кредитоспроможності в умовах припустимого рівня ризику» [12].

В. Ганін та Р. Алєкпєров відмічають, що «фінансова стійкість це стабільне перевищення доходів над витратами, завдяки якому досягається стабільний приплив грошових коштів» [5].

Жукевич С. та Рожелюк В. зазначають, що «фінансова стійкість відображає такий стан фінансових ресурсів, при якому підприємство, вільно

маневруючи коштами, здатне шляхом ефективного їхнього використання забезпечувати безперебійний процес виробництва і реалізації продукції й послуг, а також витрат по його розширенню й відновленню» [57].

В. Ізюмська та А. Нікульшина стверджують, що фінансова стійкість суб'єкта підприємництва вважається однією з ключових умов для його розвитку. Вона містить важливу інформацію для потенційних інвесторів і відображає здатність суб'єкта господарювання виконувати свої фінансові зобов'язання перед кредиторами та сплачувати борги [18].

Отже, фінансова стійкість компанії показує її поточний фінансовий стан, спосіб розподілу та ефективність використання ресурсів, що сприяє його розвитку через збільшення прибутку та капіталізацію, при цьому забезпечуючи збереження його платоспроможності та кредитної здатності на прийнятному рівні ризику.

Зважаючи на це відмітимо, що використовуючи методології аналізу фінансової стійкості суб'єкта підприємництва можна виокремити кілька етапів його оцінки: загальна оцінка фінансової стійкості компанії; аналіз фінансової стійкості компанії на основі розрахунку показників; визначення типу фінансової стійкості компанії через оцінку джерел фінансування запасів.

Щодо цього Вівчар О. та Кос, Т. зазначають, що «загальне оцінювання фінансової стійкості передбачає визначення: стійкості джерел формування капіталу; ресурсної стабільності; стійкості управління» [6, с. 116].

Для оцінки фінансової стійкості фірми, важливо включити аналіз її ресурсної стійкості, що залежить від рівня взаємодії з іншими учасниками ринку, вплетеності у систему виробничих відносин, відносин з економічним станом країни, здатності залучати кошти та контролю за грошовими ресурсами. Одночасно, для оцінки стійкості управління суб'єктом підприємництва, потрібно розглядати відповідність організаційної та виробничої структури у контексті обраної стратегії розвитку й ринкової ситуації.

Слід також відмітити, що джерела фінансування запасів характеризують три основних показники, що відображені у таблиці 2.3.

Таблиця 2.3

Джерела фінансування запасів ТОВ «Шредер» за 2021-2023 рр.

Показник	Значення показників по роках, тис.грн			Відхилення показників по роках	
	2021	2022	2023	2022/2021	2023/2022
Наявність власних коштів (Н1)	293852	398997	575085	105145	176088
Наявність власних та довгострокових позикових формування запасів (Н2)	300802	402748	580449	101946	177701
Загальна величина основних джерел формування запасів (Н3)	461089	402748	580449	-58341	177701

Із проведених розрахунків бачимо, що у 2022-2023 рр ТОВ «Шредер» для фінансування своїх запасів практично не залучає додаткових джерел фінансування (наприклад банківські кредити). Тобто фінансування запасів здійснюється практично лиш за рахунок власних коштів. Хоча й уникнення використання зовнішніх джерел може бути сприятливим, але ТОВ «Шредер» не використовується фінансовий леверидж, що дало би можливість одержання додаткового збільшення прибутку.

Слід також відмітити, що трьом показникам наявності джерел фінансування запасів суб'єкта підприємництва відповідають три показника забезпеченості запасів джерелами фінансування суб'єкта підприємництва, а саме:

- надлишок (+) або нестача (–) власних оборотних коштів (ΔВОК);
- надлишок (+) чи нестача (–) власних та довгострокових джерел (ΔВД);
- надлишок (+) чи нестача (–) основних джерел (ΔОД).

Забезпеченість запасів джерелами фінансування відображено у таблиці 2.4.

Із проведених розрахунків бачимо, що ТОВ «Шредер» є фінансово стійким. Так, на протязі 2021-2023 рр вартість запасів не перевищувала основні джерела їх формування. При чому слід відмітити, що спостерігається позитивна тенденція надлишку основних джерел фінансування, а саме: у 2021

р. – 54523 тис. грн; у 2022 р. – 228517 тис. грн.; у 2023 р. 272551 тис. грн.

Таблиця 2.4

Забезпеченість запасів джерелами їхнього фінансування на ТОВ «Шредер» за 2021-2023 рр.

Показник	Значення показників по роках, тис. грн			Відхилення показників по роках	
	2021	2022	2023	2022/2021	2023/2022
надлишок (+) або нестача (–) власних оборотних коштів (ΔВОК)	38553	64479	267187	25926	202708
надлишок (+) чи нестача (–) власних та довгострокових джерел (ΔВД)	45503	68230	272551	22727	204321
надлишок (+) чи нестача (–) основних джерел (ΔОД)	54523	228517	272551	173994	44034

Слід також відзначити, що для проведення аналізу фінансової стійкості суб'єкта господарювання можуть застосовуватись різні групи показників, а саме:

- відносні показники – коефіцієнти, що показують співвідношення окремих статей фінансової звітності компанії;
- абсолютні, що відображають ступінь забезпеченості запасів суб'єкта підприємництва джерелами їх формування;
- межа рентабельності й запас фінансової стійкості.

Аналіз абсолютних показників для визначення типу фінансової стійкості базується на співвідношенні між ресурсами, які компанія має для фінансування своїх запасів. При цьому відмітимо, що «запасами вважають готову продукцію, товари, виробничі запаси, незавершене виробництво, витрати майбутніх періодів, строк погашення яких менший ніж 12 місяців» [43].

Окрім цього відмітимо, що абсолютні показники характеризують типи фінансової стійкості суб'єкта підприємництва: абсолютний, нормальний, нестійкий та кризовий.

Так, на ТОВ «Шредер» на протязі 2021-2023 рр. спостерігається абсолютна фінансова стійкість, тобто процес поновлення запасів на

підприємстві відбувається лише за рахунок власних оборотних ресурсів, й відповідно діяльність ТОВ «Шредер» характеризується мінімальним ступенем ризику.

Слід також зазначити, що аналіз фінансової стійкості суб'єкта підприємництва на основі розрахунку коефіцієнтів, як підкреслюють Вівчар О. та Кос, Т., «виконується за допомогою відносних показників фінансової стійкості, а саме: коефіцієнт автономії; коефіцієнт фінансової залежності; коефіцієнт фінансового ризику; коефіцієнт маневреності власного капіталу; коефіцієнт фінансової незалежності капіталізованих джерел; коефіцієнт структури покриття довгострокових вкладень; коефіцієнт довгострокового залучення позикових коштів; коефіцієнт концентрації залученого капіталу; коефіцієнт питомої ваги власних коштів і довготермінових зобов'язань; коефіцієнт поточної заборгованості; коефіцієнт страхової стабільності капіталу; коефіцієнт фінансової стійкості» [6, с. 117].

Відносні показники фінансової стабільності суб'єкта підприємництва, як відмічає Чегринець К.В., включають набір коефіцієнтів, які ґрунтуються на порівнянні з теоретично визначеним рівнем та оцінці динаміки змін протягом попередніх періодів. Усі ці коефіцієнти обчислюються на основі даних фінансової звітності компанії та можуть вказувати на рівень її фінансової стабільності [53].

Динаміку відносних показників фінансової стійкості ТОВ «Шредер» відображено у таблиці 2.5.

Таким чином, за результатами аналізу відносних показників фінансової стійкості бачимо, що ТОВ «Шредер» має високий рівень фінансової стійкості. Так, значення коефіцієнта автономії показує на те, що на кінець 2021 р. частка власного капіталу у валюті балансу становила 61%, на кінець 2022 р. – 49%, а на кінець 2023 р. – 59%, що на 0,1 процентних пункти більше, ніж у 2022 р. При цьому слід відмітити, що оптимальне значення даного показника становить більше 50%. Таким чином можемо зробити висновок, що фінансова стійкість ТОВ «Шредер» у 2023 році, в порівняні із 2022 р. зросла. Високий

рівень фінансової стійкості ТОВ «Шредер» підтверджується також і іншими показниками. Так, коефіцієнт фінансової залежності є оберненим до показника автономії. Так, при оптимальному значення менше двох, на кінець 2023 року він становив 1,69, що на 0,36 менше ніж у 2022 році.

Таблиця 2.5

Розрахунок відносних показників фінансової стійкості ТОВ «Шредер» за 2021–2023 рр.

Показник	Значення показників по роках, тис.грн			Відхилення показників по роках	
	2021	2022	2023	2022/2021	2023/2022
Коефіцієнт забезпечення оборотних активів власними коштами	0,02	0,07	0,13	0,05	0,06
Коефіцієнт маневрування власного капіталу	0,69	0,73	0,77	0,04	0,04
Коефіцієнт автономії	0,61	0,49	0,59	-0,12	0,10
Коефіцієнт фінансової залежності	1,65	2,05	1,69	0,40	-0,36
Коефіцієнт фінансування	0,65	1,05	0,69	0,40	-0,36
Коефіцієнт фінансового ризику	0,02	0,29	0,00	0,27	-0,29
Коефіцієнт концентрації позикового капіталу	0,39	0,51	0,41	0,12	-0,10
Коефіцієнт довгострокового залучення позикових коштів	0,02	0,01	0,01	-0,01	0,00
Коефіцієнт фінансової стійкості	0,62	0,49	0,60	-0,13	0,10

Коефіцієнт фінансування показує, що на кінець 2023 року на 1 гривню власного капіталу припадає 0,69 грн залученого капіталу, що на 0,04 грн більше ніж у 2021 році, й на 0,36 грн більше ніж у 2022 році.

Коефіцієнт забезпеченості оборотних активів власними коштами при нормативі більше 0,1, на кінець 2021 р. мав значення 0,02. За 2022 р. даний показник зріс на 0,05 до 0,07, що свідчить про підвищення фінансової стійкості ТОВ «Шредер» у 2022 р. За 2023 р. даний коефіцієнт у порівняні з 2022 р. збільшився на 0,06, й на кінець 2023 р. становив 0,13, що відповідає значенню

оптимального рівня даного показника.

Щодо коефіцієнта маневреності власного капіталу, то відмітимо, що значення даного показника показує, що на кінець 2021 р. 69,0% власних коштів було вкладено в оборотні активи ТОВ «Шредер», а на кінець 2023 р. вже 77,0%. Тобто за 2021-2023 рр значення коефіцієнта маневреності зросло й це свідчить про підвищення фінансової стійкості компанії. Слід також відмітити, що значення даного коефіцієнта перевищує оптимальне його значення, що становить більше 0,5.

Підводячи підсумки відмітимо, що розраховані показники фінансової стійкості ТОВ «Шредер» засвідчують, що компанія є фінансово стійкою, й у порівняні із минулими роками ще й підвищилась.

Наступними показниками, які слід дослідити, є показники ліквідності та платоспроможності. Вони відображають оцінку фінансового стану в поточній діяльності або короткостроковій перспективі суб’єкта підприємництва.

Зважаючи на це відмітимо, що критерієм ліквідності суб’єкта підприємництва є перевищення вартості оборотних активів над поточними пасивами. У контексті впливу ліквідності на фінансовий стан компанії, таке переважання повинно бути максимально можливим.

Один з абсолютних показників ліквідності - робочий капітал (власні оборотні кошти), що означає залишок оборотних коштів у суб’єкта підприємництва після погашення короткострокових зобов'язань. Це визначається як різниця між поточними активами та пасивами

Так, ліквідність суб’єкта підприємництва можна визначити за допомогою коефіцієнтів: загальної ліквідності, швидкої ліквідності, абсолютної ліквідності.

Динаміку показників ліквідності ТОВ «Шредер» відображено у таблиці 2.6.

Із даних таблиці 2.6 бачимо, що ТОВ «Шредер» є платоспроможним. Так, станом на кінець 2021 р., 2022 р. та 2023 р., воно у спромозі погасити 6,3%, 11,9% та 27,7% відповідно. Нормативне значення даного показника становить

255-30%.

Таблиця 2.6

Показники ліквідності ТОВ «Шредер» за 2021–2023 рр.

Показник	Значення показників по роках, тис.грн			Відхилення показників по роках	
	2021	2022	2023	2022/2021	2023/2022
Коефіцієнт абсолютної ліквідності	0,063	0,119	0,277	0,056	0,158
Коефіцієнт швидкої ліквідності	1,166	1,119	1,528	-0,047	0,409
Коефіцієнт загальної ліквідності (покриття)	2,098	1,702	2,125	-0,395	0,423

При нормативі 70 – 80% суб'єкт підприємництва за рахунок наявних грошових коштів й їх еквівалентів та очікуваних надходжень від погашення поточної дебіторської заборгованості може розрахуватися з поточними боргами на кінець 2021 р. на 116,6%, на кінець 2022 р – на 111,9%, а на кінець 2023 р. – 152,8%. Таким чином бачимо, що на протязі усього досліджуваного періоду ТОВ «Шредер» у повному обсязі погасив би свої поточні зобов'язання. При цьому слід відмітити, що показник швидкої ліквідності у 2023 році зріс на 0,409 процентних пункти у порівняні із 2022 р.

Щодо коефіцієнта загальної ліквідності відмітимо, що цей показник вказує на те, скільки оборотних активів має суб'єкт підприємництва на кожну гривню поточних зобов'язань. Оскільки зазвичай поточні зобов'язання суб'єкт господарювання перекриває оборотними активами, і враховуючи, що у нього спостерігається переважання оборотних активів над поточними зобов'язаннями, то такий суб'єкт підприємництва вважається ліквідним. Саме величина цього перевищення визначається як коефіцієнт покриття, і рекомендовано, щоб оборотні активи перевищували поточні зобов'язання удвічі. У бухгалтерській та аналітичній практиці західних країн, критичне значення цього показника визначається в залежності від галузі та виду діяльності підприємства. Зважаючи на це відмітимо, що значення показника загальної ліквідності на ТОВ «Шредер» було менше 2 лише у 2022 році. Вже у

2023 році можна спостерігати зростання даного коефіцієнта на 0,423, й станом на кінець 2023 року він становив 2,125.

Отже, за результатами аналізу ми можемо зробити висновок, що ТОВ «Шредер» в 2021-2023 роках є платоспроможним і ліквідним.

2.3. Аналітична діагностика ділової активності як детермінанта інформаційної безпеки підприємств

На сучасному етапі економічного розвитку, успішне функціонування суб'єктів підприємництва залежить від ефективності діагностики їх ділової активності. Ділова активність, яка є важливим показником розвитку, потребує постійного моніторингу для виявлення системних проблем на різних рівнях управління та прийняття необхідних заходів для їх вирішення. Це сприяє зменшенню ризиків, підвищенню фінансової стійкості, ліквідності та конкурентоспроможності компанії. У зв'язку з цим, питання діагностики ділової активності суб'єкта підприємництва стає надзвичайно актуальним, оскільки це передумова для ефективного функціонування, що дозволить оперативно виявляти проблеми й вносити зміни стратегію розвитку компанії.

«Ділова активність – це комплексна характеристика, що охоплює різні аспекти діяльності підприємства» [58].

У широкому розумінні, як відмічають Тютюнник Ю. М., Дорогань-Писаренко Л. О. та Тютюнник С. В. «ділова активність означає зусилля, спрямовані на просування підприємства на ринках продукції, праці, капіталу» [50, с. 310].

Ткачук Г. Ю. відмічає, що «ділова активність – це економічна категорія, яка характеризує економічну діяльність підприємства з позицій внутрішніх його змін і виявляється через зміну її інтенсивності в часі [48].

Водночас Н. Б. Кащена та О. О. Горошанська відмічають, що «ділова активність підприємства відображає ступінь його життєздатності в умовах

нестабільної економіки, який залежить від застосовуваних керівництвом управлінських принципів, що виявляються через спектр реальних дій, спрямованих на динамічність розвитку суб’єкта господарювання і досягнення ним поставлених цілей та заданих програм» [22].

Таким чином, ділова активність - це комплексна оцінка ефективності споживання суб’єктом підприємництва ресурсів, як виробничих так і фінансових й яка відображає результативність його функціонування та встановлює оптимальне співвідношення темпів зростання ключових показників. Проявом ділової активності суб’єкта підприємництва є його постійний розвиток та зростання обсягів доходів та рівня прибутку.

Управління діловою активністю становить основу для успішної діяльності компанії, оскільки вона визначає її конкурентоспроможність. Ефективне використання ресурсів суб’єкта підприємництва залежить від рівня ділової активності, який може бути досягнутий шляхом встановлення правильних пріоритетів і цілей. Керівники та фахівці з фінансів повинні проводити об'єктивну оцінку ділової активності фірми, що дозволить покращити ефективність діяльності суб’єкта підприємництва, оперативно виявляти загрозливі тенденції та уникати їх. Зважаючи на це відмітимо, що Ясіновська І. та Фелісєєв, В. виокремлюють «три рівні ділової активності підприємства» [58] (рис. 2.3.).

Слід також відмітити, що оцінка ділової активності суб’єкта підприємництва включає дві основні групи критеріїв, а саме:

- ефективність використання суб’єктом підприємництва ресурсів;
- інтенсивність використання ресурсів суб’єктом підприємництва. Ефективність визначається відношенням результату діяльності суб’єкта підприємництва до обсягу ресурсів, що призвели до цього результату. Основними показниками ефективності є показники прибутковості або рентабельності. Інтенсивність використання ресурсів оцінюється з урахуванням чинника часу, й для «її вимірювання використовують показники оборотності, які відображають загальний час обороту в днях та швидкість обороту» [58].

-

Рис. 2.3. «Рівні ділової активності підприємств» [58]

«Оцінка інтенсивності використання ресурсів передбачає визначення та аналіз наступних показників: коефіцієнт оборотності активів; коефіцієнт оборотності власного капіталу; коефіцієнт оборотності дебіторської заборгованості; коефіцієнт оборотності кредиторської заборгованості; тривалість обертів дебіторської та кредиторської заборгованостей; коефіцієнт оборотності матеріальних запасів; коефіцієнт оборотності основних засобів (фондовіддачі); період обороту чистого робочого капіталу» [58].

Враховуючи це, у таблиці 2.7. відображено результати аналізу рівня ділової активності ТОВ «Шредер» (табл. 2.7).

Таблиця 2.7.

Основні показники ділової активності ТОВ «Шредер» за 2022–2023 р.

Показник	2022 р.	2023 р.
Коефіцієнт оборотності активів	0,18	2,14
Оборотність необоротних активів (фондовіддача)	1,12	15,50
Коефіцієнт оборотності дебіторської заборгованості	0,38	6,32
Коефіцієнт оборотності власного капіталу	0,33	3,95
Тривалість обертів дебіторської заборгованості	969	58
Коефіцієнт оборотності кредиторської заборгованості	0,39	4,73
Тривалість обертів кредиторської заборгованості	944	77
Коефіцієнт оборотності матеріальних запасів	4,34	6,34

Із таблиці 2.7 можемо зробити висновок про позитивну тенденцію до зростання рівня ділової активності ТОВ «Шредер» у 2023 р. у порівняні із 2022 р. Так, у 2023 рр. прослідковувалося зростання коефіцієнта оборотності активів на 1,96 й становить 2,14.

Ефективне використання основних засобів ТОВ "Шредер" відображається у зростанні оборотності необоротних активів (фондовіддачі), що є позитивним показником. Як видно з таблиці даний показник зріс на 14,38 з 1,12 до 15,5.

Наступним коефіцієнтом є коефіцієнт оборотності власного капіталу, який показує ефективність останнього. ТОВ «Шредер» має позитивне значення даного показника. Так, на кінець 2023 р. було вироблено продукції на 3,98 гривень на кожну гривню залучених коштів власників. Це позитивна тенденція, викликана суттєвим зростанням доходу фірми.

Щодо коефіцієнта оборотності запасів відмітимо, що він відображає кількість оборотів товарно-матеріальних ресурсів суб’єкта підприємництва за 2022-2023 рр. період. Зростання цього показника вказує на відносне зменшення запасів і незавершеного виробництва або на зростання попиту на готову продукцію фірми. На ТОВ «Шредер» коефіцієнт оборотності запасів

підвищився з 4,34 до 6,34 обороти в рік, що дозволяє зробити висновок про ефективність управління запасами на ТОВ «Шредер»

Щодо коефіцієнта оборотності дебіторської заборгованості відмітимо, що даний показник відображає, скільки разів дебітори виплатили свої зобов'язання перед компанією протягом року. За результатами аналізу встановлено, що на ТОВ «Шредер» прослідковується зростання оборотності дебіторської заборгованості. Так, якщо в 2022 р дебіторська заборгованість фірми зробила 0,38 обороти, то в 2023 р. – вже аж 6,32 оборотів. Такий результат є наслідком коригування політики фірми щодо управління дебіторською заборгованістю.

Коефіцієнт оборотності кредиторської заборгованості показує, скільки разів кредиторська заборгованість обернулася протягом року. Іншими словами можна сказати, що даний коефіцієнт показує, скільки разів суб’єкт підприємництва погашав свої зобов'язання перед постачальниками, підрядниками та іншими контрагентами. За результатами аналізу встановлено, що оборотність кредиторської заборгованості збільшилася з 0,39 у 2022 році до 4,73 у 2023 році. Таким чином можемо стверджувати, що у 2023 році ТОВ «Шредер» пришвидшилось в погашенні своєї заборгованості.

Отже, ділова активність визначається як показник, що оцінює ефективність та потенціал компанії через систему якісних і кількісних критеріїв. Цей показник дозволяє оцінити рівень ефективності, конкурентоздатність та готовність суб’єкта підприємництва пристосовуватися до кризових умов. Аналіз ділової активності ТОВ "Шредер" підтверджує, що компанія проявляє високу ефективність у кризових умовах.

Висновки до розділу 2

Узагальнюючи результати дослідження методики аналізу складових інформаційної безпеки підприємства, можна зробити наступні висновки:

1. Встановлено, що на ТОВ «Шредер» відслідковується постійний ріст вартості майна протягом 2021-2023 років. У структурі майна ТОВ «Шредер»

левову частину займають оборотні активи, які у 2021 році становили 80,3% від валюти балансу, у 2022 році - 86,5%, а у 2023 році - 85,9%, що свідчить про позитивну тенденцію. Щодо необоротних активів ТОВ «Шредер, то з'ясовано, що у порівнянні з 2021 роком, у 2022 році вартість необоротних активів зросла на 11752 тис. грн. або на 8,4%, досягнувши рівня 152469 тис. грн. У 2023 році відбулося подальше зростання на 27688 тис. грн. або на 18,1%. Левову частку у структурі необоротних активів займають основні засоби, а саме 92,7% у 2021 р.; 90,7% у 2022 р.; 91,4% у 2023 р.

2. Величина власного капіталу на підприємстві постійно зростає. Так, протягом досліджуваного періоду спостерігається зростання капіталу з 434569 тис. грн. до 755222 тис. грн., або на 73,8%. Однак не зважаючи на таке зростання, частка власного капіталу у валюті балансу зменшилася на 1,5 процентних пункти з 60,7% у 2021 році до 59,2 % у 2023 році. Разом з тим, якщо порівнювати із 2022 роком, то простежується зростання частки власного капіталу у валюті балансу на 10,3 процентних пункти.

3. За результатами аналізу відносних показників фінансової стійкості встановлено, що ТОВ «Шредер» має високий рівень фінансової стійкості. Так, значення коефіцієнта автономії показує на те, що на кінець 2021 р. частка власного капіталу у валюті балансу становила 61%, на кінець 2022 р. – 49%, а на кінець 2023 р. – 59%, що на 0,1 процентних пункти більше, ніж у 2022 р. При цьому слід відмітити, що оптимальне значення даного показника становить більше 50%. Високий рівень фінансової стійкості ТОВ «Шредер» підтверджується також і іншими показниками. Так, коефіцієнт фінансової залежності є оберненим до показника автономії, й при оптимальному значенні менше двох, на кінець 2023 року він становив 1,69, що на 0,36 менше ніж у 2022 році. Коефіцієнт фінансування показує, що на кінець 2023 року на 1 гривню власного капіталу припадає 0,69 грн залученого капіталу, що на 0,04 грн більше ніж у 2021 році, й на 0,36 грн більше ніж у 2022 році. Коефіцієнт забезпеченості оборотних активів власними коштами при нормативі більше 0,1, на кінець 2021 р. мав значення 0,02. За 2022 р. даний показник зріс на 0,05 до

0,07, що свідчить про підвищення фінансової стійкості ТОВ «Шредер» у 2022 р. За 2023 р. даний коефіцієнт у порівняні з 2022 р. збільшився на 0,06, й на кінець 2023 р. становив 0,13, що відповідає значенню оптимального рівня даного показника. Коефіцієнт маневреності власного капіталу показує, що на кінець 2021 р. 69,0% власних коштів було вкладено в оборотні активи ТОВ «Шредер», а на кінець 2023 р. вже 77,0%. Тобто за 2021-2023 рр значення коефіцієнта маневреності зросло й це свідчить про підвищення фінансової стійкості компанії. Слід також відмітити, що значення даного коефіцієнта перевищує оптимальне його значення, що становить більше 0,5.

4. За результатами аналізу ліквідності балансу ТОВ «Шредер» встановлено, що баланс підприємства є ліквідним, а підприємство відповідно платоспроможним. Так, станом на кінець 2021 р., 2022 р. та 2023 р., ТОВ «Шредер» був у спромозі погасити поточних зобов’язань 6,3%, 11,9% та 27,7% відповідно. За рахунок наявних грошових коштів й їх еквівалентів та очікуваних надходжень від погашення поточної дебіторської заборгованості компанія може розрахуватися з поточними боргами на кінець 2021 р. на 116,6%, на кінець 2022 р – на 111,9%, а на кінець 2023 р. – 152,8%. При цьому слід відмітити, що показник швидкої ліквідності у 2023 році зріс на 0,409 процентних пункти у порівняні із 2022 р. Значення показника загальної ліквідності на ТОВ «Шредер» було менше 2 лише у 2022 році, а вже у 2023 році можна спостерігати зростання даного коефіцієнта на 0,423, й станом на кінець 2023 року він становив 2,125.

5. Ділова активність визначається як показник, що оцінює ефективність та потенціал компанії через систему якісних і кількісних критеріїв. Цей показник дозволяє оцінити рівень ефективності, конкурентоздатність та готовність суб’єкта підприємництва пристосовуватися до кризових умов. Аналіз ділової активності ТОВ "Шредер" підтверджує, що компанія проявляє високу ефективність у кризових умовах.

РОЗДІЛ 3
ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

3.1. Сучасні практики впровадження аудиту інформаційної безпеки підприємства

У світі, що постійно змінюється через технологічні інновації та ростучі загрози кібератак, безпека інформації стає все важливішою для суб'єктів підприємництва будь-яких сфер. Дані, які вони мають, стають ключовим активом, і захист цих активів стає вирішальним для забезпечення стабільності та успішності роботи суб'єкта господарювання.

Загрози кібербезпеки постійно збільшуються, ставлячи перед керівництвом компанії «питання»: потрібно забезпечити належний захист інформації в умовах постійних змін технологій та вдосконалення методів атак. Порушення безпеки, такі як витік конфіденційної інформації або крадіжки даних, можуть значно нашкодити репутації суб'єкта підприємництва, призвести до фінансових втрат та негативно вплинути на його функціонування.

Для ефективного захисту інформації суб'єкт підприємництва має проводити аудит, щоб оцінити поточні заходи захисту, виявити можливі вразливості та ризики і розробити стратегії для їхнього недопущення.

Аудит інформаційної безпеки — це процес об'єктивного оцінювання рівня захищеності інформації на фірмі. Даний аудит включає незалежні перевірки системних файлів та операцій з документами. Його метою є виявлення можливих прогалин у технічному захисті, що можуть виникати через неправильну конфігурацію програм для захисту інформації на фірмі.

Зазвичай для проведення аудиту інформаційної безпеки залучаються зовнішні консалтингові компанії, які спеціалізуються у цій сфері. Ініціатором аудиту може бути керівництво суб'єкта підприємництва, відділ автоматизації або служба інформаційної безпеки. У деяких випадках аудит може бути

проведений за вимогою страхових компаній або регулюючих органів.

Щодо різновидів аудиту інформаційної безпеки підприємства Рой Я. В., Мазур Н. П. та Складанний П. М. відмічають, що можна виокремити: «експертний аудит безпеки, в ході якого виявляються недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в процедурі обстеження; оцінка відповідності рекомендаціям міжнародного стандарту ISO 17799, а також вимогам керівних документів; інструментальний аналіз захищеності інформацій, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи; комплексний аудит, який включає в себе всі перераховані вище форми проведення обстеження» [44, с. 87].

Зважаючи на це відмітимо, що кожен із наведених різновидів аудиту інформаційної безпеки підприємства може проводитися ізольовано або у поєднанні, в залежності від того, які завдання стоїть перед суб'єктом підприємництва. Як об'єкт аудиту може бути як інформаційна система суб'єкта підприємництва в цілому, так і його окремі частини, де здійснюється обробка інформації, що потребує захисту.

Слід також зазначити, що аудит інформаційної безпеки, незалежно від його способу здійснення, включає чотири основні етапи, на кожному з яких проводиться конкретний набір процедур.

Так, на першому етапі спільно з клієнтом узгоджується план, що визначає обсяг і послідовність робіт. Основна мета цього плану - чітко визначити параметри обстеження. Це допомагає уникнути можливих непорозумінь після завершення аудиту, оскільки враховує права й обов'язки кожної сторони. Зазвичай план містить таку основну інформацію:

- склад робочих груп від виконавця та клієнта для проведення аудиту інформаційної безпеки суб'єкта господарювання;
- перелік та місцезнаходження об'єктів клієнта, які підлягають огляду;
- модель загроз інформаційній безпеці суб'єкта підприємництва, на основі якої здійснюється її аудит;

- список інформації, що буде передана виконавцю;
- перелік інформаційних, програмних та інших ресурсів, що розглядаються як об'єкти захисту;
- категорії користувачів, які розглядаються як потенційні порушники.

На другому етапі здійснюється збір вихідної інформації. Методи збору даних включають інтерв'ювання працівників компанії замовника, заповнення анкет, аналіз організаційних та технічних документів, а також використання спеціальних інструментів.

На третьому етапі аудиту інформаційної безпеки суб’єкта господарювання проводиться аналіз отриманої інформації з метою оцінки поточного рівня захисту його інформаційних систем. Результати цього аналізу використовуються на четвертому етапі для розробки рекомендацій щодо підвищення рівня захисту інформаційних систем від можливих загроз.

Зважаючи на вищесказане відмітимо, що якість аудиту інформаційної безпеки значно впливає на повноту та точність інформації, що збирається під час початкової фази. У зв’язку з цим потрібно включити такі дані, як організаційно-розпорядчі документи, що стосуються питань інформаційної безпеки суб’єкта підприємництва, відомості про програмне та апаратне забезпечення інформаційних систем компанії, інформацію про захисні засоби, встановлені в цих системах і т. д. (табл. 3.1)

Як вже зазначалося, для отримання вихідних даних використовуються різноманітні методи. Перший метод - інтерв'ювання працівників компанії замовника, які мають потрібну інформацію. Інтерв'ю зазвичай проводиться з технічними фахівцями та керівниками фірми, і перелік питань обговорюється заздалегідь. Другий метод - надання опитувальних листів, які співробітники заповнюють самостійно. У випадках, коли ця інформація не є достатньою, проводиться додаткове інтерв'ю. Третій метод - аналіз організаційно-технічної документації, яку використовує замовник. Четвертий метод - використання спеціалізованого програмного забезпечення, яке надає необхідну інформацію про програмно-апаратне забезпечення суб’єкта підприємництва.

Таблиця 3.1

Вихідні дані, потрібні для аудиту інформаційної безпеки компанії

Тип інформації	Склад вихідних даних
«Організаційно-розпорядча документація з питань інформаційної безпеки» [44]	«політика інформаційної безпеки ІС; керівні документи (накази, розпорядження, інструкції) з питань зберігання, порядку доступу і передачі інформації; регламенти роботи користувачів з інформаційними ресурсами ІС» [44]
«Інформація про апаратне забезпечення хостів» [44]	«перелік серверів, робочих станцій і комунікаційного устаткування, встановленого в ІС; апаратні конфігурації серверів і робочих станцій; відомості по периферійному обладнанні» [44]
«Інформація про загальносистемне ПЗ» [44]	«відомості про операційну систему встановлену на робочих станціях і серверах; відомості про СУБД, встановлену в ІС» [44]
«Інформація про прикладне ПЗ» [44]	«перелік прикладного ПЗ загального і спеціального призначення, встановленого в ІС; опис функціональних завдань, що вирішуються за допомогою прикладного ПЗ» [44]
«Інформація про засоби захисту, що встановлені в ІС» [44]	«виробник засобів захисту; конфігураційні налаштування засобів захисту; схема встановлення засобів захисту» [44]
«Інформація про топологію ІС» [44]	«карта локальної обчислювальної мережі, включаючи схему розподілу серверів і робочих станцій за сегментами мережі; типи каналів зв'язку, що використовуються в ІС; використовувані в ІС мережеві протоколи; схема інформаційних потоків ІС» [44]

Після збирання відповідної інформації відповідними експертами здійснюється її аналіз для оцінки поточного рівня захисту системи. Під час такого аналізу визначаються можливі ризики інформаційної безпеки суб'єкта підприємництва, що можуть виникнути. Ризик, по суті, представляє собою оцінку того, наскільки ефективно існуючі засоби захисту можуть запобігти інформаційним атакам на суб'єкт господарювання.

Слід також відмітити, що існують дві основні групи методів оцінки ризиків інформаційної безпеки суб'єкта господарювання. Перша група дає можливість визначити рівень ризику шляхом оцінки відповідності певним

вимогам щодо інформаційної безпеки компанії. Такі вимоги можуть бути визначені в різних документах, включаючи політику безпеки компанії, законодавство, міжнародні стандарти та рекомендації виробників програмного та апаратного забезпечення.

Друга група методів базується на визначенні ймовірності і наслідків атак. Ризик кожної атаки обчислюється як добуток ймовірності атаки та величини можливого збитку. Ці значення визначаються відповідно власником інформаційних ресурсів та експертами, що проводять аудит інформаційної безпеки компанії.

При чому відмітимо, що методи обох груп можуть застосовувати якісні або кількісні шкали для оцінки ризиків. У випадку застосування кількісних шкал ймовірність та збиток можуть виражатися числами, тоді як у випадку якісних шкал вони оцінюються певними поняттями, які відповідають певним інтервалам числової шкали.

Кількість рівнів, як відмічають Рой Я., Мазур Н., та Складанний П. може коливатися в залежності від методів оцінки ризиків, що використовуються. Так, у табл. 3.2 та табл. 3.3. наведено приклади якісних шкал оцінки ризиків інформаційної безпеки, де для визначення рівнів збитків та ймовірності атаки використовується п’ять концептуальних рівнів.

Таблиця 3.2

«Якісна шкала оцінки рівня збитку» [44]

№	Рівень збитку	Опис
1	Малий	«Незначні втрати матеріальних активів, які швидко відновлюються, або незначні наслідки для репутації компанії» [44]
2	Помірний	«Помітні втрати матеріальних активів або помірні наслідки для репутації компанії» [44]
3	Середньої тяжкості	«Істотні втрати матеріальних активів або значної шкоди репутації компанії» [44]
4	Великий	«Великі втрати матеріальних активів і великих втрат репутації компанії» [44]
5	Критичний	«Критичні втрати матеріальних активів або повна втрата репутації компанії на ринку, що робить неможливим її подальшу діяльність»

Таблиця 3.3

«Якісна шкала оцінки ймовірності проведення атаки» [44]

№	Імовірність атаки	Опис
1	Дуже низька	«Атака практично ніколи не буде проведена» [44]. «Відповідає числовому інтервалу ймовірності [0, 0,25)» [44]
2	Низька	«Вірогідність проведення атаки досить низька» [44]. «Відповідає числовому інтервалу ймовірності [0,25, 0,5)» [44]
3	Середня	«Вірогідність проведення атаки приблизно дорівнює 0,5» [44]
4	Висока	«Атака швидше за все буде проведена» [44]. « Відповідає числовому інтервалу ймовірності (0,5, 0,75)» [44]
5	Дуже висока	«Атака напевно буде проведена» [44]. «Відповідає числовому інтервалу ймовірності (0,75, 1) [44]

Для оцінки рівня ризику за якісними шкалами використовуються спеціальні таблиці. У цих таблицях у першому стовпці вказуються концептуальні значення збитку, а у першому рядку - рівні можливості атаки. Кожна комірка таблиці, яка знаходиться на перетині певних рядків та стовпців, містить відповідний рівень ризику безпеки (табл. 3.4). Розмірність цих таблиць залежить від кількості рівнів можливості атаки і збитків.

Таблиця 34

«Визначення рівня ризику інформаційної безпеки по якісної шкалою» [44]

	Вірогідність атаки				
Збиток	**Дуже низька**	**Низька**	**Середня**	**Висока**	**Дуже висока**
Малий	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
Помірний	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
Середньої тяжкості	Низький ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Великий	Середній ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Критичний	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

При розрахунку рівня ризику за допомогою якісних шкал використовуються різні методи, а саме: експертні оцінки, статистичні методи та елементи теорії прийняття відповідних управлінських рішень. Статистичні методи включають передбачають аналіз існуючих даних про минулі події, що

стосуються порушень інформаційної безпеки суб’єкта підприємництва, для прогнозування ймовірності атак і рівнів збитку. Однак, через обмежену кількість статистичних даних, ці методи не завжди застосовні.

Експертні оцінки передбачають аналіз результатів групи експертів у галузі інформаційної безпеки, які використовують свій досвід для визначення рівнів ризику. Елементи теорії прийняття рішень дозволяють застосовувати складні алгоритми обробки даних, що отримані від групи експертів.

Слід також відмітити, що існують спеціалізовані програмні продукти, які автоматизують процес аналізу вихідних даних і розрахунку ризиків під час аудиту інформаційної безпеки суб’єкта підприємництва.

Після проведення аудиту інформаційної безпеки суб’єкта господарювання розробляються рекомендації з покращення організаційно-технічного забезпечення безпеки на фірмі. Ці рекомендації можуть включати в себе заходи для зменшення виявлених ризиків, такі як встановлення додаткових засобів захисту або зміна архітектури інформаційних потоків. Також розглядається можливість страхування для зменшення ризику. Наприкінці процедури аудиту результати формалізуються у вигляді звітного документа для замовника, який включає опис меж аудиту, структуру ІС, виявлені вразливості, використані методи і засоби, рекомендації та пропозиції до подальших заходів.

Слід також зазначити, що для забезпечення відповідного рівня інформаційної безпеки у системах обліку необхідно вживати ряд заходів, що гарантують доступність даних, цілісність та конфіденційність [19]. Серед таких заходів можна виділити наступне:

- регулярна оцінка ризиків, що пов’язані зі обліком, для виявлення потенційних загроз та ризиків;
- захист від шкідливих програм, через використання антивірусного програмного забезпечення та введення політики безпеки щодо користування електронною поштою, Інтернетом та USB-накопичувачами;
- систематичне оновлення програмного та апаратного забезпечення для зменшення ризику кібератак;

- ефективний контроль доступу до даних, щоб уникнути несанкціонованого доступу до конфіденційної інформації;
- навчання та підвищення кваліфікації працівників компанії щодо заходів забезпечення інформаційної безпеки та культури безпеки загалом;
- проведення регулярного резервного копіювання даних для забезпечення можливості відновлення у разі проблем із системою обліку;
- проведення регулярних аудитів систем інформаційної безпеки для виявлення можливих порушень та недоліків і прийняття заходів щодо їх усунення.

Підводячи підсумки відмітимо, що аудит інформаційної безпеки суб’єкта підприємництва є одним із ключових методів для отримання незалежної та об'єктивної оцінки рівня його захищеності від потенційних загроз. Результати такої перевірки становлять основу для розробки стратегії розвитку системи інформаційної безпеки суб’єкта господарювання. Важливо зрозуміти, що аудит інформаційної безпеки не може бути одноразовим, він повинен проводитися регулярно. Лише в такий спосіб аудит інформаційної безпеки буде ефективним та сприятиме підвищенню рівня захисту інформації в компанії.

Окрім цього відмітимо, що система обліку суб’єкта господарювання повинна бути захищеною від потенційних кібератак і забезпечувати цілісність, доступність та конфіденційність інформації. Для досягнення цього необхідно систематично оновлювати програмне забезпечення, оцінювати ризики, використовувати надійні паролі, захищати мережу та здійснювати систематичне резервне копіювання інформації. Крім того, працівники компанії повинні мати відповідну підготовку та розуміти культуру безпеки та принципи інформаційної безпеки.

3.2. Інтегральний аналіз ризиків у системі досягнення інформаційної безпеки підприємства

Ризик є невід'ємною частиною нашого життя, пов'язаною з усіма сферами нашої діяльності. Він виникає внаслідок соціальної взаємодії та прагнення досягти різноманітних цілей, таких як забезпечення національних інтересів чи безпеки держави, а також успішної діяльності суб'єктів підприємництва. «Виникнення ризику відбулося на початковому етапі становлення цивілізації з першою людиною, яка усвідомила можливість небезпеки, набувши ще більшої актуальності із усвідомленням відповідальності за прийняті рішення» [15].

На Заході більшість компаній має досвід аналізу ризиків, але в Україні ця практика недостатньо розвинена. Найчастіше аналізом ризику називають будь-які, отримані в ході роботи, дані, використовуючи це словосполучення як "модного".

Для виявлення ризиків інформаційної безпеки суб’єкта господарювання застосовують різні методики й стандарти управління інформаційними ризиками.

Аналіз ризиків інформаційної безпеки суб’єкта господарювання дозволяє виявити «слабкі місця», оцінити їх можливий вплив та обрати відповідні захисні заходи для необхідних систем і процесів. Ці методи дозволяють забезпечити ефективний захист інформаційного простору суб’єктів господарювання і реагувати на загрози вчасно.

Ризик є складовою фінансово-економічної активності суб’єктів підприємництва і вимагає належної уваги від фінансових керівників. Наявність певного рівня ризику в операціях не обов'язково означає, що їх слід уникати. Відмова від певних дій може призвести до втрати очікуваних економічних ефектів. Управління ризиками вимагає збалансованості та обдуманості фінансових рішень.

У зв’язку з цим, для визначення зв'язку між ризиком діяльності і загрозою інформаційній безпеці суб’єкта господарювання, розглянемо визначення

ризику.

Так,Жук Н.Т. відмічає, що «ризик – це результат впливу невизначеності на досягнення поставлених цілей; безпосередня певна подія, яка здатна принести кому-небудь прибуток або збитки» [15].

М. Парфентія відмічає, що під ризиком слід розуміти «ймовірність настання негативних фінансових наслідків (економічного збитку або фінансових втрат) його дій по причині його прорахунків чи у силу непрогнозованості та некерованості певних факторів» [39, с. 44]

І. Бланк розглядає ризик як специфічну категорію, що виникає внаслідок невизначеності у внутрішніх і зовнішніх умовах діяльності суб’єкта господарювання [3]. Науковець виокремлює основні характеристики ризику,а саме: «наявність економічної природи, об'єктивність проявлення, дія в умовах вибору, альтернативність вибору, цілеспрямована дія, імовірність досягнення мети, невизначеність наслідків, очікувана несприятливість наслідків, динамічність рівня, суб'єктивність оцінки» [3].

Карпишин Н.І. та Жукевич С.М. трактують ризик «як об'єктивну категорію, яка може мати вартісну оцінку та притаманна кожному фінансовому або господарському рішенню» [20]. Таким чином, науковці розглядають ризик як всепроникаючий феномен, який необхідно враховувати при прийнятті рішень, інакше це може призвести до невдач у діяльності суб’єкта підприємництва.

На нашу думку, слід погодитись із твердженням Мельник С. І. щодо суб’єктивно-об’єктивної природи ризику, визначаючи його як економічну категорію, де реальний очікуваний результат управління та оцінювання є невизначеним [33]. Основним аргументом даного твердження, як відмічають Карпишин Н.І. та Жукевич С.М. «є той факт, що процес фінансово-господарської діяльності, прийняття управлінських рішень здійснюється людиною, колективом, які вступають в суб’єктивні відносини» [20].

Таким чином, ризик є як суб’єктивним, так і об’єктивним, як якісне, так і кількісне вираження наявних чинників невизначеності. У зв’язку з цим, в

умовах невизначеності ризик вимагає вибору серед різних альтернатив та оцінки ймовірних результатів, що свідчить про його діалектичну природу, що об’єднує об’єктивне та суб’єктивне.

Отже, більшість вчених стверджують, що сутність ризику полягає в невизначеності результатів будь-якої економічної діяльності суб’єкта господарювання. По суті, як зазначає Горячева К.С., «невизначеність трактується як наявність неповної інформації про умови прийняття господарських рішень або відсутність такої вичерпної інформації» [10]. Варто зазначити, що джерелом ризику є фактори, які впливають на фінансову, господарську та комерційну діяльність суб’єкта підприємництва, що призводить до невизначеності у результаті їх діяльності.

Слід також відмітити, що оскільки оцінка підприємницького ризику є складним завданням, вона не може бути безпосереднім об'єктом системи обліку, оскільки остання, може лише реєструвати ймовірні та фактичні наслідки ризику, а також відображати результати заходів з управління ризиками в господарській діяльності.

У зв’язку з цим, як відмічає Василішин С.І., «в системі обліково-аналітичного забезпечення управління підприємствами важливо аналізувати взаємозв`язок між видами ризиків та об`єктами обліку, на які вони впливають, і статтями фінансової звітності, які такі об`єкти репрезентують» [5].

Найбільш значущі, на нашу думку, типи ризиків, які потребують належного інформаційного забезпечення відображено у таблиці 3.5.

Таблиця 3.5

Обліково-аналітичний базис управління окремими ризиками в системі безпеки підприємства

Класифікаційні групи ризиків	Сутність	Статті фінансової звітності чи об`єкти обліку
1	**2**	**3**
«Інвестиційний ризик» [5]	«Полягає у загрозі нездійснення інвестування чи отримання збитків від здійснення інвестицій» [5]	«Показники зі статтями капітальних чи фінансових інвестицій» [5]

Продовження таблиці 3.5

1	2	3
«Ризик неефективності управління активами» [5]	«Визначається через низький рівень віддачі необоротного та оборотного капіталу, що загрожує внутрішній економічній безпеці підприємства» [5]	«Запаси, дебіторська заборгованість, основні засоби та нематеріальні активи» [5]
«Інфляційний ризик» [5]	«Пов`язаний із негативним впливом на господарську діяльність зростання індексу інфляції» [5]	«Монетарні статті фінансової звітності, особливо гроші та їх еквіваленти» [5]
«Юридичний ризик» [5]	«Полягає в імовірності настання необхідності суттєвих поточних виплат за договірними зобов`язаннями» [5]	«Кредиторська заборгованість та інші види зобов`язань» [5]
«Валютний ризик» [5]	«Зумовлює ймовірність утрати економічних вигід чи зниження вартості окремих об`єктів обліку внаслідок стрімкого зниження валютного курсу» [5]	«Монетарні статті, оцінені в іноземній валюті» [5]
«Кредитний ризик» [5]	«Виникає в разі несплати дебіторами вартості реалізованої продукції, виконаних робіт чи наданих послуг згідно з договірними умовами» [5]	«Статті дебіторської заборгованості» [5]
«Інформаційний ризик» [5]	«Дії або події, які можуть спричинити втрати інформації чи несанкціоноване її використання, а також розголошення комерційної таємниці» [5]	«Рахунки управлінського та фінансового обліку» [5]

«Обліково-аналітичне забезпечення ідентифікації ризиків підприємства являє собою систему збирання, підготовки, реєстрації та обробки даних первинного, бухгалтерського, фінансового, податкового, статистичного та управлінського обліку, а також даних аналітичних розрахунків та необлікової інформації для прийняття на їх основі управлінських рішень, спрямованих на забезпечення захисту інтересів підприємства від зовнішніх та внутрішніх загроз» [47, с. 83].

Однією з ключових вимог до методології обліково-аналітичного забезпечення управління ризиками в системі інформаційної безпеки є урахування різноманітних аспектів, зокрема:

- особливостей функціонування суб’єктів господарювання у конкретних

сферах економіки та їх впливу на систему обліку загалом;

- впровадження діагностики інформаційної безпеки суб'єкта підприємництва;

- інституційних основ системи обліку у контексті управління інформаційною безпекою з огляду на міжнародний та національний досвід;

- розробка методології забезпечення інформаційної безпеки та встановлення організаційних стандартів її захисту;

- обґрунтування архітектури системи обліково-аналітичного забезпечення управління інформаційною безпекою суб'єктів підприємництва;

- розробка методичних підходів до підвищення інформаційної безпеки суб'єкта підприємництва на основі стратегічного аналізу.

Отже, за допомогою послідовного функціонування підсистем обліку, аналізу та контролю забезпечується ухвалення управлінських рішень, зокрема щодо управління ризиками діяльності, що сприятиме належному рівню інформаційної безпеки суб'єктів господарювання (рис. 3.1.).

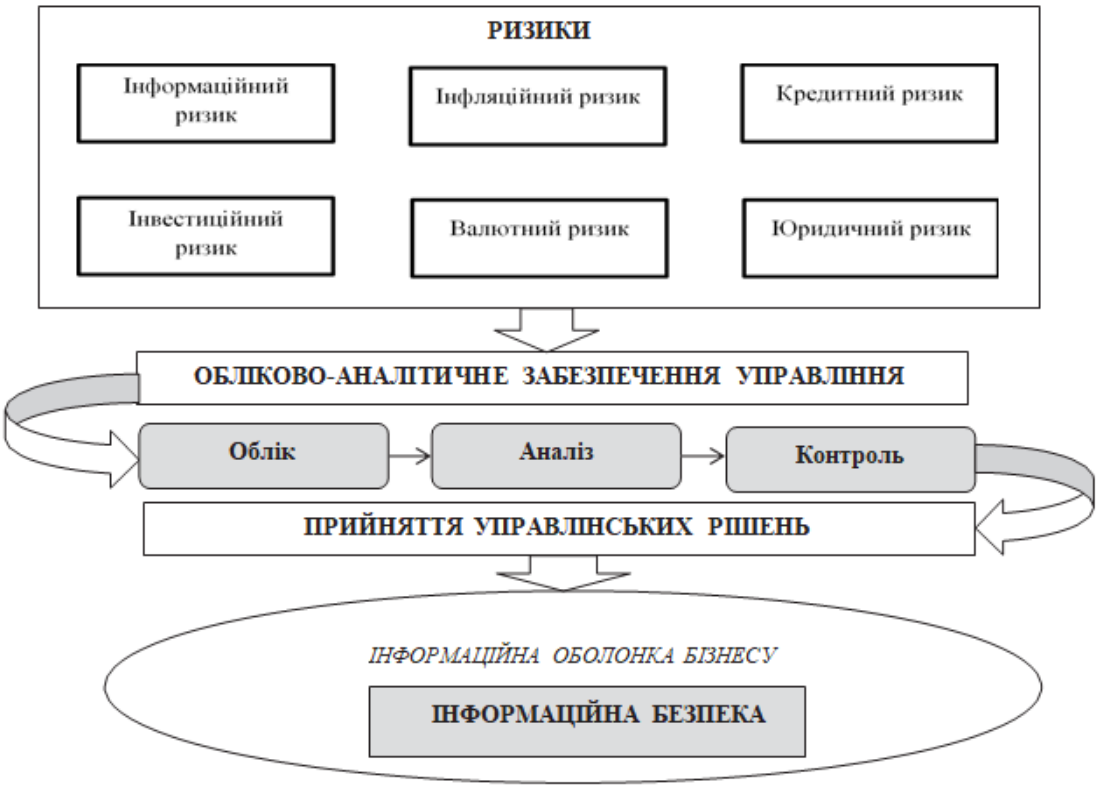

Рис. 3.1. «Структурно-логічна модель обліково-аналітичного забезпечення управління інформаційною безпекою підприємств» [5]

Отже, лише чітке та систематичне організування обліку, аналізу та контролю на кожному етапі виробничого процесу допоможе забезпечити належний рівень безпеки та зменшити ризики для роботи компанії та її інформаційної системи.

Вплив чинників на інформаційну безпеку підприємства відображено на рисунку 3.2.

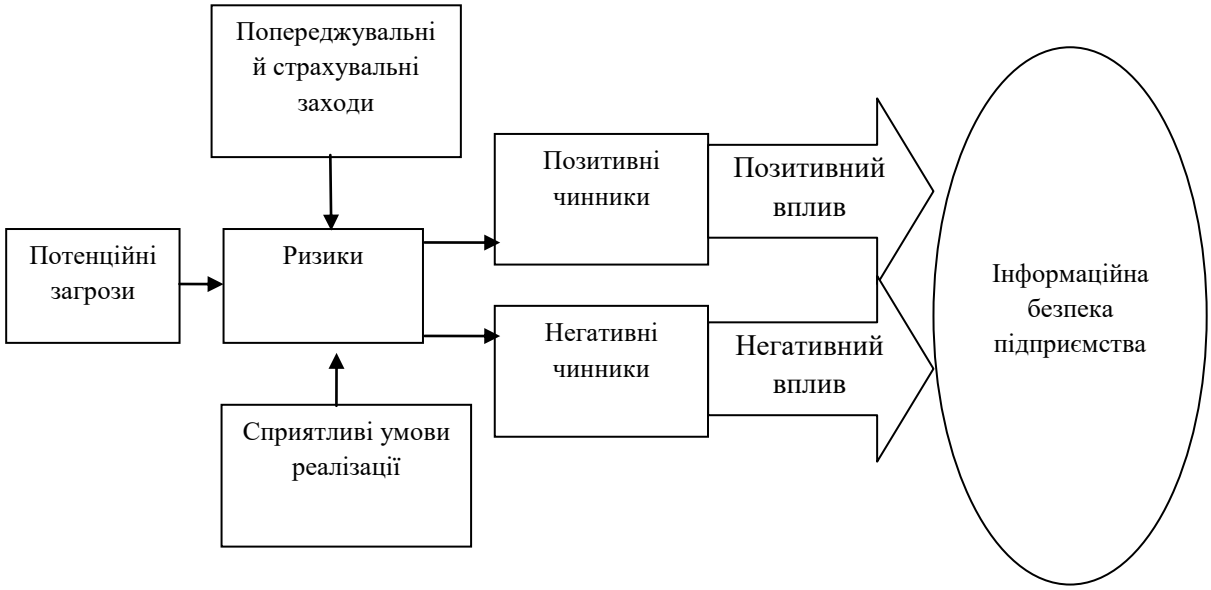

Рис. 3.2. Вплив чинників на інформаційну безпеку підприємства [15, с. 91]

З рисунку бачимо, що чинник негативного впливу є загрозою для суб'єкта підприємництва, а чинник позитивного впливу створює належні умови для суб'єкта підприємництва.

Слід також відмітити, що «важлива роль у визначенні допустимого рівня ризику, прогнозуванні ймовірності настання ризикових подій та своєчасній нейтралізації їх негативних наслідків відводиться ризик-менеджменту» [30].

Для ефективного управління ризиками необхідно мати спеціальну структуру, яка відповідала б за цей процес та мала достатні ресурси: кадрові, фінансові, матеріальні та інформаційні. У кожній великій фірмі має бути

відповідальна особа, що спеціалізується на управлінні ризиками, яка спільно з іншими менеджерами приймає відповідальні рішення. Ризик-менеджер аналізує можливості уникнення або прийняття небажаних ризиків для суб'єкта господарювання.

На даний час, як відмічають Лагун А та Кухарська Н., «існують різні методології, за допомогою яких здійснюється оцінка ризиків, а саме: аналіз і управління ризиками – CRAMM; оцінка активів та вразливості інформаційної безпеки – OCTAVE; управління ризиками в системі інформаційних технологій – NIST SP800-30; методи управління ризиками інформаційної безпеки – ISO / IEC 27005: 2011; оцінка ризиків інформаційної безпеки – ENISA» [30].

Так, метод CRAMM, розроблений Центральним комп'ютерним і телекомунікаційним агентством Великої Британії, є програмним засобом для аналізу та управління ризиками. Він використовує комплексний підхід, поєднуючи кількісні та якісні методи оцінки. CRAMM підходить для різних видів організацій та галузей. Він має комерційний профіль для комерційних організацій та державний профіль для державних установ.

Разом з тим, як відмічають Літвінчук І.С., Корчомний Р.О. та Коршун Н.В. система CRAMM має як переваги, так і недоліки [32].

Переваги використання CRAMM полягають у можливості ідентифікації різних елементів ризику, таких як матеріальні та нематеріальні активи, загрози та заходи безпеки, а також в оцінці потенційного збитку та ймовірності реалізації загрози [32].

До недоліків даної системи варто віднести відсутність звітів з оцінки ризиків та перерахунку максимально допустимих ризиків. Використання CRAMM є складним та тривалим процесом, який вимагає участі висококваліфікованих фахівців та обробки великих обсягів документації, згенерованої цим програмним продуктом. Крім того, вартість ліцензії на програму CRAMM є досить високою.

Методологія OCTAVE, розроблена в США в Інституті програмної інженерії при Університеті Карнегі–Меллона, є інструментом для оцінки

активів та вразливостей інформаційної безпеки. Вона надає можливість розробити практичні методи та рекомендації для оцінювання ризиків і визначає стратегію оцінювання та планування дій забезпечення безпеки інформації на основі цих оцінок.

Методологія OCTAVE має перевагу в тому, що вона оцінює різноманітні ризики, включаючи ті, які не враховані безпосередньо в методології, такі як технічні ризики чи ризики порушення законодавства (це виявляється під час здійснення опитування).

Проте, методологія OCTAVE також має свої недоліки, зокрема, відсутність чітких інструкцій щодо організації моніторингу стану ризиків та відсутність кількісної оцінки ризиків.

«Методологія оцінки ризиків Національного Інституту Стандартів і Технологій США (NIST) передбачає виконання таких етапів: характеристика системи (активу); ідентифікація загроз; ідентифікація вразливостей; аналіз заходів захисту; визначення ймовірності реалізації загроз; аналіз збитків (втрат); визначення ризиків; рекомендації щодо заходів безпеки; формування звітної документації» [30].

Таким чином бачимо, що методологія NIST SP800-30 вичерпно описує всі можливі загрози для інформаційних ресурсів і є придатною для застосування як великим, так і малими суб’єктами господарювання. Однак, недоліком цієї методології є тривалий процес аналізу та відсутність автоматизованих функцій для деяких аспектів.

Окрім цього відмітимо, що більшість існуючих методик, як показують результати дослідження, виявляються непродуктивними та недостатньо інформативними для практичного застосування. Вони часто не містять чітких рекомендацій або настанов щодо конкретних дій, а замість цього базуються на стандартах тієї країни, де були розроблені. Це часто призводить до оцінки не рівня безпеки, а відповідності стандарту. Більшість міжнародних методик залишаються недосяжними для українського ринку через фінансові обмеження. Крім того, втручання людини в процес оцінки ризиків залишається

невирішеним питанням.

Зважаючи на вищесказане відмітимо, що для прогнозування ймовірності виникнення негативних подій у майбутньому, суб’єкти господарювання повинні ретельно аналізувати загрози разом з можливими вразливостями та виявлені там, де їх можна очікувати. Оцінка рівня впливу здійснюється шляхом визначення масштабу можливих збитків, які можуть бути завдані в результаті цих загроз.

Джерела загроз можуть бути різного характеру: природні, антропогенні або екологічні. У процесі аналізу ризиків важливо врахувати всі можливі джерела небезпеки, які можуть призвести до збитків суб’єкта господарювання. Людський фактор є одним з основних джерел загроз через можливість навмисних дій зловмисників або недбалості та помилок співробітників компанії. Навмисні атаки можуть бути спрямовані на отримання несанкціонованого доступу до інформації суб’єкта підприємництва з метою порушення цілісності, доступності або конфіденційності даних.

На рисунку 3.3 наведено структурну схему, що відображає методологію оцінки ризиків для підприємства.

Отже, ідентифікація ризиків інформаційної безпеки є неможливою без вдосконалення наявних методів обліково-аналітичного забезпечення управлінських процесів, які формують стратегію та тактику управлінських рішень. У зв’язку з цим, на нашу думку, ключові напрямки вдосконалення обліково-аналітичного забезпечення управління інформаційною безпекою компанії включають: створення відділів моніторингу інформаційної безпеки компанії; оприлюднення інформації щодо інформаційної безпеки у управлінській звітності; встановлення специфічних підходів до облікової політики, включаючи визнання, оцінку та реєстрацію операцій, пов'язаних з інформаційною безпекою; розроблення документообігу для складання та обробки документів, пов'язаних з інформаційною безпекою; постійний моніторинг та прогнозування рівня безпеки на основі економетричного моделювання та факторного аналізу.

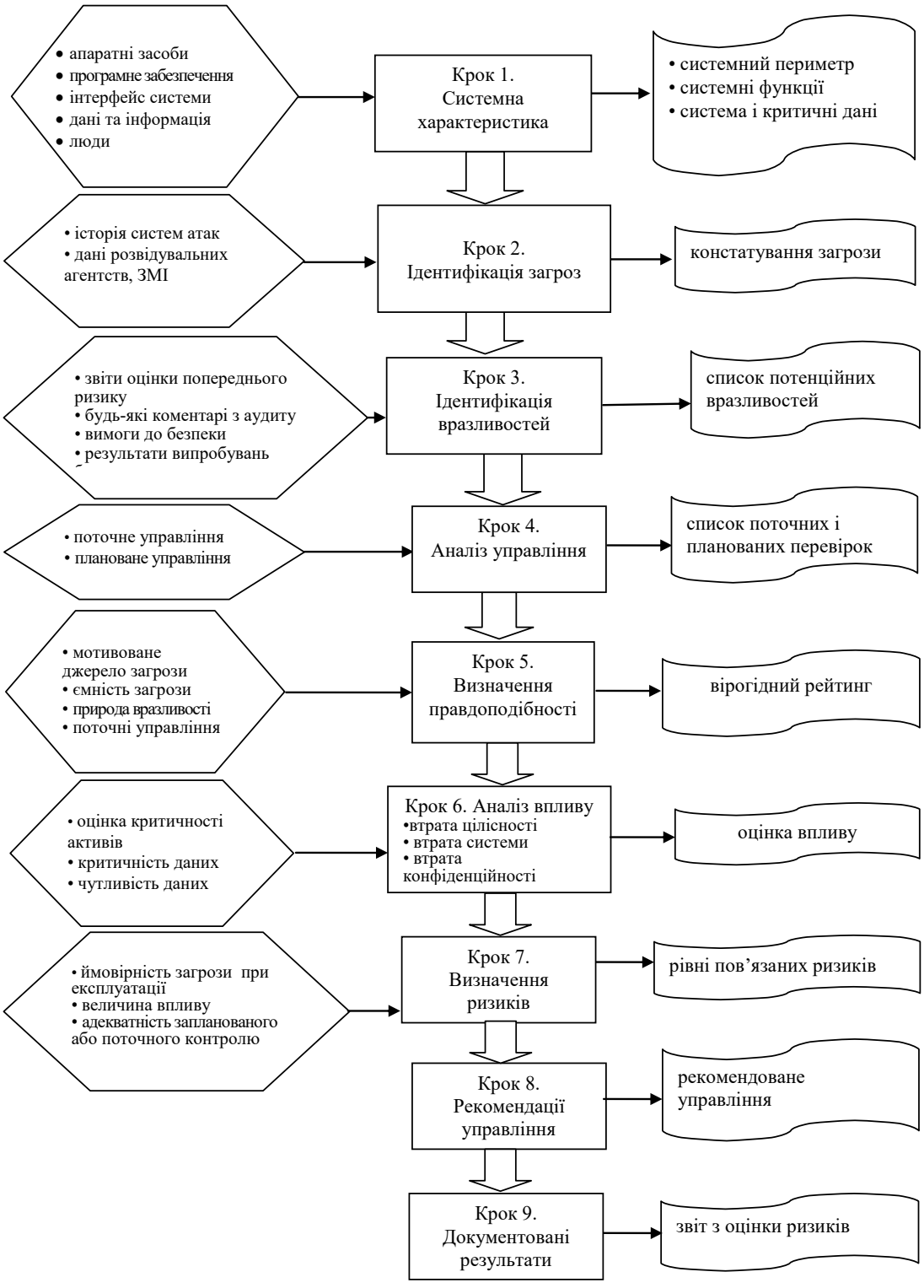

Рис. 3.3. Методика оцінки ризиків інформаційної безпеки підприємства

Окрім цього встановлено, що одним із найбільш прийнятних підходів оцінки ризиків є методологія, розроблена Національним інститутом стандартів і технологій (NIST), яка включає в себе визначення загроз і «вразливих місць»,

аналіз можливих збитків і надання рекомендацій щодо заходів безпеки. Застосування даної методології на практиці сприятиме значному підвищенню рівня інформаційної безпеки суб’єктів господарювання.

Висновки до розділу 3

Узагальнюючи результати дослідження вдосконалення інформаційної безпеки підприємств, можна зробити наступні висновки:

1. Аудит інформаційної безпеки суб’єкта підприємництва є одним із ключових методів для отримання незалежної та об'єктивної оцінки рівня його захищеності від потенційних загроз. Результати такої перевірки становлять основу для розробки стратегії розвитку системи інформаційної безпеки суб’єкта господарювання. Важливо зрозуміти, що аудит інформаційної безпеки не може бути одноразовим, він повинен проводитися регулярно. Лише в такий спосіб аудит інформаційної безпеки буде ефективним та сприятиме підвищенню рівня захисту інформації в компанії.

2. Система обліку суб’єкта господарювання повинна бути захищеною від потенційних кібератак і забезпечувати цілісність, доступність та конфіденційність інформації. Для досягнення цього необхідно систематично оновлювати програмне забезпечення, оцінювати ризики, використовувати надійні паролі, захищати мережу та здійснювати систематичне резервне копіювання інформації. Крім того, працівники компанії повинні мати відповідну підготовку та розуміти культуру безпеки та принципи інформаційної безпеки.

3. Одним із найбільш прийнятних підходів оцінки ризиків є методологія, розроблена Національним інститутом стандартів і технологій (NIST), яка включає в себе визначення загроз і «вразливих місць», аналіз можливих збитків і надання рекомендацій щодо заходів безпеки. Застосування даної методології на практиці сприятиме значному підвищенню рівня інформаційної безпеки суб’єктів господарювання.

ВИСНОВКИ

Узагальнюючи результати проведеного дослідження з питань інформаційної безпеки підприємства на національному та міжнародному рівнях можна зробити наступні висновки і пропозиції:

1. Інформаційна безпека – це набір заходів, спрямованих на захист інформації від неправомірного використання, незаконного доступу, розголошення, пошкодження, маніпулювання або небажаних змін, які можуть вплинути на її конфіденційність, цілісність та доступність.

2. Встановлено, що серед основних вимог до проведення комерційних операцій суб'єктами господарювання важливою є конфіденційність, аутентифікація, цілісність та гарантії збереження таємниці. При забезпеченні власної інформаційної безпеки суб'єкти господарювання намагаються забезпечити її цілісність, конфіденційність, доступність та юридичну значимість, що є основними напрямами. Якщо перші чотири вимоги можна забезпечити технічними засобами, то виконання двох останніх залежить не лише від технічних засобів, а й від організаційних аспектів, зокрема від відповідальності працівників та дотримання інструкцій та законів, що захищають права контрагентів від можливих зловживань.

3. У сучасних умовах конкуренції, коли інформація про стратегію, продукцію, збутову та інші аспекти діяльності суб'єкта господарювання стає ключовою у боротьбі за успіх, й тому важливо пам'ятати про захист цієї інформації. Суб'єкт підприємництва повинен постійно відслідковувати джерела потенційних загроз та бути готовим захищати свою інформацію. Ефективна система управління інформаційною безпекою є ключовим елементом, що дозволяє суб'єкту господарювання працювати ефективно, стійко та залишатися конкурентоспроможним на ринку. Ефективне управління інформаційною безпекою становить основу для розвитку суб'єкта господарювання та підвищення його конкурентоспроможності на ринку. Без належного захисту інформації неможлива забезпеченість економічної стійкості суб'єкта

господарювання.

4. Виокремленні етапи управління інформаційною безпекою, дадуть можливість одержати суб’єкту господарювання такі переваги; систематичне виявлення загроз та вразливостей безпеки компанії; оцінка ризиків та прийняття рішень на основі бізнес-цілей суб’єкта господарювання; ефективне керування інформаційними активами суб’єкта господарювання у критичних ситуаціях.

5. Ідентифікація ризиків інформаційної безпеки є неможливою без вдосконалення наявних методів обліково-аналітичного забезпечення управлінських процесів, які формують стратегію та тактику управлінських рішень. У зв’язку з цим, ключові напрямки вдосконалення обліково-аналітичного забезпечення управління інформаційною безпекою компанії включають: створення відділів моніторингу інформаційної безпеки компанії; оприлюднення інформації щодо інформаційної безпеки у управлінській звітності; встановлення специфічних підходів до облікової політики, включаючи визнання, оцінку та реєстрацію операцій, пов'язаних з інформаційною безпекою; розроблення документообігу для складання та обробки документів, пов'язаних з інформаційною безпекою; постійний моніторинг та прогнозування рівня безпеки на основі економетричного моделювання та факторного аналізу.

6. Встановлено, що одним із найбільш прийнятних підходів оцінки ризиків є методологія, розроблена Національним інститутом стандартів і технологій (NIST), яка включає в себе визначення загроз і «вразливих місць», аналіз можливих збитків і надання рекомендацій щодо заходів безпеки. Застосування даної методології на практиці сприятиме значному підвищенню рівня інформаційної безпеки суб’єктів господарювання.

7. Встановлено, що на ТОВ «Шредер» відслідковується постійний ріст вартості майна протягом 2021-2023 років. Так, у 2022 році вартість майна зросла на 413247,00 тис. грн. або на 57,7% у порівнянні з 2021 роком, а в 2023 році вона зросла на ще 147758 тис. грн. або 13,1% порівняно з 2022 роком. Ці

дані свідчать про зростання майнового потенціалу ТОВ «Шредер». У структурі майна ТОВ «Шредер» левову частину займають оборотні активи, які у 2021 році становили 80,3% від валюти балансу, у 2022 році - 86,5%, а у 2023 році - 85,9%, що свідчить про позитивну тенденцію. За період з 2021 по 2023 рік вартість оборотних активів зросла на 521585 тис. грн. або на 90,7%, досягнувши рівня 1096458 тис. грн. Значну частку у складі оборотних активів ТОВ «Шредер» займає короткострокова дебіторська заборгованість, величина якої упродовж 2022 року зросла на 271551 тис. грн. (90,9%), а у 2023 році зросла на 81486 тис. грн. (14,3%). Сума грошових коштів та їх еквівалентів у 2022 році порівняно з 2021 роком зросла в 4 рази, на 50917 тис. грн., а до кінця 2023 року на 74644 тис. грн. або 109,6%. Щодо запасів, то відмітимо, що у 2023 році також спостерігається їх зростання у порівняні із 2021 роком. Так, станом на кінець 2023 року вартість запасів збільшилась на 52599 тис грн, або 20,6%. Разом з тим слід відмітити, що у порівняні із 2022 роком простежується зменшення запасів на 26620 тис грн, або 8,0%. Щодо необоротних активів ТОВ «Шредер, то з’ясовано, що у порівнянні з 2021 роком, у 2022 році вартість необоротних активів зросла на 11752 тис. грн. або на 8,4%, досягнувши рівня 152469 тис. грн. У 2023 році відбулося подальше зростання на 27688 тис. грн. або на 18,1%. Левову частку у структурі необоротних активів займають основні засоби, а саме 92,7% у 2021 р.; 90,7% у 2022 р.; 91,4% у 2023 р.

8. За результатами аналізу складу джерел формування капіталу ТОВ «Шредер» можна зробити висновок, що величина власного капіталу на підприємстві постійно зростає. Так, протягом досліджуваного періоду спостерігається зростання капіталу з 434569 тис. грн. до 755222 тис. грн., або на 73,8%. Однак не зважаючи на таке зростання, частка власного капіталу у валюті балансу зменшилася на 1,5 процентних пункти з 60,7% у 2021 році до 59,2 % у 2023 році. Разом з тим, якщо порівнювати із 2022 роком, то простежується зростання частки власного капіталу у валюті балансу на 10,3 процентних пункти. Слід відмітити, що причиною зростання власного капіталу є одержання ТОВ «Шредер» прибутку. У порівнянні з 2021 роком, у 2022 році величина

нерозподіленого прибутку зросла на 116897 тис. грн. або на 121,8%, досягнувши рівня 212877 тис. грн. У 2023 році відбулося подальше зростання на 203756 тис. грн. або на 95,7%. досягнувши рівня 416633 тис. грн.

9. У структурі позикового капіталу ТОВ «Шредер» найбільшу частку складають поточні зобов'язання і забезпечення (97,5% у 2021 році, 99,0% у 2023 році). Протягом 2023 року спостерігається збільшення суми поточних зобов'язань і забезпечення на 109,3% або 299549 тис. грн., а на кінець 2023 року вона зменшилася на 57611 тис. грн або 10,0%. Величина довгострокових зобов'язань і забезпечень у 2022 році зменшується на 3199 тис. грн або 46,0%, а у 2023 році збільшується на 1613 тис. грн або 43% у порівняні із 2022 роком.

10. Встановлено, що 2022-2023 роках ТОВ «Шредер» для фінансування своїх запасів практично не залучає додаткових джерел фінансування (наприклад банківські кредити). Тобто фінансування запасів здійснюється практично лиш за рахунок власних коштів. Хоча й уникнення використання зовнішніх джерел може бути сприятливим, але ТОВ «Шредер» не використовується фінансовий леверидж, що дало би можливість одержання додаткового збільшення прибутку. Окрім цього відмітимо, що ТОВ «Шредер» є фінансово стійким. Так, на протязі 2021-2023 рр вартість запасів не перевищувала основні джерела їх формування. При чому слід відмітити, що спостерігається позитивна тенденція надлишку основних джерел фінансування, а саме: у 2021 р. – 54523 тис. грн; у 2022 р. – 228517 тис. грн.; у 2023 р. 272551 тис. грн.

11. За результатами аналізу відносних показників фінансової стійкості встановлено, що ТОВ «Шредер» має високий рівень фінансової стійкості. Так, значення коефіцієнта автономії показує на те, що на кінець 2021 р. частка власного капіталу у валюті балансу становила 61%, на кінець 2022 р. – 49%, а на кінець 2023 р. – 59%, що на 0,1 процентних пункти більше, ніж у 2022 р. При цьому слід відмітити, що оптимальне значення даного показника становить більше 50%. Таким чином можемо зробити висновок, що фінансова стійкість ТОВ «Шредер» у 2023 році, в порівняні із 2022 р. зросла. Високий рівень

фінансової стійкості ТОВ «Шредер» підтверджується також і іншими показниками. Так, коефіцієнт фінансової залежності є оберненим до показника автономії. Так, при оптимальному значення менше двох, на кінець 2023 року він становив 1,69, що на 0,36 менше ніж у 2022 році.

12. Коефіцієнт фінансування показує, що на кінець 2023 року на 1 гривню власного капіталу припадає 0,69 грн залученого капіталу, що на 0,04 грн більше ніж у 2021 році, й на 0,36 грн більше ніж у 2022 році.

13. Коефіцієнт забезпеченості оборотних активів власними коштами при нормативі більше 0,1, на кінець 2021 р. мав значення 0,02. За 2022 р. даний показник зріс на 0,05 до 0,07, що свідчить про підвищення фінансової стійкості ТОВ «Шредер» у 2022 р. За 2023 р. даний коефіцієнт у порівняні з 2022 р. збільшився на 0,06, й на кінець 2023 р. становив 0,13, що відповідає значенню оптимального рівня даного показника.

14. Коефіцієнт маневреності власного капіталу показує, що на кінець 2021 р. 69,0% власних коштів було вкладено в оборотні активи ТОВ «Шредер», а на кінець 2023 р. вже 77,0%. Тобто за 2021-2023 рр значення коефіцієнта маневреності зросло й це свідчить про підвищення фінансової стійкості компанії. Слід також відмітити, що значення даного коефіцієнта перевищує оптимальне його значення, що становить більше 0,5.

15. За результатами аналізу ліквідності балансу ТОВ «Шредер» встановлено, що баланс підприємства є ліквідним, а підприємство відповідно платоспроможним. Так, станом на кінець 2021 р., 2022 р. та 2023 р., ТОВ «Шредер» був у спромозі погасити поточних зобов’язань 6,3%, 11,9% та 27,7% відповідно. За рахунок наявних грошових коштів й їх еквівалентів та очікуваних надходжень від погашення поточної дебіторської заборгованості компанія може розрахуватися з поточними боргами на кінець 2021 р. на 116,6%, на кінець 2022 р – на 111,9%, а на кінець 2023 р. – 152,8%. При цьому слід відмітити, що показник швидкої ліквідності у 2023 році зріс на 0,409 процентних пункти у порівняні із 2022 р. Значення показника загальної ліквідності на ТОВ «Шредер» було менше 2 лише у 2022 році, а вже у 2023 році

можна спостерігати зростання даного коефіцієнта на 0,423, й станом на кінець 2023 року він становив 2,125.

16. Аудит інформаційної безпеки суб’єкта підприємництва є одним із ключових методів для отримання незалежної та об'єктивної оцінки рівня його захищеності від потенційних загроз. Результати такої перевірки становлять основу для розробки стратегії розвитку системи інформаційної безпеки суб’єкта господарювання. Важливо зрозуміти, що аудит інформаційної безпеки не може бути одноразовим, він повинен проводитися регулярно. Лише в такий спосіб аудит інформаційної безпеки буде ефективним та сприятиме підвищенню рівня захисту інформації в компанії.

17. Система обліку суб’єкта господарювання повинна бути захищеною від потенційних кібератак і забезпечувати цілісність, доступність та конфіденційність інформації. Для досягнення цього необхідно систематично оновлювати програмне забезпечення, оцінювати ризики, використовувати надійні паролі, захищати мережу та здійснювати систематичне резервне копіювання інформації. Крім того, працівники компанії повинні мати відповідну підготовку та розуміти культуру безпеки та принципи інформаційної безпеки.

18. Одним із найбільш прийнятних підходів оцінки ризиків є методологія, розроблена Національним інститутом стандартів і технологій (NIST), яка включає в себе визначення загроз і «вразливих місць», аналіз можливих збитків і надання рекомендацій щодо заходів безпеки. Застосування даної методології на практиці сприятиме значному підвищенню рівня інформаційної безпеки суб’єктів господарювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адонін С. В., Калашнікова Ю. М. Проблеми оцінки економічної безпеки сучасного підприємства. Економічний простір. Випуск №148, 2019. URL: http://dspace.nbuv.gov.ua/handle/123456789/12538

2. Акімова Н. С., Кирильєва Л. О., Наумова Т. А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*. 2023. № 35. С. 5-10. https://doi.org/10.32782/2522-1256-2023-35-01

3. Бланк И. А. Управление финансовой безопасностью предприятия К.: Ника-Центр, Эльга, 2004. 784 с.

4. Босак А. О., Вержиковський В. П., Калінін І. Є., Максимів І. Д., Приступа Д. А., Ривак О. І. Засади формування інформаційної безпеки підприємства. *Міжнародний науковий журнал "Інтернаука"*. Серія: "Економічні науки". 2023. № 11. doi: https://doi.org/10.25313/2520-2294-2023-11-9157

5. Василішин С.І. Ризики економічної безпеки в системі обліково-аналітичного забезпечення управління підприємствами. URL: https://repo.btu.kharkov.ua/bitstream/123456789/9502/3/Vasylyshyn_Problems_of_system_approach_in_economy_article_3_71_2019.pdf

6. Вівчар О., Кос Т. Сучасні методи оцінювання фінансової стійкості підприємства. *Молодий вчений.* 2023. №, 4 (116), 115-119. https://doi.org/10.32839/2304-5809/2023-4-116-23

7. Гаджиєв, М., Стайкуца, С., Хряпа, А., & Вербецький, А. (2024). Програмна реалізація аудиту стану інформаційної безпеки підприємства малого бізнесу. *Scientific Collection «InterConf»*, (186), 421–424. URL: https://archive.interconf.center/index.php/conference-roceeding/article/view/5290

8. Ганін В., Алєкпєров Р. Оцінка системи управління фінансовою стійкістю підприємства в сучасних умовах господарювання. *Молодий вчений.* 2020. № 11 (87). С. 149–152. DOI: https://doi.org/10.32839/2304-5809/2020-11-87-32

9. Гончаров А.Б. Фінансовий менеджмент : *навч. посібник*. Харків : ВД «ІНЖЕК», 2003. 240 с.

10. Горячева К.С. Оцінка рівня фінансової безпеки підприємства. URL: https://essuir.sumdu.edu.ua/bitstreamdownload/123456789/55127/5/Horiacheva_Finansova_bezpeka.pdf;jsessionid=C01D

11. Дейнега О. Інформаційна безпека підприємств в умовах глобалізації 4.0. *Економіка та суспільство*. 2019. Вип. 20. С. 70–79.

12. Докієнко Л. Концептуальні підходи до комплексної діагностики фінансової стійкості підприємства. *Підприємництво та інновації*. 2020. № 14. С. 25–31. DOI: https://doi.org/10.37320/2415-3583/14.5

13. Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою. *Радіоелектроніка, інформатика, управління*. 2017. № 1. С. 107–114.

14. Дудченко Н. В., Карбівничий І. В. Аналіз сучасного стану фінансової безпеки в Україні. Економіка. Фінанси. Право. 2017. № 2. С. 17-20

15. Жук Н.Т. Аналіз фінансової безпеки підприємств харчової промисловості. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 071 – Облік і оподаткування (галузь знань 07 – Управління та адміністрування) – Західноукраїнський національний університет, Тернопіль, 2023.

16. Жукевич С., Рожелюк В. Фінансова стійкість підприємства в контексті сталого розвитку України. *Світ фінансів*. Тернопіль, ТНЕУ, «Економічна думка», 2018 р. С. 75-85.

17. Захарова Н.Ю. Методичні підходи щодо оцінки фінансового стану підприємства. *Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки).* 2013. № 2 (3). С. 128–133.

18. Ізюмська В., Нікульшина А. Управління фінансовою стійкістю підприємства. *Економіка та суспільство*. 2021. № 34. DOI: https://doi.org/10.32782/2524-0072/2021-34-26

19. Ілляшенко К.В. Інформаційна безпека сучасного бухгалтерського

обліку. Науковий вісник Міжнародного гуманітарного університету. 2019. № 40. С. 179–183. URL: http://vestnik-econom.mgu.od.ua/journal/2019/40-2019/25.pdf

20. Карпишин Н.І., Жукевич С.М. Аналіз й оцінка фінансових ризиків в системі управління суб'єктів господарювання. *Інноваційна економіка*. №5-6 [63]. Тернопіль. 2017, С.180 – 185.

21. Качан О.І. Інформаційна безпека підприємства в умовах глобалізації URL : https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf

22. Кащена Н. Б., Горошанська О. О., Польова Т. В. Ділова активність підприємства: сутність та методика аналізу : *монографія*. Харків, 2016. 196 с.

23. Клочко Т. Фінансова безпека як умова фінансової стійкості підприємства. *Економіка та суспільство*. 2021. № 23. DOI: https://doi.org/10.32782/2524-0072/2021-23-17

24. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. 2010. № 3. С. 123–129.

25. Колісник О. Альтернативні підходи в теорії безпеки і їх застосування у фінансовій науці. *Наукові записки*, Випуск 15, 2006.

26. Костюченко В.В., Шиковець К.О. Особливості організації інформаційної безпеки сучасної інформаційної системи та її економічна доцільність. *Економіка і суспільство*. 2017. № 10. С. 89-93

27. Кочетков О. В., Гаур Т. О., Машін В. М. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. *Наукові праці ОНАЗ ім. О. С. Попова*. 2019. № 1. С. 97-104.

28. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Зб. наук. пр. ДВНЗ «КНЕУ ім. Вадима Гетьмана».* 2021. С. 26–28.

29. Лагун А., Небельський А. Аналіз ризиків інформаційної безпеки ІТ підприємства. Інформаційна безпека та інформаційні технології: *збірник тез доповідей IV Міжнародної науково-практичної конференції*, ІБІТ 2022, м. Львів, 30 листопада 2022 року. Львів: Растр-7, 2022. С. 33-35.

30. Лагун А., Кухарська Н. Ризики інформаційної безпеки IT-підприємства. Захист інформації і безпека інформаційних систем: *VII Міжнародна науково-технічна конференці*я, м. Львів, 30–31 травня 2015 року. URL:: https://webcache.googleusercontent.com/search?Q=cache:_mlalmxnnaej: https:// sci.ldubgd.edu.ua/bitstream/handle/123456789/750/11.doc%3Fsequence% 3D1%26isallowed%3Dy+&cd=2&hl=ru&ct=clnk&gl=u a&client=firefox-b-d

31. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес.* 2015. № 3(13). С. 87–92.

32. Літвінчук І.С., Корчомний Р.О., Коршун Н.В. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». URL: https://elibrary.kubg.edu.ua/id/eprint/34065/1/I_Litvinchuk_R_Korchomnyi_N_Kors hun_M_Vorokhob_2_10_CEST.pdf

33. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика: *монографія*. Львів : «Растр-7», 2020. 384 с.

34. Нагорний П.Д., Базюк Д.С. Оцінка фінансового стану як передумова ефективного управління підприємством. URL: https://www.transformations.in.ua/ index.php/ journal/article/view/8

35. Одношевна О., Бугаєску В., Якименко В. Аналіз та економічна діагностика активів підприємства і пов'язаних з ними витрат: особливості та передумови здійснення. *Економіка та суспільство. 2023. №* (55). https://doi.org/10.32782/2524-0072/2023-55-79

36. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика.* 2015. № 2(46). С. 32–38.

37. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства.* 2020. № 1 (21). С. 103-109.

38. Пармаклі Д. М., Бахчиванжи Л. А., Євтушок О. В. Методи аналізу і моделювання показників ділової активності в управлінському консалтингу. Economic Bulletin of the Black Sea Littoral. 2022, Issue 1. P. 68-76.

39. Парфентій Л. А. Управління фінансовою безпекою підприємств в умовах економічної нестабільності : *монографія*. Суми: видавничо-виробниче підприємство «Мрія», 2019. 184 с.

40. Петик Л. О., Фелісєєв В. А. Ділова активність промислових підприємств України. *Економічний простір*. 2022. № 181. С. 188-191.

41. Поддєрьогін А.М., Білик М.Д., Буряк Л.Д., Булгакова С.О., Куліш А.П. Фінанси підприємств : *підручник*, 6. вид., пере- роб. та доп. Київ : КНЕУ, 2006. 552 с.

42. Приймак С. В. Ділова активність як фактор зростання економічного потенціалу підприємства. Збірник тез звітної наукової конференції Львівського національного університету імені Івана Франка за 2017 рік (електронне видання): Львів, ЛНУ ім. І. Франка, 2018. С. 121–125.

43. Про затвердження Національного положення (стандарту) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності»: Наказ Міністерства фінансів України 07.02.2013 № 73.Приймак С., Волкова О. Діагностика фінансової стійкості підприємств в умовах посилення глобальної конкуренції. *Економіка та суспільство*. 2021. № 30. DOI: https://doi.org/10.32782/2524-0072/2021-30-58

44. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки - основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. № 1. С. 86-93.

45. Русіна Ю.О., Острякова В.Ю. Удосконалення системи управління інформаційною безпекою підприємства. URL: https://www.inter-nauka.com/uploads/public/1489761446540.pdf#page=124

46. Тарасенко Н.В. Економічний аналіз: *навч. посібник*, 4-е вид., стереотип. Львів : Новий Світ-2000, 2006. 344 с.

47. Ткачук Г. Ідентифікація економічних ризиків в обліково-аналітичній системі підприємства. *Економіка харчової промисловості.* 2015. Вип. 4. Т. 7. С. 80–88.

48. Ткачук Г. Ю. Оцінка ділової активності підприємства. *Науковий*

вісник Херсонського державного університету. Серія: Економічні науки. 2015. Вип. 13. Ч. 4. С. 88–90.

49. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. Дисертація док. юрид. наук: 12.00. Ужгород. 2019. С. 487. URL: https://www. uzhnu.edu. ua/uk/infocentre/get/19617.

50. Тютюнник Ю. М., Дороган-Писаренко Л. О., Тютюнник С. В. Фінансовий аналіз: навчальний посібник (2-ге видання, змінене і доповнене). Полтава : Видавництво ПП «Астрая», 2020. 434 с.

51. Фінанси підприємств : *навч. посіб.* / за ред. Аніловської Г.Я., Висоцької І.Б. Львів : ЛьвДУВС, 2018. 440 с.

52. Храпкін О. Стратегічне управління інформаційною безпекою підприємства: сучасні підходи та сиклики. Проблеми і перспективи економіки та управління. 2024. № 4 (36) С. 86-94.

53. Чегринець К.В. Фінансова стійкість підприємства: економічна сутність та методи оцінки. *Управління розвитком*. 2012. № 10. С. 51–54.

54. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. Ефективна економіка. № 5, 2020. С. 24-32.

55. Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підпримств торгівлі. *Цифрова економіка*. 2022. № 1. С. 106–117.

56. Швиданенко Г.О., Олесю О.І. Сучасні технології діагностики фінансово-економічної діяльності підприємства : *монографія*. Київ : КНЕУ, 2002.

57. Юдін О. К., Зюбіна Р. В., Матвійчук-Юдіна О. В. Сучасні практики впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури. URL: https://jrnl.nau.edu.ua/index.php/SBT/article/view/13527

58. Ясіновська І., Фелісєєв, В. Ділова активність промислових підприємств України: оцінка, проблеми та напрями забезпечення. *Економіка та суспільство.* 2022. № 44. https://doi.org/10.32782/2524-0072/2022-44-16

59. Яцух О.О., Захарова Н.Ю. Фінансовий стан підприємства та

методика його оцінки. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Економіка і управління*. 2018. № 3. Т. 29 (68). С. 173-180.

60. Brandenburg G. The Role and Implementation of an Information Security Management System in Modern Enterprises URL: https://ctrl-dis-rupt.nl/-insights-news/the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises.

61. What is Information Security Management? URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/what-is-information-security-management