Центральноукраїнський національний технічний університет
(повне найменування закладу вищої освіти)

Економічний факультет
(повне найменування інституту, назва факультету (відділення))

Кафедра «Економіка, менеджмент та комерційна діяльність»
(повна назва кафедри (предметної, циклової комісії))

«Допущена до захисту»
Зав. кафедри ЕМКД
канд. екон. наук., доцент
________Тетяна РЯБОВОЛИК
«11»__грудня_____ 2024 р.
(протокол засідання кафедри ЕМ та КД
№ 6 від «11» грудня 2024 р.)

КВАЛІФІКАЦІЙНА РОБОТА

за другим (магістерським) рівнем вищої освіти
на тему:

«Дослідження інформаційної компоненти фінансово-економічної безпеки підприємства»

Виконав: здобувач вищої освіти
на другому (магістерському) рівні
ОПП «Управління фінансово-економічною безпекою» спеціальності 073 «Менеджмент»
групи УФЕБ-23М
Ражаб Алі Саед Алі
«11»__грудня________ 2024 р.

Керівник: канд. екон. наук., доцент
______________Пітел Наталія Сергіївна
«11»__грудня________ 2024 р.

Рецензент: канд. екон. наук., доцент
_________Запірченко Людмила Дмитрівна

м. Кропивницький – 2024 рік

Стор.

ЗМІСТ

ВСТУП

У сучасних умовах функціонування підприємств, що характеризуються динамічним розвитком інформаційних технологій та зростанням обсягів інформаційних потоків, питання забезпечення фінансово-економічної безпеки стає дедалі актуальнішим. Особливої уваги потребує інформаційна компонента фінансово-економічної безпеки, адже саме вона є ключовим чинником ефективного управління ризиками, збереження конфіденційності даних і забезпечення стійкого розвитку підприємства.

Інформаційна складова безпеки охоплює управління потоками інформації, захист даних від внутрішніх та зовнішніх загроз, а також формування ефективної системи обробки й зберігання інформації. Її важливість зумовлена тим, що значна частина рішень у сфері фінансово-економічного управління базується на якісній та достовірній інформації. Водночас, підприємства стикаються з новими викликами, такими як кібератаки, витоки конфіденційних даних, неправомірне використання інформації тощо.

Актуальність теми дослідження полягає у зростанні значення інформаційних ресурсів для забезпечення стабільності підприємств та підвищення їх конкурентоспроможності. Вивчення інформаційної компоненти фінансово-економічної безпеки сприятиме ефективнішому захисту даних та формуванню стратегій протидії загрозам, що, у свою чергу, позитивно вплине на результати діяльності підприємства.

Дослідження інформаційної безпеки підприємств активно ведуться як зарубіжними (М. Портер, Р. Каплан, Д. Нортон, К. Мітнік, Д. Паркер, К. і Д. Лаудон), так і вітчизняними вченими (С. Ілляшенко, О. Бєлєнький, І. Розпутенко, В. Шевченко, Г. Вітренко). Таким чином, дослідження інформаційної компоненти фінансово-економічної безпеки має міждисциплінарний характер і базується на результатах робіт багатьох вчених. Вищезазначені підходи та напрацювання є основою для подальших теоретичних і практичних рішень у сфері забезпечення стійкого функціонування підприємств в умовах сучасних викликів.

Об'єктом дослідження у цій роботі є процеси забезпечення фінансово-економічної безпеки підприємства, а предметом – інформаційна компонента цих процесів. Метою кваліфікаційної роботи є розробка теоретичних підходів і практичних рекомендацій щодо удосконалення управління інформаційною складовою фінансово-економічної безпеки ПрАТ «Кіровоградобленерго».

Відповідно до мети кваліфікаційної роботи було поставлено та вирішено наступні завдання: досліджено сутність фінансово-економічної безпеки підприємства та визначено роль інформаційної компоненти у її забезпеченні; проаналізовано нормативно-правове забезпечення інформаційної безпеки; проведено характеристику господарської діяльності та оцінку поточного стану фінансово-економічної безпеки ПрАТ «Кіровоградобленерго»; виконано аналіз впливу інформаційних загроз на фінансово-економічну діяльність підприємства; розроблено рекомендації щодо удосконалення системи моніторингу інформаційної безпеки, а також запропоновано інноваційні рішення для мінімізації інформаційних ризиків у діяльності підприємства.

Для досягнення мети кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти застосовано комплекс методів дослідження, зокрема: теоретичні методи, такі як аналіз, синтез, порівняння та узагальнення для вивчення наукової літератури, нормативно-правової бази та визначення сутності фінансово-економічної безпеки; емпіричні методи, зокрема спостереження, аналіз статистичних даних і господарської діяльності ПрАТ «Кіровоградобленерго» для оцінки стану фінансово-економічної безпеки підприємства; методи системного підходу для виявлення взаємозв'язків між інформаційною безпекою та фінансово-економічною діяльністю підприємства; методи моделювання для розробки рекомендацій та інноваційних рішень щодо підвищення ефективності інформаційної компоненти безпеки. Застосування цього комплексу методів забезпечило всебічність і наукову обґрунтованість отриманих результатів.

Наукова новизна кваліфікаційної роботи полягає у комплексному дослідженні ролі інформаційної складової у забезпеченні фінансово-економічної безпеки підприємства. Вона включає систематизацію теоретичних підходів до визначення взаємозв'язку між інформаційною та фінансово-економічною безпекою, ідентифікацію та аналіз інформаційних загроз для фінансово-економічної діяльності, а також удосконалення методичних підходів до моніторингу та управління інформаційною безпекою.

Особливу увагу приділено розробці практичних рекомендацій щодо впровадження інноваційних рішень для мінімізації інформаційних ризиків на прикладі ПрАТ «Кіровоградобленерго».

Отримані результати дозволять підвищити ефективність управління інформаційною безпекою підприємства в умовах цифровізації та актуалізувати проблему захисту від сучасних кіберзагроз.

Результати проведеного дослідження були презентовані на VII Міжнародній науково-практичній конференції «Конкурентоспроможна модель інноваційного розвитку економіки України», яка відбулася 7-8 листопада 2024 року у Центральноукраїнському національному технічному університеті. У рамках конференції було представлено доповідь на тему «Роль інформаційних технологій у забезпеченні економічної безпеки підприємства».

Для дослідження теми використано наукову літературу з фінансово-економічної та інформаційної безпеки, нормативно-правові акти України, звітні дані ПрАТ «Кіровоградобленерго», фахові публікації та матеріали науково-практичних конференцій, що забезпечило обґрунтованість і практичну значущість роботи.

Випускна кваліфікаційна робота другого (магістерського) рівня вищої освіти має таку структуру: вступ, три основні розділи, висновки, список використаних джерел і додатки. Основний текст займає 60 сторінок, а загальний обсяг роботи разом із додатками становить 65 сторінки. У роботі представлено ілюстративний матеріал, зокрема 11 таблиць і 14 рисунків, що сприяє більш ефективному сприйняттю та аналізу інформації.

РОЗДІЛ 1

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ КОМПОНЕНТИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Сутність фінансово-економічної безпеки підприємства

У сучасному світі, що характеризується високою динамічністю змін, нестабільністю ринкових умов і зростаючою конкуренцією, питання фінансово-економічної безпеки підприємства стає однією з ключових складових успішного функціонування та довгострокового розвитку. Збереження фінансової стабільності та захищеності економічних інтересів підприємства є необхідною умовою для його життєздатності, здатності адаптуватися до змін і ефективно використовувати свої можливості [3, с. 13].

Фінансово-економічна безпека підприємства є багатогранним поняттям, яке включає захист від зовнішніх і внутрішніх загроз, забезпечення стабільності фінансових потоків, ефективне управління ресурсами та реалізацію стратегічних цілей [5, с. 22]. На наш погляд, сутність поняття фінансово-економічна безпека підприємства полягає у створенні механізмів, що дозволяють мінімізувати ризики, пов'язані із змінами на ринку, впливом державного регулювання, конкуренцією, фінансовими кризами, а також забезпечувати безперервність операційної діяльності.

В умовах глобалізації та постійного ускладнення економічних процесів підприємства стикаються з новими викликами, такими як кіберзагрози, валютні коливання, кризи в постачанні ресурсів, інфляційні ризики та інші. Зазначені обставини зумовлюють необхідність розробки ефективних інструментів для ідентифікації, оцінки та управління ризиками. Крім того, важливим є забезпечення прозорості фінансової діяльності та дотримання міжнародних стандартів [7, с. 14-15].

У наукових колах переважає тенденція до адаптації концепції фінансової безпеки держави на мікрорівень, тобто на рівень окремого підприємства.

Фінансова безпека суб'єкта господарювання розглядається як багатогранний механізм, що інтегрує два ключові аспекти:

захисний аспект орієнтований на забезпечення стабільності та стійкості фінансової системи підприємства шляхом впровадження превентивних заходів та використання спеціалізованих фінансових інструментів для мінімізації ризиків та нейтралізації потенційних загроз.

оптимізаційний аспект орієнтований на підвищення ефективності функціонування фінансової системи підприємства через удосконалення управлінських процесів, раціональний розподіл та використання фінансових ресурсів, а також максимізацію прибутковості [16, с. 122].

Таким чином, фінансова безпека підприємства є невід'ємною складовою його успішного функціонування та сталого розвитку, що досягається шляхом синтезу захисних та оптимізаційних стратегій в управлінні фінансами.

Незважаючи на різноманіття наукових інтерпретацій поняття «фінансово-економічна безпека», його глибоке дослідження залишається актуальним та необхідним. Адже саме чітке розуміння сутності цього поняття є фундаментом для розробки ефективної системи управління фінансово-економічною безпекою та формування дієвих механізмів її забезпечення. Вчені, досліджуючи це поняття, акцентують увагу на різних його аспектах, враховуючи специфіку функціонування підприємств в сучасних умовах [6, с. 27-31].

В таблиці 1.1 представлено погляди відомих науковців на сутність фінансово-економічної безпеки підприємства. Порівняльний аналіз цих визначень дозволить глибше зрозуміти ключові характеристики та складові цього поняття, а також виявити спільні та відмінні риси у підходах різних авторів.

Науковий досвід досліджень у сфері фінансово-економічної безпеки однозначно вказує на складність та комплексність цього поняття, що передбачає підтримку фінансової стабільності через платоспроможність та ліквідність активів, ефективне управління та контроль за всіма видами діяльності, професійний менеджмент, раціональне використання всіх видів ресурсів та заходи щодо попередження збитків від внутрішніх та зовнішніх загроз тощо.

Таблиця 1.1 – Фінансово-економічна безпека підприємства: погляди науковців

Науковці	Визначення фінансово-економічної безпеки підприємства
Столбов В.Ф., Шаповал Г.М.	Стан захищеності ресурсів та інтелектуального потенціалу від загроз, що характеризується високими фінансовими показниками та перспективою розвитку.
Варналій З.С.	Результат комплексу складових, спрямованих на усунення фінансово-економічних загроз та забезпечення фінансової стійкості, конкурентоспроможності, оптимальності структури, правового захисту тощо.
Трухан О.Л., Коknaєва М.О.	Розглядається з двох позицій: статичної (результат на певну дату) та динамічної (розвиток в умовах безпеки).
Мойсеєнко І.П., Марченко О.М.	Фінансово-економічний стан, що забезпечує захищеність інтересів від загроз та створює передумови для стійкого розвитку.
Лисенко Ю.Г.	Кількісно та якісно детермінований рівень фінансового стану, що забезпечує захист інтересів від загроз, визначений фінансовою політикою.
Горячева К.С.	Фінансовий стан, що характеризується збалансованістю інструментів, стійкістю до загроз, здатністю забезпечувати реалізацію інтересів та сталий розвиток.
Бланк І.А.	Кількісно та якісно детермінований рівень фінансового стану, що забезпечує захищеність інтересів від загроз, визначений фінансовою філософією та створює передумови для стійкого зростання.

Джерело: узагальнено автором [3,5,6,7]

Отже, фінансово-економічна безпека підприємства досягається завдяки комплексному підходу до управління, що враховує всі внутрішні та зовнішні фактори.

Дослідження наукових праць, присвячених фінансовій безпеці суб'єктів підприємництва, дозволяє виділити наступні ключові детермінанти:

ресурсне забезпечення: достатній рівень забезпеченості фінансовими ресурсами для здійснення операційної та інвестиційної діяльності;

фінансова стабільність: стійкість та стабільність фінансового стану, що характеризується здатністю підприємства протистояти негативним внутрішнім та зовнішнім впливам;

збалансованість фінансових потоків: оптимальне співвідношення вхідних та вихідних фінансових потоків, що забезпечує безперервність операційного циклу та своєчасне виконання фінансових зобов'язань;

ефективність діяльності: високий рівень ефективності фінансово-економічної діяльності, що вимірюється за допомогою відповідних фінансових показників;

управління ризиками: ефективний контроль за внутрішніми та зовнішніми ризиками, що дозволяє мінімізувати їх негативний вплив на діяльність підприємства [2, с. 19].

Як бачимо, фінансова безпека підприємства є комплексним поняттям, що відображає його здатність забезпечувати стабільне функціонування, ефективний розвиток та захист від фінансових загроз.

Збереження фінансової безпеки є критично важливим для будь-якого підприємства, оскільки воно забезпечує стабільність його діяльності та створює умови для досягнення стратегічних цілей. Ефективність заходів, вжитих керівництвом та менеджерами для виявлення, попередження та мінімізації негативного впливу загроз, визначає рівень фінансової безпеки підприємства.

На рис. 1 зображено типову модель забезпечення фінансової безпеки, яка демонструє основні заходи та механізми, що сприяють захисту від деструктивних факторів зовнішнього та внутрішнього середовища.

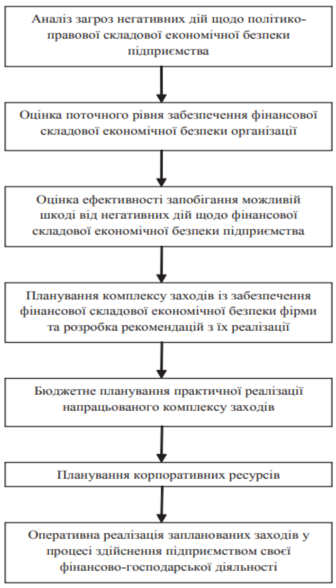

Рисунок 1.1 – Процес управління фінансовою складовою економічної безпеки

Джерело: узагальнено автором за матеріалами [19, с. 51].

Алгоритм дій, представлений на рис. 1.1, ілюструє основні етапи побудови системи управління фінансовою складовою економічної безпеки підприємства, охоплює процеси від аналізу потенційних загроз до оперативного впровадження запланованих заходів.

У науковій літературі існує кілька підходів до оцінювання рівня фінансової безпеки підприємства, які базуються на різних концептуальних підходах та методологіях. Основними серед них є системний, функціональний, індикативний і комплексний підходи (рис. 1.2).

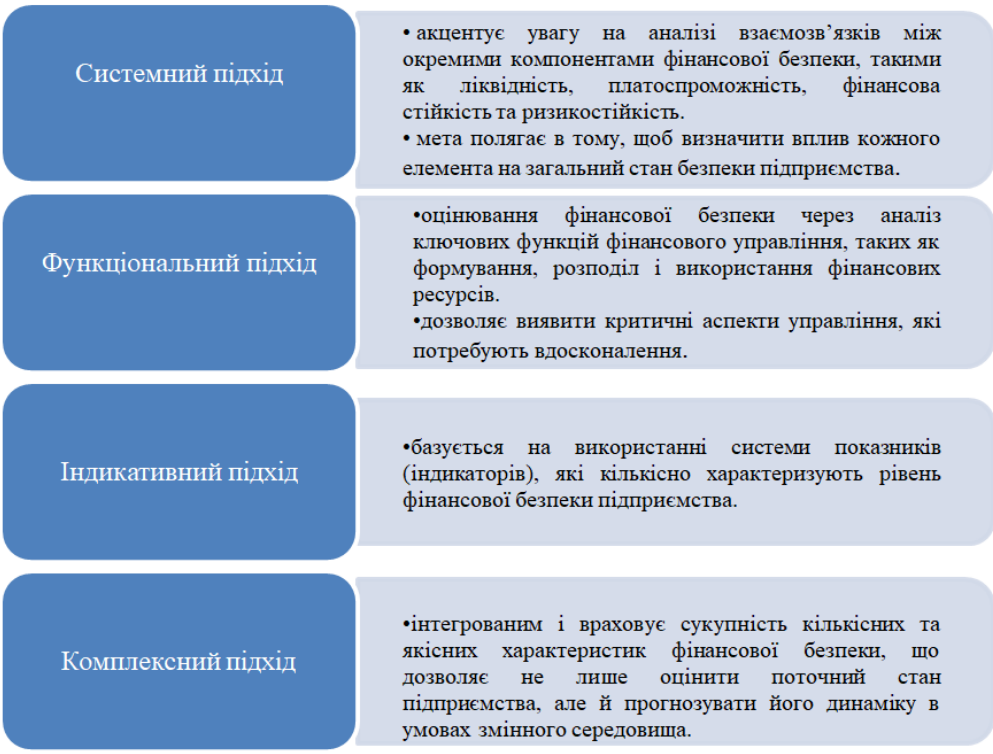

Рисунок 1.2 – Підходи до оцінювання фінансової безпеки

Джерело: узагальнено автором за матеріалами [25, с. 48-52].

На рис. 1.2 бачимо, що кожен із зазначених підходів має свої переваги та обмеження, тому їхнє поєднання може забезпечити найбільш об'єктивну та повну оцінку фінансової безпеки підприємства. У цьому контексті особливе значення має розробка ефективних методик, адаптованих до специфіки діяльності конкретного підприємства та умов ринкового середовища.

На сучасному етапі розвитку економіки забезпечення фінансово-економічної безпеки підприємства є важливою умовою його стабільного функціонування та розвитку. Фінансово-економічна безпека включає широкий спектр завдань, спрямованих на попередження ризиків, забезпечення стійкості фінансової системи та досягнення стратегічних цілей.

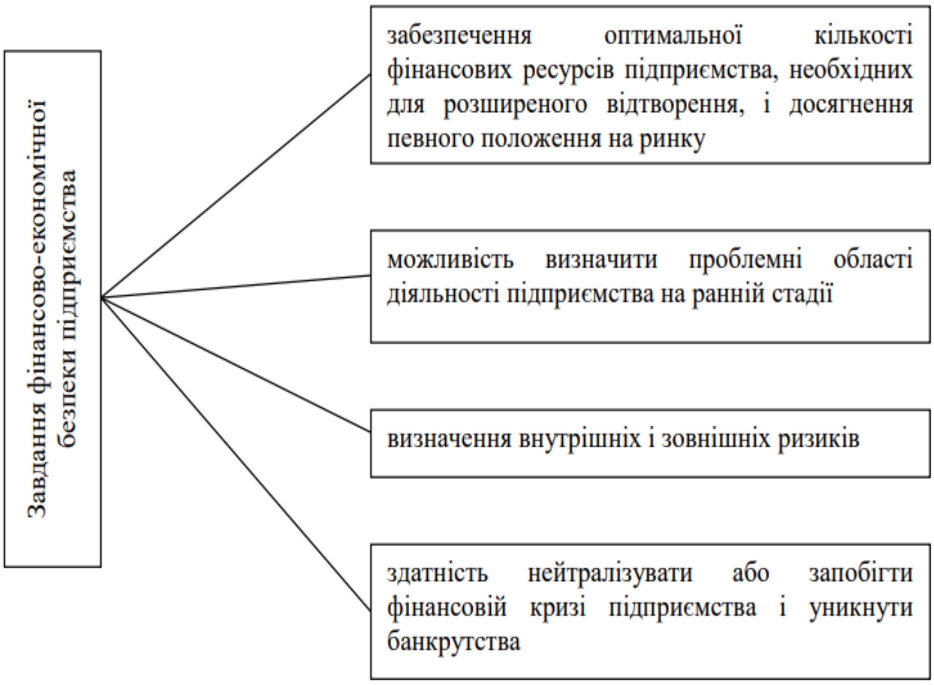

Рисунок 1.3 – Основні завдання фінансово-економічної безпеки підприємства

Джерело: узагальнено автором за матеріалами [33, с. 17]

На рис. 1.3 наведено ключові завдання фінансово-економічної безпеки підприємства, які охоплюють як внутрішні, так і зовнішні аспекти її забезпечення. Зазначені завдання є основою для формування ефективної системи управління фінансовою безпекою та підвищення конкурентоспроможності підприємства.

Забезпечення фінансово-економічної безпеки підприємства тісно пов’язане зі сталим фінансовим розвитком, що вимагає ефективного та адаптивного фінансового механізму. Водночас важливо досягати не максимального, а оптимального рівня фінансової стійкості, який забезпечує ефективне функціонування та довгостроковий розвиток підприємства.

1.2. Інформаційна компонента у забезпеченні фінансово-економічної безпеки підприємства

У сучасних умовах інформація є одним із найцінніших ресурсів, який значно впливає на ефективність управління фінансово-економічною безпекою підприємства. Інформаційна компонента виступає ключовим елементом системи забезпечення безпеки, оскільки саме від якості, повноти та своєчасності інформації залежить здатність підприємства приймати стратегічно важливі рішення [36, с. 12].

Сучасний бізнес-середовище характеризується високою динамікою змін, зростанням обсягів даних і ускладненням процесів їх обробки. В таких умовах ефективне управління фінансово-економічною безпекою неможливе без належного інформаційного забезпечення, яке включає збирання, аналіз, обробку та зберігання даних про внутрішні та зовнішні чинники, що впливають на діяльність підприємства [29, с. 32].

Доцільно у рамках дослідження розглянути роль та значення інформаційної компоненти у забезпеченні фінансово-економічної безпеки підприємства, визначити її основні складові, а також розкрити механізми формування ефективної інформаційної системи для мінімізації ризиків і підвищення рівня безпеки. Це дозволить зрозуміти, як використання інформаційних ресурсів може сприяти досягненню стратегічних цілей та забезпеченню стабільного розвитку підприємства.

Інформаційна безпека відіграє ключову роль в забезпеченні економічної безпеки підприємства тому, що інформація є життєво важливим ресурсом, і її втрата або витік можуть призвести до втрати конкурентних переваг або навіть банкрутства (рис. 1.4).

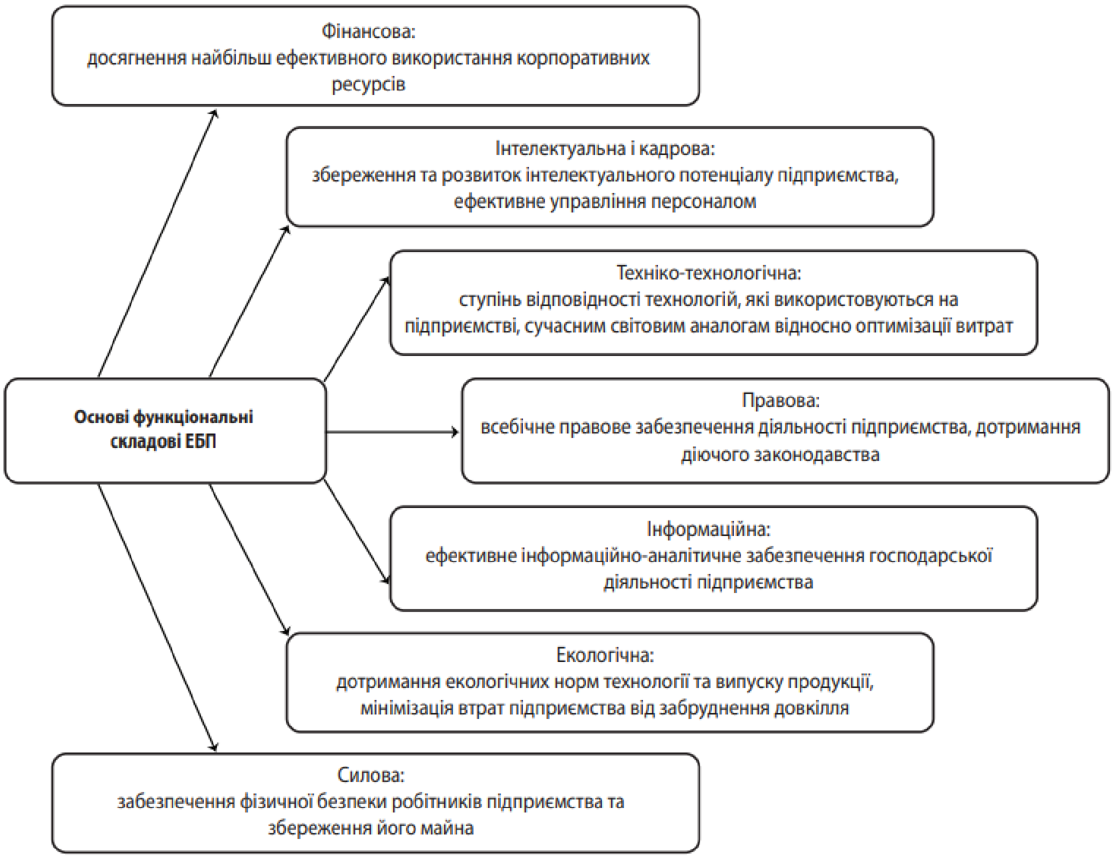

Рисунок 1.4 – Функціональні складові економічної безпеки підприємства

Джерело: за матеріалами [4, с. 157]

Важливість забезпечення інформаційної безпеки підприємств для економіки країни обумовлена наступними факторами:

критична роль інформації – інформація є невід'ємним ресурсом для функціонування будь-якого підприємства;

серйозність інформаційних загроз – кібератаки, витік даних та інші інформаційні загрози можуть завдати значної шкоди підприємствам;

захист від збитків – ефективна система інформаційної безпеки дозволяє підприємствам захистити свою інформацію та мінімізувати ризик фінансових та репутаційних втрат;

необхідність досліджень – вивчення інформаційної складової економічної безпеки допоможе розробити дієві заходи захисту інформації та підвищити стійкість підприємств до кіберзагроз.

Отже, забезпечення інформаційної безпеки є необхідною умовою для сталого розвитку підприємств та економіки країни в цілому.

Поняття «інформаційна безпека підприємства» може бути визначено як стан захищеності інформаційного середовища організації, що забезпечує захист даних від несанкціонованого доступу, витоку, спотворення або знищення. Іншими словами – це комплексний процес, спрямований на попередження будь-яких загроз, пов’язаних із несанкціонованими або ненавмисними впливами на інформацію, що має стратегічне значення для підприємства .

Загрози інформаційній безпеці підприємства являють собою сукупність внутрішніх і зовнішніх факторів, що створюють ризики для конфіденційності, цілісності та доступності інформаційних ресурсів. У сучасних умовах загрози стають більш складними, динамічними та багатовимірними, що вимагає від підприємств системного підходу до їхнього виявлення, аналізу та нейтралізації (рис. 1.5).

Рисунок 1.5 – Загрози інформаційній безпеці підприємства

Джерело: узагальнено автором за матеріалами [8]

Вплив зазначених загроз може призвести до фінансових втрат, репутаційних ризиків і порушення операційної діяльності підприємства. Тому важливо забезпечити своєчасне виявлення, оцінку та управління загрозами, застосовуючи сучасні технологічні рішення та організаційні заходи, спрямовані на мінімізацію ризиків, що дозволяє забезпечити стабільне функціонування підприємства в умовах зростаючих викликів інформаційної безпеки [26, с. 46].

Забезпечення інформаційної безпеки охоплює низку заходів, серед яких ідентифікація критично важливих інформаційних ресурсів, розробка системи управління інформаційними ризиками, створення технічних і організаційних засобів захисту інформації. Такий підхід спрямований на збереження конфіденційності, цілісності та доступності інформації, яка використовується в операційній, фінансовій та стратегічній діяльності підприємства [26, с. 48].

Особливу увагу в контексті інформаційної безпеки приділяють запобіганню зовнішнім загрозам, таким як кібератаки, шпигунство чи несанкціонований доступ до інформаційних систем, а також внутрішнім ризикам, зокрема ненавмисним помилкам персоналу або умисним діям. Ефективна система інформаційної безпеки повинна враховувати як технологічні аспекти, так і людський фактор, що потребує постійного моніторингу, навчання співробітників та вдосконалення захисних механізмів.

Інформація є стратегічним ресурсом підприємства, який безпосередньо впливає на його конкурентоспроможність, стабільність і розвиток. Забезпечення інформаційної безпеки вимагає впровадження системного підходу, що охоплює різні методи та засоби захисту інформаційних ресурсів від зовнішніх і внутрішніх загроз [35, с. 52].

Загальні методи забезпечення інформаційної безпеки включають організаційні, технічні, правові та програмні заходи. Поєднання зазначених методів дозволяє створити комплексну систему, яка мінімізує ризики несанкціонованого доступу до інформації, її втрати, спотворення або несанкціонованого використання. Важливими елементами цієї системи є побудова політик інформаційної безпеки, впровадження сучасних засобів захисту даних, а також навчання персоналу, спрямоване на підвищення обізнаності щодо потенційних загроз (табл. 1.2).

Таблиця 1.2 – Етапи забезпечення інформаційної безпеки підприємства

Стадія	**Опис**	**Практичні аспекти**
1. Визначення області та контексту інформаційної загрози	Ідентифікація інформаційних ресурсів, що піддаються загрозі, потенційних винуватців та їх мотивів.	- Аналіз ризиків: оцінка ймовірності та потенційного збитку від реалізації загроз. - Класифікація інформації: визначення рівня конфіденційності інформації та встановлення відповідних заходів захисту.
2. Розробка загальної стратегії	План дій для запобігання, виявлення та усунення інформаційних загроз у політичній, економічній, соціальній та інших сферах.	- Визначення цілей ІБ: чітке формулювання того, чого підприємство прагне досягти в сфері інформаційної безпеки. - Розробка політик ІБ: створення документів, що регламентують правила поводження з інформацією та використання інформаційних систем.
3. Інформування співробітників	Повідомлення про існуючі загрози та методи їх запобігання.	- Проведення навчань з ІБ: регулярне навчання персоналу з питань інформаційної безпеки, включаючи ознайомлення з політиками безпеки, правилами використання паролів, методами розпізнавання фішингових атак тощо. - Підвищення обізнаності з ІБ: формування культури інформаційної безпеки на підприємстві.
4. Виділення коштів та ресурсів	Забезпечення фінансування та необхідних ресурсів для ІБ.	- Інвестування в технології захисту: впровадження сучасних систем захисту інформації, таких як антивірусне програмне забезпечення, файрволи, системи виявлення вторгнень тощо. - Залучення експертів з ІБ: співпраця з кваліфікованими фахівцями з інформаційної безпеки для консультування та аудиту систем захисту.
5. Розробка політики безпеки	Створення документа, що визначає правила та процедури забезпечення ІБ з урахуванням існуючих загроз.	- Регулярний перегляд політики безпеки: оновлення політики безпеки з урахуванням змін в інформаційному середовищі та появи нових загроз. - Впровадження систем управління ІБ: використання стандартів та методологій управління інформаційною безпекою, таких як ISO 27001.

Джерело: узагальнено автором за матеріалами [37]

На основі аналізу сучасних методів і моделей забезпечення інформаційної безпеки підприємства було створено концептуальну модель її оцінювання та аналізу. Інформаційна система управління інформаційною безпекою є центральним елементом загальної системи управління, яка базується на комплексному аналізі ризиків. Ця система забезпечує основу для проектування, впровадження, моніторингу, супроводу та вдосконалення заходів, спрямованих на захист інформаційних ресурсів підприємства.

Дана модель складається з основних етапів, представлених на рис. 1.5.

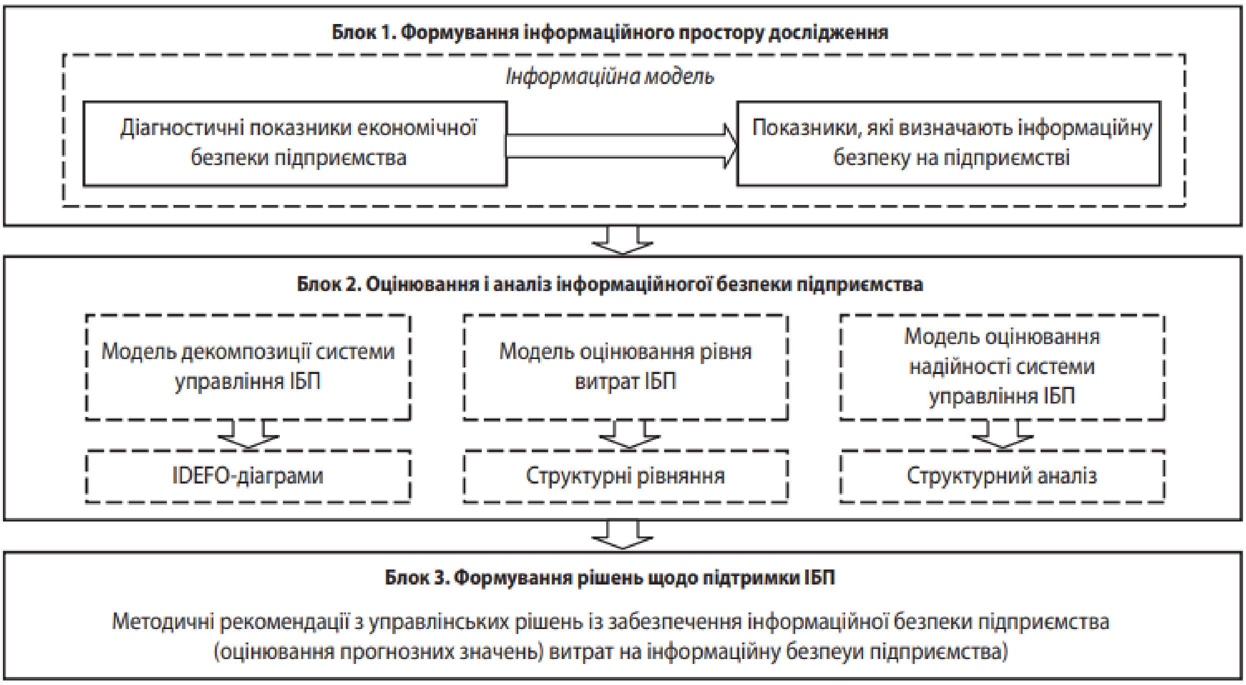

Рисунок 1.6 – Оцінка та аналіз інформаційної безпеки: концептуальна модель

Джерело: за матеріалами [4; с. 161]

Представлена на рис. 1.6, концептуальна модель є інструментом для системного підходу до управління інформаційною безпекою підприємства, забезпечуючи цілісний аналіз її стану та обґрунтування управлінських рішень, складається з трьох взаємопов’язаних блоків:

Перший блок моделі «Формування інформаційного простору дослідження» спрямований на створення інформаційного середовища для аналізу інформаційної безпеки підприємства. У цьому блоці визначаються діагностичні показники економічної безпеки, які є основою для оцінювання стану інформаційної безпеки. Важливим етапом є формування інформаційної моделі, яка включає ключові показники, що відображають як внутрішні, так і зовнішні аспекти захисту інформації на підприємстві. Цей блок забезпечує базу даних і аналітичну платформу для подальших етапів аналізу.

Другий блок моделі «Оцінювання і аналіз інформаційної безпеки підприємства» охоплює комплексний підхід до оцінювання та аналізу інформаційної безпеки. Він передбачає використання декількох моделей і методів, що дозволяють детально дослідити всі аспекти управління ІБП.

Зокрема, застосовується модель декомпозиції системи управління інформаційною безпекою із використанням IDEF0-діаграм, яка забезпечує деталізацію процесів і взаємозв’язків у системі. Також проводиться оцінювання рівня витрат на забезпечення ІБП та оцінка надійності системи захисту, що дозволяє виявити слабкі місця та потенційні ризики. Для глибшого аналізу використовуються структурні рівняння та методи структурного аналізу, які забезпечують розуміння взаємозв’язків між компонентами інформаційної безпеки.

Третій блок моделі «Формування рішень щодо підтримки ІБП» зосереджений на формуванні рекомендацій для управлінських рішень, спрямованих на підвищення рівня інформаційної безпеки підприємства. Особлива увага приділяється оцінюванню прогнозних значень витрат, необхідних для забезпечення надійного захисту інформації. Це дозволяє не лише оптимізувати витрати, але й визначити пріоритетні напрями інвестицій у систему безпеки.

1.3. Нормативно-правове забезпечення інформаційної безпеки підприємства

У сучасних умовах глобалізації, цифровізації та стрімкого розвитку інформаційних технологій забезпечення інформаційної безпеки підприємства набуває стратегічного значення. Захист інформаційних ресурсів, які є основою ефективного функціонування бізнесу, вимагає чіткого дотримання нормативно-правових вимог, що регулюють дану сферу. Нормативно-правове забезпечення є важливим інструментом, який встановлює правові рамки для розробки, впровадження та управління системою інформаційної безпеки, забезпечуючи захист даних від загроз та ризиків [17].

Управління інформаційною безпекою базується на трьох ключових складових: конфіденційності, цілісності та доступності інформації. Їх досягнення значною мірою залежить від відповідності нормативно-правовим актам, які регулюють захист інформації як на міжнародному, так і на національному рівнях. Міжнародні стандарти, такі як ISO/IEC 27001, визначають загальні вимоги до побудови систем управління інформаційною безпекою, тоді як національні законодавчі акти забезпечують адаптацію цих стандартів до специфіки кожної країни. Галузеві норми, у свою чергу, деталізують вимоги до інформаційної безпеки в окремих секторах, таких як банківська справа, енергетика або охорона здоров'я [40] .

Особливу роль у забезпеченні інформаційної безпеки відіграють внутрішні нормативні документи підприємств, які враховують специфіку їхньої діяльності та конкретизують порядок дій, спрямованих на захист інформаційних ресурсів. Політики інформаційної безпеки, регламенти доступу до інформаційних систем, інструкції щодо роботи з конфіденційними даними є важливими елементами організаційного механізму, що дозволяє ефективно запобігати потенційним загрозам і реагувати на інциденти [38].

У правовому аспекті інформаційна безпека підприємства забезпечується шляхом дотримання міжнародних стандартів, національного законодавства, галузевих регуляторних норм та внутрішніх нормативних актів підприємства. Наступним кроком є доцільність детального аналізу кожного з цих видів нормативних документів.

Міжнародні стандарти відіграють ключову роль у формуванні системи управління інформаційною безпекою підприємства. Вони встановлюють загальні вимоги, рекомендації та кращі практики для забезпечення захисту інформаційних ресурсів від загроз, незалежно від їхнього джерела. Дотримання цих стандартів дозволяє підприємствам досягати високого рівня інформаційної безпеки, підвищувати довіру з боку партнерів і клієнтів, а також відповідати вимогам регуляторних органів [24, с. 57-60].

Нижче подано основні міжнародні стандарти, які визначають підходи до управління інформаційною безпекою (табл. 1.3)

Таблиця 1.3 – Порівняння стандартів інформаційної безпеки

Стандарт	Опис	Ключові аспекти
ISO/IEC 27001	Встановлює вимоги до створення, впровадження та управління системою управління інформаційною безпекою (СУІБ).	✓ Структурований підхід: забезпечує чітку структуру для управління інформаційною безпекою. ✓ Ідентифікація та управління ризиками: допомагає визначити та оцінити ризики, пов'язані з інформаційною безпекою. ✓ Заходи захисту: спрямовані на збереження конфіденційності, цілісності та доступності інформації. ✓ Постійне вдосконалення: передбачає регулярний перегляд та оновлення СУІБ.
ISO/IEC 27002	Містить рекомендації щодо впровадження практик управління інформаційною безпекою.	✓ Практичні поради: надає конкретні рекомендації щодо застосування стандартів інформаційної безпеки. ✓ Перелік контролів безпеки: пропонує широкий спектр контролів для захисту інформаційних активів. ✓ Роз'яснення щодо застосування: допомагає зрозуміти, як правильно впроваджувати контролі безпеки.
NIST Cybersecurity Framework	Забезпечує інструменти для виявлення, запобігання та реагування на кіберзагрози.	✓ Гнучкість та масштабованість: може бути адаптована до різних типів організацій та рівнів ризику. ✓ П'ять ключових функцій: ідентифікація, захист, виявлення, реагування та відновлення. ✓ Орієнтація на кіберзагрози: допомагає організаціям ефективно протидіяти сучасним кіберзагрозам.

Джерело: узагальнено автором за матеріалами [40]

Таким чином, міжнародні стандарти є фундаментом для побудови ефективної системи управління інформаційною безпекою. Їх застосування дозволяє підприємствам створити надійний захист своїх інформаційних ресурсів, відповідати вимогам регуляторів і зміцнювати конкурентоспроможність у сучасному бізнес-середовищі.

Національне законодавство кожної країни відіграє важливу роль у регулюванні питань інформаційної безпеки підприємств, встановлюючи обов’язкові вимоги для захисту інформаційних ресурсів. Одним із ключових аспектів є захист персональних даних, що передбачає дотримання конфіденційності та законне використання інформації про фізичних осіб. Також важливим елементом є регулювання комерційної таємниці, що захищає стратегічно важливі дані підприємства від несанкціонованого розголошення [23, с. 138].

Окрему увагу приділяють протидії кіберзлочинності, яка спрямована на запобігання незаконному доступу до інформаційних систем і боротьбу з різними видами кіберзагроз. Крім того, законодавство визначає обов'язки підприємств щодо впровадження заходів інформаційної безпеки, таких як створення внутрішніх політик, застосування технологічних засобів захисту та проведення аудиту інформаційної безпеки. Усі ці аспекти забезпечують правову основу для побудови ефективної системи управління інформаційною безпекою на підприємстві.

У різних галузях економіки діють спеціалізовані нормативні акти та стандарти, які враховують специфіку діяльності підприємств та встановлюють вимоги до забезпечення інформаційної безпеки. Наприклад, у банківській сфері та фінансових установах широко використовуються стандарти PCI DSS (Payment Card Industry Data Security Standard), які спрямовані на захист платіжної інформації та зниження ризиків шахрайства з банківськими картками. В енергетичній галузі діють регуляції, що забезпечують захист критично важливої інфраструктури від кіберзагроз, таких як атаки на енергомережі або системи управління енергоресурсами. У сфері охорони здоров’я нормативи зосереджені на захисті медичних даних, зокрема інформації про пацієнтів, забезпечуючи дотримання конфіденційності та захист систем електронної охорони здоров'я. Такі галузеві норми дозволяють не лише враховувати специфічні загрози для кожного сектора, але й розробляти цільові заходи для мінімізації ризиків та підвищення рівня інформаційної безпеки [40].

Ефективне управління інформаційною безпекою на підприємстві неможливе без розробки внутрішніх нормативних документів, які регламентують ключові аспекти захисту інформаційних ресурсів. Такі документи враховують специфіку діяльності підприємства та встановлюють чіткі правила доступу, зберігання та використання інформації, а також визначають відповідальність співробітників за порушення цих правил (рис. 1.7).

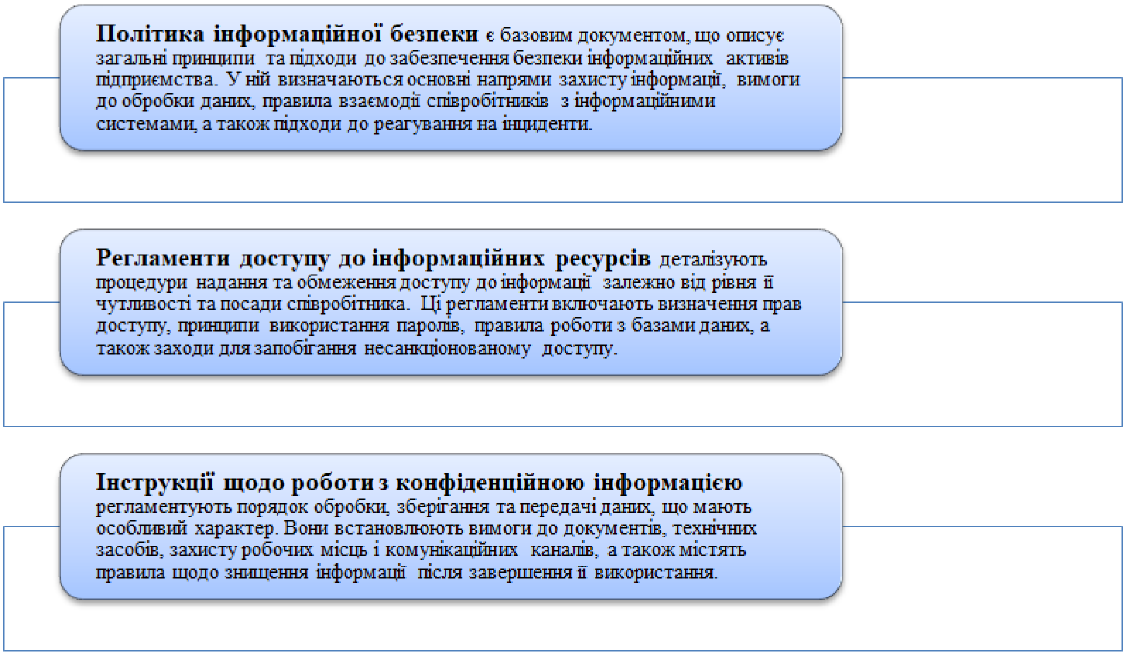

Рисунок 1.7 – Внутрішні нормативні документи підприємства

Джерело: узагальнено автором за матеріалами [27]

Розробка та впровадження таких внутрішніх нормативних документів дозволяє підприємству забезпечити комплексний захист інформаційних ресурсів, мінімізувати ризики, пов’язані з внутрішніми та зовнішніми загрозами, і сприяє підвищенню загальної культури інформаційної безпеки серед персоналу.

Нормативно-правове забезпечення є фундаментом для створення та ефективного функціонування системи управління інформаційною безпекою підприємства. Воно формує правову основу, яка регламентує всі аспекти захисту інформаційних ресурсів, включаючи збереження конфіденційності, цілісності та доступності даних. Завдяки міжнародним стандартам, національному законодавству, галузевим нормам і внутрішнім регламентам підприємства отримують інструменти для створення комплексної системи захисту, що враховує сучасні виклики та загрози [27].

Дотримання правових норм дозволяє мінімізувати ризики, пов’язані з інформаційними загрозами, а також запобігти фінансовим втратам, репутаційним збиткам та порушенням операційної діяльності. Впровадження таких заходів підвищує довіру партнерів, клієнтів і регуляторних органів, що сприяє зміцненню конкурентних позицій підприємства.

Крім того, нормативно-правова база сприяє формуванню культури інформаційної безпеки, як серед співробітників, так і серед керівництва, що в свою чергу, забезпечує злагоджену роботу всіх елементів системи управління, дозволяючи підприємству адаптуватися до змінного середовища та оперативно реагувати на нові виклики.

Таким чином, нормативно-правове забезпечення не лише захищає інформаційні активи підприємства, але й створює умови для його стабільного функціонування, розвитку та побудови довгострокових взаємин із зацікавленими сторонами.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРАТ «КІРОВОГРАДОБЛЕНЕРГО»

2.1. Характеристика господарської діяльності ПрАТ «Кіровоградобленерго»

Приватне акціонерне товариство «Кіровоградобленерго» є ключовим енергетичним підприємством регіону, що забезпечує передачу та постачання електроенергії споживачам Кіровоградської області. Господарська діяльність підприємства має важливе значення для стабільного функціонування економіки області, розвитку інфраструктури та підвищення якості життя населення. Як учасник національного енергетичного ринку, підприємство виконує важливі завдання у сфері енергозабезпечення, дотримуючись принципів енергоефективності, надійності та прозорості [18].

Діяльність ПрАТ «Кіровоградобленерго» охоплює широкий спектр послуг, включаючи транспортування електроенергії через розподільчі мережі, облік споживання, технічне обслуговування енергетичної інфраструктури, а також модернізацію та будівництво нових об’єктів. Компанія орієнтована на впровадження інноваційних технологій і сучасних методів управління, що дозволяє забезпечувати безперебійне енергопостачання навіть в умовах зростаючих потреб споживачів і складних економічних умов [18].

Важливим напрямом роботи підприємства є розвиток партнерських відносин із клієнтами, формування високої культури обслуговування та забезпечення прозорості у взаємодії, що включає автоматизацію процесів, удосконалення системи обліку та впровадження цифрових платформ для зручності споживачів.

У цьому розділі дипломної роботи доцільно провести детальний аналіз діяльності ПрАТ «Кіровоградобленерго», включаючи його організаційну структуру, основні напрями діяльності, економічні показники та стратегічні цілі.

Діяльність ПрАТ «Кіровоградобленерго» спрямована на забезпечення стабільного енергопостачання регіону, підвищення ефективності енергетичної інфраструктури та вдосконалення сервісу для споживачів. У своїй роботі підприємство дотримується стратегічних напрямів, що охоплюють технічний, економічний, екологічний та соціальний аспекти розвитку.

У таблиці 2.1 наведено основні цілі діяльності ПрАТ «Кіровоградобленерго», які відображають пріоритети компанії, спрямовані на сталий розвиток, задоволення потреб споживачів і забезпечення енергетичної безпеки. Зазначені напрями роботи підприємства є основою для реалізації стратегічних планів підприємства, що дозволяють підвищувати його конкурентоспроможність і зміцнювати позиції на енергетичному ринку.

Таблиця 2.1 – Ключові напрямки діяльності ПрАТ «Кіровоградобленерго»

СФЕРА ДІЯЛЬНОСТІ	КЛЮЧОВІ НАПРЯМКИ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА
ЕЛЕКТРОПОСТАЧАННЯ	- забезпечення надійного та якісного електропостачання споживачам області - дотримання сучасних стандартів енергетичної безпеки
ЕНЕРГОЕФЕКТИВНІСТЬ	- впровадження інноваційних технологій для зниження втрат електроенергії оптимізація енергоспоживання - підвищення загальної ефективності роботи енергосистеми
ІНФРАСТРУКТУРА	- модернізація, реконструкція та будівництво нових електричних мереж та підстанцій - підвищення надійності енергопостачання
СПОЖИВАЧІ	- орієнтація на споживача - оперативне реагування на заявки - вдосконалення сервісу та підвищення якості обслуговування - прозорість у взаємодії
ЕКОЛОГІЯ	- зменшення впливу на навколишнє середовище - впровадження екологічно чистих технологій - раціональне використання ресурсів
ЕКОНОМІКА	- забезпечення фінансової стійкості - ефективне управління ресурсами - розвиток нових напрямків діяльності - впровадження інноваційних рішень - підвищення конкурентоспроможності
ПЕРСОНАЛ	- підвищення кваліфікації працівників - навчання та професійне зростання - створення безпечних і комфортних умов праці

Джерело: сформовано автором за матеріалами підприємства

Зазначимо, Статут Приватного акціонерного товариства «Кіровоградобленерго» є основним установчим документом, який визначає правові, організаційні та економічні основи діяльності компанії. Цей документ регулює внутрішню структуру, принципи функціонування, порядок прийняття рішень, а також права та обов’язки акціонерів, органів управління та працівників підприємства.

Статут ПрАТ «Кіровоградобленерго» встановлює: мету та завдання діяльності підприємства; організаційну структуру підприємства; порядок розподілу прибутку; права та обов’язки акціонерів; питання взаємодії з державними органами; порядок внесення змін до Статуту тощо.

Статут є юридичною основою для всіх видів діяльності ПрАТ «Кіровоградобленерго», забезпечуючи відповідність операцій підприємства нормам законодавства України та спрямовуючи його на досягнення стратегічних цілей. Цим документом визначено правову базу для прийняття управлінських рішень, забезпечуючи прозорість і ефективність функціонування компанії.

Ефективне управління діяльністю енергетичного підприємства значною мірою залежить від його організаційної структури. Організаційна структура ПрАТ «Кіровоградобленерго» розроблена з урахуванням специфіки функціонування енергетичної галузі та орієнтована на досягнення стратегічних цілей компанії, що забезпечує розподіл функцій, відповідальності та повноважень між підрозділами, що сприяє злагодженій роботі всіх елементів системи (рис 2.1).

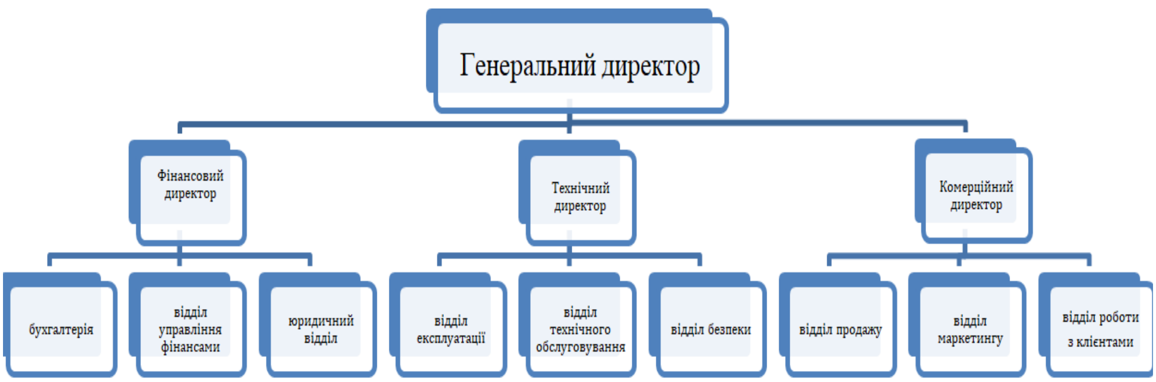

Рисунок 2.1 – Організаційна структура ПрАТ «Кіровоградобленерго»

Джерело: узагальнено автором за матеріалами додатку А

На рис. 2.1 представлено організаційну структуру ПрАТ «Кіровоградобленерго», яка включає ключові управлінські рівні, підрозділи та їх взаємозв'язки. Відображення цієї структури дозволяє зрозуміти принципи побудови системи управління підприємством, її функціональні особливості та роль кожного підрозділу у забезпеченні стабільної роботи компанії.

ПрАТ «Кіровоградобленерго» виконує низку важливих функцій, спрямованих на забезпечення енергетичної стабільності регіону, вдосконалення інфраструктури та задоволення потреб споживачів. Діяльність підприємства охоплює широкий спектр завдань, включаючи розподіл і постачання електроенергії, технічне обслуговування мереж, впровадження енергоефективних рішень та модернізацію енергетичних об'єктів (рис. 2.2)

Рисунок 2.2 – Основні види діяльності ПрАТ «Кіровоградобленерго»

Джерело: узагальнено автором за матеріалами додатку А

На рис. 2.2 візуалізовано основні види діяльності ПрАТ «Кіровоградобленерго», що ілюструють багатовекторність функціональної спрямованості компанії. Представлені напрямки діяльності орієнтовані на забезпечення сталого функціонування регіональної енергетичної системи шляхом: гарантування надійного енергопостачання; підвищення ефективності операційної діяльності; дотримання екологічних стандартів; вдосконалення якості обслуговування споживачів тощо.

ПрАТ «Кіровоградобленерго» активно проводить інформаційно-роз'яснювальну роботу серед населення з метою підвищення обізнаності щодо раціонального використання електроенергії та енергоефективності. Особливу увагу приділяють роз'ясненню правил безпечного користування електрообладнанням, що сприяє зниженню ризиків аварійних ситуацій та травмувань. Зазначені заходи включають проведення тематичних лекцій, інформаційних кампаній, а також публікацію матеріалів у відкритих джерелах і соціальних мережах.

Крім того, компанія «Кіровоградобленерго» виконує регуляторні вимоги та забезпечує відповідність своєї діяльності чинному законодавству і встановленим стандартам енергетичної галузі. ПрАТ «Кіровоградобленерго» активно співпрацює з державними органами та регуляторами, беручи участь у процесах формування політик і стандартів у сфері енергетики. Така взаємодія дозволяє підприємству залишатися прозорим у своїй роботі, відповідати вимогам сучасного ринку та сприяти розвитку енергетичного сектору.

ПрАТ «Кіровоградобленерго» демонструє високу соціальну відповідальність, беручи участь у реалізації програм, спрямованих на покращення життя місцевих громад. Підприємство підтримує соціальні ініціативи, які включають розвиток інфраструктури, допомогу освітнім і медичним закладам, а також реалізацію екологічних проєктів. Така діяльність сприяє підвищенню рівня довіри з боку населення та зміцненню іміджу компанії як надійного партнера для громади.

Отже, підприємство «Кіровоградобленерго» є ключовим елементом регіональної енергетичної системи, що сприяє економічному зростанню та підвищенню якості життя населення завдяки впровадженню нових технологій, дотриманню принципів енергоефективності, екологічної безпеки та реалізації соціальних програм.

2.2. Оцінка поточного стану фінансово-економічної безпеки ПрАТ «Кіровоградобленерго»

Фінансово-економічна безпека підприємства є ключовою умовою для його стабільного функціонування, розвитку та досягнення стратегічних цілей. Вона забезпечує захист економічних інтересів, збереження ресурсів і стійкість до внутрішніх та зовнішніх ризиків. Для ПрАТ «Кіровоградобленерго», як одного з провідних енергетичних підприємств регіону, фінансово-економічна безпека набуває особливого значення в умовах динамічного розвитку енергетичного ринку, підвищення конкуренції та впливу економічних криз.

Аналіз поточного стану фінансово-економічної безпеки дозволяє оцінити рівень стійкості підприємства до фінансових ризиків, його здатність ефективно використовувати ресурси та адаптуватися до змін у зовнішньому середовищі. Оцінка включає аналіз основних фінансових показників, виявлення ключових загроз та недоліків, а також оцінку ефективності заходів, спрямованих на їх нейтралізацію, що є важливим інструментом для прийняття управлінських рішень, спрямованих на підвищення конкурентоспроможності та економічної стабільності компанії.

Для комплексної оцінки фінансово-економічної стабільності ПрАТ «Кіровоградобленерго» проведемо аналіз структури активів за 2021-2023 роки. Зокрема, дослідимо динаміку змін у складі необоротних та оборотних активів і їх вплив на загальний фінансовий стан компанії (табл. 2.2).

Аналіз табл. 2.2 показав, що необоротні активи ПрАТ «Кіровоградобленерго» включають нематеріальні активи, основні засоби та незавершені капітальні інвестиції. За період з 2021 по 2023 рік спостерігається зменшення загальної вартості необоротних активів на 240 898 грн. Основним фактором цього скорочення є зниження вартості основних засобів, що може бути пов’язано із їхнім зносом або недостатніми інвестиціями в модернізацію. Зокрема, первісна вартість основних засобів зменшилася на 225 837 грн, що свідчить про певну деградацію активів, важливих для операційної діяльності підприємства.

Таблиця 2.2 – Структура активів ПрАТ «Кіровоградобленерго» за 2021-2023 роки

Показник	Код рядка Ф1	2021	2022	2023	Відхилення 2023-2021
I. Необоротні активи					
Нематеріальні активи	1000	9 227,00	9 727,00	8 678,00	-549,00
первісна вартість	1001	20 648,00	24 739,00	27 947,00	7 299,00
накопичена амортизація	1002	11 421,00	15 012,00	19 269,00	7 848,00
Незавершені капітальні інвестиції	1005	45 141,00	76 462,00	30 629,00	-14 512,00
Основні засоби	1010	2 739 913,00	2 606 817,00	2 514 076,00	-225 837,00
первісна вартість	1011	3 871 912,00	4 046 952,00	4 205 023,00	333 111,00
знос	1012	1 131 999,00	1 440 135,00	1 690 947,00	558 948,00
Усього за розділом I	**1095**	**2 794 281,00**	**2 693 006,00**	**2 553 383,00**	-240 898,00
II. Оборотні активи					
Запаси	1100	31 067,00	56 001,00	52 212,00	21 145,00
Дебіторська заборгованість за продукцію, товари, роботи, послуги	1125	21 739,00	40 824,00	115 684,00	93 945,00
Дебіторська заборгованість за розрахунками:					
за виданими авансами	1130	13 550,00	10 116,00	4 980,00	-8 570,00
з бюджетом	1135	5,00	15 144,00	15 135,00	15 130,00
у тому числі з податку на прибуток	1136	0	15 139,00	15 135,00	15 135,00
Гроші та їх еквіваленти	1165	46 398,00	30 290,00	23 825,00	-22 573,00
Інші оборотні активи	**1190**	**5 015,00**	**17 542,00**	**59 532,00**	54 517,00
Усього за розділом II	**1195**	**117 774,00**	**169 917,00**	**271 368,00**	153 594,00
III. Необоротні активи, утримувані для продажу, та групи вибуття	**1200**	**0**	**0**	**0**	0,00
Баланс	**1300**	**2 912 055,00**	**2 862 923,00**	**2 824 751,00**	-87 304,00

Джерело: складено автором за матеріалами додатків В, Г, Д

Оборотні активи за період дослідження зросли на 153 594 грн, що свідчить про покращення поточної ліквідності підприємства. Найбільше зростання відбулося у дебіторській заборгованості за продукцію, товари, роботи та послуги, яка збільшилася на 93 945 грн. Це може вказувати на проблеми з розрахунками з боку клієнтів або зміну умов кредитної політики підприємства. Також зросли запаси (+21 145 грн) та інші оборотні активи (+54 517 грн), що демонструє певну активізацію операційної діяльності. Однак грошові кошти та їх еквіваленти скоротилися на 22 573 грн, що може свідчити про зменшення швидкої ліквідності.

Загальна балансова вартість активів підприємства зменшилася на 87 304 грн у 2023 році порівняно з 2021 роком. Це свідчить про скорочення ресурсної бази компанії, що може бути пов'язане із зниженням інвестиційної активності та накопиченням зносу основних засобів. Незважаючи на зростання оборотних активів, скорочення необоротних активів чинить негативний вплив на загальну фінансову стабільність підприємства.

Розрахуємо на основі даних таблиці 2.2 показники структури активів за формулами та отримані результати представимо графічно (рис. 2.3):

$$\text{Частка необоротних активів} = \frac{\text{Усього за розділом I (необоротні активи)}}{\text{Баланс}} \times 100\% \quad (1)$$

$$\text{Частка оборотних активів} = \frac{\text{Усього за розділом II (оборотні активи)}}{\text{Баланс}} \times 100\% \quad (2)$$

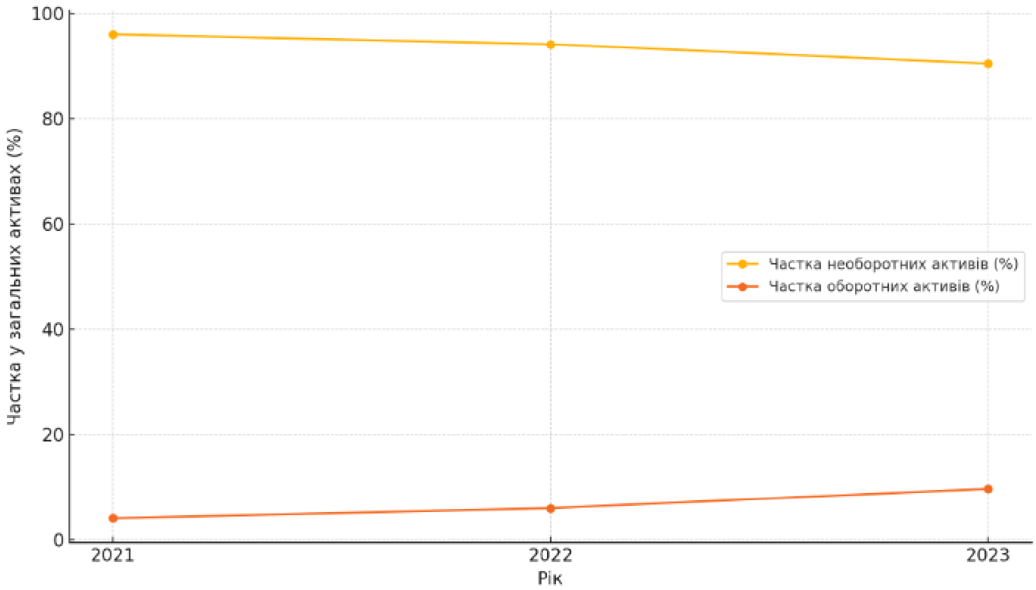

Рисунок 2.3 – Динаміка часток необоротних та оборотних активів у загальних активах ПрАТ «Кіровоградобленерго» за 2021–2023 роки.

Джерело: побудовано автором за матеріалами додатків В, Г, Д

На рис. 2.3 представлено динаміку часток необоротних та оборотних активів у загальних активах ПрАТ «Кіровоградобленерго» за 2021–2023 роки.

Протягом аналізованого періоду частка необоротних активів у загальних активах поступово зменшувалася: з 95,96% у 2021 році до 90,39% у 2023 році, що свідчить про зниження інвестицій у довгострокові активи, яке може бути пов’язане із накопиченням зносу основних засобів або зменшенням обсягу капітальних інвестицій.

Частка оборотних активів у структурі активів, навпаки, зросла: з 4,04% у 2021 році до 9,61% у 2023 році. Зазначена тенденція може свідчити про підвищення ліквідності підприємства, зокрема через збільшення запасів і дебіторської заборгованості, але також може вказувати на тимчасове нагромадження оборотних активів, яке потребує ефективного управління.

Зміна часток необоротних і оборотних активів відображає перерозподіл ресурсів компанії, який може бути викликаний змінами у фінансовій стратегії, економічним станом підприємства чи зовнішніми ринковими умовами. Аналіз цих показників є важливим для оцінки стабільності та ефективності використання активів компанії.

При аналізі фінансової стійкості підприємства важливо розрахувати коефіцієнт маневреності власного капіталу, щоб оцінити, яка частина власного капіталу вкладена в оборотні активи та наскільки вільно підприємство може розпоряджатися цими коштами для фінансування поточної діяльності. Цей коефіцієнт показує співвідношення між власними обіговими коштами та власним капіталом. Високе значення коефіцієнта свідчить про те, що підприємство має достатньо власних коштів для фінансування поточної діяльності та менше залежить від зовнішніх джерел фінансування.

$$\text{Коефіцієнт маневреності} = \frac{\text{Оборотні активи}}{\text{Усього активів}}, \qquad (3)$$

В табл. 2.3 представлено дані щодо структури активів ПрАТ «Кіровоградобленерго» за 2021-2023 роки.

Таблиця 2.3 – Показники структури активів та коефіцієнт маневреності власного капіталу ПрАТ «Кіровоградобленерго» за 2021–2023 роки

Рік	Частка необоротних активів, (%)	Частка оборотних активів, (%)	Коефіцієнт маневреності
2021	95.96	4.04	0.0404
2022	94.06	5.94	0.0594
2023	90.39	9.61	0.0961

Джерело: побудовано автором за матеріалами додатків В, Г, Д

Аналіз даних табл. 2.3 демонструє певні тенденції у структурі активів ПрАТ «Кіровоградобленерго» за 2021-2023 роки. По-перше, спостерігається поступове зменшення частки необоротних активів у загальній структурі. У 2021 році вона становила 95,96%, а до 2023 року знизилася до 90,39%. Це може бути пов'язано з оновленням основних засобів, наприклад, списанням застарілого обладнання та придбанням нового, або зі зміною інвестиційної політики компанії, що призвела до зменшення інвестицій у довгострокові активи.

По-друге, частка оборотних активів, навпаки, зростає. У 2021 році вона становила 4,04%, а до 2023 року збільшилася до 9,61%. Таке зростання може бути обумовлене збільшенням обсягів діяльності компанії, що призводить до зростання дебіторської заборгованості, запасів тощо. Також це може свідчити про оптимізацію управління оборотними коштами та підвищення ефективності їх використання.

Зростання коефіцієнта маневреності з 0,0404 у 2021 році до 0,0961 у 2023 році вказує на підвищення фінансової гнучкості компанії. Цей коефіцієнт показує, яка частина необоротних активів фінансується за рахунок оборотних, і його зростання означає, що підприємство має більше можливостей для маневрування своїми коштами та швидкої адаптації до змін у зовнішньому середовищі.

Загалом, можна говорити про тенденцію до збільшення частки оборотних активів та підвищення фінансової гнучкості ПрАТ «Кіровоградобленерго».

Далі доцільно розглянути динаміку структури пасивів ПрАТ «Кіровоградобленерго» за досліджуваний період 2021-2023 роки (табл. 2.4).

Динаміка власного капіталу ПрАТ «Кіровоградобленерго» за період 2021–2023 років демонструє зниження на 226 421 грн, що становить суттєвий вплив на фінансову стійкість підприємства. Основним чинником зменшення є скорочення капіталу у дооцінках на 240 549 грн, що може бути наслідком перегляду вартості активів. Натомість, нерозподілений прибуток за аналізований період зріс на 14 128 грн, що свідчить про певну стабільність операційної діяльності підприємства, хоча й у невеликих масштабах.

Таблиця 2.4 – Структура пасивів ПрАТ «Кіровоградобленерго» за 2021-2023 роки

Показник	Код рядка Ф1	2021	2022	2023	Відхилення 2023-2021
1	2	3	4	5	6
I. Власний капітал					
Зареєстрований капітал	1400	29 844,00	29 844,00	29 844,00	0,00
Капітал у дооцінках	1405	1 098 277,00	959 620,00	857 728,00	-240 549,00
Додатковий капітал	1410	102 060,00	102 060,00	102 060,00	0,00
Резервний капітал	1415	4 481,00	4 481,00	4 481,00	0,00
Нерозподілений прибуток (непокритий збиток)	1420	1 000 094,00	1 169 617,00	1 014 222,00	14 128,00
Усього за розділом I	**1495**	**2 234 756,00**	**2 265 622,00**	**2 008 335,00**	-226 421,00
II. Довгострокові зобов’язання і забезпечення					
Відстрочені податкові зобов’язання	1500	200 109,00	184 009,00	177 404,00	-22 705,00
Інші довгострокові зобов’язання	1515	2 787,00	1 938,00	942,00	-1 845,00
Усього за розділом II	**1595**	**202 896,00**	**185 947,00**	**178 346,00**	-24 550,00
III. Поточні зобов’язання і забезпечення					
Короткострокові кредити банків	1600	5 000,00	1,00	5 000,00	0,00
Поточна кредиторська заборгованість за: довгостроковими зобов’язаннями	1610	1 469,00	1 469,00	1 469,00	0
товари, роботи, послуги	1615	17 614,00	88 511,00	337 342,00	319 728,00
розрахунками з бюджетом	1620	36 698,00	21 954,00	23 587,00	-13 111,00
у тому числі з податку на прибуток	1621	11 302,00	0	0	-11 302,00
розрахунками зі страхування	1625	5 883,00	4 354,00	4 919,00	-964,00
розрахунками з оплати праці	1630	21 165,00	16 561,00	19 847,00	-1 318,00
Поточні забезпечення	1660	75 136,00	102 768,00	108 876,00	33 740,00
Інші поточні зобов’язання	1690	93 954,00	46 982,00	68 165,00	-25 789,00
Усього за розділом III	**1695**	**474 403,00**	**411 354,00**	**638 070,00**	163 667,00
IV. Зобов’язання, пов’язані з необоротними активами, утримуваними для продажу, та групами вибуття	**1700**	**0**	**0**	**0**	**0**
Баланс	**1900**	**2 912 055,00**	**2 862 923,00**	**2 824 751,00**	**-87 304,00**

Джерело: складено автором за матеріалами додатків В; Г; Д

Довгострокові зобов’язання підприємства зазнали зниження на 24 550 грн, переважно за рахунок скорочення відстрочених податкових зобов'язань на 22 705 грн. Це може свідчити про покращення управління податковими платежами або про зменшення оподатковуваної бази. Інші довгострокові зобов'язання також скоротилися на 1 845 грн, що є незначним впливом у загальній структурі фінансування підприємства.

Поточні зобов'язання зросли на 163 667 грн, що може вказувати на підвищення потреби у короткостроковому фінансуванні або на зростання обсягів операційної діяльності. Найбільший приріст відбувся за кредиторською заборгованістю за товари, роботи та послуги, яка зросла на 319 728 грн. Це може свідчити про збільшення відтермінування платежів постачальникам або активізацію господарської діяльності. Водночас зниження поточних забезпечень (-33 740 грн) і зобов'язань перед бюджетом (-13 111 грн) свідчить про часткове виконання підприємством своїх фінансових зобов'язань.

Загальна сума активів підприємства за аналізований період скоротилася на 87 304 грн. Це зменшення вказує на зниження ресурсної бази компанії, що може бути пов'язано із зменшенням власного капіталу та скороченням довгострокових зобов'язань. Попри збільшення поточних зобов'язань, зниження власного капіталу може негативно вплинути на фінансову стійкість підприємства.

Отже, структура фінансування ПрАТ «Кіровоградобленерго» демонструє змішані тенденції. Зниження власного капіталу і зростання поточних зобов'язань можуть свідчити про тимчасові труднощі у фінансовому управлінні або збільшення залежності від короткострокового фінансування. Водночас скорочення довгострокових зобов'язань є позитивним сигналом для зниження фінансових ризиків у довгостроковій перспективі. Для покращення фінансової стійкості підприємства доцільно зосередитися на підвищенні капіталізації, оптимізації управління зобов'язаннями та покращенні ефективності використання активів.

З метою оцінки фінансової стійкості, структури капіталу, рівня залежності підприємства від зовнішніх зобов'язань та динаміки ключових елементів фінансової діяльності ПрАТ «Кіровоградобленерго» проведемо розрахунок фінансових показників та отримані результати зведемо у таблицю 2.5. Зазначимо, що ці показники дозволяють зробити висновки про ефективність управління фінансовими ресурсами, виявити можливі ризики для фінансово-економічної безпеки підприємства та сформувати обґрунтовані рекомендації для покращення фінансового стану. На рисунку 2.4 представлено методику розрахунку фінансових показників, які використовуються для аналізу фінансового стану підприємства.

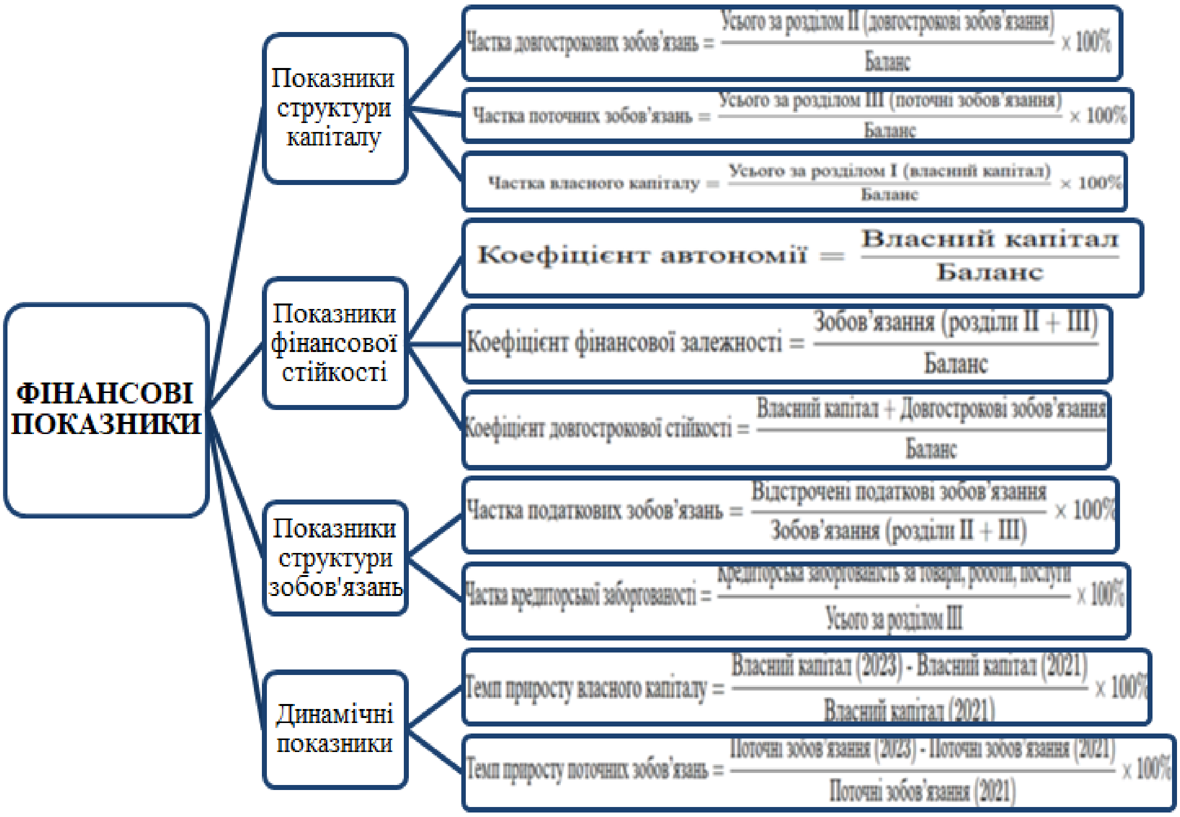

Рисунок 2.4 – Структура фінансових показників для оцінки фінансового стану підприємства

Джерело: узагальнено автором

Аналізуючи показники структури капіталу бачимо, що у 2021 році частка власного капіталу складала 76,74%, але зросла до 79,12% у 2022 році, що свідчить про тимчасове покращення фінансової автономії підприємства. Однак у 2023 році вона знизилася до 71,10%, що може бути наслідком збільшення зобов'язань або зменшення власного капіталу. Протягом трьох років частка довгострокових зобов'язань зменшувалася: з 6,97% у 2021 році до 6,31% у 2023 році. Це свідчить про зниження довгострокового боргового навантаження. Частка поточних зобов'язань збільшилася з 16,29% у 2021 році до 22,59% у 2023 році, що вказує на зростання короткострокових зобов'язань, які потребують оперативного управління.

Таблиця 2.5 – Фінансові показники структури капіталу, фінансової стійкості, структури зобов'язань та динаміки зобов'язань ПрАТ «Кіровоградобленерго» за 2021–2023 роки

Рік	Частка власного капіталу, (%)	Частка довгострокових зобов'язань, (%)	Частка поточних зобов'язань, (%)	Коефіцієнт автономії	Коефіцієнт фінансової залежності	Коефіцієнт довгострокової стійкості	Частка податкових зобов'язань у загальних зобов'язаннях, (%)	Частка кредиторської заборгованості за товари, (%)	Темп приросту власного капіталу, (%)	Темп приросту поточних зобов'язань, (%)
2021	76.74	6.97	16.29	0.7674	0.2326	0.8371	29.55	3.71	0.00	0.00
2022	79.12	6.50	14.37	0.7912	0.2086	0.8562	30.81	21.42	1.36	-13.29
2023	71.10	6.31	22.59	0.7110	0.2890	0.7741	21.73	52.87	-10.13	34.50

Джерело: розраховано автором за матеріалами додатків В; Г; Д

Розраховані показники фінансової стійкості свідчать, що коефіцієнт автономії залишався на стабільно високому рівні протягом 2021–2022 років (0,7674 та 0,7912 відповідно). Однак у 2023 році він знизився до 0,7110, що вказує на зменшення рівня фінансової незалежності підприємства.

Коефіцієнт фінансової залежності у 2021 році складав 0,2326, але зріс до 0,2890 у 2023 році. Це вказує на поступове збільшення залежності підприємства від зовнішнього фінансування.

Показник коефіцієнту довгострокової стійкості демонструє тенденцію до зниження: з 0,8371 у 2021 році до 0,7741 у 2023 році. Це вказує на зменшення довгострокової стабільності капітальної структури.

Аналіз динаміки структури зобов'язань ПрАТ "Кіровоградобленерго" виявляє кілька важливих тенденцій. По-перше, спостерігаються коливання в частці відстрочених податкових зобов'язань. Після зростання з 29,55% у 2021 році до 30,81% у 2022 році, вона знизилася до 21,73% у 2023 році. Такі зміни можуть бути обумовлені низкою факторів, включаючи зміни в податковому законодавстві, облікову політику підприємства або структуру його зобов'язань в цілому.

По-друге, спостерігається значне збільшення частки кредиторської заборгованості за товари, роботи і послуги. Вона зросла з 3,71% у 2021 році до 52,87% у 2023 році. Таке різке зростання може свідчити про декілька можливих ситуацій:

затримки в оплаті зобов'язань перед постачальниками, що може бути пов'язано з тимчасовими фінансовими труднощами або зміною умов розрахунків з контрагентами;

збільшення обсягів господарської діяльності, тобто якщо компанія активно розширює свою діяльність, це природно веде до зростання кредиторської заборгованості за товари та послуги, необхідні для забезпечення цього зростання.

Аналіз динамічних показників структури зобов'язань ПрАТ "Кіровоградобленерго" виявляє певні тривожні тенденції. Після незначного зростання на 1,36% у 2022 році, він суттєво скоротився на 10,13% у 2023 році, що свідчить про втрату капітальної стабільності і може бути наслідком збитків, виплати дивідендів, або інших факторів, що негативно впливають на власний капітал. Відбувається стрімке зростання поточних зобов'язань – на 34,50% у 2023 році, що може бути пов'язано з кількома причинами: збільшення короткострокового боргового навантаження та зростання обсягів закупівель:

Отже, динаміка показників структури зобов'язань свідчить про погіршення фінансової стійкості ПрАТ «Кіровоградобленерго». Зменшення власного капіталу та зростання поточних зобов'язань можуть негативно вплинути на платоспроможність та ліквідність компанії. Необхідно провести додатковий аналіз для виявлення причин таких змін та розробки заходів щодо стабілізації фінансового стану підприємства.

2.3. Аналіз впливу інформаційних загроз на фінансово-економічну діяльність

Сучасна фінансово-економічна діяльність підприємств усе більше залежить від інформаційних технологій, які забезпечують обробку, зберігання та передачу даних. Інформація стала стратегічним ресурсом, що визначає конкурентоспроможність компанії, її здатність адаптуватися до ринкових змін та ефективно управляти фінансовими ресурсами. Водночас розвиток цифрових технологій супроводжується зростанням загроз інформаційній безпеці, які можуть суттєво вплинути на фінансово-економічну діяльність підприємств [39, с. 11].

В сучасних умовах стрімкого розвитку інформаційних технологій та їх всебічного проникнення в усі сфери діяльності, питання інформаційної безпеки набуває особливої актуальності. Для підприємств, що оперують критично важливою інфраструктурою, таких як ПрАТ «Кіровоградобленерго», забезпечення надійного захисту інформації є невід'ємною складовою сталого функціонування та запорукою фінансово-економічної стабільності.

Інформаційні загрози, такі як кібератаки, витоки конфіденційних даних, технічні збої або дії зловмисників, здатні завдати значної шкоди підприємству. Вони можуть спричинити фінансові втрати, порушення ділових процесів, погіршення репутації та навіть призвести до юридичних наслідків. У зв’язку з цим аналіз впливу інформаційних загроз є важливим етапом управління фінансово-економічною безпекою підприємства [34, с. 113].

Для розуміння поточного стану системи захисту інформації, визначення її вразливостей і потенційних шляхів розвитку доцільно провести SWOT-аналіз. На рис. 2.5 відображено результати SWOT-аналізу інформаційної безпеки підприємства, який дозволяє оцінити сильні та слабкі сторони, а також можливості та загрози, що впливають на стан інформаційної безпеки.

Проведений SWOT-аналізу допомагає інтегрувати результати аналізу в розробку ефективної стратегії покращення інформаційної безпеки, мінімізації ризиків і зміцнення фінансово-економічної стабільності підприємства.

Сильні сторони демонструють переваги підприємства, зокрема наявність базових заходів захисту та усвідомлення важливості інформаційної безпеки. Слабкі сторони вказують на внутрішні недоліки, як-от застаріле обладнання чи недостатня кваліфікація персоналу. Можливості дають змогу визначити перспективні напрями вдосконалення системи захисту, наприклад, впровадження сучасних технологій або співпраця з державними органами. Загрози, такі як зростання кіберзагроз і геополітична нестабільність, визначають ризики, які можуть вплинути на безпеку інформаційних систем.

Сильні сторони (Strengths)

- Наявність базових заходів захисту (антивірусне ПЗ, файрволи, системи контролю доступу)
- Усвідомлення важливості інформаційної безпеки
- Державна підтримка у сфері захисту критичної інфраструктури

Слабкі сторони (Weaknesses)

- Застаріле обладнання та програмне забезпечення
- Недостатня кваліфікація персоналу з питань ІБ
- Обмежені ресурси для забезпечення ІБ

Можливості (Opportunities)

- Впровадження сучасних технологій захисту (хмарні технології, штучний інтелект)
- Співпраця з державними органами та іншими компаніями
- Підвищення обізнаності співробітників з питань ІБ

Загрози (Threats)

- Зростання кількості та складності кібератак
- Використання зловмисниками штучного інтелекту
- Геополітична нестабільність та зростання кібератак на критичну інфраструктуру

Рисунок 2.5 – SWOT-аналіз інформаційних загроз для ПрАТ «Кіровоградобленерго»

Джерело: узагальнено автором за матеріалами підприємства

Проведений SWOT-аналіз інформаційної безпеки підприємства дозволив виділити ключові аспекти, які впливають на стан захисту інформаційних систем і даних. Аналізуючи сильні сторони бачимо, що підприємство має базові механізми захисту, включаючи антивірусні програми, фаєрволи та системи контролю доступу. Усвідомлення важливості інформаційної безпеки керівництвом та співробітниками є додатковою перевагою, яка створює основу для вдосконалення. Державна підтримка в сфері захисту критичної інфраструктури також підсилює стійкість компанії до зовнішніх загроз.

Однак, основними викликами для підприємства є застарілі технічні засоби захисту, недостатня кваліфікація персоналу та обмежені фінансові ресурси для забезпечення сучасного рівня безпеки. Зазначені недоліки збільшують ризики інформаційних атак і ускладнюють оперативне реагування на інциденти.

Говорячи про можливості, можна справедливо стверджувати, що ПрАТ «Кіровоградобленерго» має перспективи впровадження новітніх технологій захисту, таких як хмарні обчислення, штучний інтелект та інші інновації. Співпраця з державними органами і приватними компаніями, а також навчання співробітників з питань інформаційної безпеки відкривають додаткові шляхи для покращення системи захисту.

Основними загрозами є зростання кількості та складності кіберзагроз, використання зловмисниками сучасних технологій, таких як штучний інтелект, а також геополітична нестабільність, яка може посилити ризики для критичної інфраструктури підприємства.

Отже, для підвищення рівня інформаційної безпеки підприємству слід зосередитися на усуненні слабких сторін, зокрема оновленні технічної бази, підвищенні кваліфікації персоналу та оптимізації фінансових ресурсів для впровадження сучасних заходів захисту. Водночас важливо використовувати доступні можливості для розробки довгострокової стратегії протидії загрозам та адаптації до змінного середовища кібербезпеки.

Кібератаки на енергетичні компанії, такі як ПрАТ «Кіровоградобленерго» можуть мати серйозні наслідки, оскільки це підприємство є частиною критичної інфраструктури. Кібератаки становлять серйозну загрозу для фінансового стану, репутації та операційної діяльності досліджуваного підприємства. Враховуючи ці ризики, підприємству необхідно приділити особливу увагу розвитку системи інформаційної безпеки, впровадженню сучасних технологій захисту, навчання персоналу та розробці планів реагування на інциденти, що дозволить мінімізувати негативні наслідки від кіберзагроз і забезпечити стабільність роботи компанії в довгостроковій перспективі.

Ураження інформаційних систем та компрометація даних можуть впливати на різні аспекти діяльності компанії (табл. 2.6).

Таблиця 2.6 – Ризики інформаційної безпеки для ПрАТ «Кіровоградобленерго»

Категорія наслідків	Вид наслідків	Сутнісна характеристика
Фінансові	Прямі фінансові втрати	Витрати на відновлення систем. Компенсації клієнтам. Штрафи за порушення норм безпеки.
	Втрати доходів	Зниження обсягів реалізації електроенергії.
	Зниження інвестиційної привабливості	Ускладнення залучення капіталу.
Репутаційні	Втрата довіри клієнтів	Відтік клієнтів. Негативні відгуки у медіа.
	Негативний імідж у медіа	Погіршення репутації. Ускладнення залучення нових клієнтів та партнерів.
	Втрата довіри регуляторних органів	Жорсткі перевірки та штрафи.
Операційні	Перебої у постачанні електроенергії	Збої в роботі енергомереж. Незадоволення клієнтів.
	Зниження ефективності операцій	Збій у роботі облікових систем та баз даних.
	Втрата критичних даних	Втрата конфіденційної інформації. Ускладнення планування.
	Витрати часу на відновлення	Зниження продуктивності.
Додаткові	Юридичні наслідки	Судові позови та штрафи.
	Зростання вартості страхування	Підвищення страхових премій.
	Загроза національній безпеці	Масштабні перебої в енергопостачанні.

Джерело: узагальнено автором за матеріалами підприємства

Аналіз даних табл. 2.6 дозволяє зробити висновок про те, що інформаційні загрози можуть мати серйозні та багатогранні наслідки для ПрАТ «Кіровоградобленерго», впливаючи на всі аспекти діяльності компанії. Основні ризики включають:

фінансові втрати такі, як прямі витрати на усунення наслідків кібератак, втрата доходів через перебої в енергопостачанні, зниження інвестиційної привабливості;

репутаційні втрати, а саме втрата довіри клієнтів та партнерів, негативний імідж у медіа, втрата довіри з боку регуляторних органів;

порушення операційної діяльності у зв’язку з перебоями в енергопостачанні, зниження ефективності операцій, втрата критичних даних;

додаткові ризики такі, як юридичні наслідки, зростання вартості страхування, загроза національній безпеці тощо.

Маємо розуміння, що для мінімізації цих ризиків ПрАТ «Кіровоградобленерго» необхідно вживати комплексних заходів щодо забезпечення інформаційної безпеки, включаючи: впровадження сучасних систем захисту інформації; підвищення кваліфікації персоналу з питань кібербезпеки; розробку планів реагування на кіберінциденти; співпрацю з державними органами та іншими компаніями у сфері кібербезпеки та ін.

Враховуючи критичну важливість енергетичної інфраструктури для економіки та суспільства, забезпечення інформаційної безпеки ПрАТ «Кіровоградобленерго» є пріоритетним завданням, що вимагає постійної уваги та інвестицій.

ПрАТ «Кіровоградобленерго» впроваджує комплексний підхід до забезпечення інформаційної безпеки, який базується на використанні сучасних технологій та організаційних заходів. Одним із ключових елементів захисту є антивірусне програмне забезпечення, яке забезпечує виявлення та блокування шкідливих програм. Компанія регулярно оновлює антивірусні бази для своєчасного виявлення нових загроз.

Для забезпечення мережевої безпеки підприємство використовує фаєрволи, які обмежують несанкціонований доступ до внутрішніх систем. Налаштування правил доступу до мережевих ресурсів дозволяє знизити ризики зовнішніх атак. Додатково впроваджено системи контролю доступу (Access Control), які забезпечують обмеження доступу до інформаційних ресурсів лише для уповноважених співробітників. Для критично важливих систем використовується двофакторна автентифікація.

З метою запобігання втратам даних ПрАТ «Кіровоградобленерго» здійснює регулярне резервне копіювання інформації. Резервні копії зберігаються у захищених місцях, що дозволяє відновити дані у разі інцидентів. Додатково для захисту конфіденційних даних компанія застосовує шифрування, яке гарантує безпечну передачу інформації через мережу.

Постійний моніторинг інформаційних систем здійснюється за допомогою сучасних платформ, таких як SIEM (Security Information and Event Management). Це дозволяє виявляти підозрілу активність у режимі реального часу та оперативно реагувати на інциденти. Особлива увага приділяється підвищенню обізнаності співробітників щодо кіберзагроз. Компанія проводить регулярні навчання та тренінги, спрямовані на підвищення рівня кібергігієни.

Хоча ПрАТ «Кіровоградобленерго» застосовує базові методи кібербезпеки, для протидії сучасним загрозам потрібна модернізація, що передбачає впровадження сучасних технологій, посилення контролю доступу, регулярне тестування безпеки та інтеграцію стандарту ISO/IEC 27001.Зазначені рекомендації дозволять підприємству підвищити стабільність та ефективність, зміцнити ризики та забезпечити довгострокову фінансово-економічну стабільність в умовах цифрової трансформації.

Вдосконалення кіберзахисту дозволить компанії «Кіровоградобленерго» не лише знизити ризики, але й підвищити стабільність та ефективність діяльності, зміцнити свої позиції на ринку та забезпечити довгострокову фінансово-економічну стабільність в умовах цифрової трансформації.

РОЗДІЛ 3

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ КОМПОНЕНТИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПРАТ «КІРОВОГРАДОБЛЕНЕРГО»

3.1. Удосконалення системи моніторингу та управління інформаційною безпекою підприємства «Кіровоградобленерго»

Інформаційна безпека є важливою складовою ефективного функціонування будь-якого підприємства, особливо якщо воно належить до критичної інфраструктури, як ПрАТ «Кіровоградобленерго». Сучасні кіберзагрози постійно змінюються, стаючи дедалі складнішими та небезпечнішими. У цих умовах підприємства повинні забезпечувати не лише базові заходи захисту, а й створювати адаптивні системи моніторингу та управління інформаційною безпекою, які здатні оперативно виявляти загрози, реагувати на них і мінімізувати можливі наслідки.

Система моніторингу інформаційної безпеки виконує роль першої лінії захисту, забезпечуючи постійний контроль за станом інформаційних систем, аналізуючи активність у мережі та виявляючи аномалії, які можуть бути ознаками кібератак або внутрішніх порушень. Водночас система управління інформаційною безпекою дозволяє створювати стратегії, політики та процедури, які забезпечують інтегрований підхід до захисту інформаційних ресурсів і сприяють підвищенню рівня кіберстійкості [20].

Керівництво підприємства розуміє, що потрібно вдосконалювати системи моніторингу та управління інформаційною безпекою ПрАТ «Кіровоградобленерго». На наш погляд, особлива увага має бути приділена впровадженню новітніх технологій, таких як платформи SOAR, штучний інтелект (AI), автоматизовані системи виявлення та реагування на загрози, а також інтеграції міжнародних стандартів безпеки. Удосконалення системи моніторингу та управління інформаційною безпекою є стратегічно важливим напрямом, що дозволить ПрАТ «Кіровоградобленерго» зміцнити свою конкурентоспроможність і гарантувати безпеку критичних інформаційних ресурсів у динамічному цифровому середовищі.

У період військових дій підприємства критичної інфраструктури, зокрема ПрАТ «Кіровоградобленерго», стикаються з посиленими ризиками в галузі інформаційної безпеки. Атаки на інформаційні системи енергетичних компаній стають стратегічною метою для агресорів, оскільки їхній успіх може призвести до масштабних збоїв у функціонуванні енергосистем, що напряму впливає на життєздатність економіки та соціальної інфраструктури регіону (табл. 3.1).

Таблиця 3.1 – Проблеми управління інформаційною безпекою в умовах війни та шляхи їх подолання

Проблема	**Опис**	**Шляхи подолання**
Посилення кібератак	Збільшення кількості та складності кібератак, спрямованих на енергетичну інфраструктуру.	▪ Впровадження рішень на основі штучного інтелекту для виявлення аномалій. ▪ Використання резервних серверів та хмарних технологій. ▪ Оновлення політик управління доступом.
Обмежені ресурси	Дефіцит фінансових, технічних та людських ресурсів для забезпечення кібербезпеки.	▪ Оптимізація використання наявних ресурсів. ▪ Пошук додаткових джерел фінансування. ▪ Співпраця з державними органами та іншими компаніями.
Ризики фізичного знищення	Загрози фізичного пошкодження центрів обробки даних та вузлів управління.	▪ Створення дублюючих центрів обробки даних у безпечних регіонах. ▪ Забезпечення фізичної охорони об'єктів.
Ненадійність каналів зв'язку	Перебої у роботі Інтернету та електропостачання.	▪ Використання резервних каналів зв'язку. ▪ Забезпечення автономної роботи критичних систем.
Недостатня готовність персоналу	Нестача фахівців з кібербезпеки та ризики помилок через психологічний тиск.	▪ Проведення навчань для співробітників. ▪ Підвищення кваліфікації персоналу.
Інсайдерські загрози	Збільшення ризику інсайдерських атак.	▪ Посилення контролю доступу до критичних систем. ▪ Використання інструментів для аналізу поведінки користувачів.

Джерело: запропоновано автором

Таблиця 3.1 ілюструє основні проблеми управління інформаційною безпекою, з якими стикаються енергетичні підприємства, такі як ПрАТ «Кіровоградобленерго», в умовах війни. Водночас вона демонструє можливі шляхи подолання цих викликів, що є важливим для забезпечення стабільності діяльності критичної інфраструктури.

Воєнні дії значно підвищують рівень кіберзагроз, роблячи енергетичну інфраструктуру однією з ключових цілей для ворожих атак. Зростання кількості та складності таких атак вимагає від підприємства постійного вдосконалення систем захисту, впровадження сучасних технологій моніторингу, а також використання автоматизованих інструментів виявлення та реагування на кіберінциденти. Воєнний стан створює значні перешкоди у доступі до фінансових, технічних і людських ресурсів, необхідних для підтримки належного рівня кібербезпеки, що змушує підприємство шукати ефективні рішення, що дозволяють оптимізувати використання наявних ресурсів. Крім того, актуальною є співпраця з державними органами та іншими організаціями для залучення додаткової технічної та інформаційної підтримки.

Фізична інфраструктура енергетичних компаній стає особливо вразливою в умовах військових дій. Атаки на центри обробки даних, вузли управління та інші елементи інфраструктури можуть спричинити значні збої у роботі. Для зменшення цих ризиків важливо впроваджувати заходи фізичного захисту, а також створювати резервні копії систем управління у безпечних регіонах.

Пошкодження інфраструктури зв’язку через військові дії ускладнює обмін інформацією між підрозділами підприємства та знижує ефективність управління критичними системами. Для вирішення цієї проблеми необхідно забезпечити наявність резервних каналів зв’язку, що здатні функціонувати автономно в умовах пошкодження основних комунікацій.

Рівень підготовки персоналу до роботи в умовах підвищених кіберзагроз є ще однією важливою проблемою. Постійне навчання співробітників щодо сучасних методів кіберзахисту, реагування на інциденти та забезпечення інформаційної безпеки є критично важливим для мінімізації людського фактора у виникненні загроз.

Ризик внутрішніх загроз зростає у період війни, коли недобросовісні співробітники або агенти ворога можуть використовувати свій доступ до критичних систем для завдання шкоди. Це вимагає посилення контролю за діями співробітників, впровадження принципу найменших привілеїв у доступі до інформаційних систем, а також використання інструментів моніторингу поведінки користувачів.

Загалом, подолання цих проблем потребує інтегрованого підходу, який включатиме як технічні заходи, так і організаційні стратегії. Енергетичним підприємствам слід зосередитися на посиленні своєї кібербезпеки та підвищенні стійкості до сучасних викликів, пов’язаних із військовими діями.

В умовах зростання кількості кіберзагроз, що спрямовані на підприємства критичної інфраструктури, ПрАТ «Кіровоградобленерго» має впровадити інтегровану систему управління інформаційною безпекою. Така система повинна забезпечити централізоване управління заходами захисту, автоматизацію процесів реагування на інциденти та підвищення загальної стійкості підприємства до загроз (рис. 3.1)

Рисунок 3.1 – Модель інтегрованої системи управління інформаційною безпекою ПрАТ «Кіровоградобленерго»

Джерело: запропоновано автором

На рис. 3.1, запропоновано авторське бачення моделі інтегрованої системи управління інформаційною безпекою ПрАТ «Кіровоградобленерго». Схема відображає архітектуру інтегрованої системи управління інформаційною безпекою, яка спрямована на забезпечення комплексного захисту інформаційних ресурсів підприємства. Основний вузол системи — інтегрована система управління інформаційною безпекою, яка координує роботу всіх підсистем. Ключові компоненти цієї системи:

1. Платформа SOAR, що забезпечує автоматизацію реагування на інциденти інформаційної безпеки, інтегруючи дані з усіх підсистем. Вона знижує час на реагування, оптимізує процеси управління загрозами та забезпечує аналіз кіберінцидентів.

2. Антивірусні системи, що відповідають за захист кінцевих пристроїв від шкідливого програмного забезпечення. Антивірусні системи інтегровані в загальну інфраструктуру, що дозволяє централізовано контролювати безпеку на всіх пристроях.

3. Фаєрволи, які забезпечують контроль мережевого трафіку, запобігаючи несанкціонованому доступу до внутрішніх інформаційних систем. Фаєрволи створюють перший рубіж захисту для корпоративної мережі.

4. Системи контролю доступу впроваджують принцип найменших привілеїв, забезпечуючи доступ до інформаційних ресурсів лише для авторизованих користувачів, а також включають багатофакторну автентифікацію для підвищення рівня захищеності.

5. Політики інформаційної безпеки регламентують порядок дій у разі інцидентів, встановлюють правила доступу до інформації та її використання. Політики є базовим елементом для забезпечення відповідності системи міжнародним стандартам кібербезпеки.

6. Модулі моніторингу виявляють та аналізують загрози в режимі реального часу, а також дозволяють оперативно реагувати на підозрілу активність і запобігати розвитку потенційних інцидентів.

На наше переконання основне значення схеми полягає у забезпеченні злагодженої роботи всіх компонентів з метою створення надійної та ефективної системи інформаційної безпеки, що в свою чергу, дозволить підприємству зменшити ризики кібератак, оптимізувати процеси управління безпекою та забезпечити стабільність у функціонуванні критичної інфраструктури.

3.2. Запровадження інноваційних рішень для мінімізації інформаційних ризиків на підприємстві «Кіровоградобленерго»

В умовах актуальної економічної та технологічної парадигми, що характеризується динамічним розвитком цифрових технологій та зростанням кіберзагроз, забезпечення інформаційної безпеки набуває стратегічного значення, особливо для підприємств критичної інфраструктури, таких як ПрАТ «Кіровоградобленерго».

Традиційні методи захисту інформації, що базуються на використанні антивірусного програмного забезпечення, файрволів та систем контролю доступу, втрачають свою ефективність перед обличчям сучасних кіберзагроз, які відрізняються високою складністю, масштабністю та адаптивністю.

Інформаційні ризики на підприємстві можуть виникати через зростання кількості атак на інформаційні системи, вразливості програмного забезпечення, людський фактор, технічні збої та інші чинники. Наслідки цих ризиків можуть бути критичними: від фінансових втрат і порушення операційної діяльності до зниження довіри клієнтів і репутаційних втрат. У цьому контексті ключовим завданням стає інтеграція новітніх технологій і підходів, які дозволяють мінімізувати вплив цих загроз [13, с. 15-18].

Впровадження інноваційних рішень у сфері інформаційної безпеки є стратегічно важливим кроком для ПрАТ «Кіровоградобленерго», яке належить до критичної інфраструктури та піддається підвищеним інформаційним ризикам. В контексті вищенаведеного доцільно проаналізувати переваги таких рішень, розглянути успішні приклади у світовій практиці та розробити рекомендації, які відповідають специфіці діяльності підприємства (табл. 3.2).

Таблиця 3.2 – Переваги впровадження інноваційних рішень в сфері інформаційної безпеки

ПЕРЕВАГА	ДЕТАЛІЗАЦІЯ	ПРАКТИЧНІ КРОКИ
Зниження ризиків	▪ Використання AI/ML для прогнозування нових загроз та аналізу аномалій.	▪ Впровадити системи SIEM (*Security Information and Event Management*) з функціями AI/ML для аналізу подій безпеки та виявлення аномалій. ▪ Використовувати проактивні інструменти захисту, такі як Threat Intelligence платформи, для отримання інформації про нові загрози та вразливості.
Підвищення ефективності управління	▪ Автоматизація реагування на кіберінциденти за допомогою SOAR. ▪ Зменшення впливу людського фактора.	▪ Впровадити платформи *SOAR (Security Orchestration, Automation and Response)* для автоматизації процесів реагування на інциденти та управління безпекою. ▪ Розробити чіткі процедури та інструкції для персоналу щодо дій у разі виникнення кіберінцидентів.
Відповідність стандартам	▪ Впровадження рішень, що відповідають ISO/IEC 27001. ▪ Підвищення довіри клієнтів, партнерів та регуляторів. ▪ Зменшення юридичних ризиків.	▪ Провести аудит інформаційної безпеки на відповідність стандарту *ISO/IEC 27001*. ▪ Розробити та впровадити систему управління інформаційною безпекою (СУІБ) відповідно до вимог стандарту. ▪ Отримати сертифікат відповідності *ISO/IEC 27001*.
Оптимізація витрат	▪ Зниження кількості інцидентів та втрат від простоїв. ▪ Ефективне використання ресурсів.	▪ Провести аналіз ефективності інвестицій в інформаційну безпеку (ROI). ▪ Впровадити системи моніторингу та аналізу ефективності заходів безпеки. ▪ Оптимізувати використання ліцензій на програмне забезпечення та обладнання.
Підвищення довіри	▪ Формування позитивного іміджу підприємства.	▪ Проводити інформаційні кампанії для клієнтів та партнерів про заходи, що вживаються для забезпечення інформаційної безпеки. ▪ Публікувати звіти про стан інформаційної безпеки та заходи щодо її підвищення. ▪ Брати участь у галузевих ініціативах з кібербезпеки.

Джерело: запропоновано автором

Аналіз табл. 3.2 дозволяє зробити висновок про те, що інновації відіграють ключову роль у забезпеченні надійного захисту інформаційних ресурсів ПрАТ «Кіровоградобленерго». Впровадження сучасних технологій, таких як штучний інтелект, машинне навчання та платформи SOAR, дозволить компанії знизити ризики кібератак, підвищити ефективність управління безпекою, забезпечити відповідність стандартам, оптимізувати витрати та сформувати позитивний імідж надійної компанії тощо.

Впровадження інновацій в сфері інформаційної безпеки є стратегічно важливим кроком для компанії «Кіровоградобленерго», який допоможе компанії забезпечити стабільну роботу, захистити інтереси клієнтів та партнерів, а також зміцнити свої позиції на ринку в умовах цифрової трансформації.

Сфера енергетики є критично важливою для функціонування сучасного суспільства, тому компанії, що працюють у цьому секторі, постійно стикаються з високим рівнем інформаційних ризиків. Успішне впровадження інноваційних рішень у галузі інформаційної безпеки дозволяє енергетичним компаніям не лише протидіяти сучасним загрозам, але й оптимізувати роботу інформаційних систем.

Розглянемо практичні приклади впровадження інноваційних рішень в сфері інформаційної безпеки провідними світовими енергетичними компаніями, щоб вивчити їх досвід та найкращі практики.

Сучасні енергетичні компанії, як частина критичної інфраструктури, стикаються з постійними кіберзагрозами. Впровадження інноваційних рішень стає ключовим елементом для забезпечення інформаційної безпеки та стійкості до викликів. Одним із найбільш ефективних підходів є використання платформ SOAR для автоматизації управління безпекою. Так, компанія Duke Energy у США інтегрувала SOAR у свої процеси кіберзахисту, що дозволило автоматизувати реагування на інциденти, об’єднавши всі системи захисту в єдину екосистему. Результатом стало зменшення часу на ліквідацію загроз на 60%, що мінімізувало вплив кіберінцидентів на операційну діяльність.

Інноваційні технології штучного інтелекту (AI) також демонструють високий потенціал у галузі кібербезпеки. EDF Group у Франції впровадила AI-рішення для аналізу великих обсягів даних у реальному часі. Алгоритми дозволяють ідентифікувати загрози на ранніх етапах, що значно підвищило ефективність управління ризиками та забезпечило стабільність роботи енергомережі навіть під час інтенсивних кіберзагроз.

Ще одним важливим нововведенням є блокчейн-технології. Японська компанія TEPCO інтегрувала блокчейн для забезпечення цілісності даних про енергоспоживання. Ця технологія не лише унеможливила несанкціоноване змінення даних, але й підвищила прозорість взаємодії між учасниками енергетичного ринку. Крім того, блокчейн оптимізував процес обліку електроенергії, скоротивши кількість помилок на 40%.

Хмарні рішення набувають дедалі більшої популярності у сфері резервного зберігання даних. Італійська компанія Enel Group активно використовує хмарні сервіси для забезпечення безпеки даних. Хмарні технології інтегровані із системами моніторингу, що дозволяє оперативно реагувати на інциденти та забезпечувати доступність інформації навіть за умови фізичних або кіберзагроз.

Для захисту операційних систем, таких як SCADA, компанія National Grid у Великій Британії впровадила спеціалізовані системи моніторингу. Відповідні рішення дозволяють виявляти аномалії у роботі мереж і миттєво ізолювати уражені сегменти, що мінімізує ризики порушення функціонування енергомережі.

Крім технічних рішень, важливим напрямом є навчання персоналу. Siemens Energy розробила симуляційну платформу для тренування співробітників у реальних умовах кіберзагроз. Такий підхід зменшив кількість інцидентів, пов’язаних із людським фактором, на 30%, підвищивши загальну обізнаність працівників.

Таким чином, впровадження інноваційних рішень дозволяє енергетичним компаніям значно підвищити рівень інформаційної безпеки, оптимізувати витрати та забезпечити стійкість до сучасних викликів. Досвід провідних компаній демонструє, що такі рішення можуть бути ефективно адаптовані до специфіки діяльності ПрАТ «Кіровоградобленерго» для зміцнення його конкурентних позицій та підвищення ефективності управління ризиками.

У сучасному середовищі зростання кіберзагроз потребує комплексного управління інформаційною безпекою, що охоплює всі ключові аспекти діяльності підприємства. Запропонована схема на рис. 3.2, відображає структурований підхід до розробки та впровадження стратегій кіберзахисту, побудованих на основі міжнародних стандартів, зокрема ISO/IEC 27001 (рис. 3.2).

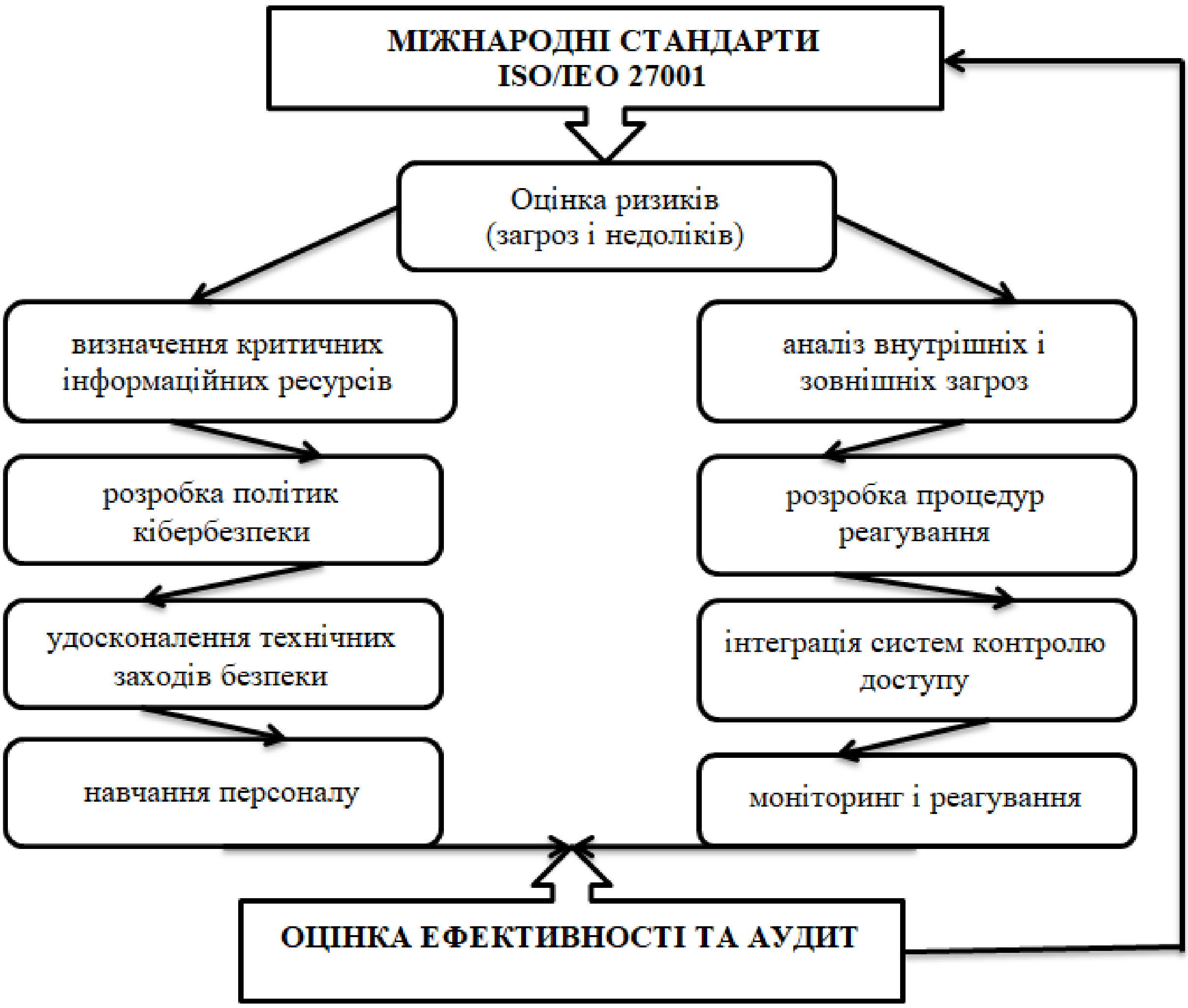

Рисунок 3.2 – Ускладнена схема розробки стратегій кіберзахисту на основі міжнародних стандартів для ПрАТ «Кіровоградобленерго»

Джерело: запропоновано автором

На початковому етапі передбачено застосування міжнародних стандартів як основи для формування системи кіберзахисту, що забезпечує єдиний підхід до оцінки ризиків, розробки політик і процедур, а також впровадження технічних рішень. Особлива увага приділяється аналізу загроз і вразливостей, що дозволяє визначити критичні інформаційні ресурси та зосередити зусилля на їх захисті.

Система включає розробку політик кібербезпеки та процедур реагування, які слугують основою для впровадження технічних заходів, таких як системи контролю доступу та інтеграція сучасних технологій. Навчання персоналу відіграє ключову роль у підвищенні обізнаності співробітників про ризики та способи їх мінімізації. Завершальним етапом є моніторинг і реагування на інциденти, а також регулярна оцінка ефективності та аудит, що дозволяє вдосконалювати існуючу систему.

Схема демонструє взаємозв'язок між ключовими елементами процесу кіберзахисту, забезпечуючи комплексний підхід до управління інформаційною безпекою ПрАТ «Кіровоградобленерго». Такий підхід сприяє мінімізації ризиків, підвищенню рівня захищеності підприємства та забезпеченню його стабільної роботи в умовах сучасних кіберзагроз.

На наше переконання, запровадження стратегій кіберзахисту на основі міжнародних стандартів, таких як ISO/IEC 27001, дозволить ПрАТ «Кіровоградобленерго» суттєво підвищити рівень інформаційної безпеки. Інтеграція таких стандартів сприятиме створенню ефективної системи управління, що забезпечить захист критичних інформаційних ресурсів від зовнішніх і внутрішніх загроз, враховуючи особливості функціонування підприємства.

Однією з головних переваг є систематизація підходів до управління ризиками. Проведення оцінки загроз і недоліків дозволить підприємству ідентифікувати найбільш критичні аспекти інформаційної безпеки, сконцентрувавши зусилля на їхньому усуненні, що мінімізує ймовірність виникнення кіберінцидентів та дозволить зменшити їхній вплив на операційну діяльність.

Запровадження інноваційних рішень, таких як платформи SOAR, забезпечить автоматизацію процесів моніторингу, аналізу та реагування на загрози, що дозволить значно скоротити час реагування на кіберінциденти, мінімізуючи вплив людського фактора та підвищуючи ефективність управління інформаційною безпекою.

Дотримання міжнародних стандартів сприятиме відповідності чинному законодавству у сфері кібербезпеки. Це не лише дозволить уникнути юридичних ризиків та можливих санкцій, але й підвищить рівень довіри з боку клієнтів, партнерів та регуляторів. Високий рівень захисту даних гарантує безпеку комерційної інформації, що є важливим фактором конкурентоспроможності підприємства. Важливою перевагою стане підвищення обізнаності персоналу. Навчання працівників основам кібергігієни та сучасним підходам до реагування на загрози сприятиме зменшенню ризиків, пов’язаних із людським фактором. Перелічене дозволить створити культуру інформаційної безпеки на підприємстві, яка стане фундаментом для довгострокового розвитку.

Запровадження стратегій кіберзахисту також дозволить оптимізувати фінансові ресурси. Незважаючи на початкові інвестиції, довгострокові вигоди включають скорочення витрат на ліквідацію наслідків інцидентів, а також економію часу і ресурсів, необхідних для забезпечення безпеки.

Систематичний підхід до моніторингу та аудиту забезпечить постійне вдосконалення системи кіберзахисту. Регулярна оцінка ефективності дозволить виявляти слабкі місця та впроваджувати необхідні зміни, що забезпечить гнучкість системи безпеки у відповідь на динамічні зміни загроз.

Таким чином, запровадження стратегій кіберзахисту на основі міжнародних стандартів для ПрАТ «Кіровоградобленерго» сприятиме зміцненню інформаційної безпеки, оптимізації операційних процесів і забезпеченню стійкості підприємства до сучасних викликів.

ВИСНОВКИ

У кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти було проведено дослідження теоретичних, аналітичних та практичних аспектів забезпечення фінансово-економічної безпеки підприємства, зосереджуючи увагу на інформаційній компоненті як ключовому елементі ефективного управління ризиками. На прикладі ПрАТ «Кіровоградобленерго» розглянуто сучасний стан інформаційної безпеки, оцінено її вплив на фінансово-економічну діяльність підприємства, а також розроблено рекомендації щодо підвищення її ефективності.

На основі проведеного аналізу теоретичних засад фінансово-економічної та інформаційної безпеки можна зробити висновок, що ефективне управління цими складовими є основою стабільності підприємства. Інтеграція інформаційної безпеки у загальну систему фінансово-економічної безпеки дозволяє підвищити її ефективність, забезпечити стійкість до сучасних загроз і створити умови для сталого розвитку підприємства.

У межах розділу було здійснено теоретичний аналіз основних аспектів фінансово-економічної безпеки підприємства з акцентом на інформаційну компоненту як ключовий елемент забезпечення стабільності діяльності. Дослідження підтвердило, що фінансово-економічна безпека є комплексною категорією, яка охоплює управління фінансовими ресурсами, мінімізацію ризиків та підтримку конкурентоспроможності в умовах динамічного середовища.

Інформаційна компонента є невіддільною частиною загальної системи безпеки, оскільки захист інформаційних ресурсів, управління інформаційними потоками та протидія кіберзагрозам набувають вирішального значення в сучасних умовах цифровізації. Належне забезпечення інформаційної безпеки створює передумови для сталого функціонування підприємства, захисту конфіденційної інформації та оперативного реагування на зовнішні й внутрішні загрози.

Також було визначено, що нормативно-правова база є основою для формування системи управління інформаційною безпекою. Дотримання міжнародних стандартів, національних законодавчих актів і внутрішніх політик дозволяє підприємству ефективно захищати свої інформаційні ресурси, підтримувати довіру партнерів і клієнтів, а також мінімізувати юридичні ризики.

У другому розділі проведено аналіз стану інформаційної безпеки в контексті забезпечення фінансово-економічної стабільності ПрАТ «Кіровоградобленерго». Дослідження охопило характеристику господарської діяльності підприємства, оцінку поточного стану його фінансово-економічної безпеки та аналіз впливу інформаційних загроз на ключові аспекти діяльності.

Аналіз господарської діяльності ПрАТ «Кіровоградобленерго» показав, що підприємство є важливим елементом енергетичної інфраструктури регіону, яке забезпечує стабільне постачання електроенергії споживачам. Разом із цим було виявлено, що складна структура діяльності вимагає належної уваги до управління ризиками, особливо в умовах підвищеної загрози кібератак.

Оцінка стану фінансово-економічної безпеки підприємства показала, що, незважаючи на задовільні фінансові показники, існують ризики, пов’язані із зростанням зовнішніх і внутрішніх загроз. Основними викликами є підвищена вразливість інформаційних систем, що може негативно вплинути на фінансову стабільність у разі реалізації загроз.

Аналіз впливу інформаційних загроз виявив, що вони є одним із найбільших ризиків для діяльності підприємства. Кібератаки, витік конфіденційної інформації, порушення роботи операційних систем можуть призводити до фінансових втрат, погіршення репутації компанії та зниження довіри з боку клієнтів і партнерів. Зазначені ризики потребують впровадження сучасних підходів до управління інформаційною безпекою.

У третьому розділі було розроблено рекомендації, спрямовані на підвищення ефективності управління інформаційною компонентою фінансово-економічної безпеки ПрАТ «Кіровоградобленерго». Основна увага приділялася удосконаленню системи моніторингу та управління інформаційною безпекою, а також запровадженню інноваційних рішень для мінімізації інформаційних ризиків.

Запропоновано заходи щодо вдосконалення системи моніторингу та управління інформаційною безпекою. Рекомендації включають впровадження централізованих платформ, таких як SOAR (Security Orchestration, Automation, and Response), що дозволяють автоматизувати процеси виявлення та реагування на загрози. Розробка політик кібербезпеки та інтеграція систем контролю доступу сприятимуть підвищенню ефективності управління ризиками. Запропоновані заходи також включають навчання персоналу, яке спрямоване на підвищення обізнаності співробітників про сучасні загрози та правила кібергігієни.

Обґрунтовано необхідність запровадження інноваційних рішень для мінімізації інформаційних ризиків. Зокрема, впровадження технологій штучного інтелекту (AI) та машинного навчання (ML) дозволить оперативно виявляти аномалії у роботі інформаційних систем і прогнозувати потенційні загрози. Використання блокчейн-технологій забезпечить цілісність і безпеку даних, а хмарні технології допоможуть оптимізувати зберігання та резервування критичної інформації. Запропоновані інновації сприятимуть як підвищенню кіберстійкості, так і оптимізації витрат на забезпечення інформаційної безпеки.

Загалом, реалізація запропонованих рекомендацій дозволить ПрАТ «Кіровоградобленерго» підвищити ефективність управління інформаційною безпекою, зменшити ризики втрати даних і забезпечити стійкість до сучасних кіберзагроз. Інтеграція новітніх технологій, оптимізація політик безпеки та підвищення обізнаності персоналу створять міцну основу для довгострокового розвитку підприємства та його стабільної роботи в умовах динамічних викликів інформаційного середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрійовський В. Підходи до управління інноваційними ризиками підприємств // Вісник ТНЕУ. 2021. № 3. С. 45–52.

2. Архипов О., Архипова Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». Інформаційні технології та безпека: основи забезпечення інформаційної безпеки (ІТБ-2014): Матеріали XIV міжнародної науково-практичної конференції. Київ : ІПРІ НАН України, 2014. С. 18–30. URL: https://ktpu.kpi.ua/ wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf.

3. Бабіна Н. О. Економіко-фінансова безпека підприємств України як елемент національної безпеки. Київ: КНУТД, 2018. 220 с.

4. Бабічев А. В., Самородов Б. В. Концептуальна модель оцінки й аналізу інформаційної компоненти економічної безпеки підприємства // Проблеми економіки. 2023. № 3 (57). С. 157–167.

5. Василенко Л. П., Гут Л. В. Фінансово-економічна безпека підприємства. Чернівці: ЧТЕІ КНТЕУ, 2005. 239 с.

6. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення. Львів: Ліга-Прес, 2012. 388 с.

7. Гладкий В. М. Основи фінансової безпеки підприємства: теоретико-методичний аспект. Київ: Центр учбової літератури, 2020. 234 с.

8. Гнатенко В. Інформаційно-економічна безпека як фактор стабільного розвитку держави. Публічне урядування. 2020. № 5 (25). С. 63–74. DOI: https://doi.org/10.32689/2617-2224-2020-5(25)-63-74

9. Гнатюк Л. М. Інноваційні інструменти ризик-менеджменту для забезпечення стійкості підприємств // Фінансово-кредитна діяльність: проблеми теорії та практики. 2022. № 2 (43). С. 133–135.

10. Гончарук О. В. Системний підхід до забезпечення фінансово-економічної безпеки підприємств // Вісник економічної науки України. 2021. № 1 (40). С. 89–95.

11. Гончарук О. В. Фінансово-економічна безпека підприємства: завдання управління та інноваційні підходи. Одеса: ОНУ, 2020. 180 с.

12. Губарик Н. П., Мотковський В. В. Актуальні проблеми сучасного бізнесу: обліково-фінансовий та управлінський аспекти. Дніпро: ДДАЕУ, 2019. 200 с.

13. Дячков Д. В. Управлінські аспекти інформаційної безпеки: теорія, методологія, практика: монографія. Запоріжжя: Вид-во «Інтр-М», 2019. 424 с.

14. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. С. 650.

15. Захаров О. І. Інформаційне забезпечення управління системою економічної безпеки підприємства // Бізнес Інформ. 2020. № 3. С. 45–50.

16. Іващенко О.В., Гельман В.М. Фінансово-економічна безпека держави / О. В. Іващенко, В. М. Гельман // Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки) . 2013. № 2(1). С. 121–131. URL:http://nbuv.gov.ua/j-pdf/znptdau_2013_2(1)__16.pdf.

17. Києво-Могилянська бізнес-школа. Інноваційне підприємництво: управління ризиками в бізнесі. URL: https://kmbs.ua/ua/article/innovacijne-pidpriyemnictvo-upravlinnya-rizikami-v-biznesi

18. Кіровоградобленерго. Офіційний вебсайт ПрАТ «Кіровоградобленерго» URL: https://kiroe.com.ua

19. Крючко Л. С. Теоретичні засади фінансової безпеки підприємства // Інвестиції: практика та досвід. 2013. № 15. С. 49–52.

20. Лаптєв В. В., Коваленко І. П. Інформаційна складова економічної безпеки підприємства в умовах глобалізації // Сталий розвиток економіки. 2020. № 3. С. 122–128.

21. Міжнародна організація праці. Рекомендації щодо захисту інформації в сучасних умовах. Женева: ILO, 2020. URL: https://www.ilo.org/information_security

22. Міжнародна організація праці. Рекомендації щодо захисту інформації в сучасних умовах. Женева: ILO, 2020. URL: https://www.ilo.org/information_security

23. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент. 2017. Вип. 24(2). С. 137–140. URL: http://nbuv.gov.ua/UJRN/Nvmgu_eim_2017_24%282%29__30.

24. Панченко О. В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти: монографія. Тернопіль: ТНЕУ, 2020. 312 с.

25. Петренко І. В. Фінансово-економічна безпека в системі управління підприємством. Дніпро: ДДАЕУ, 2017. 160 с.

26. Пономарьов В. П., Лях О. І. Інформаційна безпека підприємства в умовах цифровізації економіки // Економіка та управління. 2022. № 4. С. 45–53.

27. Постанова Кабінету Міністрів України «Про затвердження Порядку забезпечення кібербезпеки об'єктів критичної інфраструктури» від 17.01.2018 № 45. Офіційний вісник України. 2018. № 8. С. 100.

28. «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» Закон України від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

29. Пузирьова П. В. Інформаційна безпека та методи захисту інформації: навчальний посібник. Дніпро: ДДАЕУ, 2018. 150 с.

30. Пузирьова П. В. Сучасні аспекти управління ризиками в інноваційній діяльності // Матеріали міжнародної науково-практичної конференції. Київ: КНУТД, 2020. С. 127–128.

31. Ризики в інноваційній діяльності та управління ними. URL: https://pidru4niki.com/85874/ekonomika/riziki_innovatsiyniy_diyalnosti_upravlinnya_nimi

32. Родіонова І. В. Оцінка та управління ризиками впровадження інформаційних технологій на підприємствах: монографія. Суми: СумДУ, 2017. 198 с.

33. Фінансово-економічна безпека підприємств та інформаційні технології забезпечення безпеки: монографія / за ред. О. В. Губарика, В. В. Мотковського. Одеса: ОНЕУ, 2021. 280 с.

34. Христенко Л. М. Особливості управління інноваційними ризиками на вітчизняних підприємствах // Вісник Полтавської державної аграрної академії. 2019. № 4. С. 112–118.

35. Черниш І. В., Маховка В. В., Лобач Л. В. Управління інформаційною безпекою підприємства в умовах динамічного бізнес-середовища // Економіка і регіон. 2020. № 1 (76). С. 56–63.

36. Чубаєвський В. І. Корпоративна інформаційна безпека: монографія. Одеса: ОНЕУ, 2018. 350 с.

37. Шандрівська О. В. Інформаційна безпека підприємств в умовах цифрової економіки // Економічний вісник НТУУ «КПІ». 2019. № 16. С. 252–255.

38. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського національного університету. 2023. Серія ПРАВО. Випуск 78: частина 2. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058.

39. Якубенко Ю. Л. Теоретична сутність фінансово-економічної безпеки підприємства. Дніпро: ДДАЕУ, 2020. 150 с.

40. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2013. 36 p.

ДОДАТКИ