МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОЦІНКА ДОЦІЛЬНОСТІ ВПРОВАДЖЕННЯ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВИЗНАЧЕННЯ ЙОГО МІСЦЯ В ЗАГАЛЬНІЙ СИСТЕМІ УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ ПІДПРИЄМСТВА”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій ІЛЛЯШЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Олексій ІЛЛЯШЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ілляшенку Олексію Миколайовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оцінка доцільності впровадження процесу управління ризиками інформаційної безпеки та визначення його місця в загальній системі управління бізнес-ризиками підприємства”,

керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “___“ березня 2024 р. №___.

2. Строк подання кваліфікаційної роботи “20” травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління ризиками інформаційної безпеки, нормативні документи, міжнародні стандарти, наукова та технічна література*

4. Перелік питань, які мають бути розроблені:
   1. Проаналізувати основні характеристики забезпечення процесу управління ризиками інформаційної безпеки в системі управління бізнес-ризиками підприємства.
   2. Дослідити методики інтеграції процесу управління ризиками інформаційної безпеки в систему управління бізнес-ризиками підприємства.
   3. Визначити напрями та методи забезпечення інформаційної безпеки підприємства.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	13.03.2024	
2.	Збір та аналіз літератури.	30.03.2024	
3.	Аналіз основних характеристик інформаційної безпеки підприємства.	17.04.2024	
4.	Дослідження методики інтеграції процесу управління ризиками інформаційної безпеки в систему управління бізнес-ризиками підприємства.	01.05.2024	
5.	Визначення напрямів та методів забезпечення інформаційної безпеки підприємства.	15.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2024	
7.	Оформлення роботи.	24.05.2024	
8.	Оформлення презентації.	01.06.2024	
9.	Отримання рецензії на роботу.	04.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Олексій ІЛЛЯШЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Ілляшенко О.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Оцінка доцільності впровадження процесу управління ризиками інформаційної безпеки та визначення його місця в загальній системі управління бізнес-ризиками підприємства”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ІЛЛЯШЕНКО Олексій у кваліфікаційній роботі проаналізував основні характеристики забезпечення процесу управління ризиками інформаційної безпеки в системі управління бізнес-ризиками підприємства, дослідив методики інтеграції процесу управління ризиками інформаційної безпеки в систему управління бізнес-ризиками підприємства, визначив напрями та методи забезпечення інформаційної безпеки підприємства.

ІЛЛЯШЕНКО Олексій показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ІЛЛЯШЕНКА Олексія на оцінку “_____” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Ілляшенко О.М. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ІЛЛЯШЕНКА Олексія
на тему “Оцінка доцільності впровадження процесу управління ризиками інформаційної безпеки та визначення його місця в загальній системі управління бізнес-ризиками підприємства”

Актуальність. Для протидії зростаючим загрозам кібербезпеки, забезпечення дотримання нормативних вимог та захисту активів організації необхідна інтеграція управління ризиками інформаційної безпеки в загальну систему управління бізнес-ризиками. Ефективне управління ризиками зменшує фінансові втрати, юридичні наслідки та шкоду для репутації, тим самим підтримуючи стратегічні цілі організації та операційну стійкість у цифровому та взаємопов'язаному бізнес-середовищі. З огляду на зазначене дослідження проблеми впровадження ефективних процесів управління ризиками інформаційної безпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі проведено детальний аналіз сучасних стратегій управління ризиками ІБ, що забезпечує всебічне розуміння предмета дослідження.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.
3. Автор опрацював значну джерельну базу: 42 публікації, в тому числі англомовних.
4. За результатами дослідження запропоновано практичні рекомендації для організацій щодо оцінки доцільності та алгоритму впровадження процесів управління ризиками інформаційної безпеки в загальну систему управління бізнес-ризиками організації.

Недоліки.

1. Доцільно було б приділити більше уваги аналізу сучасних інструментів, які можуть бути використані для автоматизації процесу управління ризиками.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач ІЛЛЯШЕНКО Олексій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблем забезпечення інформаційної безпеки підприємства та визначення його місця в загальній системі управління бізнес-ризиками підприємства. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, висновків та списку використаних джерел, що містить 42 найменування. Загальний обсяг роботи становить 69 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Мета роботи полягає у оцінці доцільності впровадження процесу управління ризиками інформаційної безпеки на підприємстві та визначенні його місця в загальній системі управління бізнес-ризиками. Для цього у роботі використовуються методи системного аналізу та теорії інформаційної безпеки.

Об'єктом дослідження є процес управління ризиками інформаційної безпеки підприємства.

Предмет дослідження є теоретичні та практичні аспекти доцільності впровадження процесу управління ризиками інформаційної безпеки на підприємстві.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, теорії інформаційного протиборства та конкуренції між суб'єктами підприємницької діяльності. Як результат у роботі досліджено особливості управління ризиками інформаційної безпеки підприємства та його місця в загальній системі управління бізнес-ризиками, зокрема, представлено схему актуальних загроз інформаційній безпеці з урахуванням зазначеної специфіки; визначено напрями та методи забезпечення інформаційної безпеки підприємства.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, УПРАВЛІННЯ РИЗИКАМИ.

ABSTRACT

The qualification work is dedicated to researching the issues of ensuring the information security of an enterprise and determining its place in the overall system of business risk management. The work consists of an introduction, three chapters containing 9 figures, conclusions, and a list of 42 references. The total volume of the work is 69 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the work is to justify the implementation of the information security risk management process in the enterprise and its place in the overall system of business risk management. For this purpose, the work uses methods of systems analysis and information security theory.

The object of the research is the process of managing the information security risks of the enterprise.

The subject of the research is the theoretical and practical aspects of the feasibility of implementing the information security risk management process in the enterprise.

Research methods: The tasks set in the research were addressed using methods of theoretical synthesis and systems analysis, which were applied in studying the fundamental principles of information security in the context of entrepreneurship and the theory of the effectiveness of information security management systems. The analysis of the ISMS in the enterprise was carried out using economic-mathematical modeling, structural analysis, and graphical data representation. As a result, the work examines the features of managing the information security of the enterprise and its place in the overall business risk management system. Specifically, it presents a scheme of current threats to the enterprise's information security considering the specified specifics; it defines the directions and methods for ensuring the information security of the enterprise.

Application area: The developed approaches can be used in planning and implementing the enterprise's information security management system.

Keywords: ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY THREAT, INFORMATION SECURITY MANAGEMENT SYSTEM, RISK MANAGEMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення
СУІБ	Система управління інформаційною безпекою

ВСТУП

Актуальність теми. Підприємницька діяльність, в різних галузях економіки тісно пов'язана з отриманням та використанням інформації, яка в умовах сучасного розвитку ринкової економіки набуває статусу цінного ресурсу. Відтак, забезпечення надійності інформаційної безпеки є одним з ключових аспектів розвитку інформаційних технологій на підприємствах. Управління бізнесом сьогодні не можливе без інтеграції різноманітних систем, де інформаційна система відіграє роль основного каталізатора для інших процесів. Забезпечення інформаційної безпеки в діловій сфері є складним завданням, яке вимагає уваги та розуміння важливості від керівництва та власників компаній. Ефективність управління інформаційною безпекою безпосередньо впливає на загальну продуктивність підприємства. Недооцінка загроз, таких як порушення конфіденційності інформації, може призвести до серйозних проблем з інформаційною безпекою, що, у свою чергу, може мати важкі наслідки, включаючи втрату даних та потенційне банкрутство компанії.

Зважаючи на інтенсивний розвиток технологій та інструментів захисту даних, актуальність дослідження питань інформаційної безпеки в бізнес-середовищі набувають все більшого значення. Вітчизняні підприємства повинні шукати нові шляхи для підвищення ефективності систем управління інформаційною безпекою.

Дослідження питань, пов'язаних з інформаційною безпекою в бізнес-середовищі, привертало увагу таких вчених: О.В. Топоркова, В.В. Халецька, Т.А. Наумова, К. О. Утенкова, Н.С. Акімова, Т.В. Петреман, В.О. Бондаренка, І.Л. Бучила, Г.В. Козаченка. Теоретичні засади та питання інформаційної безпеки були значно розвинені завдяки дослідженням таких авторів, як: О.А. Панченко, Т.Ю. Ткачук, Л.В. Панченко, В. Чубаєвський, К. Фокіна-Мезенцева, Т.Жук, В. Кузьомко, О. В. Дейнега, Л. А. Бехтер, Г. М. Азаренкова.

Хоча існує чимало наукових робіт та аналітичних матеріалів у сфері інформаційної безпеки, ця тема залишається важливою та вимагає додаткового

вивчення. Дослідження, проведені як в Україні, так і за кордоном, підкреслюють важливість створення комплексної системи інформаційної безпеки на підприємствах, яка б інтегрувала тактичні, технічні та управлінські аспекти захисту.

Мета роботи полягає у оцінці доцільності впровадження процесу управління ризиками інформаційної безпеки на підприємстві та визначенні його місця в загальній системі управління бізнес-ризиками.

Об'єктом дослідження є процес управління ризиками інформаційної безпеки підприємства.

Предмет дослідження є теоретичні та практичні аспекти доцільності впровадження процесу управління ризиками інформаційної безпеки на підприємстві.

Для досягнення цієї мети в роботі необхідно виконати наступні ***завдання:***

1. Визначити місце і роль ризик-менеджменту в системі процесів забезпечення інформаційної безпеки підприємства;
2. Виявити фактори ризику для інформаційної безпеки підприємства;
3. Провести аналіз існуючих фреймворків, методологій та кращих практик управління ризиками інформаційної безпеки;
4. Оцінити важливості інтеграції процесу управління ризиками інформаційної безпеки в загальне управління ризиками підприємства
5. Проаналізувати організацію системи управління інформаційною безпекою підприємства;
6. Визначити необхідність впровадження процесу управління ризиками інформаційної безпеки;
7. Надати рекомендації щодо подальшого вдосконалення процесів управління ризиками інформаційної безпеки.

Методи дослідження. Вирішення завдань, поставлених у дослідженні, здійснювалося за допомогою методів теоретичного синтезу та системного аналізу, які застосовувалися при вивченні основоположних принципів інформаційної безпеки в контексті підприємництва та теорії ефективності систем

управління інформаційною безпекою. Аналіз системи управління інформаційною безпекою на підприємстві, проводився з використанням економіко-математичного моделювання, структурного аналізу та графічного представлення даних.

Практичне значення одержаних результатів. Результати дослідження допоможуть підприємствам ефективно управляти ризиками інформаційної безпеки, знижуючи ймовірність втрати даних та фінансових збитків, та підвищити ефективність управління бізнес-ризиками.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ ПІДПРИЄМСТВА

1.1 Визначення місця і ролі ризик-менеджменту в системі процесів забезпечення інформаційної безпеки підприємства

В сучасному світі, де інформація стала однією з найцінніших ресурсів, захист і забезпечення безпеки цієї інформації для підприємств стає ключовим завданням. Захист від різноманітних загроз, включаючи кібератаки, даних інсайдерів, технічні неполадки та інші ризики, стає першочерговою необхідністю для забезпечення стабільності та успішності бізнесу.

В цьому контексті роль ризик-менеджменту в системі процесів забезпечення інформаційної безпеки підприємства стає надзвичайно важливою. Ризик-менеджмент визначається як систематичний підхід до визначення, аналізу, оцінки, контролю та мінімізації ризиків, які становлять загрозу для інформаційної безпеки організації. Цей процес вимагає комплексного підходу, що враховує різноманітні аспекти діяльності підприємства, включаючи технологічні, організаційні, правові та людські фактори.

Основною метою ризик-менеджменту в контексті інформаційної безпеки є забезпечення ефективного контролю над ризиками, які можуть вплинути на конфіденційність, цілісність та доступність інформації. Це досягається шляхом ідентифікації потенційних загроз, визначення їх ймовірності та впливу, розробки стратегій мінімізації ризиків та впровадження відповідних заходів безпеки.

Ризик-менеджмент у контексті інформаційної безпеки також передбачає постійний моніторинг і аналіз змін у загрозах та ризиках, що дозволяє підприємствам адаптувати свої заходи безпеки до нових умов і викликів. Крім того, важливою складовою ризик-менеджменту є залучення всіх рівнів персоналу до процесу забезпечення безпеки інформації, що сприяє підвищенню свідомості та відповідальності всіх учасників організації.

Інформація є ключовим економічним ресурсом кожної організації, необхідним для реалізації соціального, економічного, технічного, технологічного, інтелектуального та іншого розвитку. Взаємодія програм співпраці включає в себе використання територіальних комп'ютерних мереж, які можуть бути глобальними, локальними (регіональними, муніципальними, корпоративними). Поява таких мереж обумовлена прогресом науково-технічного розвитку та випливає з наукових потреб у обміні інформацією для підвищення ефективності управління [9].

Варто відзначити, що у науковій літературі немає однозначного уявлення про сутність поняття "інформаційна безпека". Для деяких дослідників це поняття визначає активність або стан, тоді як для інших - це властивість, процес, функція або система гарантій та можливостей. Крім того, не існує загальноприйнятої норми, що містить чітку дефініцію "інформаційної безпеки", ураховуючи різницю між цим поняттям та "безпекою інформації" (табл. 1.1).

Отже, інформаційну безпеку можна визначити як неможливість компрометування властивостей об'єкта безпеки, що визначаються інформацією та інформаційною інфраструктурою. Об'єкти забезпечення інформаційної безпеки включають інформаційні ресурси, комп'ютерне обладнання, мережі та системи, а також програмне забезпечення. Основні загрози безпеці включають розкриття конфіденційної інформації, несанкціоноване використання ресурсів, злом систем та інші види вторгнень [3, с.61].

Це визначення інформаційної безпеки максимально відповідає стандартам ISO та враховує системний підхід до захисту інформації, оскільки вона зберігається не лише на електронних пристроях, але і передається між людьми.

Таблиця 1.1

Аналіз розуміння дефініції «інформаційна безпека» науковцями

Автор, джерело	**Визначення поняття**
1	2
Богуш В. [10]	Стан захищеності інформаційного середовища є важливим для держави і забезпечується через формування, використання та розвиток, незалежно від впливу інформаційних загроз, як внутрішніх, так і зовнішніх.
Гнатенко В. [11]	Стан інформаційного середовища, який забезпечує відповідь на інформаційні потреби учасників інформаційних взаємин, забезпечує безпеку інформації та захист суб'єктів від негативних впливів інформаційних загроз.
Архипов О. [12]	Поточний ступінь захищеності об'єкта від інформаційних загроз визначається мірою можливих збитків, що можуть бути завдані об'єкту у разі виникнення таких загроз. Ці загрози можуть включати в себе: використання неповної, невчасної або недостовірної інформації; негативний вплив на інформацію; незаконне використання інформаційних технологій; неповноважне поширення та використання інформації; порушення цілісності, конфіденційності та доступності інформації.
Захарова О. І. [13]	Стан захищеності важливих інтересів особи, суспільства і держави полягає в мінімізації можливої шкоди, яка може виникнути внаслідок неповної, невчасної або недостовірної інформації, негативного впливу інформації, негативних наслідків функціонування інформаційних технологій, а також несанкціонованого поширення інформації.

Поняття "інформаційна безпека підприємства" є надзвичайно актуальним у сучасному етапі розвитку інформаційних технологій, що супроводжується впровадженням інформаційних систем у всі сфери діяльності людини та постійною взаємодією підприємств в інформаційному просторі [15, с. 158–159].

Сороківська О., визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності [16].

Марущак А., визначає інформаційну безпеку підприємства як цілеспрямовану діяльність органів та посадових осіб підприємства з використанням дозволених сил і засобів для досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [17, с. 94].

Серед основних інформаційних активів, що можуть належати організації, можна відзначити такі:

– стратегічна документація: це внутрішні документи, які визначають довгострокові стратегічні та короткострокові цілі організації. Ця інформація містить конфіденційні дані, до яких конкуренти можуть прагнути отримати доступ.

– інформація про продукти (послуги): це критично важлива інформація, яка потребує захисту через управління інформаційною безпекою.

– інтелектуальна власність (патенти): організація може мати інтелектуальну власність, таку як патенти або програмне забезпечення, яка потребує захисту від конкурентів.

– комерційні секрети: це унікальні ідеї, які надають організації конкурентні переваги.

– поточна проектна документація: це документи, що містять деталі продуктів або послуг, які знаходяться в процесі розробки. Ця інформація може бути цінною для конкурентів.

– дані про співробітників: це особиста інформація про співробітників, яка може бути використана для шантажу або перехоплення співробітників.

– конфіденційні дані клієнтів: втрата таких даних може призвести до порушення довіри клієнтів та порушення стандартів інформаційної безпеки.

Інформаційна загроза настає в той момент, коли потенційна шкода від витоку інформації перевищує певний рівень, вимагаючи комплексу заходів для запобігання та захисту. Загрози інформаційній безпеці - це події або дії, що можуть призвести до спотворення, несанкціонованого використання або навіть знищення інформаційних ресурсів системи управління, апаратного та програмного забезпечення [1, с.21].

Загроза порушення цілісності та конфіденційності інформаційних ресурсів з обмеженим доступом є реальною, оскільки існує ризик створення каналу для несанкціонованого доступу до цінної інформації та документів. Такий

несанкціонований доступ неминуче призводить до втрати інформації та знищення носіїв інформації [2, с.153].

Система управління інформаційною безпекою (СУІБ) може бути розглянута як сучасний механізм для забезпечення безпеки інформаційних ресурсів будь-якого підприємства. Вона є складовою частиною загальної системи управління, яка ґрунтується на системному підході і охоплює всі аспекти інформаційної безпеки в бізнес-діяльності. СУІБ відповідає за розроблення, впровадження, функціонування, моніторинг, перегляд, підтримку та постійне вдосконалення інформаційної безпеки. Управління інформаційною безпекою в рамках СУІБ також охоплює управління персоналом, захистом інформації, ризиками, інцидентами, безперервністю бізнесу та іншими ресурсами з метою забезпечення інформаційної безпеки.

Серед основних організаційних заходів у СУІБ, які гарантують належний рівень інформаційної безпеки будь-якого підприємства, можна виділити наступні: організація ефективного використання технічних засобів для збору, обробки, накопичення і зберігання конфіденційної інформації; організація систематичного аналізу внутрішніх та зовнішніх (включаючи гібридні) загроз конфіденційній інформації та розроблення відповідних заходів щодо її захисту.

Інформаційна безпека охоплює стан захищеності інформації в усіх її аспектах, забезпечуючи конфіденційність, цілісність та доступність (табл. 1.2).

Таблиця 1.2

Цілі інформаційної безпеки підприємства [6]

Ціль	**Завдання**
Конфіденційність інформації	Доступ до інформації лише для тих, хто має на це право
Цілісність інформації	Передбачає, щоб інформація була точною та послідовною
Доступність інформації	Гарантує, що інформація відкрита лише для тих, хто має відповідні дозволи

Сучасному бізнесу інформаційна безпека стала вирішальною складовою для успішного функціонування. Захист інформаційної інфраструктури підприємства відкриває нові можливості для бізнесу і дозволяє економити

ресурси. Надійний захист інформації дозволяє залучати нових партнерів, оскільки вищий рівень довіри відкриває можливість надавати більший рівень доступу зовнішнім сторонам, таким як клієнти, партнери, співробітники та підрядники [4].

Погоджуємось з твердженням С. Онищенка та О. Ківшука про те, що повномасштабне вторгнення рф створило нові реалії та виклики у сфері безпеки як в Україні, так і в усьому світі. Глобальний масштаб загроз та небезпек вимагає негайних структурних змін у національній економіці в умовах воєнного стану. Одночасно процеси цифровізації сприяли з'яві нових інформаційних загроз та значних кібератак з боку росії, що виявили критичні проблеми у сфері інформаційної безпеки. Всі ці загрози підкреслюють необхідність створення системи безпекоорієнтованого інформаційного середовища як для підприємств-суб'єктів господарювання, так і для зміцнення безпеки на національному рівні [5].

В ході своїх досліджень В. Кузьомко виявив, що зростання цифрової трансформації економіки призводить до появи нових загроз для інформаційної безпеки бізнесу. Він стверджує, що ця проблема стає надзвичайно актуальною, і щоб успішно протистояти загрозам, що виникають у зв'язку з цифровою трансформацією, потрібна комплексна стратегія, що поєднує технічні, організаційні та економічні методи та засоби. Один з ключових напрямків для забезпечення інформаційної безпеки бізнесу - це постійне підвищення рівня цифрової грамотності серед працівників та впровадження всеосяжного організаційно-документального регулювання процесів збору, обробки та зберігання інформації [7].

О.В. Дейнега також висловлює думку, що для забезпечення захисту інформації підприємство може використовувати різноманітні підходи, включаючи організаційні, технічні методи та правове регулювання захисту своєї інформації. Автор підкреслює, що формування системи захисту інформації має базуватися на принципі економічної доцільності. Недбале ставлення до зберігання або захисту інформації, а також надмірне засекречування можуть

призвести до втрати частини прибутку або навіть спричинити серйозні економічні втрати [8].

Згідно з джерелом виникнення, загрози можна розділити на дві категорії. Зовнішні загрози виникають ззовні підприємства і, як правило, не залежать від його власної діяльності. З іншого боку, внутрішні загрози виникають всередині самого підприємства через його власну діяльність або недоліки у внутрішніх процесах (рис. 1.1).

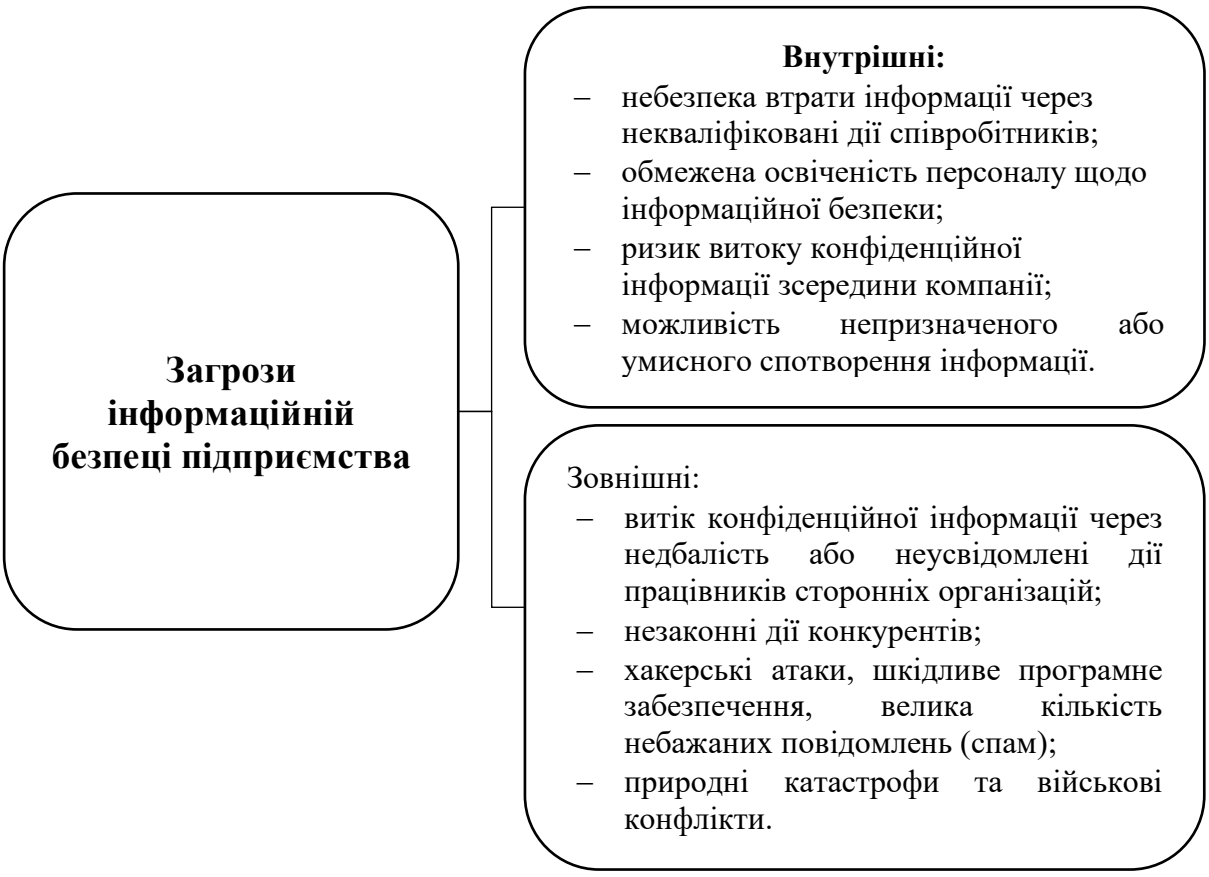

Рис. 1.1. Загрози інформаційній безпеці підприємства [14]

Захист інформації на підприємстві є надзвичайно важливим і повинен враховуватися при укладенні контрактів з працівниками, особливо з тими, хто займає керівні посади. Основна загроза пов'язана з інформацією, яка зберігається в інформаційних системах підприємства, включаючи програмне забезпечення, додатки для виконання завдань, текстові редактори та бази даних. Для забезпечення безпеки інформаційної системи необхідно надавати доступ лише зареєстрованим користувачам, обмежуючи їхні можливості використання

інформаційних технологій. Виявлення, аналіз та оцінка ризиків інформаційної безпеки є ключовим етапом у проектуванні систем інформаційної безпеки підприємства. Від правильності оцінки ризиків залежить ефективність всієї системи інформаційної безпеки підприємства. Крім цього, необхідно впроваджувати регулярні тренінги для співробітників щодо основ інформаційної безпеки та постійно оновлювати захисні механізми відповідно до нових загроз.

Таким чином, визначення місця і ролі ризик-менеджменту в системі процесів забезпечення інформаційної безпеки підприємства є ключовим для формування ефективної та надійної стратегії захисту. Ризик-менеджмент виступає фундаментальним елементом, що дозволяє вчасно виявляти, аналізувати та оцінювати потенційні загрози, зменшуючи ймовірність їх реалізації та мінімізуючи можливі збитки. Впровадження ризик-менеджменту забезпечує системний підхід до управління інформаційною безпекою, що включає моніторинг, планування, впровадження захисних заходів та постійне вдосконалення процесів. Ефективний ризик-менеджмент дозволяє підприємству не лише захищати свої інформаційні ресурси, але й забезпечувати безперервність бізнес-процесів, зберігаючи довіру клієнтів та партнерів. Він також сприяє підвищенню інформаційної культури в організації, оскільки залучає всі рівні персоналу до процесу захисту, роблячи його інтегральною частиною корпоративної політики.

1.2 Аналіз існуючих фреймворків, методологій та кращих практик управління ризиками інформаційної безпеки

Захист інформації здійснюється через застосування різних методів, включаючи захист програм від несанкціонованого читання та копіювання, забезпечення авторських прав на інформаційні матеріали, контроль доступу до програм і їх запуску, а також механізми самотестування і самовідновлення програмного коду.

Порушення інформаційної безпеки можуть призвести до значних фінансових втрат, шкоди репутації та втрати конкурентних переваг. Тому управління ризиками інформаційної безпеки є однією з пріоритетних задач для будь-якої організації.

Управління ризиками інформаційної безпеки – це комплексний процес, який включає ідентифікацію, оцінку, аналіз та контроль ризиків з метою їх мінімізації або усунення. Для ефективного управління ризиками необхідно застосовувати системний підхід, що базується на використанні фреймворків, методологій та кращих практик. Ці інструменти допомагають створити структуровану та організовану систему захисту, яка здатна адаптуватися до нових викликів та загроз.

При розробці нової Системи управління інформаційною безпекою (СУІБ) на основі стандартів або подальшої стандартизації вже існуючої СУІБ, необхідно обрати відповідний стандарт інформаційної безпеки. Існують дві основні концепції стандартів. Перша концепція пропонує загальні вимоги до побудови СУІБ та загального захисту інформації, прикладами чого є стандарти ISO, NIST тощо. Інша концепція включає чітко визначені галузеві стандарти, такі як HIPAA, PCI DSS, FINRA, GDPR тощо. Порівняння методів оцінки ризиків (додатку А)

Кожна держава також впроваджує власні стандарти, наприклад, в Україні існує власна концепція захисту інформації – Комплексна система захисту інформації (КСЗІ). Оскільки стандарти відрізняються своїми функціями та вимогами, перед вибором стандарту для побудови або сертифікації СУІБ необхідно провести ретельний аналіз. Нижче наведено аналіз найпоширеніших стандартів (рис. 1.2).

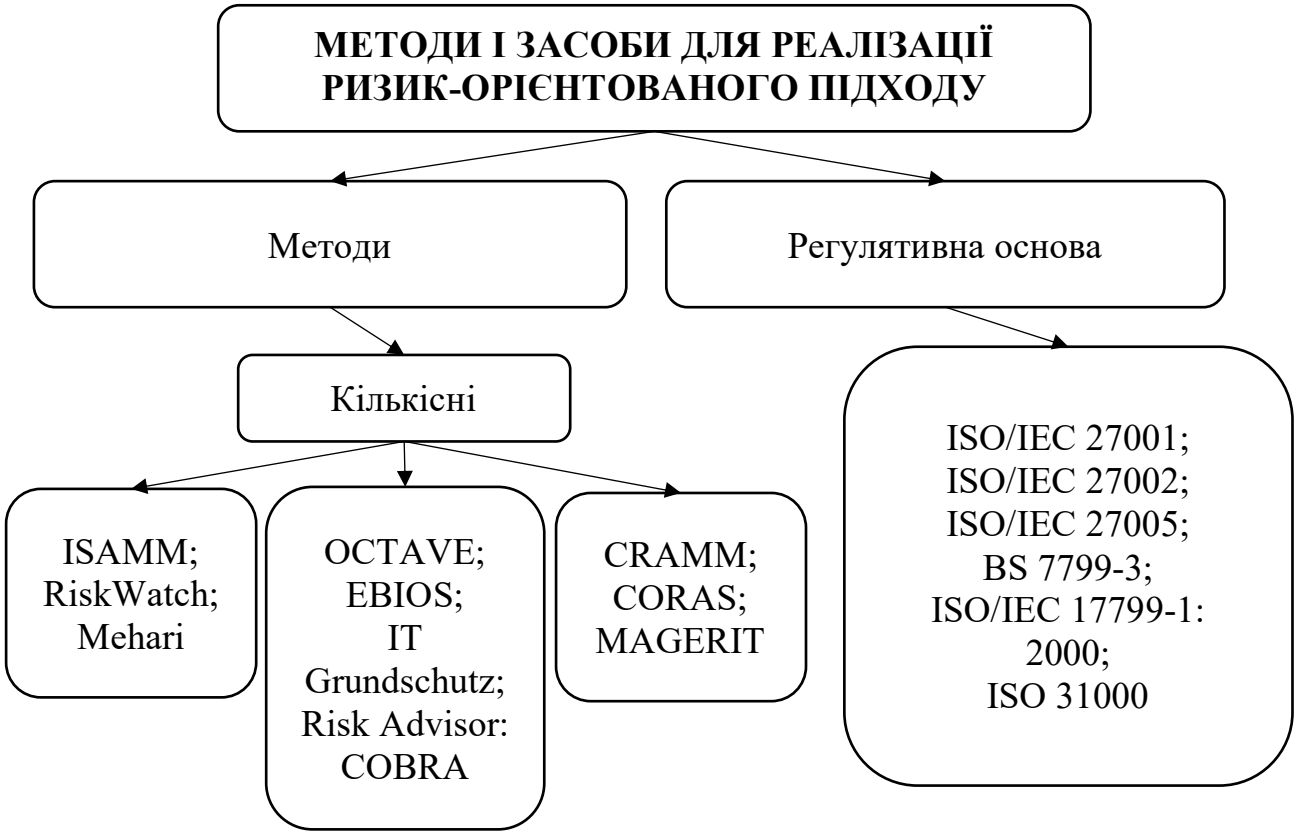

Рис. 1.2. Методи і засоби для ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства [18]

Фреймворк "NIST Risk Management Framework" (NIST RMF), заснований на стандартах Національного інституту стандартів і технологій США (NIST), включає набір взаємопов'язаних стандартів, які охоплюють різні аспекти управління ризиками:

NIST SP 800-30 "Guide for Conducting Risk Assessments" – цей стандарт є керівництвом з проведення оцінки ризиків, зосередженим на інформаційних технологіях, інформаційній безпеці та операційних ризиках. Він описує процеси підготовки, проведення оцінки ризиків, комунікації результатів та підтримки процесу оцінки. Алгоритм цієї методики зображено на рис 1.3.

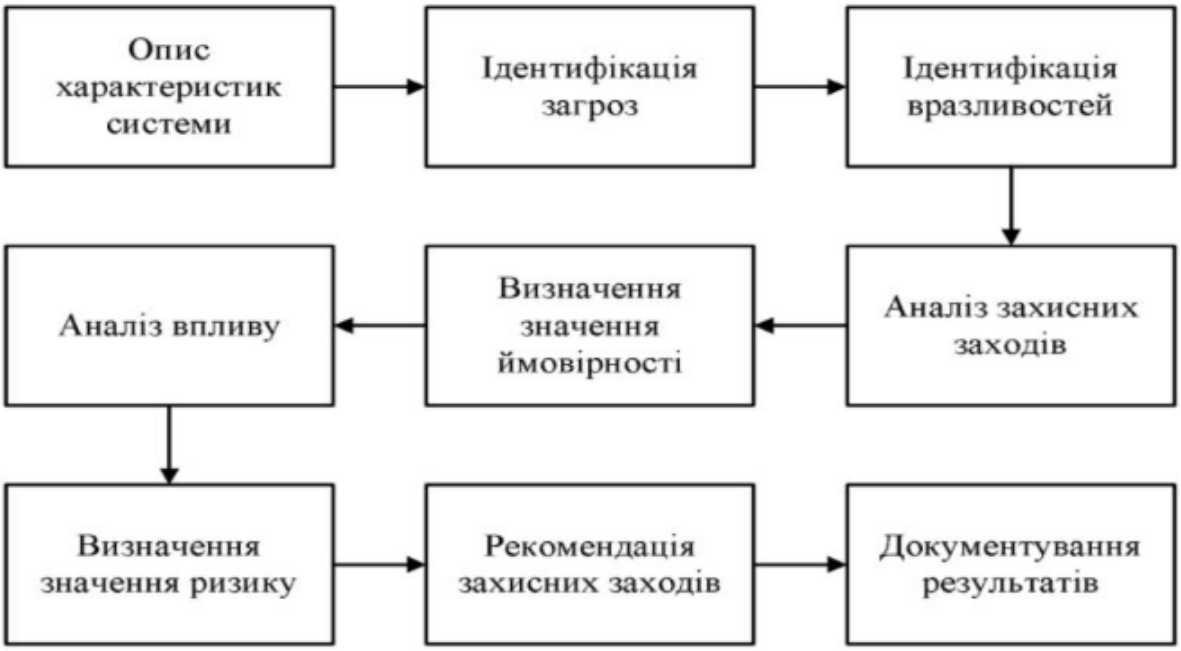

Рис. 1.3. Алгоритм методики управління ризиками NIST 800-30 [18]

Переваги методу NIST 800-30:

– легкість у виконанні процедур оцінки ризиків (ор), яка забезпечує відносно простий процес;

– можливість налаштування методу ор під вимоги конкретної організації, враховуючи її тип та масштаб;

– детальне висвітлення всіх можливих ризиків, що стосуються інформаційних активів;

– врахування різних варіантів обробки ризиків (зниження, прийняття, перенесення, уникнення ризику);

– наявність програмного забезпечення для аналізу результатів, що реалізовує принципи методики.

Метод NIST 800-30 має свої обмеження:

– довготривалий процес аналізу та оцінки ризиків, що може вимагати значного часу і зусиль;

– оцінка ризиків проводиться лише на трьохрівневій шкалі, що обмежує узагальнення методики.

NIST SP 800-39 "Managing Information Security Risk" – пропонує трирівневий підхід до управління ризиками на рівні організації, бізнес-процесів та інформаційних систем. Цей стандарт деталізує методологію управління ризиками, включаючи ідентифікацію, оцінку, реагування та моніторинг ризиків інформаційної безпеки.

NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations" – рекомендує застосовувати управління життєвим циклом систем для забезпечення безпеки та конфіденційності інформаційних систем.Цей фреймворк є комплексним інструментом, який дозволяє організаціям структуровано підходити до управління ризиками інформаційної безпеки [18].

Використання NIST RMF сприяє не лише ідентифікації та оцінці ризиків, але й розробці ефективних стратегій для реагування та моніторингу ризиків, що є критично важливим в умовах швидких технологічних змін і зростаючих загроз.

Впровадження NIST RMF допомагає організаціям відповідати регуляторним вимогам, покращувати свої процеси управління ризиками та підвищувати загальний рівень безпеки інформаційних систем. Це сприяє не тільки захисту даних, але й зміцненню довіри клієнтів та партнерів, що є ключовим фактором у сучасному бізнес-середовищі.

Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" описує підхід до постійного моніторингу інформаційних систем і IT-середовищ. Він фокусується на контролі застосованих заходів обробки ризиків інформаційної безпеки та підкреслює необхідність регулярного перегляду цих заходів для забезпечення їхньої ефективності.

Цей стандарт пропонує систематичний процес, який включає:Оцінку поточного стану безпеки – забезпечує регулярне відстеження та аналіз безпекових подій для виявлення потенційних загроз і вразливостей.

Визначення пріоритетів і реагування на ризики – допомагає встановлювати пріоритети для заходів реагування, базуючись на ступені впливу ризиків на організацію. Оновлення та вдосконалення заходів безпеки – передбачає регулярний перегляд і вдосконалення захисних заходів для забезпечення їх

відповідності новим загрозам і технологіям. Завдяки таким підходам, стандарт NIST SP 800-137 допомагає організаціям підтримувати високий рівень інформаційної безпеки, адаптуючись до змінних умов і нових викликів у сфері кібербезпеки.

Стандарти управління ризиками інформаційної безпеки, визначені Міжнародною організацією зі стандартизації ISO (МОС ISO), включають:

Стандарт ISO / IEC 27005: 2018 "Information technology – Security techniques – Information security risk management" ("Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризиків інформаційної безпеки"), що є частиною серії стандартів ISO 27000. Його особливість полягає у зосередженні на аспектах інформаційної безпеки у контексті управління ризиками [18].

Стандарт ISO / IEC 27102: 2019 "Information security management – Guidelines for cyber-insurance" надає рекомендації щодо оцінки потреби у кіберстрахуванні як одного зі засобів управління ризиками інформаційної безпеки, а також щодо взаємодії зі страховими компаніями.

Серія стандартів ISO / IEC 31000: 2018 описує загальний підхід до управління ризиками без прив'язки до інформаційних технологій. Важливим компонентом цієї серії є стандарт ISO / IEC 31010: 2019 "Risk management – Risk assessment techniques", який визначає методики оцінки ризиків.

Ці стандарти визначають важливі принципи та підходи до управління ризиками в галузі інформаційної безпеки, що допомагає організаціям ефективно реагувати на виклики та загрози у цій сфері.

Методологія FRAP (Facilitated Risk Analysis Process) представляє собою досить простий підхід до оцінки основних ризиків інформаційної безпеки, який зосереджений на найважливіших активах. Якісний аналіз здійснюється за допомогою експертної оцінки [18].

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) спрямована на самостійну роботу членів бізнес-підрозділів і використовується для широкомасштабної оцінки всіх інформаційних систем та бізнес-процесів компанії.

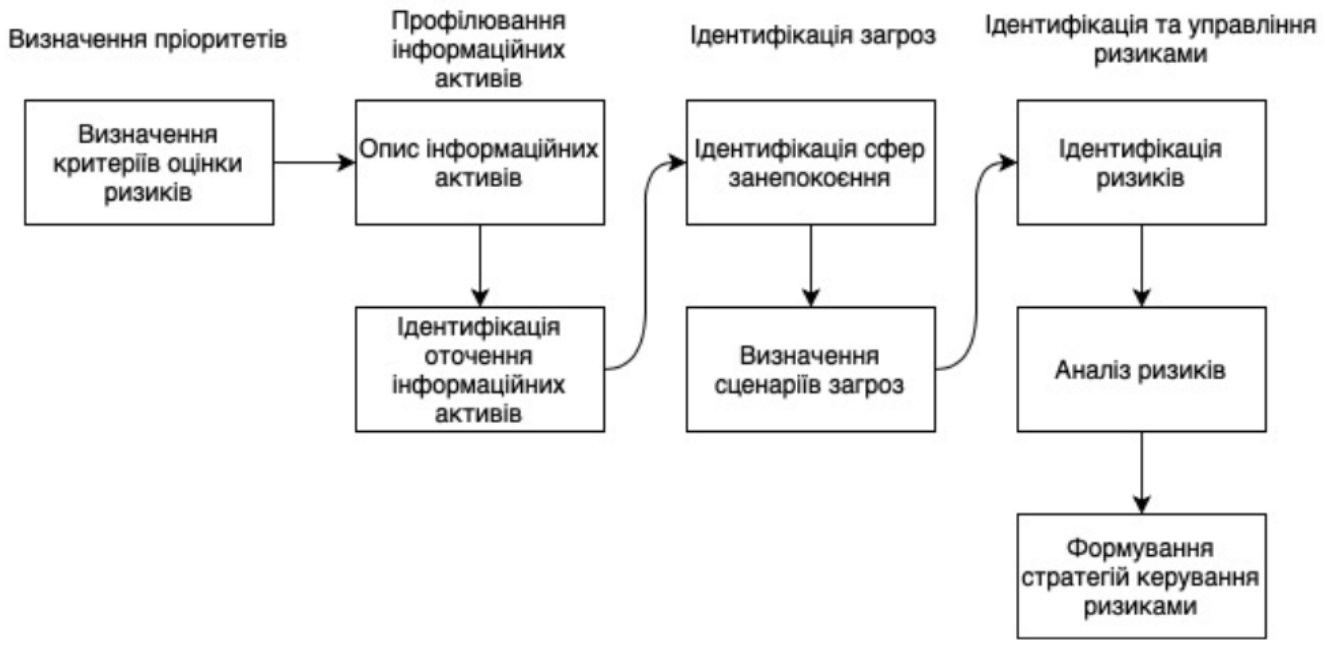

Рис. 1.4. Зальна схема застосування методики OCTAVE [18]

Стандарт AS/NZS 4360, що має походження з Австралії та Нової Зеландії, фокусується не лише на IT-системах, але і на бізнес-здоров'ї компанії, що відображає більш загальний підхід до управління ризиками інформаційної безпеки, наприклад, у банківській сфері. Важливо зауважити, що цей стандарт зараз замінений стандартом AS/NZS ISO 31000-2009.

Методологія FMEA (Failure Modes and Effect Analysis) передбачає оцінку системи з точки зору її слабких місць для виявлення ненадійних елементів.

Методологія CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) пропонує використання автоматизованих засобів для управління ризиками інформаційної безпеки (рис. 1.4).

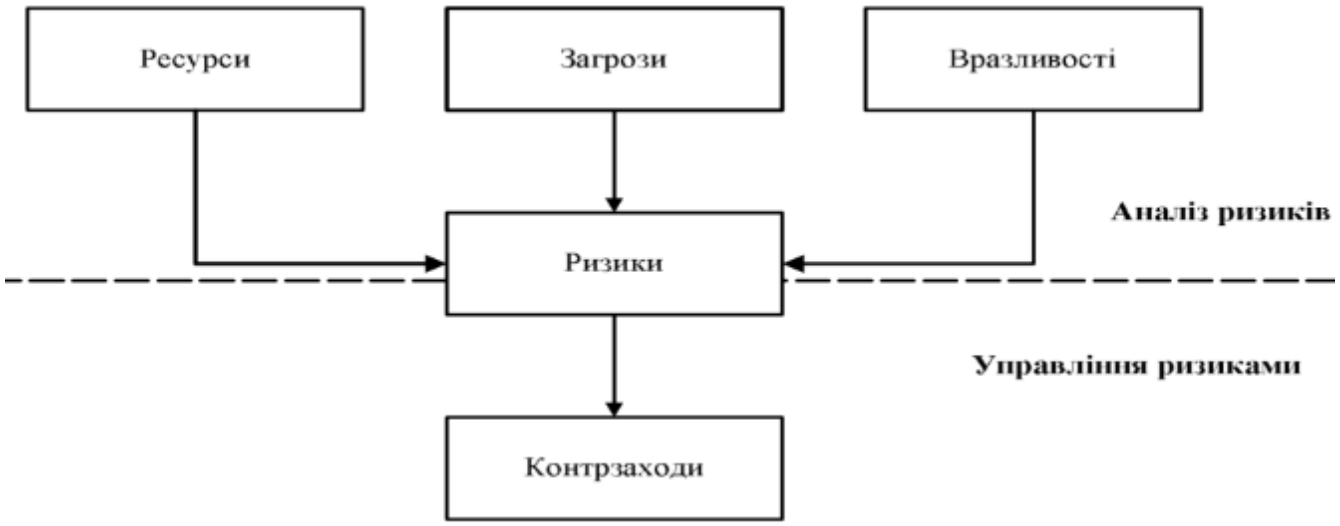

Рис. 1.5. Алгоритм методики управління ризиками CRAMM [18]

Методологія CRAMM ґрунтується на комплексному підході до оцінки ризиків, який поєднує якісні та кількісні методи аналізу. Вона відповідає потребам як великих, так і малих організацій, незалежно від їхнього сектору діяльності. Варіанти програмного забезпечення CRAMM, спрямовані на різні типи організацій, відрізняються базами знань (профілями). Для комерційних організацій існує комерційний профіль, для державних — державний. Державний варіант профілю дозволяє також проводити аудит відповідно до вимог американського стандарту ITSEC [18].

Правильне використання методології CRAMM дозволяє економічно обґрунтувати витрати на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками інформаційної безпеки може в кінцевому підсумку зекономити кошти, уникнувши непотрібних витрат.

Методологія CRAMM передбачає розділення процедури оцінки ризиків на три послідовні етапи. Перший етап полягає у відповіді на питання: "Чи достатньо застосування засобів базового рівня для захисту системи, чи потрібен детальніший аналіз?" На другому етапі проводиться ідентифікація ризиків та їхнє оцінювання. На третьому етапі вирішується питання вибору адекватних контрзаходів.

Методологія CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв'ю, списки перевірки та набір звітних документів.

Методологія FAIR (Factor Analysis of Information Risk) пропонує Фреймворк для кількісного аналізу ризиків, що базується на моделі системи управління ризиками, зорієнтованій на економічну ефективність. Вона сприяє ухваленню обґрунтованих рішень, порівнянню стратегій управління ризиками, фінансових показників та точних моделей ризику.

Концепція COSO ERM (Enterprise Risk Management) описує способи інтеграції ризик-менеджменту зі стратегічними та фінансовими аспектами діяльності підприємства, акцентуючи на значущості їх взаємозв'язку.

Таким чином, важливо відзначити, що аналіз існуючих фреймворків, методологій та кращих практик управління ризиками інформаційної безпеки виявляється як важлива складова вдосконалення загальної стратегії безпеки підприємства. Ретельне вивчення і впровадження найбільш ефективних методик дозволяє забезпечити адекватний рівень захисту інформації, а також зменшити ймовірність виникнення серйозних загроз та ризиків. Для успішного впровадження зазначених підходів важливо враховувати специфіку діяльності конкретної організації та унікальні вимоги щодо її інформаційної безпеки. Тільки таким чином можна забезпечити ефективне управління ризиками та забезпечити безпеку інформації на відповідному рівні.

1.3 Оцінка важливості інтеграції процесу управління ризиками інформаційної безпеки в загальне управління ризиками підприємства

Інформація, що зберігається та обробляється організацією, стає об'єктом потенційних загроз з боку кібератак, внутрішніх порушень безпеки, а також інших форм ризиків, які можуть спричинити серйозні шкоди. В цьому контексті інтеграція процесу управління ризиками інформаційної безпеки в загальне

управління ризиками підприємства стає необхідною складовою для забезпечення цілісності, надійності та стійкості бізнес-процесів.

Підвищення кількості кіберзагроз та рівня складності кібератак, а також зростання обсягів обробки конфіденційної інформації, зумовлює необхідність постійного вдосконалення стратегій управління ризиками. Інтеграція процесу управління ризиками інформаційної безпеки у загальну систему управління ризиками дозволяє підприємствам ефективно виявляти, оцінювати та управляти ризиками, пов'язаними з безпекою інформації, забезпечуючи тим самим стійкість бізнес-процесів та довіру у стосунках з клієнтами та партнерами.

Фінансова стійкість, що є ключовим фактором успіху та стабільності підприємств, обумовлюється не лише ефективними фінансовими стратегіями, але й здатністю керівництва швидко реагувати на потенційні небезпеки та швидко адаптуватися до змін у економічному середовищі. Кожна складова економічної безпеки, така як фінансова, правова, кадрова, технологічна та інформаційна, має свій внесок і впливає на загальний стан підприємства. Вивчаючи структуру економічної безпеки, важливо враховувати, що всі ці компоненти взаємодіють між собою та створюють основу для стабільного розвитку підприємства.

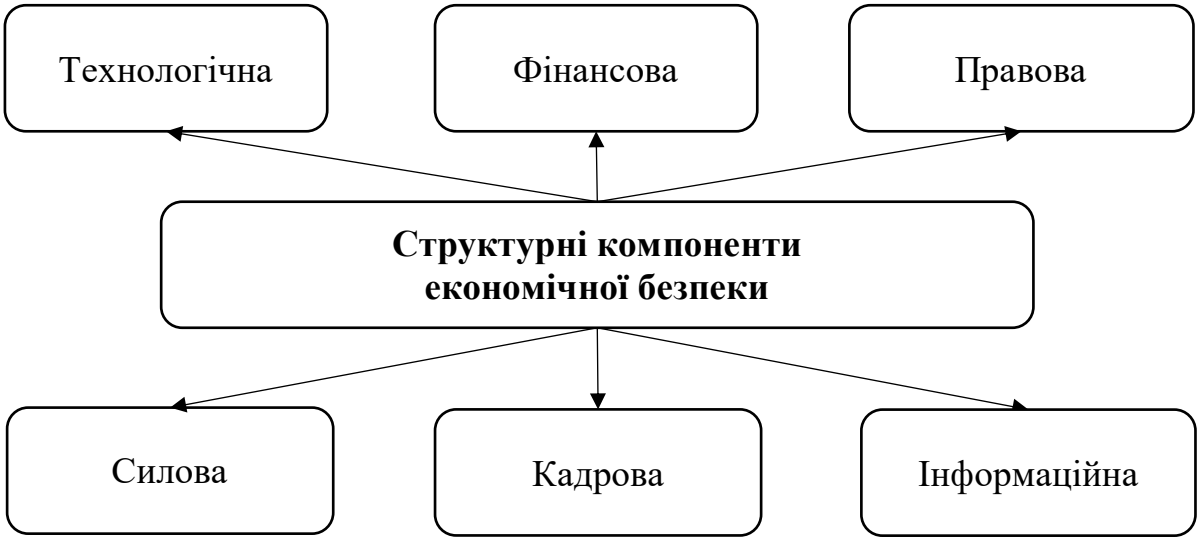

Рис. 1.6. Структурні компоненти економічної безпеки підприємства [1]

Основною умовою для ефективного управління компанією є вдосконалення системи інформаційного забезпечення.

Забезпечення інформаційної безпеки стає дедалі важливішим аспектом управління підприємством у сучасному світі. Швидкі темпи технологічного розвитку та поширення цифрових інструментів відкривають нові можливості для бізнесу. Сучасні підприємства активно використовують передові технології та автоматизовані системи обліку для оптимізації своєї роботи та підвищення конкурентоспроможності. Використання різних технічних засобів комунікації для передачі та зберігання інформації, перехід до автоматизованих систем обліку і документообігу, впровадження аналітичних систем для обробки даних – все це призводить до накопичення значного обсягу інформації, яка обробляється та зберігається для подальшого аналізу і використання. Зростаючий обсяг даних та їх розміщення на цифрових носіях створює нові загрози для безпеки інформації.

Тому важливо створити умови для забезпечення збереження інформації, щоб запобігти її витоку, викривленню, викраденню або знищенню, особливо враховуючи конфіденційний характер інформаційних даних. Це вимагає від керівництва ретельного планування, постійного моніторингу та готовності до оперативного реагування на можливі загрози. Крім того, необхідно регулярно оновлювати системи безпеки, навчати персонал щодо сучасних методів захисту інформації та впроваджувати інноваційні рішення для мінімізації ризиків, пов'язаних з інформаційною безпекою.

Існуючі методики оцінки ризиків інформаційної безпеки (ІБ) поділяються на дві основні групи: якісні та кількісні. Далі розглянемо детально кожен з цих підходів.

Якісні методики оцінки ризиків ґрунтуються на експертних оцінках та досвіді фахівців у сфері інформаційної безпеки. Вони включають аналіз загроз і вразливостей, визначення потенційних наслідків та ймовірностей їх реалізації. До переваг якісного підходу належать його відносна простота, швидкість проведення та можливість адаптації до специфіки організації. Однак, цей підхід може бути суб'єктивним та менш точним порівняно з кількісними методами.

Кількісні методики оцінки ризиків використовують математичні моделі та статистичні дані для визначення ймовірностей і потенційних втрат від реалізації ризиків. Вони забезпечують більш точні та об'єктивні результати, що дозволяє краще обґрунтувати заходи щодо мінімізації ризиків. Проте, кількісний підхід може вимагати значних ресурсів та часу для збору й аналізу даних, а також спеціалізованих знань.

Поєднання якісних та кількісних методів може забезпечити найбільш комплексний та ефективний підхід до управління ризиками інформаційної безпеки. Використовуючи обидва підходи, організації можуть отримати глибше розуміння своїх ризиків та розробити більш надійні стратегії захисту інформаційних активів.

У багатьох практичних ситуаціях важко точно визначити ймовірність ризиків та їхній вплив. Через це оцінка ризику часто виражається числом у певному діапазоні значень або класифікується за категоріями, такими як "низька", "середня" чи "висока". Такий підхід є основою методів якісного аналізу ризиків, як показано в таблиці 1.3.

Таблиця 1.3

Приклад якісного аналізу ризиків [19]

		Вплив		
		Низький	**Середній**	**Високий**
Ймовірність	**Низький**	Низький ризик	Низький ризик	Середній ризик
	Середній	Низький ризик	Середній ризик	Високий ризик
	Високий	Середній ризик	Високий ризик	Високий ризик

До того ж, використання класифікаційних категорій дозволяє спростити процес прийняття рішень і зробити його більш зрозумілим для широкого кола зацікавлених сторін. Наприклад, керівники можуть швидше оцінити рівень загроз і прийняти відповідні заходи без необхідності глибокого занурення в складні математичні моделі. Це особливо важливо в умовах обмежених ресурсів і часу, коли потрібні оперативні дії для захисту інформаційних активів підприємства.

Відповідно, якісний аналіз ризиків є ефективним інструментом для початкової оцінки ситуації, який можна доповнити більш детальними кількісними методами для глибшого розуміння та управління ризиками.

Для кількісного визначення ймовірності та впливу ризиків використовують кількісні методи аналізу. Мета такого аналізу – надати аналітику числові дані про цінність активів, ймовірність настання ризиків та ефективність контрзаходів боротьби з ними.

Кількісна оцінка дозволяє визначити можливі втрати за допомогою наступних метрик:

1) Значення активу (Asset Value, AV) – вартість ресурсів організації, враховуючи як якісні, так і кількісні показники.

2) Фактор схильності до ризику (Exposure Factor, EF) – відсоток втрат, які може зазнати актив у випадку реалізації загрози.

3) Очікувана одинична втрата (Single Loss Expectancy, SLE) – визначається за наступною формулою [19]:

$$SLE = EF * AV \quad (1.1)$$

Ця характеристика визначає обсяг втрат у разі реалізації загрози. Крім цього, кількісні методи аналізу дозволяють створювати моделі сценаріїв і прогнозувати фінансові наслідки різних типів загроз. Це сприяє більш обґрунтованому прийняттю рішень керівництвом організації, дозволяючи їм точно оцінювати необхідність та доцільність інвестицій у безпеку.

1. Щорічна частота прояву (Annualized Rate of Occurrence, ARO) – очікувана кількість випадків прояву загрози за рік щодо одного активу.

2. Очікувана щорічна втрата (Annualized Loss Expectancy, ALE) – визначається за формулою:

$$ALE = SLE * ARO \quad (1.2)$$

Ця характеристика визначає очікувані за рік фінансові втрати від однієї загрози. Крім цих показників, кількісні методи аналізу також можуть враховувати додаткові метрики, такі як ймовірність відновлення після інциденту та ефективність існуючих заходів захисту. Важливою перевагою кількісних

методів є можливість точного розрахунку економічних втрат, що дозволяє керівництву підприємства приймати більш обґрунтовані рішення щодо інвестування в інформаційну безпеку.

На практиці найкращі аналітичні звіти досягаються тоді, коли аналіз базується на попередньо проведеній кількісній оцінці даних. Це дозволяє забезпечити точність і надійність результатів, які є основою для прийняття управлінських рішень. У таблиці 1.1 наведені переваги та недоліки кожного з підходів.

Врахування цих аспектів допомагає підприємству обирати найбільш ефективні методи для конкретних ситуацій, забезпечуючи таким чином оптимальний баланс між витратами на безпеку та рівнем захисту інформаційних активів.

Таблиця 1.4

Переваги та недоліки кількісного та якісного підходів [19]

Підхід	**Переваги**	**Недоліки**
Якісний	– не вимагає значних обчислень; – немає потреби у кількісній оцінці загроз; – визначення грошової вартості активів не завжди є необхідним для оцінки нематеріальних активів; – легше залучати до аналізу персонал без технічних знань.	– базується на суб'єктивній думці аналітика та його експертності; – недостатньо даних для визначення грошової вартості активів; – відсутність кількісної інформації для застосування методів мінімізації ризиків.
Кількісний	– ґрунтується на об’єктивних метриках та процесах; – грошова вартість активів та можливі заходи для зменшення ризиків зрозумілі; – результат може бути виражений у конкретних грошових сумах та ймовірностях.	– використання комплексного підходу може вимагати значних часових витрат; – необхідно вкласти значні зусилля у попереднє зібрання та оцінку інформації про ризики; – вимагає великого рівня експертизи від аналітика.

Таким чином, управління ризиками інформаційної безпеки є важливою складовою загальної стратегії управління ризиками на підприємстві. Інтеграція цих процесів дозволяє не лише ефективно виявляти, аналізувати та зменшувати ризики, але й створює базу для стійкого розвитку та забезпечує захист від

сучасних викликів цифрової епохи. Необхідно враховувати, що цей процес вимагає постійного вдосконалення та адаптації до нових загроз та технологічних досліджень, але заслуговує на увагу як невід'ємна частина стратегічного керівництва, спрямованого на забезпечення стійкого й успішного функціонування підприємства.

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи забезпечення процесу управління ризиками інформаційної безпеки в системі управління бізнес-ризиками підприємства.

Визначення місця і ролі ризик-менеджменту в системі процесів забезпечення інформаційної безпеки підприємства показало, що ризик-менеджмент є невід'ємною частиною системи інформаційної безпеки, яка забезпечує цілісність, конфіденційність та доступність інформації. Він дозволяє виявляти, оцінювати та мінімізувати потенційні загрози, що впливають на інформаційні ресурси підприємства. Було визначено, що ефективний ризик-менеджмент сприяє зниженню можливих втрат від інцидентів інформаційної безпеки та покращує загальну стійкість організації.

Аналіз існуючих фреймворків, методологій та кращих практик управління ризиками інформаційної безпеки виявив, що найбільш відомі фреймворки та методології, такі як ISO/IEC 27005, NIST SP 800-30, CRAMM та OCTAVE, надають структуровані підходи до управління ризиками, які можуть бути адаптовані до потреб конкретного підприємства. Використання цих фреймворків та методологій допомагає підприємствам впроваджувати ефективні процеси управління ризиками та підвищувати рівень інформаційної безпеки.

Оцінка важливості інтеграції процесу управління ризиками інформаційної безпеки в загальне управління ризиками підприємства показала, що така інтеграція дозволяє забезпечити комплексний підхід до ризик-менеджменту.

Розгляд цих аспектів допоміг зрозуміти важливість інтеграції ризик-менеджменту в загальну структуру безпеки та управління компанії, а також виявити ключові процеси та підходи для ефективного управління інформаційними ризиками.

Розділ 2 ДОСЛІДЖЕННЯ МЕТОДИКИ ІНТЕГРАЦІЇ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМУ УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ ПІДПРИЄМСТВА ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

2.1 Оцінка готовності підприємства до впровадження процесу управління ризиками інформаційної безпеки

У сучасному цифровому середовищі, де інформаційні технології стають не лише необхідністю, але й стратегічним ресурсом для бізнесу, питання забезпечення інформаційної безпеки набуває особливого значення. Організації, незалежно від розміру та галузі діяльності, стикаються з високим рівнем загроз щодо конфіденційності, цілісності та доступності своєї інформації. Впровадження системи управління ризиками інформаційної безпеки стає нагальним завданням для забезпечення стабільності та успішності діяльності будь-якої компанії.

У контексті цих викликів, оцінка готовності підприємства до впровадження процесу управління ризиками інформаційної безпеки стає критичним кроком. Однією з компаній, яка стоїть перед таким завданням, є ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ».

ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» спеціалізується на інженерно-технічних рішеннях та реалізації будівельних проектів у сферах промислового та цивільного будівництва. Основні напрями діяльності компанії включають зведення об’єктів та надання інжинірингових послуг, як показано на рисунку 2.1. Організаційно, ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» є товариством з обмеженою відповідальністю, з головним офісом у місті Київ.

Рис. 2.1. Основні напрямки діяльності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Компанія присутня на ринку з 2008 року та має значний досвід співпраці з великими клієнтами з різних галузей. Завдяки стабільній фінансовій ситуації, ТОВ «ІБК «КЕПІТАЛ ІН+ЖИНІРИНГ» вдалося успішно закріпитися на ринку і постійно розширювати спектр своїх послуг. Така фінансова стійкість дозволяє компанії інвестувати в нові проекти, впроваджувати передові технології та забезпечувати високу якість своїх інженерно-технічних рішень.

У сучасному світі, де інформаційні технології відіграють важливу роль, забезпечення інформаційної безпеки стає критичним аспектом для будь-якого підприємства. ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» розуміє важливість інтеграції процесу управління ризиками інформаційної безпеки у свою загальну стратегію управління ризиками. Це дозволяє не лише захищати цінні дані компанії, але й забезпечувати безперервність бізнес-процесів, що є ключовим фактором успіху у конкурентному середовищі.

Щодо фінансово-економічного стану підприємства, у наведених таблицях представлено дані про обсяг виробництва продукції, середньооблікову чисельність персоналу, показники руху основних фондів, оборотність оборотних коштів, витрати на виробництво продукції, рентабельність, фінансовий стан та фінансову стійкість за період з 2020 по 2022 роки.

Таблиця 2.1

Обсяг виробництва продукції ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Роки	**В порівняних цінах, млн. грн.**	**У діючих цінах, млн. грн.**
2020	0,4	259,1
2021	1,4	1210,6
2022	1,3	1103,9
2022р. до 2020р., %	1,03	857,86

На основі наданих даних таблиці 2.1., можна зробити висновки, що обсяг виробництва продукції (робіт/послуг) значно зріс з 2020 року до 2021 року, збільшившись з 0,4 млн грн до 1,4 млн грн у порівнянних цінах 2000 року і з 259,1 млн грн до 1210,6 млн грн у діючих цінах. У 2022 році обсяг виробництва продукції (робіт/послуг) дещо знизився порівняно з 2021 роком, досягнувши 1,3 млн грн у порівнянних цінах 2000 року та 1103,9 млн грн у діючих цінах. Незважаючи на зниження у 2022 році, загальний тренд залишається позитивним, оскільки обсяг виробництва продукції значно зріс порівняно з 2020 роком. Це підкреслює значне зростання продуктивності підприємства впродовж останніх років, хоча незначне зниження у 2022 році може вказувати на необхідність аналізу причин та пошуку можливостей для подальшого підвищення ефективності виробництва, що є важливим для забезпечення сталого розвитку та конкурентоспроможності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ».

Таблиця 2.2

Середньооблікова чисельність ШП ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Показники	**2020р.**	**2021р.**	**Динаміка в порівн. з2021 р.**	**2022р.**	**Динаміка в порівн. з 2022р.**
Всього, працівників	110	103	-7	108	+5
У тому числі робітників	85	79	-6	81	+2

На таблиці 2.2., видно що загальна середньооблікова чисельність штату зменшилася з 110 осіб у 2020 році до 103 осіб у 2021 році, що означає зниження на 7 осіб. Середньооблікова чисельність робочих також зменшилася з 85 осіб у 2020 році до 79 осіб у 2021 році, що означає зниження на 6 осіб. Прогноз на 2023 рік показує покращення, оскільки загальна середньооблікова чисельність штату

очікується збільшитися до 108 осіб, що є зростанням на 5 осіб порівняно з 2021 роком, а середньооблікова чисельність робочих очікується збільшитися до 81 особи, що становить зростання на 2 особи порівняно з 2021 роком. Загальна тенденція вказує на зниження чисельності у 2021 році порівняно з 2020 роком, але прогнозується поступове відновлення у 2023 році. Це свідчить про можливе покращення умов праці та відновлення виробничих потужностей підприємства ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ».

Таблиця 2.3

Витрати на розробку послуг ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Витрати / роки	**2020**	**2021**	**Динаміка порівн. з 2020 р.**	**2022**	**Динаміка порівн. з 2021 р. %**
Загальна собівартість, млн. грн.	212,9	931,8	719	1150,2	218,4
Матеріальні витрати, млн. грн.	85,1	352,5	267,4	409,2	56,7
Витрати на оплату праці, млн. грн.	62,9	297	234,0	408,5	112
Амортизація ОФ, млн. грн.	14,6	48,4	33,8	68,0	19,6
Відрахування на страхування, млн. грн.	22,2	108	85,7	148,7	40,8
Інші (утому числі податки з собівартості), млн. грн.	28,1	126,1	98,0	115,8	-10,3

На основі наданих даних можна зробити наступні висновки щодо витрат на виробництво продукції ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Загальна собівартість продукції значно зросла з 212,9 млн. грн. у 2020 році до 931,8 млн. грн. у 2021 році і далі до 1150,2 млн. грн. у 2022 році, що свідчить про істотне збільшення витрат на виробництво. Матеріальні витрати також зросли з 85,1 млн. грн. у 2020 році до 352,5 млн. грн. у 2021 році і до 409,2 млн. грн. у 2022 році, що вказує на значний ріст витрат на матеріали. Витрати на оплату праці збільшилися з 62,9 млн. грн. у 2020 році до 297 млн. грн. у 2021 році і до 408,5 млн. грн. у 2022 році, що демонструє зростання витрат на зарплати.

Витрати на амортизацію основних фондів зросли з 14,6 млн. грн. у 2020 році до 48,4 млн. грн. у 2021 році і до 68 млн. грн. у 2022 році, що вказує на збільшення витрат на знос активів. Витрати на страхування збільшилися з 22,2

млн. грн. у 2020 році до 108 млн. грн. у 2021 році і до 148,7 млн. грн. у 2022 році, що свідчить про зростання страхових витрат. Інші витрати, включаючи податки, зросли з 28,1 млн. грн. у 2020 році до 126,1 млн. грн. у 2021 році, але знизилися до 115,8 млн. грн. у 2022 році, що показує зворотний тренд у витратах.

Витрати на виробництво продукції у відношенні до випуску залишалися стабільними у 2020 та 2022 роках, але зросли з 0,8 грн. у 2020 році до 1,0 грн. у 2021 році, а у 2022 році залишилися на рівні 0 грн., що може вказувати на зміни у структурі витрат. Це свідчить про загальне збільшення витрат на виробництво продукції, зокрема на матеріали, оплату праці, амортизацію та страхування, з певними коригуваннями у інших витратах.

Підвищення загальної собівартості продукції протягом розглянутого періоду пояснюється зростанням матеріальних витрат, витрат на оплату праці, амортизації та страхування. Однак у 2022 році спостерігається зниження інших витрат. Показник витрат на виробництво продукції відносно обсягу випуску збільшився у 2021 році, але залишився стабільним у 2022 році. Докладний аналіз причин змін у витратах дозволить зробити більш точні висновки щодо фінансового стану та ефективності виробництва компанії.

Таблиця 2.4

Рівень рентабельності підприємства ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Показники	**2020 р.**	**2021 р.**	**2022 р.**
Рентабельність продажів, %	6,2	5	8
Рентабельність продукції, %	47,0	11,0	9,0
Рентабельність ОПФ, %	7,7	5,4	4,0
Рентабельність Об. С, %	4,4	7,2	5,2
Рентабельність виробництва, %	3	3,1	2,3

З аналізу рентабельності можна зробити наступні висновки: спочатку рентабельність продажів знижувалася з 6,2% у 2020 році до 5% у 2021 році, але подальше зростання до 8% у 2022 році може вказувати на позитивні зміни в ефективності продажів; рентабельність продукції спочатку скоротилася з 47% у 2020 році до 11% у 2021 році, але трохи покращилася до 9% у 2022 році, свідчачи про зменшення прибутковості виробництва; рентабельність основних фондів

зменшилася з 7,7% у 2020 році до 5,4% у 2021 році і подальше до 4% у 2022 році, вказуючи на зменшення прибутковості основних активів; рентабельність оборотних коштів зросла з 4,4% у 2020 році до 7,2% у 2021 році, але знову знизилася до 5,2% у 2022 році, що може свідчити про коливання в ефективності використання оборотних активів; рентабельність залишалася стабільною протягом 2020-2022 років, з незначним зниженням з 3% у 2020 році до 2,3% у 2022 році. Дані рентабельності вказують на необхідність уважної аналізу та управлінських дій для збільшення прибутковості компанії.

Зростання витрат на виробництво продукції, зокрема на матеріали, оплату праці, амортизацію та страхування, а також певні зміни у структурі інших витрат, безпосередньо впливають на оцінку готовності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» до впровадження процесу управління ризиками інформаційної безпеки. Високі витрати можуть свідчити про значні інвестиції в основні фонди, персонал та страхування, що може створювати сприятливі умови для впровадження комплексних заходів інформаційної безпеки.

Однак, збільшення загальної собівартості продукції може також вказувати на необхідність ретельного аналізу фінансової стійкості компанії, щоб забезпечити наявність достатніх ресурсів для інвестування в нові системи управління ризиками. Підвищені витрати на матеріали та оплату праці можуть свідчити про високий рівень технологічної модернізації та кваліфікації працівників, що є позитивним фактором для впровадження складних інформаційних систем.

Для оцінки готовності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» до впровадження процесу управління ризиками інформаційної безпеки слід розглянути декілька ключових факторів: зрілість існуючих процесів інформаційної безпеки (ІБ), підтримка керівництва, фінансовий стан, технічна інфраструктура, а також рівень обізнаності та підготовки персоналу.

ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» демонструє стабільний ріст та інвестиції в основні фонди, що свідчить про наявність технологічної бази для підтримки цих процесів. Наявність ефективних процесів моніторингу безпеки та

реагування на інциденти є критично важливою для успішного впровадження управління ризиками.

Підтримка та активна участь вищого керівництва є вирішальними факторами для успішного впровадження управління ризиками інформаційної безпеки. ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» демонструє високий рівень інвестування у важливі сфери, такі як оплата праці та страхування, що свідчить про усвідомлення ризиків керівництвом.

Наявність бюджету для інформаційної безпеки проектів та готовність керівництва інвестувати в захист інформаційних активів є позитивним сигналом про готовність ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» до впровадження управління ризиками інформаційної безпеки.

Зростання витрат на виробництво та стабільна фінансова ситуація ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» вказують на її спроможність забезпечити необхідні ресурси для впровадження управління ризиками інформаційної безпеки. Витрати на амортизацію та модернізацію основних фондів свідчать про наявність сучасної технічної бази, що є важливим для ефективного управління ризиками інформаційної безпеки.

Використання передових технологій та автоматизованих систем обліку свідчить про технічну готовність ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» до впровадження комплексних систем управління ризиками. Наявність розвинених мережевих інфраструктур та захищених систем обміну інформацією є важливими компонентами для успішного впровадження управління ризиками інформаційної безпеки.

Інвестиції у навчання персоналу щодо інформаційної безпеки та управління ризиками є критичними для забезпечення ефективності процесів. Зростання витрат на оплату праці може вказувати на наявність кваліфікованого персоналу, здатного впроваджувати нові ІБ ініціативи.

Розвиток культури безпеки в організації, де всі співробітники усвідомлюють важливість інформаційної безпеки та активно беруть участь у

заходах з її забезпечення, є важливим для успішного впровадження управління ризиками ІБ.

З огляду на фінансову стабільність, значні інвестиції в основні фонди, підтримку керівництва та технічну інфраструктуру, ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» демонструє високу готовність до впровадження процесу управління ризиками інформаційної безпеки. Водночас, для забезпечення успіху необхідно продовжувати розвивати процеси моніторингу та управління інцидентами, інвестувати в навчання персоналу та зміцнювати культуру безпеки в організації.

Відповідно до методології ISF (Information Security Forum), нами було оцінено рівень інформаційної безпеки підприємства. Оцінка охоплює 21 процес ІБ, описаний з урахуванням найвідоміших міжнародних практик і загальноприйнятих стандартів (ISO27000-ISO27005) (табл. 2.5, 2.6). Критерії оцінки рівня зрілості процесів управління ІБ наведені в табл. 3.1.

Таблиця 2.5

Критерії оцінки рівня зрілості процесів менеджменту ІБ [18]

Рівень зрілості	**Позначення рівня зрілості**	**Опис**
0	Неіснуючий	Процес ІБ не виконується
1	Примітивний	Процес ІБ виконується на нерегулярній основі
2	Початковий	Процес ІБ виконується на регулярній основі і підтримується на рівні планування (включно із залученням зацікавлених сторін і використання відповідно до стандартів і керівництв)
3	Формалізований	Процес ІБ виконується, планується , і є достатній обсяг організаційних ресурсів для підтримки та управління
4	Керований	Процес ІБ виконується, планується, керується і контролюється
5	Оптимізований	Процес ІБ виконується, планується, керується, вимірюється за допомогою кількісних показників і постійно вдосконалюється

Таблиця 2.6

Оцінки рівня зрілості процесів менеджменту ІБ ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" [18]

№	Найменування процесу ІБ	Рівень зрілості
1	Стратегія ІБ	4
2	Усвідомлення керівництвом важливості ІБ	5
3	Управління ризиками ІБ	4
4	Управління комплаєнсом	4
5	Аудит ІБ	4
6	Політика ІБ	4
7	Управління доступом	2
8	Управління уразливими місцями	3
9	Управління ЖЦ АС	3
10	Управління інформаційними активами	3
11	Управління змінами	4
12	Архітектура ІБ	3
13	Управління каналами зв'язку	2
14	Управління зовнішньою взаємодією	4
15	Розвідка загроз ІБ	4
16	управління подіями ІБ	4
17	управління інцидентами ІБ	4
18	Антикризове управління	4
19	Забезпечення безперервності бізнесу	5
20	Підвищення обізнаності персоналу	5
21	Безпека персоналу	5
	Загальний рівень зрілості процесів ІБ	3,81

Оцінка рівня зрілості процесів інформаційної безпеки (ІБ) становить 3,81, що відповідає формалізованому рівню. Це свідчить про те, що процес управління ІБ виконується і планується, існує достатній обсяг організаційних ресурсів для підтримки та управління інформаційною безпекою, проте цей процес ще не є досконалим.

За результатами аналізу готовності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» до впровадження процесу управління ризиками інформаційної безпеки, можна зробити висновок, що компанія має стабільну фінансову ситуацію, значні інвестиції в технічну інфраструктуру та матеріальні ресурси, а також підтримку з боку керівництва. Це свідчить про високу готовність до інтеграції управління ризиками ІБ в загальні бізнес-процеси. Крім того, прогнозоване зростання чисельності персоналу і його підготовка вказують на відповідний рівень

обізнаності та задіянні, що забезпечує успішне впровадження нових систем управління інформаційною безпекою.

2.2 Визначення ключових зацікавлених сторін та оцінка потреб у ресурсах для впровадження процесу

Впровадження процесу управління ризиками інформаційної безпеки є актуальним завданням для багатьох сучасних підприємств, у тому числі і для ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Як провідна компанія у сфері інженерно-технічних рішень та будівництва об'єктів промисловості і цивільного будівництва, вона звертає увагу на оцінку потреб та визначення ключових зацікавлених сторін у контексті впровадження цього процесу. Аналіз вимог інтересів різних сторін, таких як клієнти, партнери, регулятори та співробітники, допомагає зрозуміти необхідність вдосконалення системи управління ризиками, а також визначити ресурси, необхідні для успішного впровадження цього процесу.

Для детального аналізу ключових зацікавлених сторін та оцінки потреб у ресурсах для ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ», можна відтворити дані в таблиці 2.7.

Таблиця 2.7

Визначення ключових зацікавлених сторін ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Зацікавлена сторона	Інтереси	Вплив на процес
Власники	ROI, репутація компанії	Високий
Клієнти	Конфіденційність даних	Високий
Співробітники	Безпека робочого місця	Середній
Постачальники	Довгострокові контракти	Низький
Регуляторні органи	Дотримання законодавства	Високий

Аналізуючи таблицю 2.7., можна відзначити, що різні зацікавлені сторони мають різні інтереси та вплив на процес управління ризиками інформаційної безпеки в ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Власники, спрямовуючись на

збільшення прибутку та підтримку репутації компанії, мають великий вплив на процес, оскільки від їхніх рішень залежить розподіл ресурсів. Клієнти, які цінують конфіденційність своїх даних, також мають значний вплив, оскільки їхні вимоги визначають стратегію захисту інформації. Співробітники, які стурбовані безпекою свого робочого місця, мають середній вплив, оскільки їхні дії та сприйняття політики безпеки можуть впливати на ефективність реалізації процесу. Постачальники, які цінують довгострокові контракти, та регуляторні органи, які наголошують на дотриманні законодавства, мають менший вплив на процес у порівнянні з іншими зацікавленими сторонами, але все ж можуть впливати на деякі аспекти управління ризиками.

Враховуючи складнощі та вимоги сучасного бізнесу, оцінка потреб у ресурсах для впровадження процесу управління ризиками інформаційної безпеки стає важливим етапом для підприємства. Вступні оцінки цих потреб відображають сукупність вимог зацікавлених сторін, стратегічні цілі компанії та її здатність до ефективного реагування на потенційні загрози та виклики у сфері інформаційної безпеки. Ретельний аналіз цих потреб допомагає визначити необхідні ресурси, які сприятимуть успішному впровадженню та функціонуванню системи управління ризиками на підприємстві.

Таблиця 2.8

Оцінка потреб у ресурсах ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Ресурс	**Оцінка потреби**	**Примітки**
Фінансові	Висока	Необхідні для оновлення IT-інфраструктури
Людські	Середня	Тренінги з безпеки, наймання фахівців
Технічні	Висока	Шифрування даних, IDS/IPS системи
Часові	Середня	Розробка та впровадження

План дій для впровадження процесу управління ризиками інформаційної безпеки включає кілька ключових кроків. По-перше, це розробка політик безпеки, що передбачає визначення стандартів та процедур, які будуть використовуватися на підприємстві. Наступним етапом є оцінка існуючої IT-інфраструктури з метою ідентифікації потреб у її оновленні для підвищення рівня безпеки. Далі, важливим елементом є проведення тренінгів для

співробітників з метою підвищення їх обізнаності з питань безпеки інформації. Після цього передбачається впровадження технічних засобів захисту, таких як шифрування, системи виявлення та запобігання вторгненням (IDS/IPS), а також системи моніторингу. Завершує план моніторинг та оцінка, що передбачає регулярний перегляд та оновлення політик та процедур з метою підтримки високого рівня безпеки на підприємстві.

2.3 Узгодження процесу управління ризиками інформаційної безпеки з цілями та стратегіями підприємства

Забезпечення високого рівня безпеки даних та інформаційних систем є необхідністю в умовах постійної загрози кібератак, витоку конфіденційної інформації та інших інцидентів інформаційної безпеки. Враховуючи це, узгодження процесу управління ризиками інформаційної безпеки з цілями та стратегіями нашої компанії відіграє ключову роль у забезпеченні стійкості та надійності наших операцій, а також захисту інтересів клієнтів та партнерів.

Гармонізація управління ризиками інформаційної безпеки з стратегічними цілями ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" передбачає системний аналіз сучасного стану компанії, визначення стратегічних цілей та впровадження відповідних процесів. Наприклад, однією з головних цілей є збільшення обсягів доходу на 20% протягом наступних трьох років, що вимагає активного розширення ринків та привернення нових клієнтів. Крім того, ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" визначає завдання оптимізації внутрішніх процесів та впровадження інноваційних технологій для підвищення якості продукції та послуг. Такий цілеспрямований підхід сприяє досягненню стратегічних цілей компанії та її конкурентоспроможності (табл. 2.9).

Таблиця 2.9

Узгодження процесу управління ризиками інформаційної безпеки ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Стратегічна ціль	**Ризики**	**Управління ризиками**
Зростання доходів	Втрата даних може призвести до фінансових збитків.	Впровадження резервного копіювання та відновлення даних.
Розширення ринку	Недостатня захищеність даних може відлякувати потенційних клієнтів.	Розробка політик конфіденційності та захисту інформації.
Оптимізація процесів	Автоматизація може створити нові вразливості.	Проведення аудиту безпеки нових систем перед їх запуском.
Інновації	Нові технології можуть мати невідомі ризики.	Застосування методології оцінки ризиків для нових проектів.

План дій для узгодження включає проведення аналізу поточного стану, що охоплює оцінку наявних ризиків та заходів безпеки, визначення вимог до інформаційної безпеки, які відповідають стратегічним цілям, розробку процесів управління ризиками, що інтегруються з бізнес-процесами, а також систематичний моніторинг і перегляд процесів.

Узгодження процесу управління ризиками інформаційної безпеки з цілями та стратегіями ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" є критично важливим етапом для забезпечення стійкості та успішності діяльності компанії в сучасному інформаційному середовищі. Аналіз поточного стану, визначення стратегічних цілей, розробка відповідних процесів та їх систематичне моніторинг та перегляд допомагають впевнитися, що заходи з управління ризиками інформаційної безпеки відповідають потребам та амбіціям компанії. Це сприяє підвищенню рівня безпеки, ефективності та конкурентоспроможності підприємства в динамічному бізнес-середовищі.

2.4 Забезпечення координації з існуючими процесами управління ризиками

Забезпечення ефективної координації з існуючими процесами управління ризиками є ключовим аспектом для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" в

контексті забезпечення стійкості та успішності своєї діяльності. Оскільки ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" займається інженерно-технічними рішеннями та реалізацією проектів у будівництві промислових та цивільних об'єктів, безпека інформації та управління ризиками пов'язаними з цією інформацією стають критично важливими аспектами для забезпечення успішності їхнього бізнесу. Відповідно, впровадження інтегрованої системи управління ризиками інформаційної безпеки, яка відповідає стратегічним цілям та стратегіям компанії, є необхідним елементом для забезпечення оптимального функціонування його бізнес-процесів.

Забезпечення взаємодії нових процесів управління ризиками з вже існуючими системами в ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" передбачає проведення ряду ключових кроків для ефективної координації. Починаючи з аналізу існуючих процесів, проводиться перегляд та оцінка поточних процедур управління ризиками. Наступним етапом є визначення точок інтеграції, де ідентифікуються можливості взаємодії нових та вже наявних процесів. Після цього розробляється детальний план координації, який конкретизує, як саме нові процеси будуть вплітатися у вже діючі. Важливим аспектом є комунікація з усіма зацікавленими сторонами, щоб забезпечити їхню підтримку та участь у впровадженні. Після цього настає етап впровадження та навчання, коли запускаються нові процеси та проводиться навчання персоналу для їхнього ефективного використання. Завершується цей цикл моніторингом та оцінкою, що передбачає регулярний перегляд процесів для забезпечення їхньої ефективності та внесення необхідних коригувань (табл. 2.8).

Впровадження процесу управління ризиками інформаційної безпеки в ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" вимагає належної координації з існуючими процесами. Аналіз та інтеграція нових методик управління ризиками здійснюються шляхом взаємодії з керівниками відділів та відповідних відділів, щоб забезпечити взаємодію між новими та існуючими системами.

Таблиця 2.10

План координації з існуючими процесами управління ризиками ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Етап	Завдання	Відповідальний	Термін
Аналіз	Оцінка існуючих процесів	Керівник відділу безпеки	1 тиждень
Інтеграція	Розробка інтеграційних точок	ІТ-відділ	2 тижні
Комунікація	Зустрічі з зацікавленими сторонами	HR	1 тиждень
Впровадження	Навчання персоналу	Відділ навчання	1 місяць
Моніторинг	Перегляд ефективності	Внутрішній аудит	Щоквартально

Крім того, проведення зустрічей з зацікавленими сторонами і навчання персоналу допомагає підтримати робочий процес і забезпечити, що персонал готовий до впровадження нових методик. Ці кроки виконуються з ретельним вивченням і врахуванням потреб компанії, що дозволяє забезпечити ефективну координацію та виконання стратегічних цілей щодо управління ризиками.

2.5 Забезпечення механізмів комунікації та звітності

У сучасному бізнес-середовищі ефективне управління комунікаціями та звітністю відіграє ключову роль у забезпеченні успішності та конкурентоспроможності підприємства. ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" у своїй діяльності стикається зі складними завданнями, пов'язаними з управлінням ризиками, забезпеченням інформаційної безпеки та ефективним функціонуванням бізнес-процесів. У такому контексті ретельне планування, розробка та впровадження механізмів комунікації та звітності є важливими елементами стратегії розвитку компанії.

Забезпечення ефективної внутрішньої комунікації між всіма рівнями управління відображається на внутрішньому кліматі та сприяє підвищенню продуктивності роботи. Вдосконалення процесів звітності допомагає вчасно і об'єктивно оцінювати результати роботи та приймати обґрунтовані управлінські

рішення. Крім того, належно розроблені механізми комунікації дозволяють підтримувати позитивні відносини з клієнтами, партнерами та іншими зацікавленими сторонами, що є ключовим аспектом будь-якого успішного бізнесу.

В умовах постійних змін у технологіях та ринкових умовах, важливою є не лише сама наявність механізмів комунікації та звітності, але й їх постійне вдосконалення та адаптація до нових викликів. Професійний підхід до цих питань відображається на конкурентоспроможності та стійкості компанії в умовах невизначеності та конкуренції на ринку.

Забезпечення ефективної комунікації та системи звітності є невід'ємною складовою успішного управління ризиками інформаційної безпеки в ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ". Компанія активно працює над розробленням детального плану дій для впровадження цих механізмів. Цей план включає розроблення комунікаційної стратегії, постійне інформування співробітників та сторін про політики безпеки, а також навчання персоналу для підвищення їхньої обізнаності. Крім того, встановлюються стандарти звітності, розробляються процедури для реагування на інциденти безпеки та забезпечується регулярний аналіз ефективності заходів безпеки. Важливим етапом є також створення каналів для збору зворотного зв'язку від співробітників та інших зацікавлених сторін. Ці заходи сприятимуть підтримці ефективної комунікації та забезпечать належний рівень звітності, що є ключовим для успішного вирішення ризиків та збереження інформаційної безпеки (табл. 2.11).

План забезпечення механізмів комунікації та звітності для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" представляє собою комплексний підхід до впровадження ефективних комунікаційних та звітних процесів у компанії.

Таблиця 2.11

План забезпечення механізмів комунікації та звітності ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» [20]

Етап	Завдання	Відповідальний	Термін
Розробка стратегії	Визначення ключових повідомлень	Керівник відділу PR	1 місяць
Внутрішня комунікація	Інформування співробітників	HR-менеджер	Щотижня
Зовнішня комунікація	Оновлення комп'ютерних програм підприємства	Веб-майстер	2 тижні
Навчання	Організація тренінгів	Керівник відділу навчання	Щокварталу
Звітність	Розробка стандартів звітності	Фінансовий директор	2 місяці
Аналіз	Проведення аудиту	Внутрішній аудитор	Щорічно

Розробка стратегії включає визначення ключових повідомлень та способів їх подачі, в той час як внутрішня комунікація передбачає систематичне інформування співробітників про важливі питання безпеки та змін. Зовнішня комунікація орієнтована на оновлення програмного забезпечення компанії та підтримку зв'язків з клієнтами та партнерами. Організація тренінгів для персоналу регулярно підвищуватиме рівень обізнаності з питань безпеки. Розробка стандартів звітності та проведення аудитів забезпечать відповідність процесів вимогам та ефективність заходів безпеки.

Висновки до розділу 2

У другому розділі було детально досліджено методику інтеграції процесу управління ризиками інформаційної безпеки в загальну систему управління бізнес-ризиками підприємства ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ».

Оцінка готовності підприємства до впровадження процесу управління ризиками інформаційної безпеки показала, що організація має базові структурні та технічні можливості для здійснення таких заходів. Виявлено, що необхідно

провести додаткову підготовку персоналу та оновити деякі технологічні компоненти для повноцінної реалізації процесу.

Було визначено ключові зацікавлені сторони та оцінено потреби у ресурсах для впровадження процесу управління ризиками інформаційної безпеки. Визначено, що успішна інтеграція вимагає залучення керівництва компанії, IT-відділу, служби безпеки та інших відповідних підрозділів. Ресурсні потреби включають фінансові інвестиції в сучасне програмне забезпечення, навчання персоналу та зовнішню консультаційну підтримку.

Було здійснено узгодження процесу управління ризиками інформаційної безпеки з цілями та стратегіями підприємства. Виявлено, що для досягнення максимального ефекту, необхідно забезпечити відповідність між заходами з інформаційної безпеки та загальними бізнес-цілями компанії.

Забезпечення координації з існуючими процесами управління ризиками в компанії виявилося критично важливим, що дозволяє уникнути дублювання зусиль, оптимізувати використання ресурсів та забезпечити більш узгоджений підхід до управління ризиками на всіх рівнях підприємства. Був підкреслений важливий аспект взаємодії між відділами та підрозділами компанії.

Також, було розглянуто забезпечення механізмів комунікації та звітності для процесу управління ризиками інформаційної безпеки. Визначено, що ефективна комунікація між зацікавленими сторонами та регулярна звітність про стан і результати заходів з управління ризиками є ключовими для підтримки безперервного вдосконалення процесу та забезпечення його успішної інтеграції в загальну систему управління ризиками підприємства.

Розділ 3 ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

3.1 Визначення необхідності впровадження процесу управління ризиками інформаційної безпеки в ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

Поглиблене розуміння внутрішніх та зовнішніх загроз, які можуть вплинути на активи компанії, важливе для забезпечення стійкості та відповідності найвищим стандартам безпеки. Небезпека кібератак, витоку конфіденційної інформації, а також несправності в системах можуть призвести до серйозних фінансових втрат та пошкоджень репутації. У цьому контексті, впровадження системи управління ризиками інформаційної безпеки стає стратегічним кроком для забезпечення стабільності та надійності функціонування компанії.

Також, в умовах стрімкого розвитку технологій та зростаючої складності інформаційних систем, важливо мати чітку стратегію управління ризиками. Проактивний підхід до ідентифікації, оцінки, аналізу та мінімізації ризиків дозволить ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" не лише уникати потенційних загроз, але й створити умови для подальшого розвитку та успішного функціонування на ринку.

Для кількісного визначення ймовірності та впливу ризиків використаємо кількісні методи аналізу.

Значення активу (AV): Для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" можна визначити вартість активів, які потенційно можуть бути піддані ризику. Це можуть бути інформаційні системи, бази даних, обладнання, програмне забезпечення тощо. Загальна вартість активів складає 10 мільйонів гривень.

Фактор схильності до ризику (EF): це відсоток втрат, які може зазнати актив у випадку реалізації загрози. Для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ", EF складає 15%.

Очікувана одинична втрата (SLE): SLE визначається за формулою (1.1) наведеною в розділі 1, пункт 1.3. Таким чином:

SLE = 0,15 * 10,000,000 = 1,500,000 грн.

Далі, розглянемо щорічну частоту прояву (ARO): це кількість разів, коли загроза може мати місце щорічно. Для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ", ARO складає 6 разів на рік.

Очікувана щорічна втрата (ALE): визначається за формулою (1.2) наведеною в розділі 1, пункт 1.3. Таким чином:

ALE = 1,500,000 * 6 = 9,000,000 грн.

На основі аналізу кількісних метрик ризиків інформаційної безпеки для ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" виявляється велика потенційна загроза, яка може вплинути на фінансову стійкість, репутацію та навіть існування компанії. Підходячи до оцінки ризиків, найбільш ефективним методом є використання кількісних методів, які дозволяють конкретно виміряти ймовірність і вплив можливих загроз.

З такою значною вартістю активів, виникає великий потенціал для різних форм загроз, включаючи кібератаки, виток інформації, або навіть природні катастрофи, що можуть призвести до серйозних втрат.

Фактор схильності до ризику (EF) в даному випадку становить 15%, що вказує на можливість серйозних наслідків в разі реалізації загрози. Очікувана одинична втрата (SLE) для компанії розрахована як 1,500,000 гривень, що представляє собою значну суму. Щорічна частота прояву загроз (ARO) становить 6 разів на рік, що підсилює ризики та можливі наслідки втрат.

Очікувана щорічна втрата (ALE) для компанії оцінюється в 9 мільйонів гривень, що є дуже значним показником, що свідчить про серйозні ризики, які стикається ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ".

Отже, враховуючи величезний обсяг можливих втрат та потенційних загроз для інформаційної безпеки, впровадження процесу управління ризиками стає невідкладною необхідністю для забезпечення стабільності та успішності діяльності компанії. Запобігання можливим загрозам, виявлення слабких місць і

вжиття заходів щодо мінімізації ризиків стануть важливими кроками для збереження конкурентних переваг та забезпечення довгострокового успіху компанії.

3.2 Інтеграція процесу управління ризиками інформаційної безпеки в систему управління бізнес-ризиками ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

Інформаційні активи компаній піддаються постійному ризику через різноманітні загрози, включаючи кібератаки, технічні збої, внутрішні загрози та природні катастрофи. Ефективне управління цими ризиками є критичним для забезпечення стабільності та стійкості організації. У зв'язку з цим інтеграція процесу управління ризиками інформаційної безпеки (ІБ) в загальну систему управління бізнес-ризиками набуває особливого значення.

Будь-яке порушення цілісності, конфіденційності або доступності інформації може призвести до значних фінансових втрат, зниження репутації та втрати довіри з боку клієнтів і партнерів. Тому компанії повинні впроваджувати надійні системи захисту інформації, що включають ефективне управління ризиками ІБ.

Впровадження системи управління інформаційною безпекою (СУІБ) у компанії ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» дозволяє чітко окреслити взаємозв'язки між процесами та підсистемами інформаційної безпеки (ІБ), визначити відповідальних осіб, а також встановити фінансові та трудові ресурси, необхідні для їх ефективного функціонування. СУІБ включає (рис. 3.1).

Рис. 3.1. Система управління інформаційною безпекою (СУІБ) ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

Основними цілями управління інформаційною безпекою ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" є: забезпечення безпеки персоналу та клієнтів компанії; управління інформаційною безпекою, включаючи визначення ролей і обов'язків у галузі ІБ та створення і підтримку системи управління ІБ (СУІБ); класифікація інформаційних активів; оцінка ризиків інформаційної безпеки; забезпечення захисту інформаційних активів відповідно до їх класифікації та оцінки ризиків; моніторинг подій інформаційної безпеки та управління інцидентами ІБ; забезпечення безперервності бізнес-діяльності компанії; безпечне управління життєвим циклом інформаційної системи.

Інтеграція процесу управління ризиками інформаційної безпеки (ІБ) у загальну систему управління бізнес-ризиками є важливим кроком для забезпечення комплексного підходу до ризик-менеджменту в ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Одним із найбільш визнаних міжнародних стандартів у цій сфері є ISO/IEC 27005, який надає керівні вказівки щодо управління ризиками інформаційної безпеки в контексті системи управління інформаційною безпекою (СУІБ).

Процес управління ризиками інформаційної безпеки розпочинається з оцінки контексту та виявлення активів, які потребують захисту. Для ТОВ «ІБК

«КЕПІТАЛ ІНЖИНІРИНГ» це означає ідентифікацію всіх інформаційних активів, включаючи апаратне забезпечення, програмне забезпечення, бази даних, мережеві ресурси та інші важливі компоненти інформаційної системи. Оцінка контексту включає визначення внутрішніх і зовнішніх факторів, які можуть впливати на інформаційну безпеку, а також встановлення меж системи управління ризиками.

Наступним кроком є виявлення загроз і вразливостей, які можуть впливати на інформаційні активи компанії. За методикою ISO 27005, це включає аналіз можливих джерел загроз (наприклад, кіберзлочинці, природні катастрофи, технічні збої) та оцінку вразливостей, які можуть бути використані для реалізації цих загроз. Для цього можуть використовуватися різні методи, включаючи аналіз журналів подій, аудити безпеки та тестування на проникнення.

Оцінка ризиків включає визначення ймовірності та потенційного впливу кожної загрози на активи компанії. ISO 27005 рекомендує використання кількісних та якісних методів для оцінки ризиків. Наприклад, кількісна оцінка може включати розрахунок очікуваних втрат (ALE) на основі значення активів (AV), фактора схильності до ризику (EF) та щорічної частоти прояву (ARO).

Після оцінки ризиків необхідно визначити відповідні заходи для їхнього зменшення або усунення. Це можуть бути технічні заходи (встановлення антивірусного програмного забезпечення, шифрування даних), організаційні заходи (розробка політик безпеки, навчання персоналу) та адміністративні заходи (впровадження процедур управління інцидентами). За методикою ISO 27005, вибір заходів має базуватися на аналізі витрат і вигод, а також на здатності заходів ефективно знижувати ризики до прийнятного рівня.

Управління ризиками є безперервним процесом, який вимагає регулярного моніторингу та перегляду для забезпечення його ефективності. Це включає моніторинг показників безпеки, проведення регулярних аудитів і тестувань, а також аналіз інцидентів для виявлення нових загроз і вразливостей. Відповідно до ISO 27005, важливо забезпечити постійне вдосконалення процесу управління

ризиками на основі отриманих результатів і змін у внутрішньому та зовнішньому середовищі.

Для ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» важливо інтегрувати процес управління ризиками інформаційної безпеки в загальну систему управління бізнес-ризиками. Це дозволяє забезпечити узгодженість процесів управління ризиками на всіх рівнях організації, знизити дублювання зусиль та оптимізувати використання ресурсів. Інтеграція також сприяє кращому розумінню взаємозв'язків між різними типами ризиків (операційними, фінансовими, репутаційними) та забезпечує більш зважене прийняття рішень на стратегічному рівні.

Таким чином, впровадження процесу управління ризиками інформаційної безпеки за методикою ISO 27005 дозволяє ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» створити ефективну систему захисту інформаційних активів, підвищити загальну стійкість підприємства та забезпечити безперервність його бізнес-діяльності.

3.3 Рекомендації щодо подальшого вдосконалення процесів управління ризиками інформаційної безпеки ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ»

ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ», як і будь-яка сучасна організація, повинна звертати особливу увагу на управління ризиками інформаційної безпеки, щоб забезпечити захист своїх активів та підтримувати стабільність бізнесу.

Для створення ефективної системи інформаційної безпеки необхідно спочатку описати бізнес-процеси, а потім визначити поріг ризику – рівень загрози, при якому вона включається в процес управління ризиками. Важливо побудувати таку систему інформаційної безпеки, яка дозволить досягти заданого рівня ризику. З метою покращення системи управління інформаційною безпекою ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ" була розроблена вдосконалена модель

процесу управління ризиками для системи інформаційної безпеки підприємства (рис.3.2).

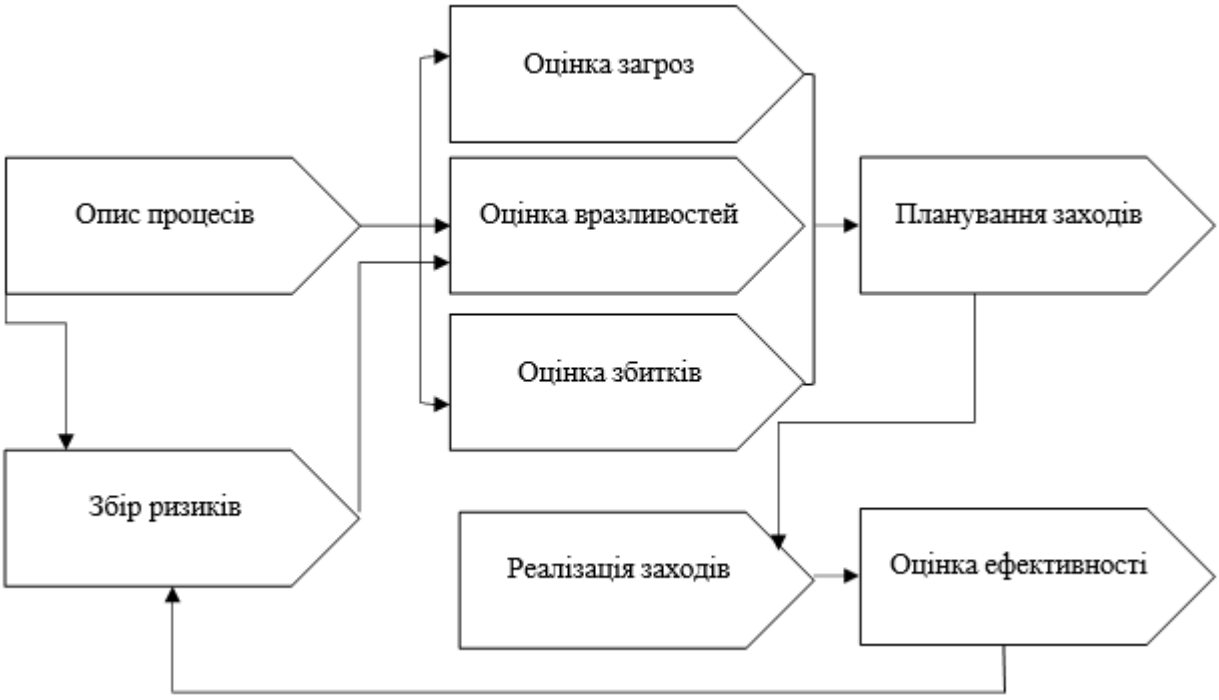

Рис. 3.2. Вдосконалена модель процесу управління ризиками для системи інформаційної безпеки ТОВ "ІБК "КЕПІТАЛ ІНЖИНІРИНГ"

Враховуючи це, важливо розуміти, що процес управління ризиками інформаційної безпеки є неперервним та динамічним. Він вимагає регулярного перегляду та адаптації до змінюваних умов зовнішнього середовища та внутрішніх процесів компанії. Подальше вдосконалення цих процесів вимагає комплексного підходу, який включає розробку стратегії, планування, впровадження контрольних заходів, моніторингу та реагування на інциденти.

Для ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» рекомендується вжити наступні кроки для підвищення ефективності управління ризиками інформаційної безпеки:

1. Впровадження антивірусного та антиспамового програмного забезпечення, яке постійно оновлюється, для виявлення та запобігання вторгнень та спаму.

2. Забезпечення захисту доступу та автентифікації, включаючи вимогу до складних паролів та використання двофакторної аутентифікації.

3. Використання шифрування даних в спокійному та транзитному режимах для збереження конфіденційності інформації.

4. Регулярні оновлення та застосування патчів для операційних систем, програмного забезпечення та апаратного забезпечення для усунення вразливостей.

5. Сегментація мережі та використання брандмауера для обмеження розповсюдження можливих загроз.

6. Навчання персоналу та прийняття обізнаних рішень у відповідь на соціально-інженерні атаки.

7. Проведення регулярних аудитів та моніторинг безпеки для виявлення аномалій та інцидентів.

8. Створення та зберігання резервних копій даних для відновлення інформації в разі катастрофи або кібератаки.

9. Розроблення політики кібербезпеки та навчання персоналу її дотримуватися.

10. Встановлення заходів для запобігання витоку конфіденційної інформації та обмеження прав доступу.

Заходи щодо зниження ризиків та забезпечення безпеки в цифровому середовищі охоплюють ряд ініціатив: використання постійно оновлюваного антивірусного та антиспамового програмного забезпечення для боротьби зі спамом та вторгненнями; застосування механізмів захисту доступу та двофакторної аутентифікації; шифрування даних для збереження їх конфіденційності; регулярні оновлення та застосування патчів для усунення вразливостей; сегментація мережі для обмеження розповсюдження загроз; навчання персоналу відповідати на соціально-інженерні атаки; аудити та моніторинг безпеки для виявлення аномалій; регулярне створення та зберігання резервних копій даних; розроблення політики кібербезпеки та навчання

персоналу її дотримуватися; встановлення заходів для запобігання витоку конфіденційної інформації та обмеження прав доступу.

Висновки до розділу 3

У третьому розділі досліджено особливості впровадження процесу управління ризиками інформаційної безпеки в ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ».

Визначення необхідності впровадження процесу управління ризиками інформаційної безпеки показало, що компанія стикається з суттєвими загрозами, які можуть негативно вплинути на її інформаційні ресурси. Проведений аналіз вказує на високий рівень потенційних втрат у разі реалізації загроз, що підкреслює критичну необхідність створення ефективної системи управління ризиками ІБ для захисту активів компанії.

Інтеграція процесу управління ризиками інформаційної безпеки в загальну систему управління бізнес-ризиками ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ» показала, що синхронізація цих процесів дозволяє досягти більшої ефективності в управлінні ризиками, що забезпечує комплексний підхід до оцінки та мінімізації ризиків, що сприяє підвищенню загальної стійкості та безпеки підприємства.

Було розроблено рекомендації щодо подальшого вдосконалення процесів управління ризиками інформаційної безпеки. Зокрема, запропоновано впровадити сучасні методології та фреймворки, такі як ISO/IEC 27005 та NIST SP 800-30, для підвищення ефективності управління ризиками. Також було рекомендовано регулярно проводити оцінку ризиків, оновлювати політики безпеки та забезпечувати постійне навчання персоналу.

ВИСНОВКИ

У даній роботі було здійснено комплексне дослідження та аналіз процесу управління ризиками інформаційної безпеки в ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Вивчення теоретичних основ, аналіз існуючих методик та практик, а також практичні рекомендації щодо впровадження та вдосконалення процесів управління ризиками інформаційної безпеки дозволили визначити важливі аспекти для підвищення рівня захищеності інформаційних ресурсів підприємства.

У першому розділі розглянуто теоретичні основи забезпечення процесу управління ризиками інформаційної безпеки в системі управління бізнес-ризиками підприємства. Було визначено місце і роль ризик-менеджменту, проаналізовано найбільш відомі фреймворки та методології, а також оцінено важливість інтеграції процесу управління ризиками інформаційної безпеки в загальну систему управління ризиками підприємства.

Другий розділ присвячено дослідженню методики інтеграції процесу управління ризиками інформаційної безпеки в систему управління бізнес-ризиками підприємства ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Було проведено оцінку готовності підприємства до впровадження цього процесу, визначено ключові зацікавлені сторони, оцінено потреби у ресурсах та узгоджено процеси управління ризиками інформаційної безпеки з цілями та стратегіями підприємства.

У третьому розділі розглянуто особливості впровадження процесу управління ризиками інформаційної безпеки. Визначено необхідність впровадження даного процесу, інтеграцію з існуючою системою управління бізнес-ризиками та розроблено рекомендації щодо вдосконалення процесів управління ризиками інформаційної безпеки. Запропоновано впровадження сучасних методик, регулярну оцінку ризиків та навчання персоналу для підвищення ефективності управління ризиками.

Загалом, дослідження підкреслює важливість комплексного підходу до управління ризиками інформаційної безпеки, інтеграції цих процесів у загальну систему управління бізнес-ризиками підприємства та постійного вдосконалення процесів управління ризиками для забезпечення надійного захисту інформаційних ресурсів ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». Це дозволить підвищити загальну стійкість та безпеку підприємства, мінімізувати потенційні втрати та забезпечити успішне функціонування в сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрухів А.І., Тарасов Д.О. Порівняння методів оцінки захищеності корпоративних інформаційних систем. *Academic Journals and Conferences*. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/dec/7287/013-9vis573.pdf (дата звернення: 18.05.2024).

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 (дата звернення: 10.05.2024)

3. Аудит інформаційної безпеки: підручник //тРомака В.А. та ін. Львів: СПОЛОМ, 2015. 363 с.

4. Богоявленська Ю. В., Свірко С. В., Бережницький Д. Ю. Забезпечення гнучкості прийняття управлінських рішень та цифровізації управління на інноваційних підприємствах і стартапах. Інфраструктура ринку. 2020. № Вип. 49. С. 83–87.

5. Богуш В., Юдін О. Інформаційна безпека держави. Київ : «МК - Прес», 2015. – 432 с.

6. Віннікова І.І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними // Східна Європа: Економіка, бізнес та управління. 2018. Вип. 5 (16). С. 110-114.

7. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кібер-ризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. №3. С. 101-115.

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 (дата звернення: 10.05.2024)

9. Гуленко Н.В. Моніторинг стану інформаційної безпеки сегментів корпоративних мереж сучасного бізнесу. Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса. Том 1 / Ред. кол. Хаджинов І. В. (голова) та ін. Вінниця: ДонНУ імені Василя Стуса, 2021. Вип. 13. Т. 1. С. 252–255.

10. Дейнега О.В. Інформаційна безпека підприємств в умовах глобалізації 4.0. *Економіка та суспільство*. 2019. Вип.20. С. 70-79. URL: DOI: https://doi.org/10.32782/2524-0072/2019-20-28

11. Дзюба Л.Ф., Чмир О.Ю. Оцінювання ризиків інформаційної безпеки з використанням методів математичної статистики //Вісник ЛДУБЖД, №26, 2022. С.47-54.

12. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

13. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911 (дата звернення: 10.05.2024)

14. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепції “глибинного захисту”. *Підприємництво і торгівля*. 2019. № 25. С. 116–121.

15. Дячков Д. В., Потапюк І. П., Капран І. В. Економічна безпека в системі стратегічного управління підприємством. *Економіка та суспільство*. 2021. № 24. URL: https://economyandsociety.in.ua/index.php/journal/article/view/173/166 (дата звернення: 10.05.2024)

16. Євтушевська О.А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту / О.А. Євтушевська // *Зовнішня торгівля: економіка, фінанси, право*. – 2015. - № 5–6 (82–83). – С. 157–162.

17. Захаров О. І. Інформаційне забезпечення управління системою економічної безпеки підприємства. URL: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf (дата звернення: 10.05.2024)

18. Інформаційна безпека. Підручник. Під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

19. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Харків: Вид. ХНЕУ, 2018. 196 с.

20. Кіндзерський Ю.В. Кібербезпека та становлення цифрової економіки. *Економічний вісник*. 2020. № 3. С. 18-26. DOI: https://doi.org/10.33271/ebdut/71.018

21. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. Х.: ХНЕУ, 2018. 510 с.

22. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки : зб. наук. пр. ДВНЗ «КНЕУ ім. Вадима Гетьмана». 2021. С. 26-28. URL: https://ir.kneu.edu.ua/handle/2010/3615 (дата звернення: 10.05.2024)

23. Лобода О.М. Захист інформації в корпоративних мережах. *Публічне управління та адміністрування у процесах економічних реформ*: матеріали IV Всеукр. наук.-практ. конф., м. Херсон, 11 лист. 2020 р. ХДАЕУ, 2020. С.61-63

24. Лобода О.М., Кириченко Н.В. Базові комунікаційні технології: навч. посіб. Херсон: Стар, 2018. 235 с.

25. Маркіна І. А., Дячков Д. В. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. 3(1). 80 с

26. Марущак А.І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А.І. Марущак // *Державна безпека України*. – 2011. – № 21. – С. 92–95.

27. Мельник М.О. Аналіз побудови моделі політики інформаційної безпеки підприємства. *Системи обробки інформації*. 2017. Вип. 2(148). С. 126–128.

28. Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних система. URL: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdfhttp://erpub.chnpu.edu.ua:8080/jspui/handle/123456789/5809 (дата звернення: 10.05.2024)

29. 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://erpub.chnpu.edu.ua:8080/jspui/handle/123456789/5809 (дата звернення: 10.05.2024)

30. Онищенко С., Ківшук О. Управління інформаційною безпекою стратегічно важливих підприємств в умовах викликів й загроз. Науковий журнал «Економіка і регіон». 2022. Т. 3(86). С. 80-85. doi:https://doi.org/10.26906/EiR.2022.3(86).2817.

31. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків. 2018. 289 с.

32. Пурій Г. М. Інформаційні системи і технології в управлінні діяльністю підприємства. Ефективна економіка. 2019. № 6. URL: http://www.economy.nayka.com.ua/pdf/6_2019/58.pdf (дата звернення: 10.05.2024)

33. Рибальченко Л. Інформаційна безпека як складова економічної безпеки країни. Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. Львів: Растр-7, 2022. С. 49–52.

34. Савельева Т. В., Панаско О. М., Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтова ного підходу в контексті забезпечення інформаційної безпеки підприємства. *Вісник Черкаського державного технологічного університету*. Серія: Технічні науки. 2018. № 1. С. 81–88

35. Секель А. Цілі інформаційної безпеки та їх значення. URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yih-znachennya (дата звернення: 10.05.2024)

36. Сороківська, О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // *Вісн. Хмельниц. нац. ун-ту*. Сер.: Екон. науки. – 2010. – № 2. – Т. 2. – С. 32–35.

37. ТОВ «ІБК «КЕПІТАЛ ІНЖИНІРИНГ». URL: https://youcontrol.com.ua/catalog/company_details/43862887/ (дата звернення: 10.05.2024)

38. Тупкало В.М. Бізнес – інжиніринг сучасних процесно – орієнтованих підприємств: монографія / В.М. Тупкало. Київ.: ДУТ, 2016. 281 с

39. Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підприємств торгівлі. *Цифрова економіка*. 2022. №1. С. 106-117. URL: http://doi.org/10.31617/visnik.knute.2022(141)080 (дата звернення: 10.05.2024)

40. Чубаєвський В.І. Методи управління корпоративною інформаційною безпекою. Економіка та суспільство. 2022 №43

41. 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 (дата звернення: 10.05.2024)

42. Якименко Ю. М., Мужанова Т. М., Легомінова С. В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2020. № 4(12). С. 36-50.

ДОДАТОК А

Таблиця А.1

Порівняння методів оцінки ризиків

Методи оцінки ризиків	Наявний переклад	Орієнтація на розмір підприємства	Наявне ПЗ	Фази підходу	Тип оцінки ризику	Обробкаризиків	Потреба в ресурсах
ISO 27005	+	Можливе застосування для організацій різного розміру ігалузей	+	• Визначення обставин • Ідентифікація ризику • Аналізування ризику • Оцінювання ризику • Оброблення ризику • Прийняття ризиків	Загальні настанови щодо якісної чи кількісної оцінки	•Модифікація •Прийняття •Усунення •Розподілення	Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження
NIST SP 800-30	-	Застосовується для підприємств різного розміру. Розроблено, в першу чергу, для використання в федеральних організаціях США	+	• Характеристика системи • Ідентифікація загроз • Ідентифікація вразливостей • Аналіз контролю • Визначення ймовірності • Аналіз впливу • Визначення ризику • Рекомендації з контролю • Документальне оформлення	Змішана оцінка ризиків	•Прийняття •Запобігання •Обмеження •Планування •Дослідження і повідомлення •Перенесення	Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження
OCTAVE	-	Можливе застосування для організацій різного розміру ігалузей	+	• Встановлення критеріїв оцінки ризику • Розробка профілю інформаційного активу • Ідентифікація контейнерів інформаційних активів • Визначення проблемнихобластей • Визначення сценаріїв загроз • Визначення ризиків • Аналіз ризиків • Підходи до зменшення ризику	Якісна оцінка ризиків	•Зниження •Прийняття	Власні ресурси організації, не експерти. Необхідне залучення співробітників як зі сторони IT, так і бізнесу